Natural for z/OS

Natural Security

Version 9.2.5

Oktober 2026

ADABAS & NATURAL

This document applies to Natural for z/OS Version 9.2.5 and all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Copyright © 1979-2026 Software GmbH, Darmstadt, Germany and/or its subsidiaries and/or its affiliates and/or their licensors.

The name Software AG and all Software GmbH product names are either trademarks or registered trademarks of Software GmbH and/or its subsidiaries and/or its affiliates and/or their licensors. Other company and product names mentioned herein may be trademarks of their respective owners.

Detailed information on trademarks and patents owned by Software GmbH and/or its subsidiaries is located at https://softwareag.com/licenses.

This software may include portions of third-party products. For third-party copyright notices, license terms, additional rights or restrictions, please refer to "License Texts, Copyright Notices and Disclaimers of Third-Party Products". For certain specific third-party license restrictions, please refer to section E of the Legal Notices available under "License Terms and Conditions for Use of Software GmbH Products / Copyright and Trademark Notices of Software GmbH Products". These documents are part of the product documentation, located at https://softwareag.com/licenses and/or in the root installation directory of the licensed product(s).

Use of this software is subject to adherence to Software GmbH's licensing conditions and terms. These terms are part of the product documentation, located at https://softwareag.com/licenses and/or in the root installation directory of the licensed product(s).

Document ID: NATMF-NATNSC-925-20261013DE

Inhaltsverzeichnis

Vorwort ix
1 Über diese Dokumentation 1
Dokumentationskonventionen 2
Online-Informationen und Support 2
Datenschutz 3
2 Struktur und Terminologie von Natural Security 5
Über diese Dokumentation 6
Verwendungszweck von Natural Security 6
Benutzer (Users) 7
Bibliotheken (Libraries) 12
Links zwischen Benutzern und Bibliotheken 13
DDMs/Dateien (Files) 13
Dienstprogramme (Utilities) 15
Anwendungen (Applications) 15
RPC Server 15
Andere Objekttypen 16
Profilparameter 16
3 Natural Security auf verschiedenen Plattformen 19
Unterstützte Plattformen 20
Natural Security auf mehreren Plattformen verwenden 21
4 Erste Schritte nach der Installation 25
Schritt 1: Ändern Sie das Passwort des Benutzers DBA. 26
Schritt 2: Administratoren definieren 27
Schritt 3: Definieren Sie Systembibliotheken 28
5 Anmeldung (Logon) 29
Vorgehensweise bei der Anmeldung 30
LOGON-Kommando 34
Automatische Anmeldung 35
Logon-Anpassung 36
Natural-Sitzung beenden 38
6 Grundlagen der Benutzung 39
Natural Security-Funktionen aufrufen 40
Drücken der Eingabetaste (ENTER) 41
Hilfe 41
Falls unsicher, was Sie eingeben sollen 41
Umgang mit einer Liste 42
Direktkommandos 46
7 Administrator Services 53
Zugriff auf das Subsystem Administrator Services 54
Administrator Services aufrufen 54
Allgemeine Optionen (Administrator Services) 55
Authentifizierungsoptionen - Authentication Options (LDAP) 74
PF-Tasten 82

Anmelde-/Gegenzeichnungsfehler - Logon/Countersign Errors 85
Anmeldesätze - Logon Records 91
Verwaltungsprotokollsätze verwalten - Maintenance Log Records 95
SAF Online Services 103
Benutzer-Standardprofile - User Default Profiles 107
Standardprofile für Bibliotheken - Library Default Profiles 109
Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values 110
Voreingestellte Werte für Bibliothekssicherheitsprofile - Library Preset Values 119
Systembibliotheken definieren - Definition of System Libraries 125
Nicht definierte Bibliotheken definieren - Definition of Undefined Libraries 126
8 Benutzer verwalten 129
Vorbereitungen treffen 130
Bestandteile eines Benutzersicherheitsprofils 130
Benutzersicherheitsprofile anlegen und verwalten 142
9 Bibliotheken verwalten 159
Bestandteile eines Bibliothekssicherheitsprofils 160
Bibliothekssicherheitsprofile anlegen und verwalten 191
10 Bibliotheken schützen 203
Geschützte Bibliotheken - Protected Libraries 204
Benutzer mit Bibliotheken verlinken 206
Welche Benutzungsbedingungen sind in Kraft? 212
11 Umgebungen schützen 215
Konzept des Umgebungsschutzes 216
Umgebungsschutz aktivieren 216
Umgebungsprofile definieren 217
Bestandteile eines Umgebungsprofils 219
Zugriff auf Bibliotheken in Umgebungen nicht erlauben/erlauben 221
Benutzern den Zugang zu Umgebungen nicht erlauben/erlauben 224
12 DDMs unter z/OS schützen 227
Bevor Sie beginnen: 228
Bestandteile eines Dateiprofils (File Profile) 229
Dateiprofile anlegen und verwalten - Creating and Maintaining File Profiles 233
13 DDMs unter Linux und Windows schützen 243
Zentrale Systemdatei für DDMs angeben (Profilparameter FDDM) 244
Status eines DDM 244
DDM-Sicherheitsprofile 249
DDM-Sicherheitsprofile anlegen und verwalten 252
DDM-Sicherheitsprofil anlegen - Add DDM Profile 254
DDM-Sicherheitsprofil kopieren - Copy DDM Profile 255
DDM-Sicherheitsprofil ändern - Modify DDM Profile 256
DDM-Sicherheitsprofil löschen - Delete DDM Profile 256
DDM-Sicherheitsprofil anzeigen - Display DDM Profile 257
Profil kopieren/Verlinken mit allen Special-Links - Copy Profile/Link to All Special Links 258

Bibliothek mit einem geschützten DDM verlinken ... 258
14 Dienstprogramme (Utilities) schützen ... 261
Allgemeine Überlegungen zum Schutz von Dienstprogrammen (Utilities) ... 262
Welche Dienstprogramme (Utilities) können geschützt werden? ... 263
Dienstprogrammprofile - Utility Profiles ... 263
Standardprofile definieren ... 275
Individuelle Profile definieren - Utility Maintenance ... 277
Bestandteile von Dienstprogrammprofilen ... 286
15 Natural Development Server-Umgebung und -Anwendungen schützen ... 297
Natural Development Server-Umgebung schützen ... 298
Natural Development Server-Anwendungen schützen ... 305
16 Natural-Entwicklungsumgebung in Eclipse schützen ... 325
Natural Server-Ansicht schützen ... 326
Navigator-Ansicht schützen ... 330
17 Natural RPC Server und Services schützen ... 339
RPC Service Requests (Dienstanforderungen) ... 340
RPC Server-Einstellungen in Natural ... 340
RPC Server-Einstellungen in Natural Security ... 342
Gültigkeitsprüfung einer RPC-Dienstanforderung ... 342
Sicherheitsprofile für Natural RPC-Server ... 347
Bestandteile eines RPC-Serverprofils ... 348
RPC Serverprofile anlegen und verwalten ... 352
Dienste erlauben/nicht erlauben ... 357
Weitere RPC-bezogene Funktionen ... 360
18 Externe Objekte schützen ... 361
Externe Objekttypen - Types of External Objects ... 362
Kennungen für externe Objekte ... 363
Bestandteile eines Sicherheitsprofils für ein externes Objekt ... 364
Sicherheitsprofile für externe Objekte anlegen und verwalten ... 367
Benutzer mit externen Objekten verlinken ... 371
19 Mailboxen ... 379
Was ist eine Mailbox? ... 380
Nachricht senden ... 380
Nachricht empfangen ... 381
Mailbox-Kennung - Mailbox ID ... 382
Bestandteile eines Mailbox-Sicherheitsprofils ... 382
Mailbox-Sicherheitsprofile anlegen und verwalten ... 385
20 Retrieval-Funktionen (Retrieval Subsystem) ... 391
Verwendungszweck der Retrieval-Funktionen ... 392
Retrieval-Funktionen aufrufen ... 392
Cross-Referenz Benutzer ... 393
Cross-Referenz Bibliothek ... 393
Cross-Referenz Datei ... 394
Cross-Referenz Dienstprogramm (Utility) ... 394
Cross-Referenz Anwendung ... 395

Cross-Referenz Externes Objekt ... 395
Cross-Reference Mailbox ... 396
Retrieval-Funktionen in Batch Mode - Program RETRIEVE ... 396
21 Gegenzeichnungen (Countersignatures) ... 399
Eigentümer verwenden ... 400
Gegenzeichnungen verwenden (Funktion Countersignature) ... 400
Gruppen als Eigentümer ... 402
Gruppen als Miteigentümer ... 403
Benutzersicherheitsprofile von Administratoren ... 403
Aufgeschobenes Gegenzeichnen ... 404
Nicht erreichbare Sicherheitsprofile ... 406
22 Funktionssicherheit ... 409
Kommandoprozessoren ... 410
Funktionssicherheit für einen Kommandoprozessor ... 410
Schlüsselwörter erlauben/nicht erlauben ... 411
Funktionssicherheit für eine Bibliothek definieren ... 411
Funktionssicherheit für einen Benutzer definieren ... 416
Funktionssicherheit für die Bibliothek SYSSEC ... 417
23 Natural Security im Batch-Modus ... 419
Allgemeine Informationen zum Batch-Modus ... 420
Anmeldung im Batch-Modus ... 420
Batch-Benutzersicherheitsprofile ... 422
Gegenzeichnungen im Batch-Modus ... 423
24 Sicherheitsdaten in eine andere Systemdatei übertragen ... 425
Allgemeine Informationen zur Übertragung von Sicherheitsdaten ... 426
SECULD2 verwenden ... 427
SECLOAD verwenden ... 431
Daten auf eine andere Hardware-Plattform übertragen ... 433
Benutzerdaten von einem externen Sicherheitssystem übertragen ... 434
Datenübertragung im Batch-Modus ... 435
25 User Exits ... 441
Anmeldungsrelevante User Exits ... 442
RPC-relevanter User Exit ... 445
Andere User Exits ... 446
26 Anwendungsprogrammierschnittstellen ... 449
Allgemeines zu Subprogrammen bei NSC ... 450
Subprogramme zur Zugangsberechtigungsprüfung und zur Benutzerauthentifizierung ... 451
Subprogramme für Administrator Services ... 456
Subprogramme zur Objektverwaltung ... 460
Subprogramme für Abruf-Funktionen (Retrieval) ... 467
27 Add-on-Produkte und Plug-ins ... 481
Plug-Ins unter Natural Security ... 482
SYSDIC unter Natural Security ... 483
SYSAOS unter Natural Security ... 484

Stichwortverzeichnis 487

Vorwort

Struktur und Terminologie von Natural Security	Konzept und Grundlagen von Natural Security.
Natural Security auf verschiedenen Plattformen	Aspekte des Einsatzes von Natural Security auf verschiedenen Plattformen und Hinweise zu Unterschieden zwischen diesen Plattformen.
Erste Schritte nach der Installation	Schritte, die nach der Erstinstallation von Natural Security durchgeführt werden müssen.
Anmeldung (Logon)	Regeln, die gelten, wenn sich ein Benutzer bei Natural unter Natural Security anmeldet.
Grundlagen der Benutzung	Verschiedene Aspekte der Bedienung der Natural Security-Benutzeroberfläche.
Administrator Services	Beschreibungen der Funktionen des Administrator Services-Subsystems von Natural Security.
Benutzer verwalten	Benutzersicherheitsprofile, ihre Bestandteile und die Funktionen, mit denen sie angelegt und verwaltet werden.
Bibliotheken verwalten	Sicherheitsprofile für Bibliotheken, ihre Bestandteile und die Funktionen, mit denen sie angelegt und verwaltet werden.
Bibliotheken schützen	Wie Sie den Zugriff von Benutzern auf geschützte Bibliotheken steuern.
Umgebungen schützen	Wie Sie den Schutz von Bibliotheken umgebungsspezifisch gestalten können.
DDMs unter z/OS schützen	Wie Sie die Verwendung von DDMs unter z/OS steuern.
DDMs unter Linux und Windows schützen	Wie Sie die Verwendung von DDMs unter Linux und Windows steuern.
Dienstprogramme (Utilities) schützen	Wie Sie die Verwendung von Natural-Dienstprogrammen (Utilities) steuern.
Natural Development Server-Umgebung und -Anwendungen schützen	Wie Sie die Verwendung der Natural Development Server-Umgebung sowie der Basisanwendungen (Base Applications) und der zusammengesetzten Anwendungen (Compound Applications) auf dem Natural Development Server steuern.
Natural-Entwicklungsumgebung in Eclipse schützen	Wie Sie die Verwendung der Server- und Navigator-Ansichten kontrollieren, die von einer Natural-Entwicklungsumgebung in Eclipse in Verbindung mit NaturalONE verwendet werden.
Natural RPC Server und Services schützen	Wie Sie die Verwendung von Natural Remote Procedure Calls in einer Client/Server-Umgebung steuern.
Externe Objekte schützen	Wie Sie die Verwendung externer Objekte steuern.
Mailboxen	Wie Sie Mailboxen anlegen, verwalten und verwenden.

Retrieval-Funktionen	Wie Sie das Retrieval-Subsystem von Natural Security benutzen, um die vorhandenen Sicherheitsprofildefinitionen und ihre Auswirkungen zu überprüfen.
Gegenzeichnungen	Wie sich Natural Security-Administratoren gegenseitig kontrollieren.
Funktionale Sicherheit	Wie Sie die Verfügbarkeit von Funktionen einschränken und verschiedene Funktionen für verschiedene Benutzer verfügbar machen.
Natural Security im Batch-Modus	Wie Sie Natural Security im Batch-Modus verwenden.
Sicherheitsdaten in eine andere Systemdatei übertragen	Wie Sie Natural Security-Daten von einer Systemdatei in eine andere übertragen.
User Exits	Informationen zu den verfügbaren User Exits.
Anwendungsprogrammierschnittstellen	Subprogramme, mit denen Sie Natural Security-Funktionen von außerhalb der Natural Security-Bibliothek `SYSSEC` ausführen können.
Add-on-Produkte und Plug-ins	Überlegungen zum Schutz verschiedener Add-On-Produkte und Plug-Ins.

1 Über diese Dokumentation

- Dokumentationskonventionen 2
- Online-Informationen und Support 2
- Datenschutz 3

Dokumentationskonventionen

Konvention	Beschreibung
Fettschrift	>Kennzeichnet Elemente auf einem Bildschirm.
`Nichtproportionale Schrift`	Kennzeichnet Namen und Orte von Diensten im Format *`Ordner.Unterordner.Dienst`*, Programmierschnittstellen (APIs), Namen von Klassen, Methoden und Properties in Java.
`Kursivschrift`	Kennzeichnet: Variablen, für die Sie situations- oder umgebungsspezifische Werte angeben müssen. Neue Begriffe, wenn sie erstmals im Text auftreten. Verweise auf andere Dokumentationsquellen.
`Nichtproportionale Schrift`	Kennzeichnet: Text, den Sie eingeben müssen. Meldungen, die vom System angezeigt werden. Programmcode.
{ }	Zeigt eine Reihe von Auswahlmöglichkeiten an, von denen Sie eine auswählen müssen. Geben Sie nur die innerhalb der geschweiften Klammern vorhandenen Informationen ein. Geben Sie nicht die Klammersymbole { } ein.
|	Trennt zwei sich gegenseitig ausschließende Auswahlmöglichkeiten in einer Syntaxzeile voneinander ab. Geben Sie eine der Auswahlmöglichkeiten ein. Geben Sie nicht das Symbol | ein.
[ ]	Zeigt eine oder mehrere Optionen an. Geben Sie nur die innerhalb der eckigen Klammern vorhandenen Informationen ein. Geben Sie nicht die Klammersymbole [ ] ein.
...	Zeigt an, dass Sie mehrere Auswahlmöglichkeiten desselben Typs eingeben können. Geben Sie nur die Informationen ein. Geben Sie nicht die drei Auslassungspunkte (...) ein.

Online-Informationen und Support

Produktdokumentation

Sie finden die Produktdokumentation auf unserer Dokumentationswebsite unter **https://documentation.softwareag.com**.

Zusätzlich können Sie auch über **https://www.softwareag.cloud** auf die Dokumentation für die Cloud-Produkte zugreifen. Navigieren Sie zum gewünschten Produkt und gehen Sie dann, je nach Produkt, zu „Developer Center“, „User Center“ oder „Documentation“.

Produktschulungen

Sie finden hilfreiches Produktschulungsmaterial auf unserem Lernportal unter **https://knowledge.softwareag.com**.

Tech Community

Auf der Website unserer Tech Community unter **https://techcommunity.softwareag.com** können Sie mit Experten der Software AG zusammenarbeiten. Von hier aus können Sie zum Beispiel:

- Unsere umfangreiche Wissensdatenbank durchsuchen.
- In unseren Diskussionsforen Fragen stellen und Antworten finden.
- Die neuesten Nachrichten und Ankündigungen der Software AG lesen.
- Unsere Communities erkunden.
- Unsere öffentlichen Repositories auf GitHub and Docker unter **https://github.com/softwareag** und **https://hub.docker.com/publishers/softwareag** besuchen und weitere Ressourcen der Software AG entdecken.

Produktsupport

Support für die Produkte der Software AG steht lizenzierten Kunden über unser Empower-Portal unter **https://empower.softwareag.com** zur Verfügung. Für viele Dienstleistungen auf diesem Portal benötigen Sie ein Konto. Wenn Sie noch keines haben, dann können Sie es unter **https://empower.softwareag.com/register** beantragen. Sobald Sie ein Konto haben, können Sie zum Beispiel:

- Produkte, Aktualisierungen und Programmkorrekturen herunterladen.
- Das Knowledge Center nach technischen Informationen und Tipps durchsuchen.
- Frühwarnungen und kritische Alarme abonnieren.
- Supportfälle öffnen und aktualisieren.
- Anfragen für neue Produktmerkmale einreichen.

Datenschutz

Die Produkte der Software AG stellen Funktionen zur Verarbeitung von personenbezogenen Daten gemäß der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union zur Verfügung. Gegebenenfalls sind in der betreffenden Systemverwaltungsdokumentation entsprechende Schritte dokumentiert.

2 Struktur und Terminologie von Natural Security

- Über diese Dokumentation 6
- Verwendungszweck von Natural Security 6
- Benutzer (Users) 7
- Bibliotheken (Libraries) 12
- Links zwischen Benutzern und Bibliotheken 13
- DDMs/Dateien (Files) 13
- Dienstprogramme (Utilities) 15
- Anwendungen (Applications) 15
- RPC Server 15
- Andere Objekttypen 16
- Profilparameter 16

In diesem Kapitel werden die grundlegenden Konzepte und alle Funktionen von Natural Security beschrieben. Die folgenden Themen werden behandelt:

Verwandte Themen:

- *Natural SAF Security*
- *SAF Security Kernel*

Über diese Dokumentation

Diese Dokumentation beschreibt alle Funktionen und Aspekte der Nutzung des Produkts Natural Security auf *allen* unterstützten Plattformen.

Die Zielgruppe dieser Dokumentation sind Natural Security-Administratoren. Diese sollten mit den Entwicklungsumgebungen auf den von Natural unterstützten Plattformen vertraut sein und ein gutes allgemeines Verständnis der Programmiersprache Natural haben.

Informationen zur Installation von Natural Security finden Sie in der *Natural Installation*-Dokumentation

Informationen zu Änderungen, Erweiterungen und neuen Funktionen der aktuellen Version finden Sie in der Natural-*Freigabemitteilung (Release Notes)*.

Vorsicht: Die Benutzerkennung `DBA` sollte nicht zu Testzwecken verwendet werden. Wie in der *Installation*-Dokumentation angegeben, sollte die Benutzerkennung DBA nur für die erstmalige Definition von Natural Security-Administratoren und für die Wiederherstellung der Natural Security-Umgebung verwendet werden. Wenn Sie mehrere Versionen von Natural Security in einer gemeinsamen FSEC-Systemdatei haben, sollten Sie nur die neueste Version für die Verwaltung Ihrer Security-Daten verwenden. Wenn Sie die Daten mit einer älteren Version verwalten, kann die Konsistenz der Daten nicht gewährleistet werden, insbesondere was die mit späteren Versionen eingeführten Einträge anbelangt.

Verwendungszweck von Natural Security

Natural Security ist ein umfassendes System zur Steuerung und Kontrolle des Zugriffs auf eine Natural-Umgebung.

Mit Natural Security können Sie Ihre Natural-Umgebung vor unberechtigtem Zugriff und zweckwidriger Nutzung schützen. Sie können genau festlegen, wer was tun darf. Sie können die Nutzung ganzer Bibliotheken und Natural-Dienstprogramme (Utilities) sowie einzelner Programme, Funktionen und DDMs einschränken. Außerdem können Sie die Bedingungen und Zeiten für die

Nutzung festlegen. So können Sie für jeden einzelnen Benutzer eine maßgeschneiderte Natural-Umgebung schaffen.

Dies geschieht durch die Definition von Objekten und der Beziehungen zwischen diesen Objekten. Ein Objekt wird in Natural Security definiert, indem ein *Sicherheitsprofil* für es erstellt wird.

Es gibt vier Haupttypen von Objekten, die unter Natural Security definiert werden können:

- Benutzer (Users)
- Bibliotheken (Libraries)
- DDMs/Dateien (Files)
- Dienstprogramme (Utilities)

Benutzer (Users)

Benutzer können entweder Personen (People) oder Terminals - oder Gruppen von Personen und/oder Terminals - sein, die Natural unter Natural Security nutzen. Wenn ein Benutzer definiert wird, muss eine *Benutzertyp*klassifizierung vorgenommen werden. Diese Klassifizierung legt fest, welche Möglichkeiten der Benutzer hat, Bibliotheken zu nutzen.

Personen können als einer der folgenden Benutzertypen definiert werden:

- MEMBER (Mitglied)
- PERSON
- ADMINISTRATOR

Terminals können als Benutzertyp definiert werden:

TERMINAL

Benutzer der oben genannten Typen können in Gruppen zusammengefasst werden, die als Benutzertyp definiert werden:

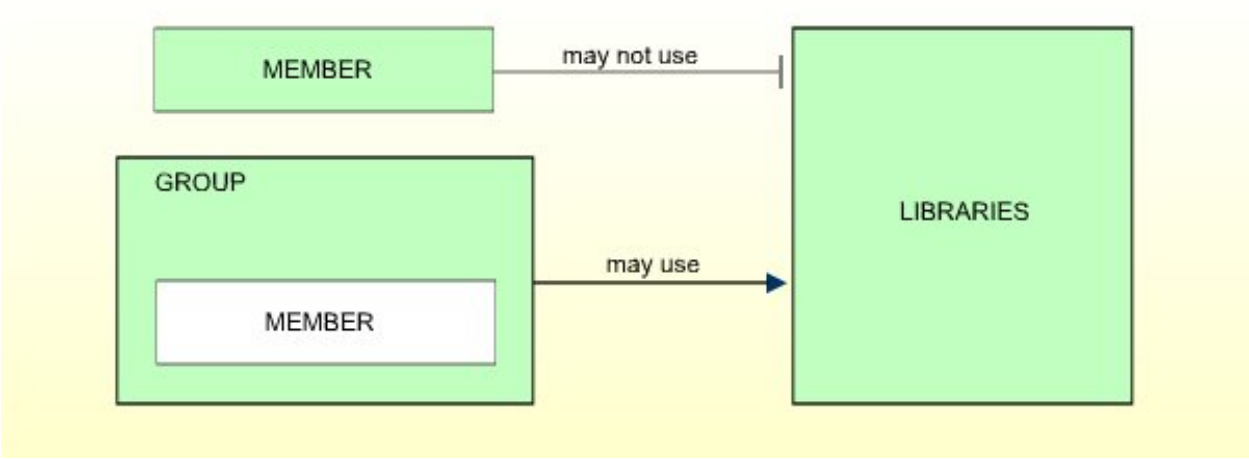
GROUP

Darüber hinaus sind folgende spezielle Benutzertypen verfügbar:

- Externer Benutzer
- Batch-Benutzer

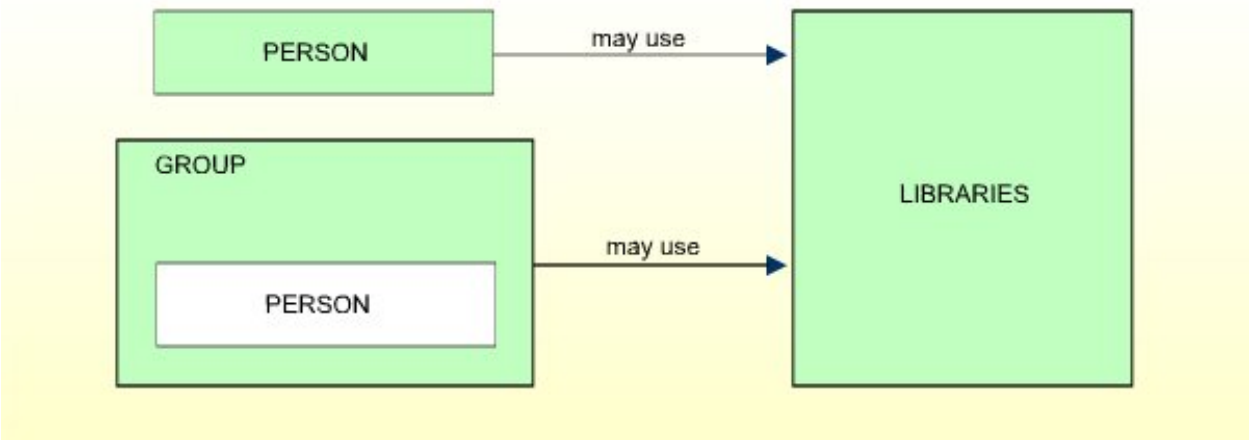
Benutzertyp MEMBER (Mitglied)

Mitglieder können Bibliotheken nicht direkt nutzen. Sie können Bibliotheken nur über die Mitgliedschaft in Gruppen nutzen. Daher müssen sie mindestens einer Gruppe zugeordnet sein, um überhaupt eine Bibliothek nutzen zu können. Normalerweise ist dies der Standard-Benutzertyp, der auf die meisten Personen zutreffen wird.



Benutzertyp PERSON

Benutzer des Typs PERSON können Bibliotheken direkt benutzen. Sie können auch Gruppen zugewiesen werden. Sie können also Bibliotheken entweder direkt oder über die Mitgliedschaft in einer GROUP nutzen. Dieser Benutzertyp ist für Personen gedacht, die spezielle, individuell definierte Zugriffsrechte auf Bibliotheken haben sollen.

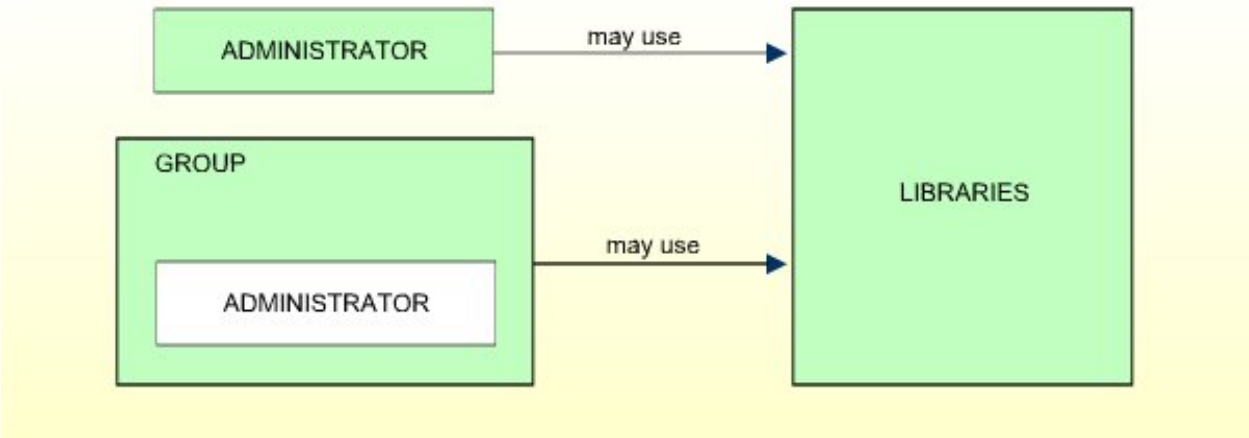


Benutzertyp ADMINISTRATOR

Administratoren dürfen Bibliotheken direkt benutzen. Sie können auch Gruppen zugewiesen werden. Sie können also Bibliotheken entweder direkt oder über die Mitgliedschaft in Gruppen nutzen. In dieser Hinsicht entsprechen sie dem Benutzertyp PERSON.

Darüber hinaus haben Administratoren das alleinige Recht, Natural Security zu verwalten, d. h. die Sicherheitsprofile von Objekten und die Beziehungen zwischen diesen Objekten anzulegen und zu ändern.

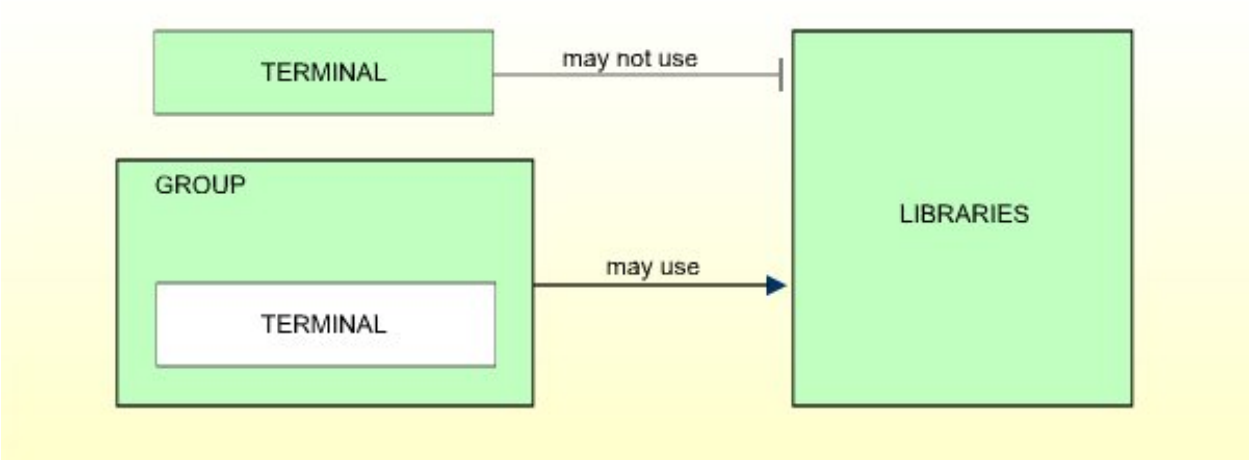
Der Benutzertyp ADMINISTRATOR ist nur für diejenigen Benutzer vorgesehen, die Systemadministratoren für Natural Security sein sollen.



Benutzertyp TERMINAL

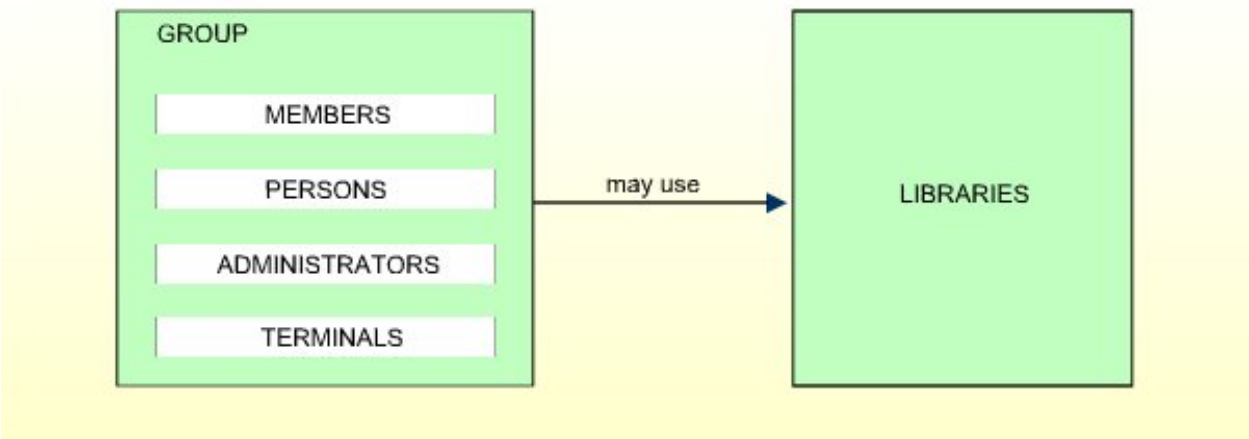
Dieser Benutzertyp gilt nur für Terminals. Terminals müssen nicht unbedingt definiert werden. Die Definition von Terminals wird nur im Zusammenhang mit Bibliotheken relevant, die nur von bestimmten Terminals aus benutzt werden sollen.

Terminals können Bibliotheken nicht direkt nutzen, sondern nur über die Mitgliedschaft in Gruppen. Terminals müssen daher mindestens einer Gruppe zugewiesen sein.



Benutzertyp GROUP (Gruppe)

Gruppen können angelegt werden, um die Verwaltung von Natural Security zu erleichtern. Eine Gruppe kann Benutzer eines beliebigen anderen Benutzertyps enthalten. Benutzer können in mehr als einer Gruppe enthalten sein.



Zugriffsrechte auf Bibliotheken können für eine Gruppe definiert werden und gelten dann für alle Benutzer, die in derselben Gruppe enthalten sind, so dass sie nicht für jeden Benutzer einzeln definiert werden müssen. (Für Administratoren und Personen, die in Gruppen enthalten sind, können optional individuelle Zugriffsrechte definiert werden, die sich von denen der Gruppen unterscheiden, in denen sie enthalten sind).

Spezielle Benutzertypen

- External User (Externer Benutzer)
- Batch User (Batch-Benutzer)

External User (Externer Benutzer)

Der Benutzertyp External User ist nur relevant, wenn die Benutzerauthentifizierung über einen LDAP-Server erfolgt.

Es gibt nur ein Benutzersicherheitsprofil für diesen Benutzertyp. Er wird verwendet, wenn die Benutzerauthentifizierung über einen LDAP-Server erfolgt und die vom LDAP-Server authentifizierte Benutzerkennung nicht in Natural Security definiert ist. In diesem Fall wird dieser Benutzerkennung nach erfolgreicher Anmeldung automatisch das External User-Profil zugewiesen, d. h. der Benutzer greift auf Natural unter den im External User-Profil definierten Bedingungen zu.

Der externe Benutzer kann Bibliotheken nicht direkt nutzen, sondern nur über die Mitgliedschaft in Gruppen. Daher muss das Profil des externen Benutzers mindestens einer Gruppe zugewiesen werden, um eine beliebige Bibliothek nutzen zu können.

Um das Sicherheitsprofil für den externen Benutzer anzulegen, verwenden Sie nicht die Funktion **Add User** (Benutzerdefinition anlegen), sondern das Feld **NSC user ID** im **LDAP Security Profile**. Weitere Einzelheiten finden Sie unter ***Bestandteile eines LDAP-Sicherheitsprofils*** im Abschnitt *Authentifizierungsoptionen (LDAP)*.

Batch User (Batch-Benutzer)

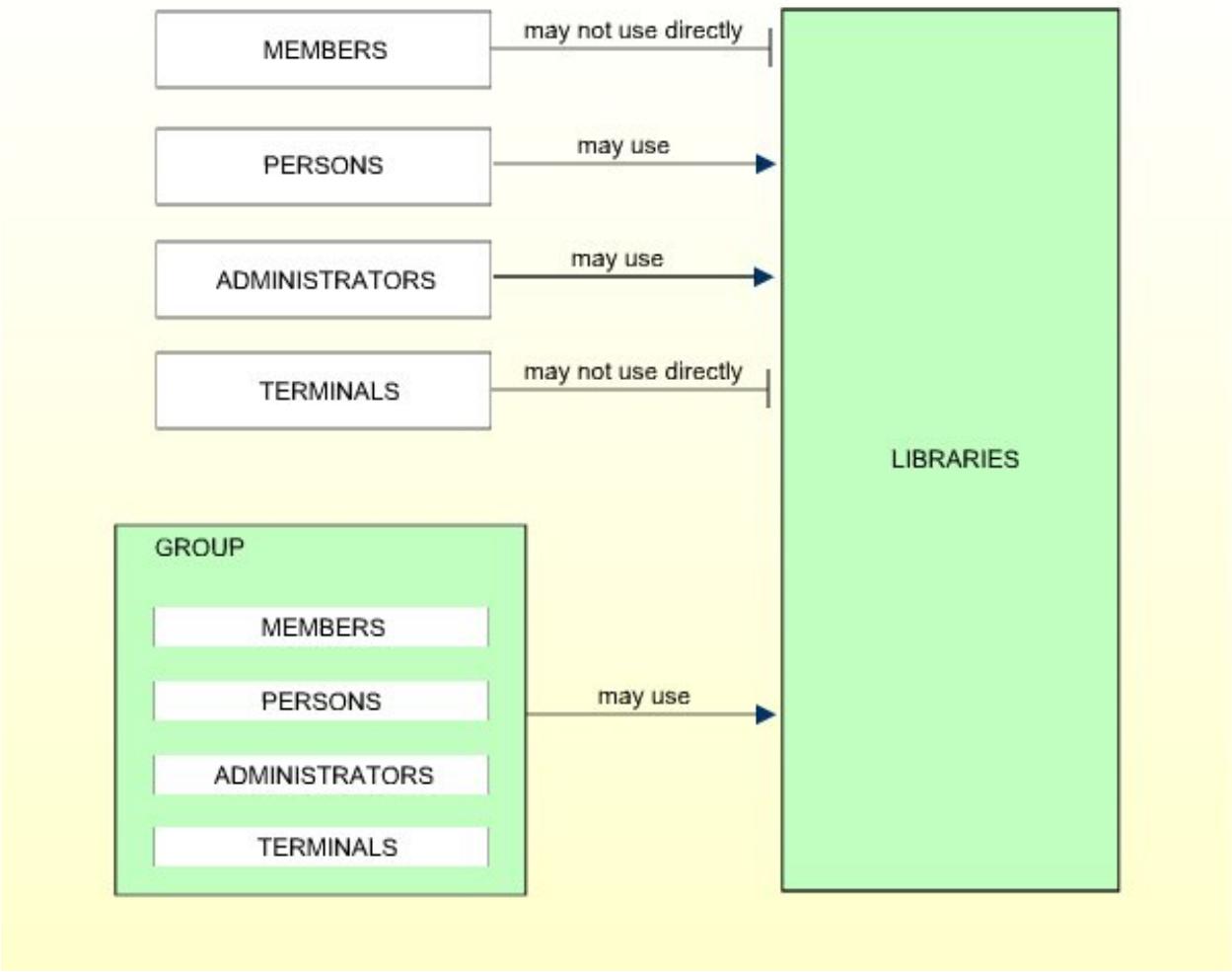
Der Benutzertyp Batch-Benutzer ist nur relevant, wenn Benutzer Natural im Batch-Modus unter anderen Bedingungen als im Online-Modus verwenden sollen. Einzelheiten dazu finden Sie unter ***Batch-Benutzersicherheitsprofile*** im Kapitel *Natural Security im Batch-Modus*.

Welcher Benutzertyp für welchen Benutzer?

Normalerweise ist es am besten, zunächst alle Personen als Mitglieder (MEMBER) zu definieren. Falls erforderlich, kann ein Mitglied zu einem späteren Zeitpunkt in eine Person geändert werden. Mitglieder und Personen können zu Administratoren hochgestuft werden.

Jeder Benutzer sollte mindestens einer Gruppe zugeordnet sein. Es wird empfohlen, so weitgehend wie möglich Gruppen zu verwenden, da dies nicht nur den Verwaltungsaufwand für Natural Security erheblich verringert, sondern auch ein konsistenteres Schutzkonzept ermöglicht.

Zusammenfassend lässt sich sagen, dass sich die Benutzertypen in Bezug auf den Zugriff auf die Bibliotheken grundsätzlich voneinander unterscheiden. Die möglichen Beziehungen sind in der folgenden Grafik dargestellt:



Bibliotheken (Libraries)

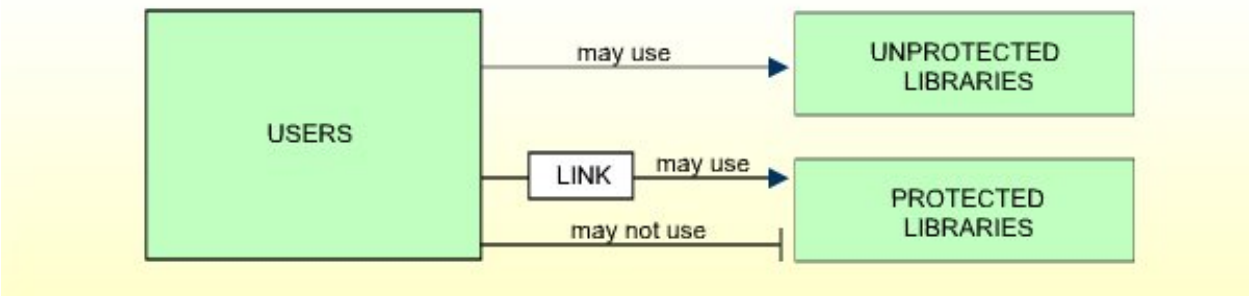
Bibliotheken sind Natural Libraries, die Bestände an Quellprogrammen und/oder Objektmodulen enthalten, die eine bestimmte Funktion erfüllen.

Bibliotheken können als *geschützt* oder *ungeschützt* definiert werden.

- *Ungeschützte* Bibliotheken können von jedem Benutzer benutzt werden, ohne dass eine spezifische Beziehung definiert werden muss. (Denken Sie daran, dass nur Benutzer des Typs ADMINISTRATOR oder PERSON Bibliotheken direkt verwenden können. MEMBERs und TERMINALs können Bibliotheken nur über die Mitgliedschaft in einer GROUP benutzen.)
- *Geschützte* Bibliotheken können nur von Benutzern verwendet werden, die eine spezifische Beziehung zu den Bibliotheken haben. Diese spezifische Beziehung wird als *Link* (oder *Verlinkung*) bezeichnet.

Links zwischen Benutzern und Bibliotheken

Ein *Link* ist die Beziehung zwischen einem Benutzer (Benutzertyp ADMINISTRATOR, PERSON oder GRUPPE) und einer geschützten Bibliothek, die es dem Benutzer erlaubt, die Bibliothek zu benutzen.



Die verschiedenen Schutzarten für Bibliotheken und Links zu Bibliotheken werden im Kapitel ***Bibliotheken schützen*** beschrieben.

DDMs/Dateien (Files)

Der Schutz von Datendefinitionsmodulen (DDMs) ist je nach verwendeter Plattform unterschiedlich. Das liegt daran, dass DDMs bei Natural auf Nicht-Großrechnerplattformen in Bibliotheken gespeichert werden, während DDMs bei Natural auf Großrechnern in einer FDIC-Systemdatei gespeichert werden und keinen direkten Bezug zu einer Bibliothek haben. Siehe auch Kapitel ***Natural Security auf verschiedenen Plattformen***.

Auf Großrechnern muss ein DDM in Natural Security als *Datei* definiert werden, bevor es unter Natural Security verwendet werden kann, d. h. es muss ein so genanntes *Dateisicherheitsprofil* für das DDM erstellt werden. Auf Nicht-Großrechnerplattformen wird ein *DDM-Sicherheitsprofil* angelegt, das dem Sicherheitsprofil der Bibliothek, die das DDM enthält, untergeordnet ist.

Für jedes DDM muss in Natural Security eine Statusklassifizierung vorgenommen werden. Dieser *Status* bestimmt, ob das DDM verwendet werden kann, d. h. ob es in einem Datenbankzugriffs-Statement innerhalb eines Natural-Programms referenziert werden kann.

Dateistatus auf Großrechnern

Auf Großrechnern hat ein DDM nur einen *Dateistatus* (der in seinem Dateisicherheitsprofil festgelegt ist), der einer der folgenden sein kann:

PUBLIC	Das DDM ist nicht geschützt. Es kann von jeder Bibliothek verwendet, d.h. gelesen (read) und geändert (update) werden.
ACCESS	Das DDM ist gegen Änderungen (Updates) geschützt. Es kann von jeder Bibliothek gelesen werden. Er kann jedoch nur von Bibliotheken geändert werden, die mit ihm *verlinkt* wurden.
PRIVATE	Das DDM ist geschützt. Es kann nur von Bibliotheken verwendet werden, die mit ihm *verlinkt* wurden. Eine solche Verlinkung kann als „read“ (d.h. nur lesen) oder „update“ (ändern, was lesen impliziert) definiert werden.

Einzelheiten finden Sie im Kapitel ***DDMs auf Großrechnern schützen***.

Interner und externer Status auf Nicht-Großrechnern

Auf Nicht-Großrechner-Plattformen hat ein DDM einen *internen Status* und einen *externen Status*.

Der interne Status steuert die Verwendung des DDMs *innerhalb* der Bibliothek, in der es enthalten ist. Er kann einer der folgenden sein:

PUBLIC	Das DDM kann von allen Programmen innerhalb der Bibliothek gelesen (read) und geändert (update) werden.
ACCESS	Das DDM kann von allen Programmen innerhalb der Bibliothek gelesen (read), aber nicht geändert (update) werden.
PRIVATE	Das DDM kann von keinem Programm innerhalb der Bibliothek verwendet werden.

Der externe Status steuert die Verwendung des DDM durch *andere* Bibliotheken - vorausgesetzt, dass die Bibliothek, die das DDM enthält, von anderen Bibliotheken als Steplib verwendet wird. Der Status kann einer der folgenden sein:

PUBLIC	Das DDM ist *nicht* geschützt. Er kann von jeder Bibliothek verwendet, d. h. gelesen (read) und geändert (update) werden.
ACCESS	Das DDM ist gegen Änderung (update) geschützt. Es kann von jeder Bibliothek gelesen (read) werden. Es kann jedoch nur von Bibliotheken geändert werden, die mit ihm *verlinkt* wurden.
PRIVATE	Das DDM ist geschützt. Er kann nur von Bibliotheken verwendet werden, die mit ihm *verlinkt* wurden. Diese Verlinkung kann als „read“ (nur lesen) oder „update“ (ändern, was lesen impliziert) definiert werden.

Weitere Informationen siehe Kapitel ***DDMs unter Linux und Windows schützen***.

Dienstprogramme (Utilities)

Mit Natural Security können Sie die Verwendung verschiedener Natural-Dienstprogramme (Utilities) steuern. Dieser Dienstprogrammschutz ist funktionsorientiert, d. h. Sie können die Funktionen eines Dienstprogramms einzeln erlauben oder nicht erlauben.

Sie können die Verwendung eines Dienstprogramms steuern, indem Sie für dieses Dienstprogramm Profile definieren. Mittels verschiedener Arten von hierarchisch gegliederten *Dienstprogrammprofilen* können Sie genau festlegen, wer welche Funktion nutzen darf.

Bei Dienstprogrammen, die den Inhalt einzelner Bibliotheken betreffen, können Sie außerdem festlegen, für welche Bibliotheken eine Funktion des Dienstprogramms erlaubt sein soll und für welche nicht. Dies können Sie auch für einzelne Benutzer unterschiedlich festlegen.

Weitere Informationen siehe Kapitel ***Dienstprogramme (Utilities) schützen***.

Anwendungen (Applications)

Anwendungen sind Basisanwendungen (*Base Application*) und Verbundanwendungen (*Compound Application*), die im Anwendungsarbeitsbereich (Application Workspace) von Natural Studio angelegt und verwaltet und in Verbindung mit dem Natural Development Server verwendet werden.

Wenn der Natural Development Server bei Ihnen installiert ist, können Sie den Zugriff auf Base und Compound Applications mit Natural Security steuern. Dazu können Sie Sicherheitsprofile für die Anwendungen definieren und Links zwischen Benutzern und Anwendungen anlegen.

Weitere Informationen siehe Kapitel ***Natural Development Server-Anwendungen schützen***.

RPC Server

In einer Client/Server-Umgebung können Sie Natural Security einsetzen, um die Verwendung von Natural Remote Procedure Calls zu schützen. Sie können sowohl Natural RPC Server als auch die Art und Weise schützen, in der von Clients abgesetzte Natural RPC-Dienstanforderungen (*Service Requests*) von diesen Servern verarbeitet werden.

Um den Zugriff auf Natural RPC Server und die Behandlung von Dienstanforderungen durch diese Server zu steuern, bietet Natural Security mehrere Optionen, die Sie einstellen können. Außerdem können Sie Sicherheitsprofile für zu schützende Natural RPC Server definieren.

Weitere Informationen siehe Kapitel ***Natural RPC Server und Services schützen*** .

Andere Objekttypen

Neben Benutzern, Bibliotheken, DDMs/Dateien, Dienstprogrammen und Anwendungen gibt es weitere Objekttypen, die unter Natural Security definiert werden können. Diese anderen Objekte sind jedoch für den Schutz Ihrer Natural-Umgebung durch Natural Security nicht unbedingt erforderlich. Diese anderen Objekttypen sind:

- **Externe Objekte**
  Hierbei handelt es sich um Objekte verschiedenen Typs, die von Predict und anderen Produkten verwendet werden (Einzelheiten siehe Kapitel *Externe Objekte schützen*).
- **Mailboxen**
  Hierbei handelt es sich um Informationsbildschirme, über die Nachrichten an Natural-Benutzer gesendet werden können (weitere Informationen siehe Kapitel *Mailboxen*).

Profilparameter

Einige Natural-Profilparameter werden von Natural Security beeinflusst. Die folgende Liste gibt einen Überblick über diese Profilparameter und ihre entsprechenden Einstellungen in Natural Security.

Profilparameter	Entsprechende Einstellung in Natural Security
CF	**CF** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.
CLEAR	**CLEAR** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.
DC	**DC** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.
DU	**DU** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.
EJ	**EJ** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.
ETA	**Error** im Abschnitt **Transaktionen** der Bibliothekssicherheitsprofile.
ETID	**Default ETID** in den Benutzersicherheitsprofilen.
FDIC	Die Einstellungen im Abschnitt **Bibliotheksdatei** in den Benutzersicherheitsprofilen.
FS	**FS** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.
FUSER	Die Einstellungen im Abschnitt **Bibliotheksdatei** der Bibliothekssicherheitsprofile.
IA	**IA** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.
ID	**ID** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.
IM	**IM** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.
LS	**LS** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.
LT	**Processing loop limit** im Abschnitt **Sicherheitslimits** der Bibliothekssicherheitsprofile.

Profilparameter	Entsprechende Einstellung in Natural Security
MADIO	**Maximum number of Adabas calls** im Abschnitt **Sicherheitslimits** der Bibliothekssicherheitsprofile.
MAXCL	**Maximum number of program calls** im Abschnitt **Sicherheitslimits** der Bibliothekssicherheitsprofile.
MT	**Maximum amount of CPU time** im Abschnitt **Sicherheitslimits** der Bibliothekssicherheitsprofile.
OPRB	**Adabas open** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.
PS	**PS** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.
RPC	Die Einstellungen im Abschnitt **Natural RPC Restrictions** der Bibliothekssicherheitsprofile.
SA	**SA** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.
SF	**SF** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.
SL	**SL** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.
SLOCK	**SLOCK** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.
SM	**Programming Mode** im Abschnitt **Allgemeine Optionen** der Bibliothekssicherheitsprofile.
STEPLIB	**Steplibs** im Abschnitt **Zusätzliche Optionen** der Bibliothekssicherheitsprofile.
TD	**Zeitdifferenz** der Benutzersicherheitsprofile.
ULANG	**Sprache** in Benutzersicherheitsprofilen.
WH	**WH** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.
ZD	**ZD** im Abschnitt **Session-Parameter** der Bibliothekssicherheitsprofile.

3 Natural Security auf verschiedenen Plattformen

- Unterstützte Plattformen 20
- Natural Security auf mehreren Plattformen verwenden 21

In diesem Kapitel werden folgende Themen behandelt:

Unterstützte Plattformen

Natural Security ist auf folgenden Plattformen verfügbar:

- Großrechner,
- Linux,
- Windows.

Natural Security ist sowohl als Vollversion als auch als Laufzeitversion verfügbar:

Vollversion

In der Regel wird Natural Security als Vollversion installiert, die den gesamten Funktionsumfang von Natural Security umfasst. Die Vollversion kann auf allen Plattformen installiert werden - mit Ausnahme einiger Windows-Plattformen (wie in den *Natural Release Notes* aufgeführt), auf denen nur die Laufzeitversion verfügbar ist.

Die Vollversion umfasst die gesamte Laufzeitfunktionalität sowie die vollständige Administrations- und Pflegefunktionalität. Sie bietet in der Anwendung `SYSSEC` alle Funktionen für die Online-Systemverwaltung und -Pflege von Natural Security-Daten und für die Erstellung und Auswertung von Zugriffsprotokollen sowie Anwendungsprogrammierschnittstellen für die Abfrage (Retrieval) und Pflege von Natural Security-Daten.

Laufzeitversion

Auf Windows-Plattformen, die sich nicht für den Stand-alone-Betrieb von Natural eignen, wird Natural Security als reine Laufzeitversion installiert. Sie enthält nur die Funktionen, die für die Benutzerauthentifizierung und die Zugriffskontrolle auf Natural-Ressourcen nötig sind: Dazu gehören die Anmeldeprozedur, die die Benutzerauthentifizierung und die Überprüfung der Zugriffsrechte bei der Anmeldung eines Benutzers an einer Natural-Sitzung durchführt, sowie die Prozeduren, die die Zugriffskontrolle durchführen, um zu prüfen, ob ein Benutzer die Berechtigung hat, die gewünschten Funktionen innerhalb einer Natural-Sitzung durchzuführen. Darüber hinaus stehen Abfragefunktionen (Retrieval) zur Verfügung, die von den Natural Security-**Anwendungsprogrammierschnittstellen** bereitgestellt werden.

Da die Laufzeitversion keine Verwaltungsfunktionen enthält, erfordert sie den Zugriff auf eine Natural Security-Systemdatei (FSEC) auf einer anderen Plattform. Daher kann eine Laufzeitversion nur in Kombination mit einer Vollversion verwendet werden, die auf einer der anderen Plattformen installiert ist.

Natural Security auf mehreren Plattformen verwenden

Folgende Themen werden behandelt:

- Zentrale FSEC-Systemdatei
- Schutz von Programmierobjekten
- Schutz von DDMs
- Zeichenumsetzung in Client/Server-Umgebungen
- Konfigurieren von Entire Net-Work

Zentrale FSEC-Systemdatei

In einer heterogenen, plattformübergreifenden Natural-Umgebung muss die Administration und Abfrage (Retrieval) von Natural Security-Daten berücksichtigt werden. Es ist möglich, für jede Installation eine eigene Natural Security-Systemdatei (FSEC) einzurichten und jede FSEC-Systemdatei unabhängig zu verwalten.

Es ist aber auch möglich, eine einzige FSEC-Systemdatei einzurichten, in der alle Natural Security-Daten zentral gespeichert werden. Die Natural Security-Installationen müssen in einem Netzwerk über Entire Net-Work verbunden sein. Der Zugriff auf die zentral gespeicherten Sicherheitsdaten wird von Entire Net-Work über Remote-Datenbankaufrufe abgewickelt.

Wenn die Konfiguration mit mehreren Plattformen keinen Großrechner umfasst, können die FSEC-Systemdatei und die Natural Security-Daten auf jeder der (Vollversions-)Installationen liegen. Es wird jedoch empfohlen, sie in der Installation zu pflegen, auf der die FSEC-Systemdatei lokal ist.

Wenn die Konfiguration mit mehreren Plattformen einen Großrechner umfasst, müssen sich die FSEC-Systemdatei auf dem Großrechner befinden und die Natural Security-Daten dort gepflegt werden. Bei Installationen ohne Großrechner wird die Pflege der Natural Security-Daten dann automatisch deaktiviert. Dies gilt auch für die Pflege für die **Anwendungsprogrammierschnittstellen** von Natural Security.

Die Zugriffsmöglichkeiten auf eine FSEC-Systemdatei in einer Konfiguration mit mehreren Plattformen sind wie folgt:

Speicherort von FSEC	Erreichbar von
Großrechner	Großrechner, Linux und Windows
Linux	Linux und Windows
Windows	Linux und Windows

Hinsichtlich des Schutzes von Programmierobjekten und DDMs ist in einer heterogenen Umgebung ist Folgendes zu beachten:

- *Schutz von Programmierobjekten*

- *Schutz von DDMs*

Schutz von Programmierobjekten

In einer heterogenen Produktionsumgebung, bei der eine zentrale Großrechner-FUSER-Systemdatei verwendet wird, wäre eine Bibliothek, die nicht in der Großrechner-FUSER-Systemdatei, sondern im Dateisystem einer anderen Plattform vorhanden ist, der Natural Security auf dem Großrechner nicht bekannt. Um in einer solchen Bibliothek enthaltene „nicht existierende“ Module definieren zu können, bietet die Funktion **Disallow/Allow Modules** die Unterfunktion **Free List of Modules** (die im Kapitel *Bibliotheken verwalten* beschrieben wird).

Mit der Option **Module Protection Mode** (siehe Kapitel *Administrator Services*) ist es möglich, den Schutz von Programmierobjekten durch Natural Security für alle Großrechner- und Nicht-Großrechner-Plattformen einheitlich zu gestalten.

Schutz von DDMs

Der Speicherort in Natural für DDMs ist nicht auf allen Plattformen gleich: Auf Großrechnerplattformen werden DDMs in einer FDIC-Systemdatei gespeichert, während DDMs unter Linux und Windows wie andere Natural-Objekte in Bibliotheken enthalten sind. Daher ist auch die Handhabung des DDM-Schutzes durch Natural Security unterschiedlich:

- Auf Großrechnerplattformen werden DDMs als separate Objekte (als „Dateien“ bezeichnet) behandelt, die über eigene Sicherheitsprofile verfügen.
- Auf Nicht-Großrechnerplattformen ist der Schutz von DDMs dem Schutz von Bibliotheken untergeordnet, und die DDM-Sicherheitsprofile sind den Bibliothekssicherheitsprofilen untergeordnet.

Weitere Informationen finden Sie unter *DDM/Dateien* im Kapitel *Struktur und Terminologie von Natural Security*.

In einer heterogenen Umgebung, in der eine zentrale FSEC-Systemdatei auf einem Großrechner verwendet wird, müssen alle DDMs auf den Nicht-Großrechnerplattformen in die Bibliothek `SYSTEM` übertragen werden, um ihre Verwendung unter Natural Security zu ermöglichen.

Profilparameter FDDM

Wenn eine Systemdatei als zentraler Speicherort für DDMs (außerhalb von Bibliotheken) mit dem Natural-Profilparameter `FDDM` auf einer Nicht-Großrechnerplattform angegeben wird, erfolgt der Schutz von Nicht-Großrechner-DDMs und die Pflege ihrer Sicherheitsprofile auf die gleiche Weise wie bei Großrechner-DDMs.

Zeichenumsetzung in Client/Server-Umgebungen

Wenn Natural Security auf mehreren Plattformen in einer Client/Server-Umgebung eingesetzt wird und eine Anmeldung auf einem Client erfolgt, der einen anderen Zeichencode als der Server verwendet, muss Natural Security die Anmeldedaten auf dem Server von ASCII nach EBCDIC oder umgekehrt umsetzen. Für diese Zeichenumsetzung verwendet Natural Security die folgenden Umsetzungstabellen:

- Auf Großrechnern verwendet Natural Security die Umsetzungstabelle `NTTABA2` im Natural-Konfigurationsmodul `NATCONFG`.
- Auf Nicht-Großrechnerplattformen verwendet es die Abschnitte `ISO8859_1->EBCDIC` und `EBCDIC->ISO8859_1` der Natural-Konfigurationsdatei `NATCONV.INI`.

Wenn diese nicht Ihren Anforderungen entsprechen, müssen Sie sie möglicherweise anpassen. Weitere Informationen finden Sie in der Natural *Operations*-Dokumentation für die jeweilige Plattform.

Konfigurieren von Entire Net-Work

Im Mittelpunkt des Umsetzungsprozesses von Entire Net-Work stehen das Format und die Länge der einzelnen Felder, die in den Such- und Formatpuffern angegeben sind, die bei jedem Adabas-Aufruf zusammen mit speziellen Parametern für die Umsetzungsdefinition übergeben werden. Wenn eine Anfrage die Netzwerkkonvertierungsroutinen durchläuft, wird jedes einzelne Feld entsprechend dem Format und der Länge umgesetzt, die im zugehörigen Such- oder Formatpuffer für das Feld definiert sind.

Um die Fehler `NAT0824` und `NAT0825` zu vermeiden, müssen Sie Umsetzungsdefinitionen für die folgenden Felder für die Datenbankkennung (DBID) und die Dateinummer (FNR) der Großrechner-FSEC-Systemdatei mit Format „X“ hinzufügen:

- LW
- LC
- LQ
- LV
- LS

Dadurch wird verhindert, dass Werte entweder umgesetzt oder vertauscht werden.

Weitere Informationen finden Sie unter *Special Handling Of Field Format `0`* im Kapitel *Heterogeneous Platform Considerations* der Entire Net-Work *Installation and Operations for Mainframes*-Dokumentation.

4 Erste Schritte nach der Installation

- Schritt 1: Ändern Sie das Passwort des Benutzers DBA. 26
- Schritt 2: Administratoren definieren 27
- Schritt 3: Definieren Sie Systembibliotheken 28

In diesem Kapitel werden die Schritte beschrieben, die Sie nach der Erstinstallation von Natural Security durchführen müssen:

Diese Schritte müssen nur nach einer Erstinstallation von Natural Security durchgeführt werden, d.h. wenn die von Ihnen installierte Version Ihre erste Version von Natural Security in dieser FSEC-Systemdatei ist. Nach Installation einer neuen Natural Security-Version in einer bestehenden FSEC-Systemdatei brauchen diese Schritte nicht ausgeführt zu werden.

Schritt 1: Ändern Sie das Passwort des Benutzers DBA.

Um das Passwort des Benutzers DBA zu ändern:

1. Rufen Sie Natural in der Umgebung auf, in der Natural Security installiert wurde.
2. Geben Sie im Anmeldebildschirm von Natural Security (bzw. im Anmeldedialogfenster) die Bibliothekskennung `SYSSEC`, die Benutzerkennung `DBA`, das Passwort `DBA` und ein neues Passwort ein, und drücken Sie ENTER.
3. Geben Sie das neue Passwort erneut ein und drücken Sie ENTER, um die Passwortänderung zu bestätigen.

Passwort-Regeln

Das neue Passwort für den Benutzer DBA muss den folgenden Regeln entsprechen:

- Es muss 8 Zeichen lang sein.
- Es muss mindestens einen Großbuchstaben enthalten.
- Es muss mindestens eine Zahl enthalten.
- Es muss mindestens ein Sonderzeichen enthalten.
- Es darf nicht die Zeichenfolge `DBA` enthalten.
- Jedes Zeichen darf nur einmal im Passwort vorkommen.

Überprüfung der Installation

Die Tatsache, dass Sie diesen Schritt ausführen konnten, bedeutet, dass Natural Security betriebsbereit ist. Eine weitere Überprüfung ist nicht erforderlich.

Schritt 2: Administratoren definieren

Erstellen Sie für jede Person, die ein Natural Security-Administrator sein soll, ein Benutzersicherheitsprofil und verlinken Sie dann jeden Natural Security-Administrator mit der Bibliothek SYSSEC.

Im Folgenden finden Sie ein *Beispiel* für diese Vorgehensweise.

Um einen Administrator zu definieren:

1 Geben Sie auf dem Anmeldebildschirm von Natural Security (bzw. im Anmeldedialogfenster) die Bibliothekskennung SYSSEC, die Benutzerkennung DBA und das neue Passwort (wie in Schritt 1 oben festgelegt) ein.

Das Natural Security **Main Menu** wird angezeigt.

2 Wählen Sie die Option **Maintenance** (Verwaltung).

Ein Fenster wird angezeigt.

3 Markieren Sie den Objekttyp **User** (Benutzer) mit einem Zeichen oder mit dem Cursor.

Die Auswahlliste **User Maintenance** (Benutzerverwaltung) wird angezeigt.

4 Geben Sie in der Kommandozeile dieser Auswahlliste das Kommando ADD (Anlegen) ein.

Ein Fenster wird angezeigt.

5 Wählen Sie eine Benutzerkennung für Ihren Natural Security-Administrator. Wäre der Name des Administrators beispielsweise „Arthur Dent“, könnten Sie „AD“ als seine Benutzerkennung wählen. In den folgenden Schritten dieses Beispiels wird diese Kennung verwendet.

6 Geben Sie die Benutzerkennung AD und den Benutzertyp „A“ ein.

Der Bildschirm **Add User** (Benutzer anlegen) wird angezeigt.

7 Geben Sie den Benutzernamen „Arthur Dent“ ein und setzen Sie das Feld **Private Library** auf N (und drücken Sie ENTER).

8 Drücken Sie PF3.

Der Benutzer „Arthur Dent“ ist nun in Natural Security unter der Benutzerkennung „AD“ definiert. Die Auswahlliste **User Maintenance** (Benutzerverwaltung) wird wieder angezeigt.

Um den Administrator mit SYSSEC zu verlinken:

1 Markieren Sie in der Spalte **Co** der **User Maintenance**-Auswahlliste den Benutzer „AD“ mit dem Funktionscode LL.

Ein Fenster wird angezeigt.

2 Geben Sie die Bibliothekskennung SYSSEC ein.

Die Auswahlliste **Link User To Libraries** (Benutzer mit Bibliotheken verlinken) wird angezeigt.

3 Markieren Sie in der Spalte **Co** der Auswahlliste die Bibliothek SYSSEC mit dem Funktionscode LK.

Der Benutzer „Arthur Dent“ ist nun mit der Bibliothek SYSSEC verlinkt.

4 Geben Sie in der Kommandozeile das Kommando LOGOFF ein.

Der Anmeldebildschirm (bzw. das Anmeldedialogfenster) von Natural Security wird angezeigt.

Jetzt können Sie sich mit der Benutzerkennung „AD“ und dem Passwort „AD“ bei SYSSEC anmelden. Wenn Sie sich zum ersten Mal mit der neuen Benutzerkennung anmelden, müssen Sie das Passwort ändern (indem Sie zusätzlich zur Benutzerkennung und zum Passwort ein neues Passwort eingeben).

Benutzer DBA löschen

Nachdem Sie erfolgreich Administratoren definiert haben, empfiehlt es sich, den Benutzer DBA zu löschen, um sicherzustellen, dass die Benutzerkennung DBA nicht von unbefugten Benutzern verwendet werden kann, um Zugriff auf SYSSEC zu erhalten.

Um den Benutzer DBA zu löschen:

1 Melden Sie sich in der Bibliothek SYSSEC mit der Benutzerkennung AD an.

2 Gehen Sie wie oben beschrieben zur Auswahlliste **User Maintenance** (Benutzerverwaltung).

3 Markieren Sie in der Liste den Benutzer DBA mit dem Funktionscode DE.

4 Ein Fenster wird angezeigt, in dem Sie die Benutzerkennung DBA eingeben müssen.

Der Benutzer DBA ist nun gelöscht.

Schritt 3: Definieren Sie Systembibliotheken

Legen Sie Sicherheitsprofile für alle Systembibliotheken von Natural und Natural-Subprodukten an, die an Ihrem Standort installiert sind. Verwenden Sie dazu die Natural Security-Funktion **Definition of System Libraries** (siehe *Systembibliotheken definieren*), die im Kapitel *Administrator Services* beschrieben ist.

5 Anmeldung (Logon)

- Vorgehensweise bei der Anmeldung 30
- LOGON-Kommando 34
- Automatische Anmeldung 35
- Logon-Anpassung 36
- Natural-Sitzung beenden 38

In diesem Kapitel wird beschrieben, welche Regeln gelten, wenn sich ein Benutzer bei Natural unter Natural Security anmeldet.

Folgende Themen werden behandelt:

Vorgehensweise bei der Anmeldung

Anmerkung: Wenn ein Benutzer Natural unter Natural Security aufruft und die in der verwendeten Parameterdatei bzw. dem verwendeten Modul angegebene FNAT-Systemdatei eine Nicht-Security-Systemdatei ist, kann Natural nicht gestartet werden, und der Benutzer erhält eine entsprechende Fehlermeldung.

Das Anmeldeverfahren wird von Natural Security verwendet, um sicherzustellen, dass der Benutzer, der sich bei Natural anmeldet, zum Zugriff auf die angeforderte Bibliothek berechtigt ist.

Eine Anmeldung muss erfolgreich durchgeführt werden, bevor eine Natural-Sitzung gestartet werden kann.

Ein Anmeldebildschirm (auf Großrechnern und Linux) bzw. ein Anmeldedialogfenster (unter Windows) wird dem Benutzer zur Eingabe der für die Anmeldung erforderlichen Informationen angeboten.

Anmeldebildschirm / Anmeldedialogfenster

Ist Natural Security installiert, wird der Anmeldebildschirm von Natural Security angezeigt, sobald ein Benutzer Natural aufruft.

Unter Windows wird der Anmeldebildschirm in Form eines Dialogfensters angezeigt (aus Gründen der Konsistenz wird er in diesem Dokument ebenfalls als Anmeldebildschirm bezeichnet).

Auf dem Anmeldebildschirm wird der Benutzer aufgefordert, Folgendes einzugeben:

Feld	Erläuterung
Library ID	**Bibliothekskennung** Die Kennung (ID) der zu verwendenden Bibliothek. Um festzustellen, welche Bibliotheken verfügbar sind, kann der Benutzer seine Benutzerkennung in das Feld **User ID** und einen Stern (*) in das Feld **Library ID** (Bibliothekskennung) eingeben: Es wird eine Liste aller für den Benutzer verfügbaren Bibliotheken angezeigt. Die Liste enthält alle nicht geschützten Bibliotheken und alle geschützten Bibliotheken, mit denen der Benutzer verlinkt ist (entweder direkt oder über eine Gruppe, deren Sicherheitsprofil aktiviert ist). Die Liste enthält auch alle Bibliotheken, die für das Terminal des Benutzers verfügbar sind (wenn das Terminal in Natural Security definiert

	ist). Um eine Liste aller für das Terminal verfügbaren Bibliotheken anzuzeigen, kann der Benutzer einen Stern (*) in das Feld **Library ID** eingeben, ohne eine Benutzerkennung einzugeben). **Anmerkung:** Bei einer Anmeldung aus Natural Studio in einer Client-Umgebung über den Natural Development Server bei einer Map-Umgebung (Map Environment) auf einem Großrechner-Server ist die Angabe eines Sterns (*) als Bibliothekskennung nicht möglich.
User ID	**Benutzerkennung** Die Benutzerkennung, mit der der Benutzer in Natural Security definiert ist. Die Kennung einer Gruppe darf nicht eingegeben werden. Auch eine Terminalkennung darf nicht eingegeben werden. Wenn eine Benutzerkennung eingegeben wird, muss auch ein Passwort eingegeben werden. Wird keine Benutzerkennung eingegeben, ist kein Passwort erforderlich. Wenn keine Benutzerkennung eingegeben wird, verwendet Natural Security die Kennung des verwendeten Terminals. In diesem Fall muss das Terminal in Natural Security definiert sein, sonst wird die Anmeldung abgelehnt.
Password	**Password** Das im Sicherheitsprofil des Benutzers angegebene Passwort. Wenn im Sicherheitsprofil des Benutzers kein Passwort angegeben wurde, ist das Passwort identisch mit der Benutzerkennung (wenn sich ein neu definierter Benutzer zum ersten Mal anmeldet und das Passwort identisch mit der Benutzerkennung ist, muss der Benutzer sein Passwort ändern, indem er ein neues Passwort in das Feld **New Password** eingibt).
New Password	**Neues Password** In dieses Feld kann ein neues Passwort eingegeben werden, wenn im Feld **Password** ein gültiges Passwort eingegeben wurde. Wenn ein gültiges Passwort in das Feld **Password** eingegeben wurde und der Benutzer dieses Passwort ändern möchte oder muss, muss er ein neues Passwort in dieses Feld eingeben. Dieses neue Passwort ersetzt dann das alte und ist ab diesem Zeitpunkt das gültige Passwort für den Benutzer. **Anmerkung:** Wenn die Benutzerauthentifizierung über einen LDAP-Server erfolgt, ist dieses Feld nicht verfügbar.

Passwörter

In der Standardeinstellung verwendet Natural Security „reguläre“ Passwörter mit bis zu 8 Zeichen. Es unterstützt jedoch auch die Verwendung von Passphrasen, d.h. Passwörtern, die länger als 8 Zeichen sind. Die Verwendung von Passphrasen wird durch die Option **Password phrases active** im Abschnitt *Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values* der **Administrator Services** aktiviert.

Wenn nicht anders angegeben, bezieht sich der Begriff *Passwort* in der Natural Security-Dokumentation auf Passwörter jeder Länge.

Im Sicherheitsprofil eines Benutzers kann ein Natural Security-Administrator das Passwort des Benutzers festlegen oder ändern. Der Administrator kann auch ein Zeitintervall festlegen, nach dem der Benutzer gezwungen ist, sein Passwort zu ändern, wenn er sich anmeldet. Siehe **New Password** und **Change after** *nnn* **days** (Änderung nach *nnn* Tagen) in *Bestandteile eines Benutzersicherheitsprofils*.

Wenn ein Benutzer sein Passwort vergessen hat, muss er sich an den Natural Security-Administrator wenden, der dann ein neues Passwort im Sicherheitsprofil des Benutzers festlegt. Dieses ist dann das gültige Passwort für den Benutzer (das er in seinem Anmeldebildschirm wieder ändern kann).

Für die Verwendung von Passwörtern können verschiedene Regeln angewendet werden. Zu diesem Zweck stehen im Abschnitt **Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values** der **Administrator Services** verschiedene Optionen zur Verfügung.

Abgelehnte Anmeldung

Eine Anmeldung bei einer Bibliothek wird in folgenden Fällen abgelehnt:

- Der Benutzer ist nicht in Natural Security definiert.
- Das Sicherheitsprofil des Benutzers ist zurzeit inaktiv (aufgrund der **Activation Dates** - Einstellungen für die Aktivierungsdaten).
- Der Benutzer ist als Benutzer des Typs Mitglied definiert und wurde keiner Gruppe zugewiesen.
- Der Benutzer ist als Benutzer des Typs Mitglied definiert, und das Sicherheitsprofil der Gruppe, der er zugewiesen ist, ist derzeit inaktiv (aufgrund der **Activation Dates** - Einstellungen für die Aktivierungsdaten).
- Die Bibliothek ist nicht in Natural Security definiert.
- Die im Sicherheitsprofil der Bibliothek definierten Zeitfenstereinschränkungen erlauben die Nutzung der Bibliothek zum Zeitpunkt der Anmeldung nicht.
- Die Bibliothek ist geschützt und der Benutzer ist nicht mit der Bibliothek verlinkt.
- Die Bibliothek ist geschützt und der Benutzer ist mit ihr verlinkt, aber der Link wurde vorübergehend gesperrt.

- Die Bibliothek ist geschützt, und die Gruppe, über die der Benutzer mit der Bibliothek verlinkt ist, ist derzeit inaktiv (aufgrund der **Activation Dates** - Einstellungen für die Aktivierungsdaten).
- Im Sicherheitsprofil der Bibliothek ist eine nicht existierende Starttransaktion angegeben.
- Die Zeile `NEXT/MORE` ist nicht erlaubt und im Sicherheitsprofil der Library ist keine Starttransaktion angegeben.

Anmeldung ohne Bibliothekskennung

Wenn im Anmeldebildschirm keine Bibliothekskennung eingegeben wird, wird die im Sicherheitsprofil des Benutzers angegebene Standardbibliothek aufgerufen.

Wenn im Sicherheitsprofil des Benutzers keine Standardbibliothek angegeben ist, werden die im Sicherheitsprofil des Benutzers angegebenen **Privilegierten Gruppen** (in der Reihenfolge ihres Eintrags) nach einer Standardbibliothek durchsucht.

Wenn auch keine der **Privilegierten Gruppen** eine Standardbibliothek hat, wird die private Bibliothek des Benutzers aufgerufen.

Wenn weder Standardbibliotheken noch eine private Bibliothek vorhanden sind, muss der Benutzer bei der Anmeldung eine Bibliothekskennung eingeben.

RESTART und FIN als Bibliothekskennung

Wird `RESTART` als Bibliothekskennung eingegeben, wird die letzte restartfähige Bibliothek aufgerufen, bei der der Benutzer angemeldet war (Einzelheiten zur Option `RESTART` siehe ***Transaktionen*** im Kapitel *Bestandteile eines Bibliothekssicherheitsprofils*).

Anmerkung: Die Kennung der letzten restartfähigen Bibliothek, bei der ein Benutzer angemeldet war, wird im Feld **Last Library** im Sicherheitsprofil des Benutzers angezeigt.

Wird `FIN` als Bibliothekskennung eingegeben, wird die Natural-Sitzung beendet.

Erfolgreiche Anmeldung

Nach einer erfolgreichen Anmeldung bei einer Bibliothek wird die im Sicherheitsprofil der Bibliothek angegebene Starttransaktion aufgerufen. Wenn dort keine Starttransaktion angegeben ist, wird das Natural-Hauptmenü aufgerufen.

Anmerkung: Intern führt Natural Security nach einer erfolgreichen Anmeldung ein `END OF TRANSACTION`-Statement aus, wenn eine der folgenden Bedingungen zutrifft:

- Das Passwort des Benutzers wurde während des Anmeldevorgangs geändert.
- Während der Anmeldung ist ein Anmeldefehler aufgetreten.
- Die Option **Logon recorded** (Anmeldung aufgezeichnet) im Sicherheitsprofil des Benutzers oder der Bibliothek ist auf `Y` gesetzt.

- Die Option **Restart** (Neustart) im Bibliothekssicherheitsprofil ist auf `Y` gesetzt.
- Die allgemeine Option **Lock User Option** (Benutzeroption sperren) in den Administrator Services ist auf `0` gesetzt.

LOGON-Kommando

Wenn die erste Anmeldung bei einer Bibliothek zu Beginn einer Natural-Sitzung erfolgreich war, kann ein Benutzer mit dem Natural-Systemkommando `LOGON` von einer Bibliothek zu einer anderen wechseln.

Informationen zum Systemkommando `LOGON` finden Sie auch in der Natural-*Systemkommandos*-Dokumentation.

Beim LOGON-Kommando gibt es die folgenden Parameter:

- Wird kein Parameter angegeben, wird die Standardbibliothek aufgerufen (entweder die des Benutzers oder eine der privilegierten Gruppen). Wird keine Standardbibliothek angegeben, wird der Natural Security-Anmeldebildschirm aufgerufen. Beispiel:

```
LOGON
```

- Wird ein Parameter angegeben, so wird er als Bibliothekskennung interpretiert. Beispiel:

```
LOGON LIBX
```

```
LOGON *
```

- Werden zwei Parameter angegeben, wird der erste als Benutzerkennung, der zweite als Passwort interpretiert. Beispiel:

```
LOGON USERX PASSWX
```

- Wenn drei Parameter angegeben werden, wird der erste als Bibliothekskennung, der zweite als Benutzerkennung und der dritte als Passwort interpretiert. Beispiel:

```
LOGON LIBX USERX PASSWX
```

- Bei Angabe von vier Parametern wird der erste als Bibliothekskennung, der zweite als Benutzerkennung, der dritte als Passwort und der vierte als neues Passwort interpretiert. Beispiel:

```
LOGON LIBX USERX PASSWX NEWPASSX
```

Fehler beim LOGON-Kommando

Wenn während der Anmeldeverarbeitung ein Fehler auftritt, zeigt Natural Security eine Fehlermeldung an.

Wenn das `LOGON`-Kommando aus einer Bibliothek heraus abgesetzt wurde, ruft Natural Security die für diese Bibliothek definierte Fehlertransaktion auf. Wenn keine Fehlertransaktion definiert ist, wird der Anmeldebildschirm aufgerufen.

Automatische Anmeldung

Normalerweise müssen sich Benutzer zweimal anmelden, einmal beim Betriebssystem und einmal bei Natural. Um diese zweite Anmeldung zu vermeiden, können Sie den Natural-Profilparameter `AUTO` auf `AUTO=ON` setzen (siehe Natural-*Parameter-Referenz*-Dokumentation).

In diesem Fall wird ein internes Natural Security-Anmeldeverfahren aufgerufen, das den Anmeldenamen zur Betriebssystemanmeldung (wie er in der Natural-Systemvariablen `*INIT-USER` enthalten ist) als Benutzerkennung verwendet, aber kein Passwort (in der Annahme, dass dies durch das Betriebssystem-Anmeldeverfahren überprüft worden ist). Der Natural Security-Anmeldebildschirm wird unterdrückt. Eine Anmeldung mit einer anderen Benutzerkennung als dem Anmeldenamen beim Betriebssystem ist nicht möglich.

Wenn `AUTO=ON` verwendet wird, hat der Benutzer keine Möglichkeit, eine Bibliothekskennung anzugeben. Die Bibliothek, bei der der Benutzer angemeldet wird, wird nach den gleichen Regeln wie unter ***Anmeldung ohne Bibliothekskennung*** oben beschrieben bestimmt. Das bedeutet, dass eine automatische Anmeldung nur möglich ist, wenn eine Standardbibliothek (für den Benutzer oder eine seiner privilegierten Gruppen) angegeben ist oder der Benutzer eine private Bibliothek hat.

Wenn Sie `AUTO=ON` mit der Angabe einer Standardbibliothek im Sicherheitsprofil eines Benutzers und mit der Angabe einer Starttransaktion für diese Bibliothek kombinieren, erhält der Benutzer sofort nach dem Aufruf von Natural den ersten Bildschirm der Standardbibliothek, ohne irgendwelche Zwischenbildschirme durchlaufen zu müssen (Standardbibliotheken sind unter ***Bestandteile eines Benutzersicherheitsprofils*** im Kapitel *Benutzer verwalten*, Starttransaktionen unter ***Transaktionen*** im Kapitel *Bibliotheken verwalten* beschrieben).

Wenn `AUTO=ON` gesetzt ist, liefert das Systemkommando `LOGOFF` das gleiche Ergebnis wie das Systemkommando `FIN` (siehe ***Natural-Sitzung beenden***).

Wenn `AUTO=ON` gesetzt ist und der Benutzer nach der ersten automatischen Anmeldung versucht, sich bei einer anderen Bibliothek anzumelden und einen Anmeldefehler verursacht, wird die Fehlertransaktion für die aktuelle Bibliothek aufgerufen. Wenn keine Fehlertransaktion angegeben

ist, wird eine Fehlermeldung ausgegeben und dann die Starttransaktion (falls angegeben) für die aktuelle Bibliothek aufgerufen.

Anmerkung: Bei Natural Single Point of Development muss der Benutzer immer seine Benutzerkennung und sein Passwort im Dialog **Map Environment** angeben, auch wenn `AUTO=ON` gesetzt ist.

Logon-Anpassung

In diesem Abschnitt werden die Optionen beschrieben, die für die Anpassung der Anmeldung zur Verfügung stehen:

- Anpassung des Anmeldebildschirms / Anmeldedialogs
- Anmeldungsrelevante User Exits
- APIs für die Zugangsüberprüfung und Benutzerauthentifizierung

Anpassung des Anmeldebildschirms / Anmeldedialogs

Sie können das Layout des Anmeldebildschirms bzw. des Anmeldedialogs Ihren Anforderungen entsprechend ändern.

Standardmäßig wird der Anmeldebildschirm bzw. das Anmeldedialogfenster durch den User Exit `LOGONEX1` aufgerufen.

- Anmeldebildschirm auf Großrechnern und Linux
- Anmeldedialogfenster unter Windows
- Anmeldebildschirm / Dialogfenster für Passphrasen
- Anmeldebildschirm/Dialogfeld mit LDAP (nur unter Linux und Windows)
- Quellcode-/Objektnamen des Anmeldebildschirms bzw. Dialogfensters

Anmeldebildschirm auf Großrechnern und Linux

Der Quellcode des Anmeldebildschirms ist die Map (Maske) `NOGONM1`, die in der Bibliothek `SYSSEC` enthalten ist.

Um den Anmeldebildschirm anzupassen:

1 Erstellen Sie eine Kopie der Map `NOGONM1` und speichern Sie sie unter dem Namen `LOGONM1`.

2 Ändern Sie die Map `LOGONM1` nach Ihren Wünschen und katalogisieren Sie sie.

3 Kopieren Sie das katalogisierte Objekt `LOGONM1` in die Bibliothek `SYSLIB`.

Sollte `LOGONM1` in der `SYSLIB` fehlen, kopiert das Natural Security-Installationsverfahren automatisch das Objektmodul `NOGONM1` aus `SYSSEC` in die `SYSLIB` und legt es dort unter dem Namen `LOGONM1`

ab. Dadurch wird sichergestellt, dass immer ein Standard-Anmeldebildschirm vorhanden ist, wenn kein benutzerdefinierter Bildschirm verwendet wird.

Anmeldedialogfenster unter Windows

Für das Anmeldedialogfeld unter Windows ist das Anpassungsverfahren dasselbe wie oben beschrieben - mit der Ausnahme, dass die Quellcode-/Objektnamen unterschiedlich sind; siehe Tabelle unten.

Anmeldebildschirm / Dialogfenster für Passphrasen

Wenn die Option **Password Phrases active** im Abschnitt *Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values* auf `Y` oder `A` gesetzt ist, wird der Anmeldebildschirm bzw. das Dialogfenster durch den User Exit `LOGONEX0` anstelle von `LOGONEX1` aufgerufen. Die Vorgehensweise bei der Anpassung ist dieselbe wie oben beschrieben - mit dem Unterschied, dass die Quellcode-/Objektnamen unterschiedlich sind; siehe Tabelle unten.

Anmeldebildschirm/Dialogfeld mit LDAP (nur unter Linux und Windows)

Wenn der **Authentication Type** im **LDAP-Sicherheitsprofil** auf "LDAP" eingestellt ist, wird der Anmeldebildschirm bzw. das Dialogfeld durch den User Exit `LOGONSX1` anstelle von `LOGONEX1` aufgerufen. Der Anpassungsvorgang ist derselbe wie oben beschrieben - mit der Ausnahme, dass die Quellcode-/Objektnamen unterschiedlich sind; siehe Tabelle unten.

Quellcode-/Objektnamen des Anmeldebildschirms bzw. Dialogfensters

Anmeldebildschirm / Dialogfenster mit Aufruf durch User Exits	Quellcode in Bibliothek SYSSEC	Objekt in Bibliothek SYSLIB
`LOGONEX1`	`NOGONM1` (map)	`LOGONM1`
	`NOGONGM1` (dialog box)	`GLOGONM1`
`LOGONEX0` (wenn Authentifizierungsoption nicht aktiv ist)	`NOGONMX1` (map)	`LOGONMX1`
	`NOGONGO1` (dialog box)	`GLOGONO1`
`LOGONEX0` (wenn Authentifizierungsoption aktiv ist)	`NOGONMZ1` (map)	`LOGONMZ1`
	`NOGONGX1` (dialog box)	`GLOGONX1`
`LOGONSX1`	`NOGONSM1` (map)	`LOGONSM1`
	`NOGONGS1` (dialog box)	`GLOGONS1`

Anmeldungsrelevante User Exits

Zusätzlich zu den oben genannten bietet Natural Security weitere User Exits, mit denen Sie den Anmeldevorgang anpassen können. Siehe *Anmeldungsrelevante User Exits*.

APIs für die Zugangsüberprüfung und Benutzerauthentifizierung

Natural Security bietet mehrere Anwendungsprogrammierschnittstellen (APIs), die für die Zugangsüberprüfung und Benutzerauthentifizierung verwendet werden können. Siehe *Anwendungsprogrammierschnittstellen*

Natural-Sitzung beenden

Die folgenden Natural-Systemkommandos können verwendet werden, um eine Natural-Sitzung unter Natural Security zu beenden:

Kommando	Erläuterung
`LOGOFF`	Mit diesem Kommando beenden Sie eine Natural-Sitzung und rufen den Anmeldebildschirm auf. Um den Anmeldebildschirm zu verlassen, müssen Sie als Bibliothekskennung `FIN` eingeben. Wenn der Profilparameter `AUTO=ON` gesetzt ist (siehe *Automatische Anmeldung* oben), hat das Kommando `LOGOFF` die gleiche Wirkung wie das Kommando `FIN`.
`LOGON` (ohne Parameter)	Dieses Kommando beendet eine Natural-Sitzung und startet die Anmeldeprozedur, wobei entweder eine Standardbibliothek oder der Anmeldebildschirm aufgerufen wird (wenn keine Standardbibliothek definiert ist). Siehe auch *Automatische Anmeldung* oben.
`FIN`	Dieses Kommando beendet eine Natural-Sitzung und dient dazu, Natural ganz zu verlassen.

Vorsicht: Natural Security kann Ihre Natural-Umgebung nicht vor unbefugter Nutzung schützen, wenn Natural-Benutzer ihre Terminals unbeaufsichtigt lassen, während sie bei Natural angemeldet sind. Daher sollten die Benutzer daran erinnert werden, das Kommando `LOGOFF` zu benutzen, bevor sie ihr Terminal verlassen. Unbefugte Personen werden dann mit dem Anmeldebildschirm von Natural Security konfrontiert und können nur das verwenden, was für sie unter Natural Security definiert wurde.

In Bibliothekssicherheitsprofilen können Sie ein Zeitlimit für die Inaktivität festlegen, nach dem automatisch eine Abmeldung erfolgt.

6 Grundlagen der Benutzung

- Natural Security-Funktionen aufrufen 40
- Drücken der Eingabetaste (ENTER) 41
- Hilfe 41
- Falls unsicher, was Sie eingeben sollen 41
- Umgang mit einer Liste 42
- Direktkommandos 46

In diesem Kapitel finden Sie grundlegende Informationen zum Umgang mit Natural Security.

Folgende Themen werden behandelt:

Natural Security-Funktionen aufrufen

Sie können Natural Security-Funktionen aus der Natural Security-Bibliothek SYSSEC oder von außerhalb von SYSSEC aufrufen.

Innerhalb von SYSSEC:

- Sie können eine Funktion aufrufen, indem Sie sie in einem Natural Security-Menü oder einer **Auswahlliste** auswählen.
- Sie können eine Funktion durch ein **Direktkommando** aufrufen.

Außerhalb von SYSSEC:

- Sie können eine Funktion über eine der zur Verfügung gestellten **Anwendungsprogrammierschnittstellen** aufrufen.
- Sie können eine Funktion aufrufen, indem Sie ein **Direktkommando** absetzen.

Profilsicherheit

Unabhängig davon, wie Sie eine Funktion aufrufen, gelten immer die Administrator-/Eigentümereinstellungen von Natural Security, d.h. Sie können Funktionen nur auf die Sicherheitsprofile anwenden, die Sie auch verwalten dürfen.

Funktionssicherheit

Alle SYSSEC-spezifischen Kommandos sind im Kommandoprozessor NSCCMD01 definiert. Sie können Natural Security-Funktionen deaktivieren, indem Sie die entsprechenden Kommandos in NSCCMD01 deaktivieren. Einzelheiten zu NSCCMD01 finden Sie im Kapitel *Funktionssicherheit für Bibliothek SYSSEC*.

Wenn im Kommandoprozessor NSCCMD01 Funktionen als nicht erlaubt definiert sind, sind die entsprechenden Menüpunkte in den Natural Security-Menüs nicht sichtbar. Das bedeutet, dass Sie innerhalb von SYSSEC nur die Funktionen sehen, die Sie benutzen dürfen.

Abbrechen einer Funktion

Verwenden Sie *nicht* das Natural-Terminalkommando %%, um eine Natural Security-Funktion abzubrechen, da dies zu Inkonsistenzen in Ihren Natural Security-Daten führen kann.

Drücken der Eingabetaste (ENTER)

Um Natural Security anzuweisen, eine bestimmte Aktion durchzuführen, müssen Sie den entsprechenden Funktionscode, ein Kommando usw. eingeben und dann die Eingabetaste (in diesem Dokument als ENTER-Taste bezeichnet) drücken.

Wenn Sie für eine Funktion eine andere Taste drücken müssen, wird dies in der Natural Security-Dokumentation ausdrücklich erwähnt.

Hilfe

Um die Online-Hilfe für eine Natural Security-Funktion aufzurufen:

- Geben Sie auf Bildschirmen mit Funktionscode-Eingabefeld ein Fragezeichen (?) als Funktionscode ein.
- In einem beliebigen Bildschirm von Natural Security können Sie PF1 drücken.

Es wird eine Erläuterung des jeweiligen Bildschirms und die zum Fortfahren erforderlichen Informationen angezeigt.

Anmerkung: Wenn bestimmte Bestandteile, die auf einem Bildschirm von Natural Security angezeigt werden, nicht direkt für die Ausführung der aktuellen Funktion relevant sind, werden diese Bestandteile in dieser Dokumentation nicht immer erläutert. In diesen Fällen finden Sie die entsprechenden Erklärungen in der Online-Hilfe.

Falls unsicher, was Sie eingeben sollen

Wenn Sie nicht sicher sind, was in ein Eingabefeld eines Natural Security-Menüs oder -Auswahlbildschirms einzugeben ist, können Sie einen Stern (*) in das Feld eingeben: Es wird ein Fenster mit allen in dem Feld möglichen Werten angezeigt. In diesem Fenster können Sie dann den gewünschten Wert auswählen.

Umgang mit einer Liste

Folgende Themen werden behandelt:

- Bereich der aufzulistenden Objekte auswählen
- In einer Liste blättern
- Ein Objekt aus einer Liste auswählen

Bereich der aufzulistenden Objekte auswählen

Wenn Sie das Subsystem zum Verwalten (Maintenance) oder Abfragen (Retrieval) für einen bestimmten Objekttyp (Benutzer, Bibliothek usw.) aufrufen, wird eine Liste dieser Objekte angezeigt. Normalerweise enthält eine solche Liste alle Objekte.

Um zum Beispiel alle Benutzer aufzulisten, die in Natural Security definiert sind, müssen Sie den Objekttyp **User** markieren.

```
+-------------MAINTENANCE-------------+
!  Please select one type of object:  !
!                                     !
!  X User                             !
!  _ Application                      !
!  _ Library                          !
!  _ File                             !
!  _ Mailbox                          !
!  _ Utility                          !
!                                     !
!                                     !
!                                     !
! Start Value .. _________________    !
! Type/Status .. ____                 !
+-------------------------------------+
```

Der Inhalt des obigen Auswahlfensters kann je nach Plattform und den verfügbaren externen Objekttypen verschieden sein. Wenn die Liste der Objekttypen die Größe des Fensters überschreitet, können Sie mit PF7 und PF8 innerhalb des Fensters blättern.

Wenn Sie nicht alle Objekte, sondern nur bestimmte Objekte aufgelistet haben möchten, können Sie die Option **Start Value** (Startwert) verwenden.

Für Benutzer, Anwendungen, Bibliotheken und Dateien können Sie auch die Option **Type/Status** verwenden - entweder allein oder in Kombination mit der Option **Start Value**. Für andere Objekte ist nur die **Option Start Value** verfügbar.

Start Value (Startwert)

In das Feld **Start Value** können Sie einen Startwert eingeben, der aus einem oder mehreren Zeichen oder aus einem oder mehreren Zeichen gefolgt von einem Stern (*) bestehen kann. Die Möglichkeit, einen Wert gefolgt von einem Stern einzugeben, wird in der Natural-Dokumentation als Stern-Notation bezeichnet.

Um zum Beispiel die Benutzer ab dem ersten Benutzer, dessen Kennung mit TOM beginnt, aufzulisten, können Sie den Objekttyp **User** markieren und Folgendes eingeben:

```
Start Value .. TOM
```

Wenn Sie beispielsweise nur die Benutzer auflisten möchten, deren Kennung mit TOM beginnt, können Sie den Objekttyp **User** markieren und Folgendes eingeben:

```
Start Value .. TOM*
```

Type/Status

In dieses Feld können Sie einen Benutzertyp, einen Anwendungstyp, einen Bibliotheksschutzstatus oder (auf Großrechnern) einen Dateistatus eingeben.

Benutzertyp (User Type)

Sie können einen der folgenden Benutzertypen eingeben:

G	Group (Gruppe)
M	Member (Mitglied)
P	Person
A	Administrator
T	Terminal
B	Batch User (Batch-Benutzer)

Bibliotheksschutzstatus (Library Status)

Sie können einen der folgenden Werte für den Schutzstatus der Bibliothek eingeben:

NN	Nicht geschützt.
LN	Nicht geschützt, aber verlinkbar für eine Gruppe.
YN	Nur personengeschützt.
NY	Nur terminalgeschützt.
YY	Personen- oder terminalgeschützt.
YA	Personen- und terminalgeschützt.
PN	Für private Bibliotheken: wie YN.
PY	Für private Bibliotheken: wie YY.
PA	Für private Bibliotheken: wie YA.

(Die oben genannten **Schutzkombinationen** werden im Kapitel *Bibliotheken schützen* erläutert).

Dateistatus (File Status)

Sie können einen der folgenden Dateistatuswerte eingeben:

PRIV	Privat.
ACCE	Zugriff (Access).
PUBL	Öffentlich.(Public).
UNDF	Nicht definiert, d.h. DDMs, für die keine Dateisicherheitsprofile erstellt wurden (*).
DEFI	Definiert, d. h. alle PRIV-, ACCE-, und PUBL-Dateien (*).
NDDM	Dateisicherheitsprofile, für die keine DDMs existieren (*). DDM
DDM	Alle PRIV-, ACCE-, PUBL- und UNDF-Dateien (*).

* Dies ist kein tatsächlicher Dateistatus, sondern dient nur der Auswahl.

Wenn Sie keinen Dateistatus auswählen, werden alle PRIV-, ACCE-, und PUBL-Dateien aufgelistet.

Anwendungstyp (Application Type)

Sie können einen der folgenden Werte für den Anwendungstyp eingeben:

B oder BASE	Base applications (Basisanwendungen)
C oder COMP	Compound applications (Verbundanwendungen)

Wenn Sie keinen Anwendungstyp auswählen, werden sowohl Basis- als auch Verbundanwendungen aufgelistet.

Beispiel 1 - Option Typ/Status:

Um alle Benutzer des Benutzertyps Mitglied (Member) aufzulisten, müssen Sie den Objekttyp **User** markieren und Folgendes eingeben:

```
Type/Status .. M
```

Beispiel 2 - Kombination von Startwert und Typ/Status:

Um nur Benutzer des Benutzertyps Mitglied (Member) aufzulisten, deren Kennungen mit `T` beginnen, müssen Sie den Objekttyp **User** markieren und Folgendes eingeben:

```
Start Value .. T*
Type/Status .. M
```

In einer Liste blättern

Sobald eine Liste von Objekten angezeigt wird, können Sie darin wie folgt rückwärts und vorwärts blättern:

- Um in einer Liste eine Seite vorwärtszublättern, drücken Sie PF8 (+).
- Um eine Liste um eine Seite zurückzublättern, drücken Sie PF7 (-).
- Um an den Anfang einer Liste zu blättern, drücken Sie PF19 (- -).
- Um in einer Liste bis zu einem bestimmten Startwert zu blättern, können Sie das *hervorgehobene* Feld oberhalb der Kennungen verwenden, und zwar auf dieselbe Weise wie oben für das Feld **Start Value** beschrieben.
- Für eine Liste von Benutzern oder Anwendungen können Sie auch das *hervorgehobene* Feld oberhalb der Spalte **Type** verwenden, wie oben für das Feld **Type/Status** beschrieben. Für eine Liste von Bibliotheken gilt das Gleiche für das Feld über der Spalte **Protection Status**. Diese Felder zeigen das aktuell gültige Typ/Status-Auswahlkriterium an.

```
11:38:39                    *** NATURAL SECURITY ***                2022-08-31
                              - User Maintenance -

Co User ID  User Name                          Type Message
__ ________ _____________________________ ____ ________________________
__ AAZ      ABDUL ALHAZRED                 A
__ AD       ARTHUR DENT                    A
__ AH       ALICE HARGREAVES               M
__ ER       ELLEN RIPLEY                   M
__ LL       LOCKE LAMORA                   M
__ TN       THURSDAY NEXT                  A
__ VV       VINCENT VEGA                   P
```

Ein Objekt aus einer Liste auswählen

Um ein Objekt aus einer Liste für eine Funktion auszuwählen, geben Sie einfach den entsprechenden Funktionscode für die Funktion neben dem Objekt in der linken Spalte (mit der Überschrift **Co**) eines Auswahlbildschirms ein.

Wenn Sie den Funktionscode für die gewünschte Funktion nicht mehr wissen, geben Sie einen Stern (*) in die Spalte **Co** ein. Es erscheint ein Fenster, in dem alle verfügbaren Funktionscodes angezeigt werden. In diesem Fenster können Sie dann den gewünschten Funktionscode auswählen.

Direktkommandos

Folgende Themen werden behandelt:

- Allgemeine Informationen zu Kommandos
- Kommandos zum Aufrufen einer Funktion
- Kommandos zum Aufrufen einer Auswahlliste
- Spezielle Kommandos
- Ein Kommando außerhalb von SYSSEC absetzen

Allgemeine Informationen zu Kommandos

Nachdem Sie sich mit Natural Security vertraut gemacht haben und wissen, wie Sie von Menü zu Menü navigieren können, können Sie die gewünschte Funktion alternativ auch direkt aufrufen. Dies geschieht mit Hilfe von *Direktkommandos*.

Sie können ein Direktkommando in jedem Natural Security-Bildschirm eingeben, der eine *Kommandozeile* aufweist:

```
Command ===>
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help        Exit                                                 Canc   ↩
```

Wenn Sie ein Direktkommando eingeben, das ungültig ist, erhalten Sie eine entsprechende Fehlermeldung. Wenn Sie ein unvollständiges Kommando eingeben, werden Sie aufgefordert, das oder die fehlenden Bestandteile anzugeben.

Nachdem eine Funktion, die durch ein Direktkommando aufgerufen wurde, ausgeführt wurde, wird der Bildschirm angezeigt, von dem aus diese Funktion normalerweise aufgerufen werden würde - *nicht* der Bildschirm, auf dem das Kommando eingegeben wurde.

Es gibt drei Arten von Direktkommandos:

- **Kommandos zum Aufrufen einer Funktion**

- **Kommandos zum Aufrufen einer Auswahlliste**
- **Spezielle Kommandos**.

Kommandos zum Aufrufen einer Funktion

Allgemeine Kommandosyntax

Ein Direktkommando, mit dem eine Funktion aufgerufen wird, besteht allgemein aus den folgenden Elementen, die Sie in der folgenden Reihenfolge angeben müssen:

```
function  object-type  object-ID  parameters
```

An erster Stelle geben Sie eine Funktion (*function*) an. Mögliche Funktionen sind:

ADD	Add security profile.	Sicherheitsprofil anlegen.
COPY	Copy security profile.	Sicherheitsprofil kopieren.
MODIFY	Modify security profile.	Sicherheitsprofil ändern.
RENAME	Rename security profile.	Sicherheitsprofil umbenennen.
DELETE	Delete security profile.	Sicherheitsprofil löschen.
DISPLAY	Display security profile.	Sicherheitsprofil anzeigen.
EDIT	Edit group members.	Gruppenmitglieder editieren.
LINK	Link object to another object.	Objekt mit einem anderen Objekt verlinken.
XREF	Cross-reference object.	Cross-Referenz-Objekt.

Nach der Funktion können Sie einen Objekttyp *object-type* angeben, (zum Beispiel: USER, LIBRARY).

Nach dem Objekttyp (*object-type*) können Sie eine Objektkennung (*object-ID*) angeben (z. B. eine Benutzer- oder Bibliothekskennung).

Nach der Kennung können Sie einen oder mehrere Parameter (*parameters*) angeben (z. B. einen Benutzertyp).

Parameter für Sicherheitsprofilbestandteile

Für die Funktionen DISPLAY und MODIFY stehen mehrere Parameter (*parameters*) zur Verfügung, mit denen Sie direkt auf die Bestandteile eines Sicherheitsprofils zugreifen können, die sich nicht auf dem Hauptbildschirm des Sicherheitsprofils befinden, sondern auf einem der **Additional Options**-Bildschirme mit zusätzlichen Optionen des Profils. Diese sind:

Für alle Objekttypen (*object-types*):

Parameter	Sicherheitsprofilbestandteil
DIR	Verwaltungsinformationen.
NOTES	Sicherheitsvermerke.
OWNERS	Eigentümer.

Für den Objekttyp (*object-type*) USER:

Parameter	Sicherheitsprofilbestandteil
MAILBOXES	Mailboxen.
ACTIVATION	Aktivierungsdaten.
FUNCSEC	Funktionssicherheit.
PRIVLIB	Private Bibliothek (nur für die Benutzertypen A und P).
SESSION	Sitzungsoptionen (nur für die Benutzertypen A und P).

Für den Objekttyp (*object-type*) LIBRARY:

Parameter	Sicherheitsprofilbestandteil
MAILBOXES	Mailboxen.
TIMEW	Time Windows (Zeitfenster).
STEPLIBS	Steplibs.
FUNCSEC	Functional Security (Funktionssicherheit).
USEREXIT	User Exit.
OPTIONS	Security Options (Sicherheitsoptionen).
LIMITS	Security Limits (Sicherheitslimits).
PARAMETERS	Session Parameters (Session-Parameter).
RPC	Natural RPC Restrictions (Natural RPC-Einschränkungen).
COMMANDS	Command Restrictions (Kommandoeinschränkungen)
EDITORS	Editing Restrictions (Bearbeitungseinschränkungen)
STATEMENTS	Statement Restrictions (Statement-Einschränkungen)
MODULES	Disallow/Allow Modules (Module nicht erlauben/erlauben).
DDMSTATUS	Set Status of DDMs (Status von DDMs setzen.)

Kommando abkürzen

Sie können den Bestandteil *function* eines Direktkommandos beliebig abkürzen, solange die Abkürzung die Funktion eindeutig identifiziert.

Den Bestandteil *object-type* eines Direktkommandos können Sie auf 2 Zeichen abkürzen.

Beispiele:

`DISPLAY USER ADE`	Dieses Kommando bewirkt, dass das Sicherheitsprofil des Benutzers ADE angezeigt wird.
`DISPLAY US ADE`, `DIS USER ADE` , `DI US ADE`	Jedes dieser drei Kommandos bewirkt ebenfalls die Anzeige des Sicherheitsprofils des Benutzers ADE.
`DE US ADE`	Jedes dieser drei Kommandos bewirkt ebenfalls die Anzeige des Sicherheitsprofils des Benutzers ADE.
`D US AE`	Dieses Kommando ist *ungültig*, da `D` keine eindeutige Identifizierung einer Funktion ist; es könnte für `DISPLAY` oder `DELETE` stehen.

Im Rahmen von Natural Security stehen mehrere Natural-Systemkommandos zur Verfügung, die bei der eindeutigen Identifizierung einer Funktion ebenfalls zu berücksichtigen sind.

Beispiele für Kommandos

`ADD`	Wenn Sie dieses Kommando in einem Verwaltungsbildschirm in der **Maintenance**-Auswahlliste eingeben, wird die Funktion **Add** (Anlegen) für diesen Objekttyp aufgerufen. Wenn Sie es an einer anderen Stelle eingeben, ist das Kommando unvollständig, da kein Objekttyp angegeben wurde.
`ADD US`	Das Fenster **Add User** (Benutzer anlegen) wird aufgerufen, in dem Sie eine Benutzerkennung und einen Benutzertyp eingeben können.
`ADD US CMOT`	Das Fenster **Add User** (Benutzer anlegen) wird aufgerufen, in dem Sie einen Benutzertyp eingeben können.
`ADD US CMOT M ANKH`	Das Fenster **Add User** (Benutzer anlegen) für den Benutzer CMOT des Benutzertyps Member (Mitglied), der das Standardprofil ANKH als Grundlage für das anzulegende Benutzersicherheitsprofil verwendet, wird aufgerufen, in dem Sie den Benutzer definieren können.
`MODIFY`	Dieses Kommando ist unvollständig, da nach der Funktion kein Objekttyp angegeben wurde.
`MODIFY LIB`	Dieses Kommando zeigt die **Library Maintenance**-Auswahlliste (Bibliotheksverwaltung) an, da keine Bibliothekskennung angegeben wurde.
`MOD LIB BOOKS`	Das Sicherheitsprofil der Bibliothek BOOKS wird zur Änderung angezeigt.
`CO US ESME`	Das Fenster **Copy User** (Benutzer kopieren) wird angezeigt, in dem Sie die Benutzerkennung des neuen Benutzers eingeben können.

`CO US ESME OGG`	Das Fenster **Copy User** (Benutzer kopieren) für den Benutzer OGG wird aufgerufen, wobei das Sicherheitsprofil des Benutzers ESME in das Sicherheitsprofil des Benutzers OGG kopiert wird. Das Kopieren erfolgt ohne Verlinkungen.
`CO US ESME OGG Y`	Der Bildschirm **Copy User** (Benutzer kopieren) für den Benutzer OGG wird aufgerufen, wobei das Sicherheitsprofil des Benutzers ESME in das Sicherheitsprofil des Benutzers OGG kopiert wird. Das Kopieren erfolgt mit Links.
`EDIT US DOC`	Ruft die Funktion **Edit Group Members** (Gruppenmitglieder editieren) für die Gruppe DOC auf.
`XREF MAIL MAIL1`	Ruft die Cross-Referenz-Funktion für die Mailbox MAIL1 auf.
`LK LI ODDS US`	Der Bildschirm **Link Users to Library** (Benutzer mit Bibliothek verlinken) wird für Benutzer aufgerufen, die mit der Bibliothek ODDS verlinkt werden sollen. Die Liste enthält alle Benutzer.
`LINK US IW LI`	Der Bildschirm **Link User To Libraries** (Benutzer mit Bibliotheken verknüpfen) wird für den Benutzer IW aufgerufen, der mit Bibliotheken verlinkt werden soll. Die Liste enthält alle Bibliotheken.

Kommandos zum Aufrufen einer Auswahlliste

Die folgenden Kommandos können verwendet werden, um eine Auswahlliste aufzurufen:

Kommando	Funktion
`MAINTENANCE` *`object-type object-ID parameters`*	Wenn Sie nur das Kommando selbst angeben, wird das Objektauswahlfenster für Verwaltungsfunktionen angezeigt. Wenn Sie nach dem Kommando einen Objekttyp (*`object-type`*) angeben, wird die Verwaltungsauswahlliste für diesen Objekttyp angezeigt. Wenn Sie nach dem Kommando einen Objekttyp (*`object-type`*) und eine Objektkennung (*`object-ID`*) angeben, wird die Verwaltungsauswahlliste für diesen Objekttyp angezeigt, wobei die Objektkennung als Startwert für die Liste verwendet wird. Nach der Objektkennung (*`object-ID`*) können Sie einen oder mehrere Parameter (*`parameters`*), z.B. Benutzertyp, als weitere Auswahlkriterien für die anzuzeigende Verwaltungsauswahlliste angeben.
`RETRIEVAL` *`object-type object-ID parameters`*	Wenn Sie nur das Kommando selbst angeben, wird das Objektauswahlfenster für Retrieval-Funktionen angezeigt. Wie beim `MAINTENANCE`-Kommando (siehe oben) können Sie auch bei diesem Kommando einen Objekttyp, eine Objektkennung und Parameter angeben.

Spezielle Kommandos

Neben den Kommandos, die eine bestimmte Funktion oder Auswahlliste aufrufen (wie oben beschrieben), und einigen Natural-Systemkommandos (die in der Natural-*Systemkommandos*-Dokumentation beschrieben sind), gibt es die folgenden speziellen Kommandos (die Unterstreichung zeigt die kürzest mögliche Abkürzung an):

Kommando	Funktion
ADMIN	Ruft das Menü **Administrator Services** auf.
ADMIN_A	Ruft die Administrator Services-Funktion **General NSF Options** auf (nur mit Natural SAF Security verfügbar).
ADMIN_B	Ruft die Administrator Services-Funktion **Authentication Options** auf.
ADMIN_D	Ruft die Administrator Services-Funktion **Library Preset Values** auf.
ADMIN_E	Entspricht dem Kommando ERROR.
ADMIN_G	Ruft die Administrator Services-Funktion **Set General Options** auf.
ADMIN_I	Ruft die Administrator Services-Funktion **Application Programming Interfaces** auf.
ADMIN_L	Entspricht dem Kommando LOGREC.
ADMIN_N	Ruft die Administrator Services-Funktion **Maintenance Log Records** auf.
ADMIN_P	Ruft die Administrator Services-Funktion **Set PF-Keys** auf.
ADMIN_S	Ruft die Administrator Services-Funktion **Definition of System Libraries** auf.
ADMIN_U	Ruft die Administrator Services-Funktion **User Default Profiles** auf.
ADMIN_V	Ruft die Administrator Services-Funktion **User Preset Values** auf.
ADMIN_X	Ruft die Administrator Services-Funktion **Utility Defaults/Templates** auf.
ADMIN_Y	Ruft die Administrator Services-Funktion **Library Default Profiles** auf.
ADMIN_1	Ruft die Administrator Services-Funktion **Environment Profiles** auf.
ADMIN_2	Ruft die Administrator Services-Funktion **SAF Online Services** auf.
ADMIN_3	Ruft die Administrator Services-Funktion **Definition of Undefined Libraries** auf.
CUSTOM1 CUSTOM2 CUSTOM3 CUSTOM4 CUSTOM5	Diese Kommandos rufen Natural-Programme mit den gleichen Namen auf. Sie können eigene Programme mit diesen Namen schreiben, um die von Ihnen benötigten Funktionen auszuführen. So können Sie solche Funktionen aus Natural Security heraus aufrufen.
ERRDEL	Löscht alle Fehlerdatensätze bei der Anmeldung/Gegenzeichnung (siehe auch *Direktkommando ERRDEL* im Kapitel *Administrator Services*).
ERROR	Ruft das **Logon/Countersign Errors Menu** auf.
LOGDEL	Löscht alle Anmeldesätze (siehe auch *Alle Anmeldesätze löschen - Direktkommando LOGDEL* im Kapitel *Administrator Services*).
LOGFILE	Ruft die Administrator Services-Funktion **Log File Maintenance** auf.

Kommando	Funktion
LOGREC	Ruft das **Logon Records Menu** auf.
MENU	Ruft das Natural Security **Main Menu** auf.
. (Punkt)	Beendet die jeweilige Verarbeitungsebene und zeigt den Bildschirm der nächsthöheren Verarbeitungsebene an (entspricht PF3).

Ein Kommando außerhalb von SYSSEC absetzen

Sie können ein Natural Security-Kommando auch direkt von außerhalb der Natural Security-Bibliothek SYSSEC ausführen. Auf diese Weise können Sie eine Natural Security-Funktion von jeder Stelle Ihrer Natural-Sitzung aus ausführen, ohne sich bei der Bibliothek SYSSEC anmelden zu müssen.

Dazu müssen Sie das Direktkommando mit dem Präfix SYSSEC in die Natural-Kommandozeile eingeben.

Zum Beispiel:

```
SYSSEC MOD LIB XYZ
```

Wenn Sie den Bildschirm, der durch das Direktkommando aufgerufen wird, verlassen, kehren Sie zu dem Natural-Bildschirm zurück, von dem aus Sie das Kommando abgesetzt haben.

Anmerkung: Wenn Sie ein Direktkommando absetzen, das eine Funktion aufruft, müssen Sie das vollständige Kommando angeben, d.h. Sie dürfen keine Kommandobestandteile auslassen, die für den Aufruf der eigentlichen Funktion (und nicht nur einen Auswahlbildschirm oder ein Startwertfenster) notwendig sind. So wäre z.B. das Kommando COPY USER ABC unvollständig, weil die neue Benutzerkennung fehlt.

7 Administrator Services

- Zugriff auf das Subsystem Administrator Services 54
- Administrator Services aufrufen 54
- Allgemeine Optionen (Administrator Services) 55
- Authentifizierungsoptionen - Authentication Options (LDAP) 74
- PF-Tasten 82
- Anmelde-/Gegenzeichnungsfehler - Logon/Countersign Errors 85
- Anmeldesätze - Logon Records 91
- Verwaltungsprotokollsätze verwalten - Maintenance Log Records 95
- SAF Online Services 103
- Benutzer-Standardprofile - User Default Profiles 107
- Standardprofile für Bibliotheken - Library Default Profiles 109
- Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values 110
- Voreingestellte Werte für Bibliothekssicherheitsprofile - Library Preset Values 119
- Systembibliotheken definieren - Definition of System Libraries 125
- Nicht definierte Bibliotheken definieren - Definition of Undefined Libraries 126

Das Subsystem **Administrator Services** bietet Funktionen, die sich auf Natural Security als Ganzes und auf alle Sicherheitsprofile beziehen.

In diesem Kapitel werden die folgenden Themen behandelt:

Zugriff auf das Subsystem Administrator Services

Der Zugriff auf das Subsystem **Administrator Services** wird a) durch die Eigentümerangaben im Sicherheitsprofil der Natural Security-Bibliothek `SYSSEC` und b) durch den Kommandoprozessor `NSCCMD01` gesteuert:

- Wenn im Sicherheitsprofil von `SYSSEC` keine Eigentümer angegeben sind, darf jeder Benutzer vom Typ Administrator auf das Subsystem **Administrator Services** zugreifen.
- Wenn im Sicherheitsprofil von `SYSSEC` Eigentümer angegeben sind, bestimmt das Feld **Functional Security Defined** für den Kommandoprozessor `NSCCMD01` in `SYSSEC`, wer auf das Subsystem **Administrator Services** zugreifen darf:
  - Wenn dieses Feld auf `Yes` gesetzt ist (dies ist die Standardeinstellung), dürfen nur die Eigentümer von `SYSSEC` auf die **Administrator Services** zugreifen.
  - Wenn dieses Feld auf `All` gesetzt ist, kann jeder Benutzer vom Typ Administrator auf die Administrator Services zugreifen.

  In beiden Fällen bestimmen die Funktionssicherheitsvorgaben im Bibliothekssicherheitsprofil von `SYSSEC` und in den Benutzersicherheitsprofilen der Administratoren, welche Funktionen der **Administrator Services** genutzt werden dürfen.

Informationen zu Eigentümern in Bibliothekssicherheitsprofilen finden Sie in den Kapiteln *Bibliotheken verwalten* und *Gegenzeichnungen*.

Informationen über den Kommandoprozessor `NSCCMD01` finden Sie im Kapitel *Funktionssicherheit für Bibliothek SYSSEC*.

Administrator Services aufrufen

Um die Administrator Services aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) den Menüpunkt **Administrator Services**.

  Wenn Sie berechtigt sind, auf die Administrator Services zuzugreifen, wird das Menü **Administrator Services** angezeigt.

2 Das Menü **Administrator Services** umfasst zwei Bildschirme. Mit PF7 und PF8 können Sie zwischen den beiden Bildschirmen umschalten.

Folgende Funktionen stehen zur Verfügung:

Administrator Services Menu 1	Beschreibung siehe:
General Options	**Allgemeine Optionen (Administrator Services)** (*)
Authentication Options	**Authentifizierungsoptionen - Authentication Options (LDAP)**
PF-Keys	**PF-Tasten**
Logon/Countersigns Errors	**Anmelde-/Gegenzeichnungsfehler - Logon/Countersign Errors**
Logon Records	**Anmeldesätze - Logon Records**
Maintenance Log Records	**Verwaltungsprotokollsätze verwalten - Maintenance Log Records**
SAF Online Services	**SAF Online Services**
Administrator Services Menu 2	Beschreibung siehe:
Environment Profiles	**Umgebungen schützen**
User Default Profiles	**Benutzer-Standardprofile - User Default Profiles** (*)
Library Default Profiles	**Standardprofile für Bibliotheken - Library Default Profiles** (*)
User Preset Values	**Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values**
Library Preset Values	**Voreingestellte Werte für Bibliothekssicherheitsprofile - Library Preset Values**
Utility Defaults/Templates	**Dienstprogramm-Standardeinstellungen/Vorlagen - Utility Defaults/Templates** (*)
Definition of System Libraries	**Systembibliotheken definieren - Definition of System Libraries**
Definition of Undefined Libraries	**Nicht definierte Bibliotheken definieren - Definition of Undefined Libraries**
Application Programming Interfaces	**Anwendungsprogrammierschnittstellen**

Sie sollten die oben mit (*) gekennzeichneten Funktionsbeschreibungen genau lesen, bevor Sie mit der Definition von Objekten in Natural Security beginnen. Die anderen Funktionen der Administrator Services stehen nicht in direktem Zusammenhang mit der Definition von Objekten in Natural Security.

Allgemeine Optionen (Administrator Services)

Bevor Sie mit der Definition von Objekten in Natural Security beginnen, sollten Sie bestimmte Optionen festlegen, die für das gesamte Natural Security-System gelten.

Um die General Options der Administrator Services aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) den Menüeintrag **Administrator Services**.

Wenn Sie **berechtigt** sind, auf die Administrator Services zuzugreifen, wird das Menü **Administrator Services Menu 1** angezeigt.

2 Wählen Sie den Menüeintrag **General Options**.

Der Bildschirm **Set General Options** (Allgemeine Optionen einstellen) wird angezeigt.

3 Die Einstellungsmöglichkeiten der **Set General Options** sind auf zwei Bildschirme verteilt. Mit PF7 und PF8 können Sie zwischen den beiden Bildschirmen umschalten. Sie bieten die folgenden Optionen:

General Options - Bildschirm 1:	Beschreibung siehe:
Transition Period Logon	**Übergangszeitraum für Anmeldung**
Activate Security for Development Server File	**Security für Development Server-Datei aktivieren**
Maximum Number of Logon Attempts	**Maximale Anzahl von Anmeldeversuchen**
Suppress Display of Logon Messages	**Anzeige von Logon-Meldungen unterdrücken**
Lock User Option	**Benutzer sperren**
User Password / Passphrase History	**Benutzerpasswort-/Benutzerpassphrasen-Historie**
Free Access to Functions via APIs	**Freier Zugriff auf Funktionen über APIs**
Minimum Number of Co-Owners	**Mindestanzahl an Miteigentümern**
Deletion of Non-Empty Libraries Allowed	**Löschung von nicht leeren Bibliotheken erlaubt**
Overwriting of Defaults Possible	**Überschreiben von Standardwerten möglich**
Display DBID/FNR of FSEC	**DBID/FNR von FSEC anzeigen**
Exit Functions with Confirmation	**Beenden von Funktionen mit Bestätigung**
Logging of Maintenance Functions	**Protokollieren von Verwaltungsfunktionen**

General Options - Bildschirm 2:	Beschreibung siehe:
Store Logon and Error Data on Separate System Files	**Anmelde- und Fehlerdaten in separaten Systemdateien speichern**
Concurrent Modifications Without Notification	**Konkurrierende Änderungen ohne Benachrichtigung**
Private Libraries in Public Mode	**Private Bibliotheken im öffentlichen Modus**
Suppress Mailboxes in Batch Mode	**Mailboxen im Batch-Modus unterdrücken**
Environment Protection	**Umgebungsschutz**
Access To Current FSEC	**Zugriff auf aktuelle FSEC**
Force Impersonation for Natural Development Server	**Impersonation für Natural Development Server erzwingen**
Record Each User's Initial Logon Daily	**Erstanmeldung jedes Benutzers täglich aufzeichnen**
Enable Error Transaction Before NAT1700/1701 Logoff	**Fehlertransaktion vor NAT1700/1701-Abmeldung aktivieren**
Logoff in Error Case if *STARTUP is Active	**Abmelden im Fehlerfall, wenn `*STARTUP` aktiv**
Set *APPLIC-NAME Always to Library Name	**`*APPLIC-NAME` immer auf Bibliotheksname setzen**

Allow Deletion of Users Who Are Owners/DDM Modifiers	**Löschen von Benutzern, die Eigentümer/DDM-Änderer sind, zulassen**

Die oben aufgelisteten Optionen werden im Folgenden beschrieben.

Übergangszeitraum für Anmeldung - Transition Period Logon

Die Option **Transition Period Logon** ermöglicht einen reibungslosen Übergang von einer ungeschützten Natural-Umgebung zu einer durch Natural Security geschützten Umgebung.

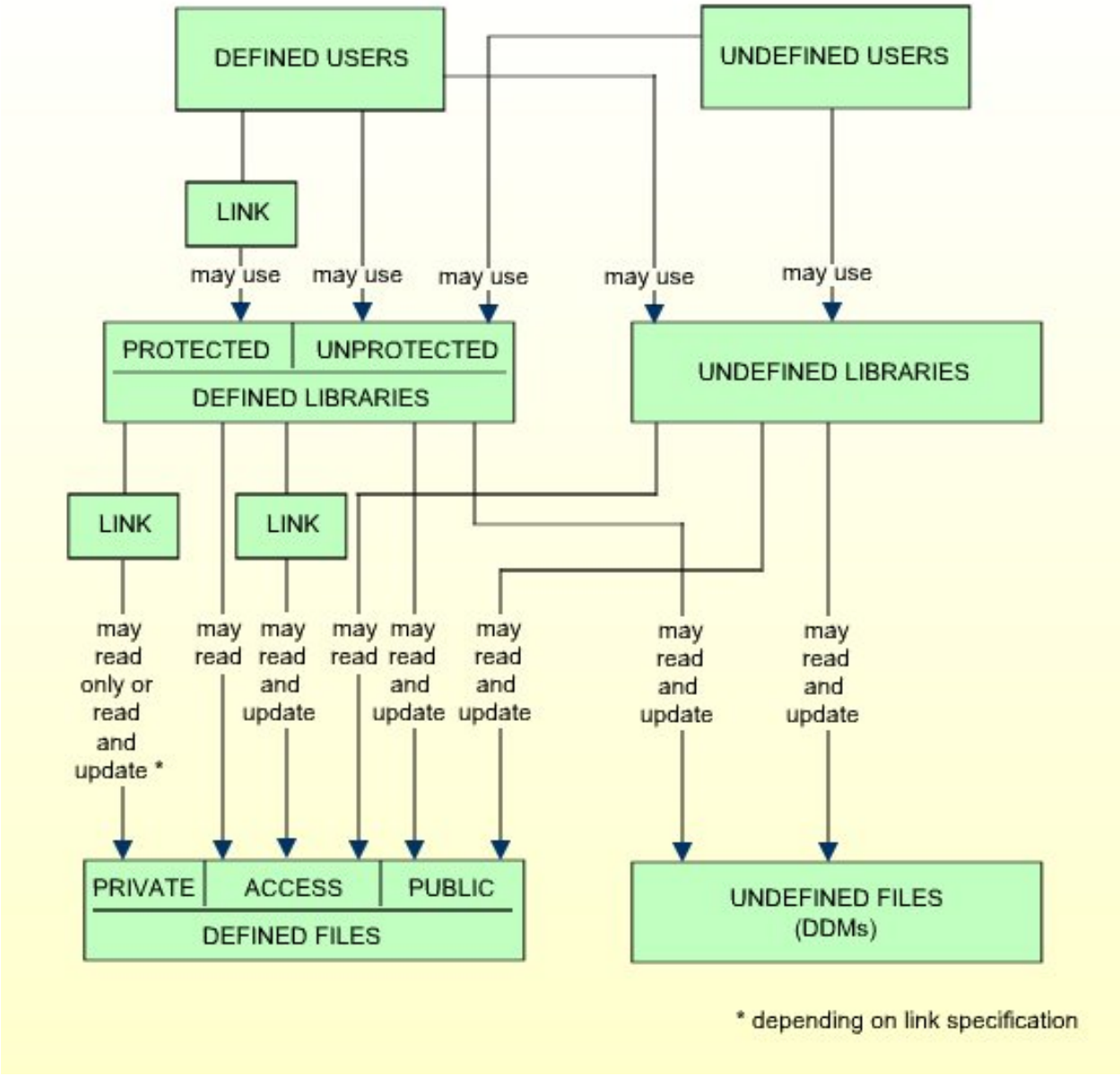
Mögliche Angaben:

Eingabe:	Erläuterung:
`Y`	■ Benutzer, die noch nicht in Natural Security definiert sind, können sich bei Bibliotheken anmelden, die noch nicht in Natural Security definiert sind oder die als nicht geschützt definiert sind. ■ Auf Bibliotheken, die noch nicht in Natural Security definiert sind, kann jeder (definierte oder nicht-definierte) Benutzer zugreifen. ■ Nicht definierte Bibliotheken können auf DDMs zugreifen, die noch nicht in Natural Security definiert sind, sowie auf Dateien mit dem Status PUBLIC und ACCESS. ■ Nicht definierte DDMs können von jeder (definierten oder nicht definierten) Bibliothek aufgerufen werden.
`N`	Nur in Natural Security definierte Benutzer dürfen Natural verwenden. Bibliotheken, die nicht in Natural Security definiert sind, können nicht verwendet werden.

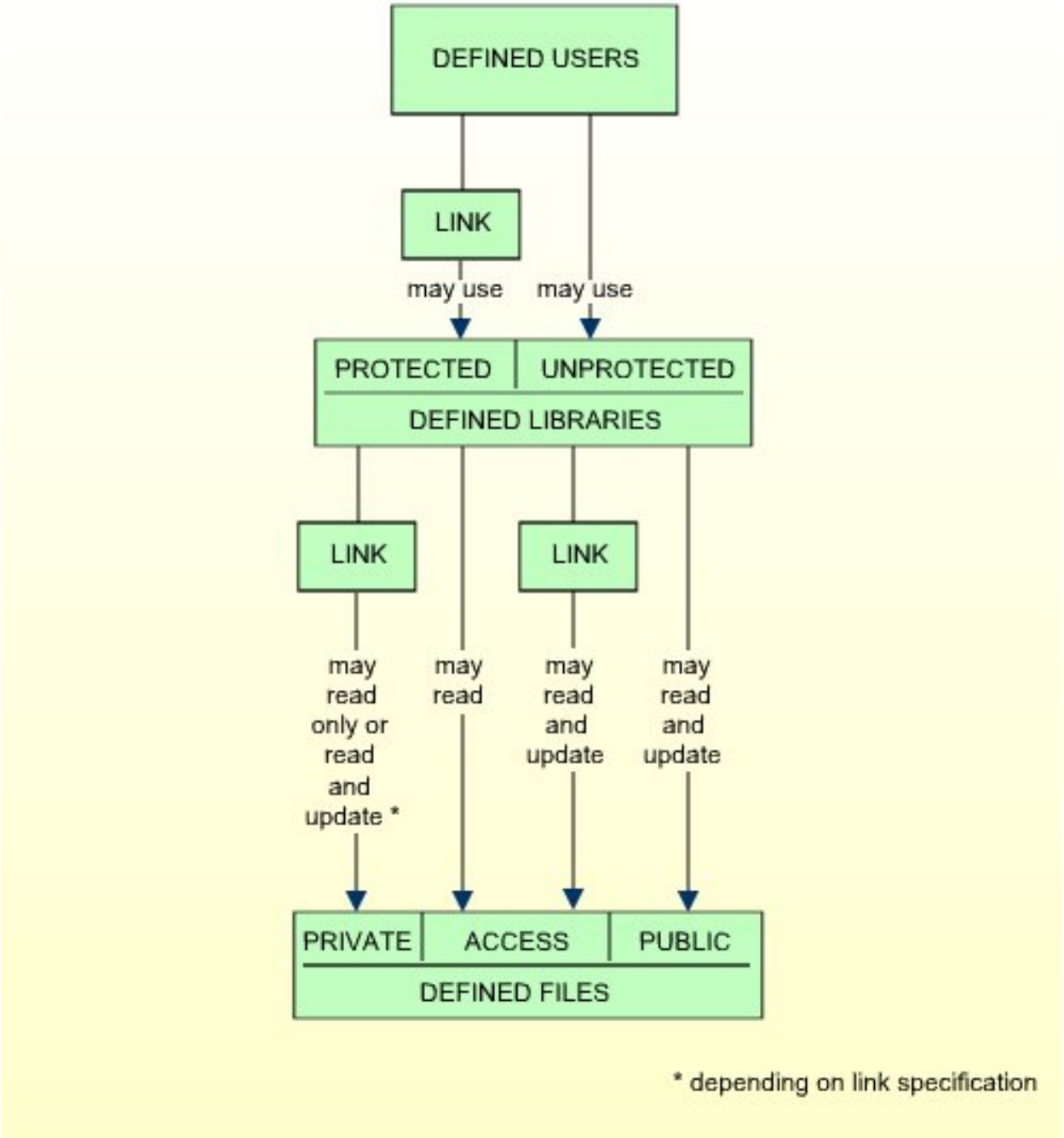
Die Auswirkungen der Einstellungen für die Übergangszeit bei der Anmeldung sind im Folgenden dargestellt.

Wenn Sie eine nicht geschützte Natural-Installation hatten und nun zum ersten Mal Natural Security installieren, ist es ratsam, die **Transition Period Logon** auf `Y` zu setzen, um sicherzustellen, dass die Arbeit mit Natural fortgesetzt werden kann, während Benutzer und Bibliotheken in Natural Security definiert werden. Sobald alle Objekte und Links definiert sind, sollte die Option **Transition Period Logon** auf `N` gesetzt werden.

Nutzungsbedingungen bei Transition Period Logon = Y:



Nutzungsbedingungen bei Transition Period Logon = N:



Security für Development Server-Datei aktivieren - Activate Security for Development Server File

Die Option **Activate Security for Development Server File** wird nur angezeigt, wenn der Natural Development Server (Produktcode NDV) installiert ist und die aktuelle Natural-Sitzung eine Development Server-Datei verwendet. Sie ist nur relevant, wenn Sie den Zugriff auf Basis- und Verbundanwendungen (Base und Compound Applications) in der Development Server-Datei steuern möchten. Einzelheiten hierzu finden Sie im Kapitel *Natural Development Server-Umgebung und -Anwendungen schützen*.

Eingabe:	Erläuterung:
`Y`	Die Security für die Development Server-Datei ist aktiv: Die in Natural Security definierten Anwendungssicherheitsprofile für Basis- und Verbundanwendungen treten in Kraft und steuern den Zugriff auf die Natural Development Server-Objekte Base Applications (Basisanwendungen) und Compound Applications (Verbundanwendungen) in der Development Server-Datei. Die Systemdatei FSEC, die verwendet wird, wenn diese Option auf `Y` gesetzt ist, wird als Development Server-Datei definiert. Diese Development Server-Datei kann dann nur in einer Natural Security-Umgebung verwendet werden. Alle Sicherheitsprüfungen, die der Natural Development Server im Application Workspace (Anwendungsarbeitsbereich) von Natural Studio durchführt, werden anhand der Sicherheitsdefinitionen in dieser FSEC-Systemdatei durchgeführt. Wenn Sie diese Option auf `Y` setzen, wird auch die Predict Security aktiviert (falls nicht bereits in Predict aktiviert, und zwar durch Setzen des Predict-Parameters **Protect Predict File** auf dem Bildschirm **General Defaults > Protection** auf `Y`). Beachten Sie, dass die Aktivierung von Predict Security nicht nur den Zugriff auf Basis- und Verbundanwendungen beeinflusst, sondern auch dazu führen kann, dass andere Predict Security-Einstellungen, die sich nicht auf Anwendungen beziehen, wirksam werden. Die Datenbankkennung (DBID) und die Dateinummer (FNR) der Development Server-Datei, für die die Option aktiviert ist, werden auf dem Bildschirm **Set General Options** (Allgemeine Optionen einstellen) angezeigt.
`N`	Die Security für die Development Server-Datei ist nicht aktiv. Anwendungssicherheitsprofile werden nicht ausgewertet.

Maximale Anzahl von Anmeldeversuchen - Maximum Number of Logon Attempts

Eingabe:	Erläuterung:
`1 - 9`	Sie können festlegen, wie viele Anmeldeversuche die Benutzer haben sollen. Nach *n* erfolglosen Anmeldeversuchen wird der Anmeldevorgang abgebrochen, der Benutzer abgewiesen und ein Anmeldefehlersatz geschrieben (Informationen zu Anmeldefehlersätzen finden Sie unter *Anmeldefehler* weiter unten).

Anzeige von Logon-Meldungen unterdrücken - Suppress Display of Logon Messages

Mit der Option **Suppress Display of Logon Messages** kann die Anzeige der Meldungen NAT0853 und NAT0854 unterdrückt werden. Die Meldungen zeigen an, dass eine Anmeldung bei einer Bibliothek erfolgreich war. Standardmäßig wird eine dieser Meldungen nach jeder erfolgreichen Anmeldung bei einer Bibliothek angezeigt.

Eingabe:	Erläuterung:
Y	Die Meldungen NAT0853 und NAT0854 werden nicht angezeigt.
N	Die Meldungen NAT0853 und NAT0854 werden angezeigt.

Benutzer sperren - Lock User Option

Die Option **Lock User** kann verwendet werden, um zu verhindern, dass Benutzer versuchen, die Benutzerkennungen und Passwörter anderer Benutzer zu missbrauchen. Sie gilt für das **Vorgehensweise bei der Anmeldung** und für die **Gegenzeichnungsfunktion**.

Eingabe:	Erläuterung:
Y	**Anmeldung (Logon):** Bei Anmeldeversuchen gilt Folgendes: Wenn ein Benutzer die **maximale Anzahl an Anmeldeversuchen** erreicht hat, ohne das richtige Passwort einzugeben, wird der betreffende Benutzer gesperrt, d.h. die Benutzerkennung wird „ungültig“ gemacht. Gesperrt werden: ■ alle Natural Security-Benutzerkennungen, die ausprobiert wurden, ■ der Anmeldename des Benutzers beim Betriebssystem (identifiziert durch die Natural-Systemvariable *INIT-USER), wenn ein Natural Security-Benutzersicherheitsprofil existiert, dessen Kennung diesem Namen entspricht. **Gegenzeichnungen (Countersignatures):** Bei Gegenzeichnungsversuchen gilt Folgendes: Nach zu vielen ungültigen Passwörtern (auch hier gilt die maximale Anzahl an Anmeldeversuchen) auf einem Gegenzeichnungsbildschirm wird der Benutzer, der die entsprechende Funktion aufgerufen hat (identifiziert durch seine Natural Security-Benutzerkennung), gesperrt.
F	**Anmeldung (Logon):** Bei Anmeldeversuchen hat F die gleichen Auswirkungen wie Y - zusätzlich wird die Natural-Sitzung beendet, wenn der Benutzer gesperrt wird. **Gegenzeichnungen (Countersignatures):** Bei Gegenzeichnungsversuchen hat F die gleiche Wirkung wie Y.
X	**Anmeldung (Logon):** Bei Anmeldeversuchen hat O die gleichen Auswirkungen wie F - mit dem Unterschied, dass Natural Security sich erfolglose Versuche über mehrere Sitzungen hinweg „merkt“: Bei Y und F

	werden die Zähler der Anmeldeversuche für die Benutzerkennungen, die erfolglos ausprobiert wurden, zurückgesetzt, wenn der Benutzer den Anmeldevorgang abbricht. Bei `0` hingegen werden diese Fehlerzähler für Anmeldevorgänge in nachfolgenden Sitzungen beibehalten, wodurch die Anzahl der nachfolgenden Anmeldeversuche um diese Benutzerkennungen reduziert wird. Das bedeutet, dass die Wahrscheinlichkeit, dass sich jemand mit einer anderen Benutzerkennung Zugang verschafft, erheblich verringert wird. Bei `0` wird der Fehlerzähler für eine Benutzerkennung erst nach einer erfolgreichen Anmeldung zurückgesetzt. **Gegenzeichnungen (Countersignatures):** Bei Gegenzeichnungsversuchen hat `0` die gleiche Wirkung wie `Y`. Die Fehlerzähler eines Benutzers können durch Drücken von PF16 in dessen Sicherheitsprofil angezeigt werden. Eine Liste aller Benutzer, deren Fehlerzähler größer als `0` sind, kann über die Anwendungsprogrammierschnittstelle **NSCXRUSE** abgerufen werden.
`Z`	**Anmeldung (Logon):** Bei Anmeldeversuchen hat `Z` die gleichen Auswirkungen wie `0` - zusätzlich gilt Folgendes: Wenn die Benutzerkennung, die dem Wert der Natural-Systemvariablen `*INIT-USER` entspricht, gesperrt ist, kann die Natural-Sitzung *mit keiner Benutzerkennung* gestartet werden (weder mit `AUTO=ON` noch mit `AUTO=OFF`). Daher sollte diese Einstellung nicht in Umgebungen verwendet werden, in denen mehrere Benutzersitzungen mit demselben `*INIT-USER`-Wert gestartet werden. **Gegenzeichnungen (Countersignatures):** Bei Gegenzeichnungsversuchen hat `0` die gleiche Wirkung wie `Y`.
`N`	Die Funktion **Lock User** (Benutzer sperren) ist nicht aktiv.

Natural RPC Service Calls

Bei Anmeldeversuchen bei Bibliotheken über Natural RPC Service Calls (RPC-Dienstaufrufe) wird diese Option nur wirksam, wenn die Option **Lock user** in den **Library Preset Values** auf `*` gesetzt ist. Für Natural RPC Service Calls gilt Folgendes:

- Die Einstellungen `Y` und `F` haben die gleiche Wirkung wie `0`.
- Wenn die Sperren eintritt, enthalten die gesperrten Client-Benutzerkennungen nicht die Kennung, die in der Systemvariablen `*INIT-USER` enthalten ist.

Benutzerpasswort-/Benutzerpassphrasen-Historie - User Password / Passphrase History

Diese Option entspricht der Option **User password / passphrase history**, die in den **User Preset Values** (siehe *Voreingestellte Benutzersicherheitsprofilwerte*) gesetzt wird.

Freier Zugriff auf Funktionen über APIs - Free Access to Functions via APIs

Mit der Option **Free Access to Functions via APIs** können festlegen, wer von außerhalb von Natural Security über die bereitgestellten Anwendungsprogrammierschnittstellen (APIs) auf die Verwaltungs- und Abfragefunktionen (Maintenance und Retrieval) von Natural Security zugreifen darf. Einzelheiten zu diesen APIs finden Sie im Kapitel *Anwendungsprogrammierschnittstellen*.

Eingabe:	Erläuterung:
`Y`	Auf Verwaltungs- und Retrieval-Funktionen kann von außerhalb von Natural Security über die APIs von jedem zugegriffen werden, der die APIs verwenden darf. Wenn Sie diese Option auf `Y` setzen, können Sie jede Verwaltungs-/Abruffunktion separat mit Funktionssicherheit schützen (siehe Kapitel *Funktionssicherheit*).
`R`	Auf Retrieval-Funktionen (aber nicht auf Verwaltungsfunktionen) kann von außerhalb von Natural Security über die APIs von jedem zugegriffen werden, der die APIs verwenden darf. Wenn Sie diese Option auf "R" setzen, können Sie jede Abruffunktion separat durch Funktionssicherheit schützen (siehe Kapitel *Funktionssicherheit*).
`N`	Auf die Verwaltungs- und Retrieval-Funktionen dürfen von außerhalb von Natural Security nur Benutzer (vom Typ "Administrator") zugreifen, die auch die Natural Security-Bibliothek `SYSSEC` verwenden dürfen. Mit den APIs dürfen sie nur die Funktionen ausführen, die sie auch innerhalb von `SYSSEC` ausführen dürfen, und zwar nur unter denselben Bedingungen, unter denen sie sie in `SYSSEC` ausführen dürfen.

Verwaltungsfunktionen sind alle Funktionen der Subprogramme `NSCFI`, `NSCLI`, `NSCOB` und `NSCUS` - mit Ausnahme ihrer Anzeigefunktionen (Display).

Retrieval-Funktionen sind:

- alle Funktionen der Subprogramme `NSCCHCK`, `NSCDEF`, `NSCDU` und `NSCXR` und der Subprogramme, deren Namen mit `NSCDA` beginnen,
- die Anzeigefunktionen (Display) der Subprogramme `NSCFI`, `NSCLI`, `NSCOB` und `NSCUS`.

Mindestanzahl an Miteigentümern - Minimum Number of Co-Owners

Eingabe:	Erläuterung:
0 - 3	Sie können die Mindestanzahl an Miteigentümern bei jedem Eigentümer eines Sicherheitsprofils angeben. Die hier festgelegte Anzahl gilt für alle Sicherheitsprofile und kann nicht individuell geändert werden.

Eine Erläuterung zu den Miteigentümern finden Sie im Kapitel *Gegenzeichnungen*. Lassen Sie den Wert auf 0 stehen, bis Sie dieses Kapitel gelesen haben.

Löschung von nicht leeren Bibliotheken erlaubt - Deletion of Non-Empty Libraries Allowed

Die Option **Deletion of Non-Entry Libraries Allowed** legt fest, ob das Sicherheitsprofil einer Bibliothek gelöscht werden kann, wenn die Bibliothek Quellcode- oder Objektmodule enthält.

Eingabe:	Erläuterung:
Y	Das Sicherheitsprofil einer Bibliothek kann auch dann gelöscht werden, wenn die Bibliothek Quellcode- oder Objektmodule enthält. Wenn Sie versuchen, ein Bibliothekssicherheitsprofil zu löschen, gibt Natural Security eine Warnung aus, wenn die Bibliothek nicht leer ist. Diese Option wirkt sich nur auf das Löschen des *Sicherheitsprofils* einer Bibliothek aus. Die Natural-Bibliothek selbst und die in ihr enthaltenen Module werden nicht gelöscht.
N	Das Sicherheitsprofil einer Bibliothek kann nicht gelöscht werden, solange die Bibliothek selbst noch Quellcode- oder Objektmodule enthält.

Überschreiben von Standardwerten möglich - Overwriting of Defaults Possible

Die Option **Overwriting of Defaults Possible** legt fest, ob die auf den Bildschirmen **Preset User Values** und **Preset Library Values** eingestellten Werte in den einzelnen Sicherheitsprofilen überschrieben werden dürfen.

Eingabe:	Erläuterung:
Y	Die auf den **Preset**-Bildschirmen gemachten Angaben dürfen in den einzelnen Sicherheitsprofilen überschrieben werden.
N	Die auf den **Preset**-Bildschirmen gemachten Angaben können in keinem Sicherheitsprofil überschrieben werden. Sie sind ausnahmslos für alle Bibliotheken/Benutzer gültig.

Die voreingestellten Werte sind unter *User Preset Values* bzw. *Library Preset Values* beschrieben.

DBID/FNR von FSEC anzeigen - Display DBID/FNR of FSEC

Die Option **Display DBID/FNR of FSEC** legt fest, ob die Datenbankkennung (DBID) und die Dateinummer (FNR) der aktuellen Natural Security-Systemdatei (FSEC) auf den Menü- und Auswahlbildschirmen innerhalb der Bibliothek SYSSEC angezeigt werden sollen.

Eingabe:	Erläuterung:
Y	Die Datenbankkennung und die Dateinummer der aktuellen Natural Security-Systemdatei (FSEC) werden auf den Menü- und Auswahlbildschirmen innerhalb der Bibliothek SYSSEC angezeigt. Sie werden in der oberen rechten Ecke unter dem aktuellen Datum gezeigt.
N	Die Datenbankkennung und die Dateinummer der FSEC-Datei werden in SYSSEC nicht angezeigt.

Beenden von Funktionen mit Bestätigung - Exit Functions with Confirmation

Die Option **Exit Function with Confirmation** legt fest, wie sich Natural Security verhält, wenn Sie eine Funktion durch Drücken von PF2, PF3, PF12 oder PF15 verlassen.

Eingabe:	Erläuterung:
Y	Wenn Sie eine Funktion in Natural Security durch Drücken von PF2, PF3, PF12 oder PF15 verlassen, wird ein Fenster angezeigt, in dem Sie angeben müssen, ob die Änderungen, die Sie vor dem Drücken der Taste vorgenommen haben, gespeichert werden sollen oder nicht, oder ob Sie zur Funktion zurückkehren möchten.
N	Wenn Sie eine Funktion durch Drücken von PF2, PF3 oder PF15 verlassen, werden die Änderungen, die Sie vor dem Drücken der Taste vorgenommen haben, gespeichert. Wenn Sie eine Funktion durch Drücken von PF12 verlassen, werden die Änderungen, die Sie vor dem Drücken der Taste vorgenommen haben, *nicht* gespeichert.

Einzelheiten zu den Funktionen, mit denen diese Tasten belegt sind, finden Sie im Abschnitt ***PF-Tasten***.

Protokollieren von Verwaltungsfunktionen - Logging of Maintenance Functions

Mit der Option **Logging of Maintenance Functions** können Sie feststellen, wer welche Sicherheitsprofile und Administrator Services-Einstellungen geändert hat.

"Ändern" bezieht sich in diesem Zusammenhang auf alle Verwaltungsfunktionen, die auf ein Sicherheitsprofil angewendet werden (einschließlich Anlegen, Kopieren, Löschen, Verlinken usw.). Es umfasst auch das Übertragen eines Sicherheitsprofils mit den Programmen SECULD2 und SECLOAD.

Eingabe:	Erläuterung:
Y	Bei Änderungen an Sicherheitsprofilen und Einstellungen in den Administrator Services werden Protokollsätze geschrieben.
N	Änderungen werden nicht protokolliert.

Wenn Sie diese Option auf Y setzen, wird ein Fenster angezeigt, in dem Sie Folgendes angeben können:

Eingabe:	Erläuterung:

Log file DBID/FNR	Die Datenbankkennung (DBID) und die Dateinummer (FNR) der Datei, in der die Protokolleinträge gespeichert werden sollen.
	
	Diese Datei muss, wie in der Installationsdokumentation für Natural Security beschrieben, geladen worden sein. Auf Großrechner-Plattformen muss die FDT dieser Datei mit dem entsprechenden Installationsjob geladen worden sein, der durch System Maintenance Aid bereitgestellt wird. Auf Nicht-Großrechner-Plattformen muss sie mit dem Natural-Dienstprogramm SYSPCI erstellt worden sein: Wählen Sie in SYSPCI das Produkt Natural Security und dann die Option **Create new Adabas file**.
	
	Anmerkung: Sobald die Option **Logging of Maintenance Functions** aktiviert ist, können Sie die Zuordnung der Protokolldatei nicht mehr ändern. Sie müssen die Option deaktivieren, bevor Sie eine andere Datenbankkennung oder Dateinummer vergeben können.
	
	Sollte die Protokolldatei unzugänglich geworden sein, so dass Sie die Protokollierung der Verwaltungsfunktionen nicht mehr deaktivieren können, können Sie die Zuordnung der Protokolldatei mit dem Natural-Systemkommando INPL mit Code R (Recover) und Option A (Adjust) ändern. Als Parameter für das Kommando geben Sie die Datenbankkennung und die Dateinummer der aktuellen (unzugänglichen) Protokolldatei sowie deren gewünschten neuen Speicherort an. Die Eingabe im Batch-Modus für diesen Vorgang wäre wie folgt:
	
	`//CMSYNIN DD *`
	`R,A`
	`old-DBID,old-FNR,new-DBID,new-FNR`

Logging even if no actual modification	Y Änderungen werden auch dann protokolliert, wenn nichts geändert wurde, d.h. wenn ein Sicherheitsprofil oder eine Einstellung der Administrator Services zur Änderung aufgerufen wurde, aber keine tatsächliche Änderung an dem Profil oder an der Einstellung vorgenommen wurde. N Änderungen werden nur protokolliert, wenn ein Profil/eine Einstellung tatsächlich geändert wurde.
Logging of changes to	Mögliche Werte: N, Y und (für Benutzersicherheitsprofile und Bibliothekssicherheitsprofile) X. Mit Y markieren Sie die Objekttypen, deren Änderungen protokolliert werden sollen:

- Administrator Services-Einstellungen (*),
- Benutzersicherheitsprofile,
- Bibliothekssicherheitsprofile (einschließlich Profil für Special-Links),
- Dateisicherheitsprofile,
- Anwendungssicherheitsprofile,
- Mailbox-Sicherheitsprofile,
- verschiedene Arten von Sicherheitsprofilen für externe Objekte.

(*) „Administrator Services-Einstellungen“ bedeutet in diesem Zusammenhang alle im **Administrator Services Menu** aufgeführten Funktionen (außer **Anwendungsprogrammierschnittstellen**).

Zugehörige Profile

Wenn ein Sicherheitsprofil geändert wird, passt Natural Security automatisch die zugehörigen Sicherheitsprofile an, um die Konsistenz aller Natural Security-Definitionen zu gewährleisten. Wenn Sie beispielsweise ein Gruppenprofil ändern, um einen Benutzer aus der Gruppe zu entfernen, ändert Natural Security automatisch das Benutzersicherheitsprofil, um diese Gruppe, falls erforderlich, aus der Liste der privilegierten Gruppen des Benutzers zu entfernen. Diese automatischen Anpassungen der zugehörigen Profile werden ebenfalls protokolliert.

Dienstprogrammprofile - Utility Profiles

Änderungen an Dienstprogramm-Sicherheitsprofilen werden nicht separat protokolliert. Stattdessen werden Standardprofile und Vorlagen unter **Administrator Services settings**, bibliotheksspezifische Utility Profiles unter „Library security profiles“ und benutzerspezifische und bibliotheksspezifische Utility-Profile unter „User security profiles“ behandelt.

Erweiterte Protokollierung für Benutzer- und Bibliothekssicherheitsprofile

Sie können Benutzersicherheitsprofile und Bibliothekssicherheitsprofile mit `0` (anstelle von `Y`) markieren, damit die folgenden zusätzlichen Daten protokolliert werden.

Für Benutzersicherheitsprofile:

- Wenn die Funktion **Copy User** (Benutzer kopieren) mit der Option **with links** (mit Verlinkungen) verwendet wird, werden alle Beziehungen, die durch das Kopieren zwischen dem Benutzer und anderen Objekten hergestellt wurden, protokolliert.
- Wenn die Funktion **Delete User** (Benutzer löschen) verwendet wird, wird jede Beziehung protokolliert, die zwischen dem Benutzer und anderen Objekten bestand und die durch das Löschen entfernt wurde.

Für Bibliothekssicherheitsprofile:

- Wenn die Funktion **Copy Library** (Bibliothek kopieren) mit der Option **with links** verwendet wird, wird jede Beziehung, die durch das Kopieren zwischen der Bibliothek und anderen Objekten hergestellt wurde, protokolliert.

	■ Wenn ein Link zwischen einer Gruppe und einer Bibliothek verwaltet wird, wird eine Liste der Mitglieder der Gruppe protokolliert. ■ Wenn sich eine Verwaltungsfunktion auf den Bereich **Disallow/Modules** eines Bibliothekssicherheitsprofils (oder eines Profils für Special-Links) auswirkt, werden Informationen über jedes Modul protokolliert, dessen Status geändert wurde. ,

Um, nachdem Sie das Schreiben von Protokollsätzen aktiviert haben, die obigen Angaben zu ändern, müssen Sie auf dem Bildschirm **Set General Options** PF4 drücken.

Um die Protokollsätze einzusehen, können Sie die Funktion **Maintenance Log Records** (siehe unten) verwenden.

Anmelde- und Fehlerdaten in separaten Systemdateien speichern - Store Logon and Error Data on Separate System Files

Die Option **Store Logon and Error Data on Separate System Files** kann verwendet werden, um bestimmte Natural Security-Daten in separaten Systemdateien zu speichern.

Eingabe:	Erläuterung:
Y	Die folgenden Daten können in separaten Systemdateien gespeichert werden: ■ Anmeldedatensätze, wie sie von der Funktion **Logon Records** geschrieben werden, ■ Anmelde-/ Gegenzeichnungsfehlerprotokollsätze, wie sie von der Funktion **Logon/Countersign Errors** geschrieben werden, ■ Verwaltungsprotokollsätze, wie sie von der Funktion **Logging of Maintenance Functions** geschrieben werden. Wenn Sie dieses Feld auf Y setzen und PF5 drücken, wird ein Bildschirm angezeigt, auf dem Sie die DBID (Datenbankkennungen) und FNR (Dateinummern) dieser Systemdateien angeben müssen. Auf Großrechnerplattformen müssen die File Definition Tables (FDTs) dieser Dateien mit dem entsprechenden Installationsjob, der durch System Maintenance Aid bereitgestellt wird, geladen worden sein. Auf Nicht-Großrechnerplattformen müssen diese Dateien mit dem Natural-Dienstprogramm SYSPCI erstellt worden sein: Wählen Sie in SYSPCI das Produkt **Natural Security** und dann die Option **Create new Adabas file** (aber nicht die Option **Initialize**!).
N	Alle Natural-Sicherheitsdaten werden in der gleichen FSEC-Systemdatei gespeichert.

Anmerkung: Wenn Sie ein Adabas-Dienstprogramm verwenden, um die Datenbankkennung (DBID) oder Dateinummer (FNR) einer dieser Systemdateien zu ändern, müssen Sie dieses Feld *vor* der Änderung auf N und dann nach der Änderung wieder auf Y setzen, damit Natural Security die neue Systemdatei kennt.

Konkurrierende Änderungen ohne Benachrichtigung - Concurrent Modifications Without Notification

Die Option **Concurrent Modifications Without Notification** legt fest, wie Natural Security in einer Situation reagiert, in der zwei Administratoren gleichzeitig dasselbe Sicherheitsprofil ändern. Eine solche Situation würde wie folgt ablaufen:

1. Administrator 1 ruft ein Sicherheitsprofil zur Änderung auf.
2. Administrator 2 ruft das gleiche Sicherheitsprofil zur Änderung auf.
3. Administrator 1 verlässt die Funktion, nachdem er seine Änderungen vorgenommen hat - die Änderungen werden auf das Sicherheitsprofil angewendet. Dies bedeutet, dass Administrator 2 zu diesem Zeitpunkt mit Daten arbeitet, die „veraltet“ sind, sich dessen aber nicht bewusst ist.
4. Administrator 2 verlässt die Funktion, nachdem er seine Änderungen vorgenommen hat. Nun gibt es zwei mögliche Reaktionen von Natural Security:
   - Die von Administrator 2 vorgenommenen Änderungen werden übernommen - und überschreiben damit unwissentlich die von Administrator 1 vorgenommenen Änderungen.
   - Administrator 2 wird per Fenster darüber informiert, dass das betreffende Sicherheitsprofil in der Zwischenzeit von einem anderen Administrator geändert wurde. Er kann sich daraufhin mit dem anderen Administrator in Verbindung setzen, um die vorgenommenen Änderungen zu besprechen, und kann dann entscheiden, ob er seine eigenen Änderungen rückgängig machen oder sie übernehmen und damit die von Administrator 1 vorgenommenen Änderungen überschreiben möchte.

Die Option **Concurrent Modifications Without Notification** legt fest, welche der beiden Reaktionen erfolgen soll, d.h:

Eingabe:	Erläuterung:
Y	Die Änderungen werden in jedem Fall durchgeführt.
N	Es wird ein Fenster angezeigt, in dem der Administrator wählen kann, ■ seine Änderungen zu verwerfen, ■ seine Änderungen anzuwenden, ■ zu dem betreffenden Sicherheitsprofil zurückzukehren.

Diese Option gilt nur für konkurrierende Änderungen, die an Sicherheitsprofilen von Benutzern, Bibliotheken, Special-Links und Postfächern vorgenommen werden.

Private Bibliotheken im öffentlichen Modus - Private Libraries in Public Mode

Die Option **Private Libraries in Public Mode** legt fest, ob private Bibliotheken im Private Mode oder im Public Mode verfügbar sein sollen.

Eingabe:	Erläuterung:
Y	Private Bibliotheken sind im öffentlichen Modus verfügbar.
N	Private Bibliotheken sind im privaten Modus für die ausschließliche Nutzung durch Benutzer mit denselben Benutzerkennungen verfügbar (nicht empfohlen).

Weitere Informationen finden Sie unter *Private Bibliothek* im Kapitel *Benutzer verwalten*. Sie sollten dieses Kapitel lesen, bevor Sie diese Option einstellen.

Mailboxen im Batch-Modus unterdrücken - Suppress Mailboxes in Batch Mode

Die Option **Suppress Mailboxes in Batch Mode** legt fest, ob Mailboxen im Batch-Modus ausgegeben werden oder nicht.

Eingabe:	Erläuterung:
Y	Mailboxen werden im Batch-Modus nicht ausgegeben.
N	Mailboxen werden im Batch-Modus ausgegeben.

Informationen zu Mailboxen finden Sie im Kapitel *Mailboxen*.

Umgebungsschutz - Environment Protection

Die Option **Environment Protection** legt fest, ob Natural-Umgebungen - d. h. Systemdatei-Kombinationen - geschützt sind.

Eingabe:	Erläuterung:
N	Der Umgebungsschutz ist nicht aktiv: Benutzer können auf jede Umgebung zugreifen. Natural Security führt keine Zugriffsberechtigungsprüfungen hinsichtlich der Umgebung durch.
Y	Der Umgebungsschutz ist aktiv: Benutzer können nur auf Umgebungen zugreifen, für die Sicherheitsprofile definiert sind. Standardmäßig ist der Zugriff auf eine Bibliothek in einer definierten Umgebung für alle Benutzer erlaubt. Für einzelne Bibliotheken und Benutzer können Sie den Zugriff auf eine Umgebung verbieten.

Wenn Sie die Einstellung dieser Option ändern, müssen Sie Ihre Natural-Sitzung neu starten, damit die Änderung wirksam wird.

Einzelheiten zum Umgebungsschutz finden Sie im Kapitel *Umgebungen schützen*.

Zugriff auf aktuelle FSEC - Access To Current FSEC

Das Feld **Access To Current FSEC** legt fest, ob auf die in dieser FSEC-Systemdatei gespeicherten Natural Security-Daten von einer Natural Security-Sitzung aus zugegriffen werden kann, die mit einer anderen FSEC-Systemdatei läuft.

Eingabe:	Erläuterung:
N	Auf die Daten kann nicht zugegriffen werden.
U	Auf die Daten kann über die Anwendungsprogrammierschnittstellen (APIs) zugegriffen werden, die in der Bibliothek SYSEXT bereitgestellt werden. Dies gilt nur für APIs, bei denen eine FSEC-Systemdatei angegeben werden kann.

Impersonation für Natural Development Server erzwingen - Force Impersonation for Natural Development Server

Die Option **Force Impersonation for Natural Development Server** ist nur für den Natural Development Server (NDV) relevant. Sie steuert, wie der Zugriff auf einen NDV-Server gehandhabt wird.

Es wird davon ausgegangen, dass der Zugriff auf das Betriebssystem, auf dem ein NDV-Server läuft, durch ein SAF-kompatibles externes Sicherheitssystem gesteuert wird. Die Benutzerauthentifizierung (Überprüfung von Benutzerkennung und Passwort) wird von diesem externen Sicherheitssystem durchgeführt. Nach erfolgreicher Authentifizierung erzeugt es ein Accessor Environment Element (ACEE) für den Benutzer, das für nachfolgende Autorisierungen zur Verfügung steht.

Eingabe:	Erläuterung:
N	Ein Benutzer kann auf einen NDV-Server entweder mit der vom externen Sicherheitssystem generierten ACEE oder direkt mit seiner Natural Security-Benutzerkennung und seinem Passwort zugreifen.
Y	Ein Benutzer kann nur mit der vom externen Sicherheitssystem generierten ACEE auf einen NDV-Server zugreifen. Ohne ACEE ist der Zugriff auf einen NDV-Server nicht möglich. Dadurch wird sichergestellt, dass die Benutzerauthentifizierung des externen Sicherheitssystems nicht umgangen werden kann. Wenn der Benutzer über eine ACEE verfügt, werden keine weiteren Authentifizierungsprüfungen durchgeführt, wenn er sich beim NDV-Server anmeldet.

Erstanmeldung jedes Benutzers täglich aufzeichnen - Record Each User's Initial Logon Daily

Die Option **Record Each User's Initial Logon Daily** kann verwendet werden, um unbenutzte Benutzerkennungen zu erkennen, d. h. Benutzersicherheitsprofile, die über einen längeren Zeitraum nicht verwendet wurden. Dies kann hilfreich sein, wenn Sie beschließen, nicht mehr verwendete Benutzersicherheitsprofile zu löschen.

Eingabe:	Erläuterung:
N	Erstanmeldungen werden nicht täglich aufgezeichnet.
Y	Die Erstanmeldung jedes Benutzers zu Beginn der Natural-Sitzung wird täglich aufgezeichnet. Das Datum der letzten Erstanmeldung eines Benutzers wird in seinem Sicherheitsprofil angezeigt (durch Drücken von PF16 auf dem Hauptbildschirm des Benutzersicherheitsprofils). Beachten Sie, dass nur Anmeldungen aufgezeichnet werden können, die bei aktivierter Option erfolgen.

Wenn diese Option auf Y gesetzt ist, können Sie die Anwendungsprogrammierschnittstelle NSCXRUSE verwenden, um eine Liste der Benutzer zu erhalten, die sich seit einem bestimmten Datum nicht mehr angemeldet haben.

Fehlertransaktion vor NAT1700/1701-Abmeldung aktivieren - Enable Error Transaction Before NAT1700/1701 Logoff

Die Option **Enable Error Transaction Before NAT1700/1701 Logoff** legt fest, ob bei den Natural-Fehlern NAT1700 (**Zeitfenster** überschritten) und NAT1701 (**Zeitlimit für Nichtaktivität** überschritten) das entsprechende ON ERROR-Statement und/oder die Fehlertransaktion der aktuellen Natural-Anwendung verarbeitet wird oder nicht.

Die Fehlertransaktion wird durch den Wert der Natural-Systemvariablen *ERROR-TA bestimmt.

Eingabe:	Erläuterung:
N	Wenn der Fehler NAT1700 oder NAT1701 auftritt, werden sowohl das ON ERROR-Statement als auch die Fehlertransaktion der Anwendung ignoriert. Natural Security führt eine Abmeldung durch, unabhängig davon, ob es ein ON ERROR-Statement oder eine Fehlertransaktion gibt.
S	Wenn der Fehler NAT1700 oder NAT1701 auftritt, wird das entsprechende ON ERROR-Statement der Anwendung verarbeitet, bevor Natural Security eine Abmeldung durchführt. Jede Fehlertransaktion wird ignoriert.
E	Wenn der Fehler NAT1700 oder NAT1701 auftritt, wird die Fehlertransaktion der Anwendung verarbeitet, bevor Natural Security eine Abmeldung durchführt. Jedes ON ERROR-Statement wird ignoriert.
G	Wenn der Fehler NAT1700 oder NAT1701 auftritt, wird das entsprechende ON ERROR-Statement der Anwendung verarbeitet, und wenn kein ON ERROR-Statement gefunden wird, wird die Fehlertransaktion aufgerufen, bevor Natural Security eine Abmeldung durchführt.

Diese Option ist nur auf Großrechnern wirksam. Auf Nicht-Großrechnerplattformen reagiert Natural Security immer so, als ob sie auf G gesetzt wäre (unabhängig von der tatsächlichen Einstellung).

Abmelden im Fehlerfall, wenn *STARTUP aktiv - Logoff in Error Case if *STARTUP is Active

Die Option **Logoff in Error Case if *STARTUP is Active** legt fest, wie im Falle eines Natural-Laufzeitfehlers innerhalb der ON ERROR-Bedingung einer Startup-Transaktion (*STARTUP) verfahren werden soll.

Wenn ein Laufzeitfehler innerhalb der ON ERROR-Bedingung einer Startup-Transaktion auftritt, kann die Fehlerverarbeitung von Natural dazu führen, dass die Startup-Transaktion erneut ausgeführt wird. Dies würde zu einer Fehlerschleife führen. Um eine solche Schleife zu verhindern, können Sie diese Option setzen.

Eingabe:	Erläuterung:
Y	Im Falle eines Laufzeitfehlers, der durch eine Startup-Transaktion verursacht wurde, wird ein LOGOFF-Kommando zu dem Zeitpunkt ausgeführt, an dem die Startup-Transaktion im Zuge der Fehlerverarbeitung von Natural zur Ausführung anstehen würde.
N	Im Falle eines Laufzeitfehlers, der durch eine Startup-Transaktion verursacht wurde, wird die Natural-Systemvariable *STARTUP auf Leerzeichen gesetzt, und die Fehlerverarbeitung von Natural wird fortgesetzt.

Wenn keine Startup-Transaktion definiert ist, hat diese Option keine Auswirkung.

*APPLIC-NAME immer auf Bibliotheksname setzen - Set *APPLIC-NAME Always to Library Name

Die Option **Set *APPLIC-NAME Always to Library** bestimmt den Wert der Natural-Systemvariablen *APPLIC-NAME.

Eingabe:	Erläuterung:
Y	Die Natural-Systemvariable *APPLIC-NAME enthält den Namen der Bibliothek, bei der der Benutzer angemeldet ist, unabhängig davon, ob der Benutzer über einen speziellen Link angemeldet ist oder nicht.
N	Die Natural-Systemvariable *APPLIC-NAME enthält den Namen der Bibliothek, bei der der Benutzer angemeldet ist. Wenn der Benutzer über einen speziellen Link angemeldet ist, enthält sie stattdessen den Namen des speziellen Links.

Löschen von Benutzern, die Eigentümer/DDM-Änderer sind, zulassen - Allow Deletion of Users Who Are Owners/DDM Modifiers

Die Option **Allow Deletion of Users Who Are Owners/DDM Modifiers** legt fest, ob ein Benutzersicherheitsprofil gelöscht werden kann, wenn der Benutzer noch entweder als Eigentümer in einem Sicherheitsprofil oder als DDM-Änderer in einem DDM-/Datei-Sicherheitsprofil angegeben ist.

Diese Option kann nur gesetzt werden, wenn der Natural Security-Bibliothek `SYSSEC` Eigentümer zugewiesen sind.

Eingabe:	Erläuterung:
`N`	Sicherheitsprofile von Benutzern, die Eigentümer oder DDM-Änderer sind, können *nicht* gelöscht werden. Dadurch wird sichergestellt, dass die Löschung keine unerwünschte Eigentümer- oder DDM-Änderer-Konstellation bewirkt.
`O`	Sicherheitsprofile von Benutzern, die Eigentümer oder DDM-Änderer sind, können gelöscht werden. Sie können nur von Administratoren gelöscht werden, die Eigentümer der Bibliothek `SYSSEC` sind.
`A`	Sicherheitsprofile von Benutzern, die Eigentümer oder DDM-Änderer sind, können gelöscht werden. Sie können nur von dem Administrator (oder der Gruppe von Administratoren) gelöscht werden, dessen/deren Kennung im Feld **By Administrator** angegeben ist.

Wenn diese Option auf `O` oder `A` gesetzt ist und das Sicherheitsprofil eines Benutzers gelöscht wird, wird seine Kennung automatisch aus allen Sicherheitsprofilen entfernt, in denen er als Eigentümer oder DDM-Änderer angegeben ist. Dennoch kann es ratsam sein, vor der Löschung die Funktion **Cross-Reference User** zu benutzen, um festzustellen, welche Profile/DDMs betroffen sind, und nach der Löschung sicherzustellen, dass die geänderten Konfigurationen von Eigentümer/Miteigentümer und DDM-Änderer/Mit-Änderer noch Ihren Anforderungen entsprechen.

Authentifizierungsoptionen - Authentication Options (LDAP)

In diesem Abschnitt werden die Optionen beschrieben, die für die Authentifizierungsart LDAP (Light Directory Authentication Protocol) zur Verfügung stehen. Bevor Sie diese Optionen verwenden, sollten Sie mit den entsprechenden Informationen in der Dokumentation der *Software AG Security eXtensions (SSX)* vertraut sein.

Ein LDAP-Server ist ein Server, der das Light Directory Authentication Protocol verwendet. Wenn die Benutzerauthentifizierung über einen LDAP-Server erfolgen soll, müssen die SSX-Sicherheitsbibliotheken im Rahmen der Natural Security-Installation installiert worden sein.

Die Benutzerauthentifizierung über einen LDAP-Server ist für Online- und Batch-Sitzungen unter Linux und Windows (einschließlich Natural Development Server) möglich. Sie wird aktiviert, indem das Feld **Protection Level** im LDAP-Master Security Profile auf `1` gesetzt wird (siehe unten).

Wenn ein LDAP-Server verwendet werden soll, muss er in Natural Security definiert werden, indem ein Sicherheitsprofil für ihn erstellt wird.

- LDAP-Sicherheitsprofiltypen
- LDAP-Sicherheitsprofilverwaltung aufrufen
- LDAP-Sicherheitsprofile anlegen und verwalten
- Archiviertes Sicherheitsprofil zurückholen
- Bestandteile eines LDAP-Sicherheitsprofils

LDAP-Sicherheitsprofiltypen

Sie können die folgenden Typen von LDAP-Sicherheitsprofilen definieren:

- ein Masterprofil,
- ein alternatives Profil,
- mehrere archivierte Profile.

Standardmäßig kann nur ein LDAP-Sicherheitsprofil - das Masterprofil - definiert werden. Das Masterprofil ist das Profil für den LDAP-Server, der tatsächlich für die Authentifizierung verwendet wird.

Zusätzlich zum Masterprofil können Sie ein alternatives Profil für einen anderen LDAP-Server definieren. Dieser alternative Server wird in den folgenden Situationen für die Authentifizierung verwendet:

- der im Masterprofil definierte Server ist zum Zeitpunkt der Authentifizierung nicht verfügbar, oder
- die vom Master Server durchgeführte Authentifizierung ist fehlgeschlagen.

Bevor Sie ein alternatives Profil definieren können, müssen Sie im Masterprofil das Feld **Allow alternative profile** auf `Y` setzen.

Sowohl das Masterprofil als auch das alternative Profil sind nach ihrer Definition entweder aktiv oder nicht aktiv. Um sie zu aktivieren, müssen Sie das Feld **Protection Level** (Schutzstufe) im LDAP-Master-Sicherheitsprofil auf `1` setzen; um sie zu deaktivieren, müssen Sie es auf `0` setzen (siehe unten).

Zusätzlich zu dem Masterprofil und dem Alternativprofil können Sie archivierte Profile definieren, d.h. weitere LDAP-Sicherheitsprofile, die archiviert werden und inaktiv sind. Auf diese Weise können Sie zusätzliche LDAP-Server für künftige Verwendung oder zu Testzwecken definieren.

LDAP-Sicherheitsprofilverwaltung aufrufen

Um die LDAP- Sicherheitsprofilverwaltung aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) den Menüeintrag **Administrator Services**.

Wenn Sie **berechtigt** sind, auf die Administrator Services zuzugreifen, wird das Menü **Administrator Services Menu 1** angezeigt.

2 Wählen Sie in diesem Menü die **Authentication Options**.

Es wird die Auswahlliste **Authentication Types** angezeigt, in der alle vorhandenen LDAP-Sicherheitsprofile aufgeführt sind.

Die Spalte **Pr Ty** zeigt den Profiltyp und den Aktivierungsstatus an:

- `M1` = Masterprofil - aktiv.
- `M3` = Masterprofil - aktiv - NSC Authentifizierung, wenn LDAP fehlschlägt.
- `A1` = alternatives Profil - aktiv.
- `M0` = Masterprofil - nicht aktiv.
- `A0` = alternatives Profil - nicht aktiv.
- `A3` = alternatives Profil - aktiv - NSC Authentifizierung, wenn LDAP fehlschlägt.
- `Ar` = archiviertes Profil.

3 Von dieser Auswahlliste aus können Sie, wie nachfolgend beschrieben, alle Funktionen zum Anlegen und Verwalten von LDAP-Sicherheitsprofilen aufrufen.

LDAP-Sicherheitsprofile anlegen und verwalten

Um ein neues LDAP-Sicherheitsprofil anzulegen:

1 Drücken Sie in der Auswahlliste **Authentication Types** die Taste `PF5` oder geben Sie das Direktkommando `ADD` ein.

2 Es wird ein Fenster angezeigt, in dem Sie folgende Angaben machen können:

- **Profile type** - Wenn Sie Ihr erstes LDAP-Profil anlegen, können Sie angeben, ob es das Masterprofil sein oder archiviert werden soll.

  Wenn bereits ein Masterprofil existiert, können Sie angeben, ob das neue Profil das alternative Profil sein oder archiviert werden soll.
- **Profile ID** - Für ein alternatives oder archiviertes Profil müssen Sie eine Kennung angeben (für das Masterprofil ist die Kennung immer `* LDAP *`).

- **Copy from * LDAP *** - Für ein alternatives oder archiviertes Profil können Sie wählen, ob Sie die Bestandteile aus dem Masterprofil übernehmen wollen.

Es wird der erste Bildschirm des LDAP-Sicherheitsprofils angezeigt.

Die Bestandteile, die Sie darin definieren können, werden im Folgenden unter *Bestandteile eines LDAP-Sicherheitsprofils* beschrieben.

Um ein bestehendes LDAP-Sicherheitsprofil zu verwalten:

- In der Auswahlliste **Authentication Types** (Authentifizierungstypen) können Sie eine der folgenden Funktionen aufrufen, indem Sie ein Profil mit einem der folgenden Funktionscodes (mögliche Codeabkürzungen sind unterstrichen) in der Spalte **Co** markieren:

Code	Funktion	
MO	Modify security profile.	Sicherheitsprofil ändern.
DE	Delete security profile.	Sicherheitsprofil löschen.
DI	Display security profile.	Sicherheitsprofil anzeigen.
AR	Archive security profile.	Sicherheitsprofil archivieren.
RV	Revive security profile.	Archiviertes Sicherheitsprofil zurückholen

Archiviertes Sicherheitsprofil zurückholen

Sie können ein archiviertes Profil entweder als Masterprofil oder als alternatives Profil zurückholen.

Um ein archiviertes LDAP-Sicherheitsprofil zurückzuholen:

1 Markieren Sie in der Auswahlliste **Authentication Types** das betreffende Profil mit dem Funktionscode `RV`.

2 Der Bildschirm **Revive Profile** *`Profilkennung`* wird angezeigt. Wählen Sie eine der folgenden Optionen:

- **Revive as master profile**
  Als Masterprofil zurückholen. Das aktuelle Masterprofil wird archiviert, und das zurückgeholte Profil wird zum neuen Masterprofil.

  Die Kennung des zurückgeholten Profils wird `* LDAP *`. Wenn Sie diese Option wählen, werden Sie aufgefordert, die Kennung anzugeben, unter der das alte Masterprofil archiviert werden soll.

- **Revive as alternative profile**
  Als alternatives Profil zurückholen. Das aktuelle alternative Profil wird archiviert, und das zurückgeholte Profil wird zum neuen alternativen Profil.

  Wenn Sie diese Option wählen, werden Sie aufgefordert, die Kennung anzugeben, unter der das zurückgeholte Profil das neue alternative Profil sein soll, sowie die Kennung, unter der das alte alternative Profil archiviert werden soll. Die neuen Kennungen sind optional, Sie können auch die bestehenden Kennungen beibehalten.
- **Revive as master profile with exchange**
  Wiederherstellen als Masterprofil mit Austausch. Das aktuelle alternative Profil wird archiviert, das aktuelle Masterprofil wird zum neuen alternativen Profil, und das zurückgeholte Profil wird zum neuen Masterprofil.

  Die Kennung des zurückgeholten Profils wird zu `* LDAP *`. Wenn Sie diese Option wählen, werden Sie aufgefordert, neue Kennungen für die beiden anderen ausgetauschten Profile anzugeben. Für das alte Masterprofil müssen Sie eine neue Kennung angeben. Für das alte alternative Profil ist dies optional, Sie können auch die bestehende Kennung beibehalten.

Bestandteile eines LDAP-Sicherheitsprofils

Die Bildschirme, die sich auf das Masterprofil beziehen, tragen den Titel **General LDAP Options**. Die Bildschirme, die sich auf ein alternatives oder archiviertes Profil beziehen, tragen den Titel **Profile** *Profilkennung* **Options**.

Die Bestandteile, die Sie als Teil eines LDAP-Sicherheitsprofils definieren können, werden im Folgenden beschrieben. Einige Bestandteile können nur im Masterprofil definiert werden; sie gelten für alle Profile und werden gegebenenfalls in alternativen/archivierten Profilen angezeigt, ihre Einstellungen können jedoch nur im Masterprofil geändert werden.

Feld	Erläuterung
LDAP Options 1	
Profile ID	Die Natural Security-Kennung des LDAP-Sicherheitsprofils. Die Kennung des Masterprofils kann nicht geändert werden, sie lautet immer `* LDAP *`. Die Kennungen von alternativen und archivierten Profilen sind frei wählbar und können bis zu 8 Zeichen lang sein. Sie können die Kennungen ändern, wenn Sie LDAP-Sicherheitsprofile archivieren und zurückholen.
Profile name	Sie können einen Namen für das Profil angeben, der bis zu 32 Zeichen lang sein kann.
Authentication type	`LDAP` (kann nicht geändert werden).
Protection level	Schutzstufe. Mögliche Werte: ■ `0` = Die Benutzerauthentifizierung wird von Natural Security durchgeführt.

Feld	Erläuterung
LDAP Options 1	
	■ 1 = Die Benutzerauthentifizierung erfolgt über einen LDAP-Server. Dies gilt für Natural Online- und Batch-Sitzungen unter Linux und Windows. Nach erfolgreicher Benutzerauthentifizierung gelten alle Natural Security-Einstellungen für definierte Benutzer (für nicht definierte Benutzer siehe **NSC user ID** (Natural Security-Benutzerkennung) unten). Zu beachten ist, dass bei LDAP die Groß- und Kleinschreibung bei der Angabe des Passworts berücksichtigt wird und eine Änderung des Passworts nicht möglich ist. ■ 3 = Wie Schutzstufe 1, außer dass der Benutzer, wenn die LDAP-Authentifizierung fehlschlägt, weiter mit Natural Security authentifiziert wird. **Anmerkung:** Wenn die LDAP-Authentifizierung aktiv ist, wird bei den Feldern für die Benutzerkennung und das Passwort zwischen Groß- und Kleinschreibung unterschieden.
Allow alternative profile	Alternatives Profil zulassen. Dieses Feld ist nur im Masterprofil verfügbar. Wenn Sie zusätzlich zum Masterprofil ein alternatives Profil verwenden möchten, müssen Sie dieses Feld auf Y setzen.
Error record if alternative used	Fehlersatz bei Verwendung eines alternativen Profils. Dieses Feld ist nur verfügbar, wenn **Allow alternative profile** (siehe oben) auf Y gesetzt ist. Wenn Sie möchten, dass jedes Mal ein Anmeldefehlersatz geschrieben wird, wenn der mit dem alternativen Profil definierte LDAP-Server anstelle des im Masterprofil definierten für die Authentifizierung verwendet wird, müssen Sie dieses Feld auf Y setzen. Anhand dieser Anmeldefehlersätze können Sie überprüfen, welcher LDAP-Server - Master oder alternativ - tatsächlich für die Authentifizierung verwendet wurde. Einzelheiten zu den Anmeldefehlersätzen finden Sie unter *Anmelde-/Gegenzeichnungsfehler*.
Alternative profile / Archived profile	Alternatives Profil / Archiviertes Profil. Diese Felder zeigen an, ob es sich um ein alternatives oder archiviertes Profil handelt. Sie werden nur angezeigt, wenn sie zutreffen.
Natural Security system	FSEC (kann nicht geändert werden).
Support user names as IDs	Benutzernamen als Kennungen unterstützen. Diese Option ermöglicht die Anmeldung mit dem Benutzernamen (wie im Sicherheitsprofil des Benutzers angegeben) als Benutzerkennung. Für diese Option sind drei Voraussetzungen zu erfüllen. Wenn sie aktiviert ist (indem Sie dieses Feld mit Y markieren), wird ein zusätzlicher Bildschirm angezeigt, auf dem Sie die folgenden Prüfungen durchführen müssen, um sicherzustellen, dass diese Voraussetzungen erfüllt sind: 1. **Adabas FDT FSEC-Systemdatei:** In der FDT der FSEC-Systemdatei muss das Feld mit dem Adabas-Kurznamen LI als Deskriptor definiert sein. Mit dieser Prüfung wird festgestellt, ob dies der Fall ist. Sollte dies nicht der Fall sein, wenden Sie sich an Ihren Adabas-Administrator.

Feld	Erläuterung
LDAP Options 1	
	2. **FSEC mittels Scan auf Eindeutigkeit der Namen prüfen:** X Alle Benutzersicherheitsprofile werden auf doppelte oder leere Benutzernamenseinträge geprüft. D Das Ergebnis der Prüfung wird angezeigt: Eine Liste aller Profile, in denen der Eintrag für den Benutzernamen entweder leer oder nicht eindeutig ist. W Die Ergebnisliste wird in die Arbeitsdatei 1 geschrieben. (Dies setzt voraus, dass die Arbeitsdatei zu Beginn der Natural Security-Sitzung gesetzt worden ist.) B Das Ergebnis der Prüfung wird sowohl angezeigt als auch in die Arbeitsdatei 1 geschrieben. 3. **Logon Exit LOGONSX1 in SYSLIB:** Der User Exit LOGONSX1 muss in der Bibliothek SYSLIB enthalten sein. Diese Prüfung verifiziert, ob dies der Fall ist. Wenn diese Option verwendet wird, enthält die Natural-Systemvariable *USER-NAME den Benutzernamen, der als Kennung für die Anmeldung verwendet wird, und die Systemvariable *USER die entsprechende Benutzerkennung, wie sie im Sicherheitsprofil des Benutzers definiert ist.
NSC user ID	NSC- Benutzerkennung. Diese Option steuert den Zugriff von Benutzern, die nicht in Natural Security definiert sind. N Die allgemeine **Transition Period Logon** (Übergangszeit für die Anmeldung) bestimmt, bei welchen Bibliotheken sich ein nicht definierter Benutzer anmelden darf. E Ein nicht definierter Benutzer kann sich nur bei ungeschützten Bibliotheken anmelden (nicht aber bei nicht definierten Bibliotheken), unabhängig von der Einstellung der Übergangszeit bei **Transition Period Logon**. Y Ein nicht definierter Benutzer kann sich bei keiner Bibliothek anmelden, unabhängig von der Einstellung der Übergangszeit bei **Transition Period Logon**. P Für alle nicht definierten Benutzer wird der Zugang zu Bibliotheken durch ein Benutzersicherheitsprofil mit der Kennung * LDAP * und dem Benutzertyp E bestimmt. Der Zugriff auf eine (geschützte oder nicht geschützte) Bibliothek ist nur möglich, wenn diese Kennung zu einer Gruppe hinzugefügt wird, die mit der Bibliothek verlinkt ist. Die Kennung selbst kann nicht explizit in der Anmeldeprozedur angegeben werden. Siehe auch ***Externer Benutzer***. Wenn Sie dieses Feld auf P setzen, wird dieses Benutzersicherheitsprofil automatisch hinzugefügt. Das Benutzersicherheitsprofil wird gelöscht, wenn Sie den Wert dieses Feldes von P auf einen anderen Wert ändern. Die Änderung dieses Benutzersicherheitsprofils wird in der Benutzerpflege durchgeführt. Der volle Funktionsumfang der Benutzerverwaltung ist für dieses Benutzersicherheitsprofil jedoch nicht verfügbar.

Feld	Erläuterung
LDAP Options 1	
Log file path	Pfad zur Protokolldatei. Der vollständige Pfad zu der Datei, in die die Protokolldaten geschrieben werden, wenn die Protokollierung der LDAP-Server-Kommunikation aktiv ist. Enthält der angegebene Pfad die Zeichenkette `*USER`, so wird diese durch den aktuellen Wert der Natural-Systemvariable `*USER` ersetzt.
Log level	Protokollierungsstufe. Mit diesem Feld wird die Protokollierung der LDAP-Server-Kommunikation aktiviert. Mögliche Werte: `0` Die Protokollierung ist nicht aktiv. `1` und `2` Die Protokollierung ist bei Fehlern aktiv. `3` and `4` Die Protokollierung ist zur Information aktiv. `5` and `6` Die Protokollierung ist zur Information beim Debugging aktiv. Weitere Informationen finden Sie in der *Software AG Security eXtensions (SSX)*-Dokumentation.
LDAP Options 2	
LDAP host	LDAP-Host. Die IP-Adresse oder der Domänenname des LDAP-Servers.
LDAP port	LDAP-Anschluss. Die Portnummer des LDAP-Servers. Die Standardeinstellung ist 389.
LDAP server type	Der Typ des LDAP-Servers. Mögliche Typen sind: ■ `OpenLDAP` ■ `ActiveDirectory` ■ `SunOneDirectory`
SSL connection	SSL-Verbindung. Markieren Sie dieses Feld mit `0`, wenn die LDAP-Verbindung über einen SSL-gesicherten Port hergestellt wird (standardmäßig ist dies Port 636). Sie können entweder dieses Feld oder das darunter befindliche Feld markieren, aber nicht beide.
Start TLS connection	TLS-Verbindung starten. Markieren Sie dieses Feld mit `0`, um zu versuchen, eine verschlüsselte Kommunikation über den normalen LDAP-Port aufzubauen, wenn der LDAP-Server dies unterstützt. Sie können entweder dieses Feld oder das obige Feld markieren, aber nicht beide.
Technical user support	Technische Benutzerunterstützung. Auf LDAP-Servern, die keine anonymen Anfragen unterstützen, können Sie die technischen Benutzeranmeldedateien verwenden, um LDAP-Benutzer auf sichere Weise zu suchen und zu finden. Informationen zur technischen Benutzerunterstützung finden Sie in der *Software AG Security eXtensions* (SSX)-Dokumentation unter *Creating Technical User Credential Files*. Die in dieser Dokumentation beschriebene Funktion `createTechUserCreds` wird verwendet, um die Eigenschafts- und Schlüsselwertdateien eines technischen Benutzers zu erstellen. Die Pfade zu diesen Dateien müssen in den folgenden Feldern angegeben werden:

Feld	Erläuterung
LDAP Options 1	
	Path to output file Pfad zur Ausgabedatei: Geben Sie den vollständigen Pfad zu der Datei an, die die Benutzerkennung und das verschlüsselte Passwort des „technischen Benutzers“ enthält. **Path to key file** Pfad zur Schlüsseldatei: Geben Sie den vollständigen Pfad zu der Datei an, die den Schlüsselwert enthält, der zur Entschlüsselung des Passworts des „technischen Benutzers“ verwendet wird. **Support AUTO=ON** `AUTO=ON` unterstützen. Markieren Sie dieses Feld mit `O`, wenn Sie möchten, dass Benutzerkennungen für Natural-Sitzungen, die mit dem Profilparameter `AUTO=ON` gestartet wurden, per LDAP überprüft werden. Diese Option setzt voraus, dass der „technischen Benutzer“ definiert wurde.
LDAP Options 3	
Default domain	Der Name der Standarddomäne.
LDAP person DN	Der Personal Bind Distinguished Name des Knotens, in dem sich die Benutzereinträge befinden. Beispiel: `ou=user,ou=germany,dc=sag` wobei `ou` für die Organisationseinheit und `dc` für die Domänenkomponente steht.
Attribute name user ID	Der Attributname, der die Benutzerkennung enthält.
Object class person	Die Objektklasse, die einen Benutzer bezeichnet.

PF-Tasten

Um die Funktion PF-Keys aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) den Menüeintrag **Administrator Services**.

Wenn Sie **berechtigt** sind, auf die Administrator Services zuzugreifen, wird das Menü **Administrator Services Menu 1** angezeigt.

2 Wählen Sie in diesem Menü den Eintrag **PF-keys**.

Der Bildschirm **Set PF-Keys** (PF-Tastenbelegung einstellen) wird angezeigt.

3 Auf diesem Bildschirm können Sie den Tasten Funktionen und Namen zuweisen, wie unten beschrieben.

Funktionen können nur bestimmten Tasten zugewiesen werden. Namen können allen Tasten zugewiesen werden.

PF-Tasten-Funktionen

Die den folgenden PF-Tasten zugewiesenen Funktionen können nicht geändert werden:

Taste	Funktion	Erläuterung
PF01	Help	Hilfe. Wenn Sie PF1 auf einem beliebigen Bildschirm von Natural Security drücken, werden Hilfeinformationen zu diesem Bildschirm angezeigt.
PF02	Previous Menu	Vorheriges Menü. Mit dieser Taste kehren Sie zu dem Menübildschirm zurück, von dem aus Sie die aktuelle Bearbeitungsebene aufgerufen haben. Standardmäßig werden die Änderungen, die Sie vor dem Verlassen einer Funktion mit PF2 vorgenommen haben, gespeichert; siehe auch die allgemeine Option **Exit Functions with Confirmation** (Beenden von Funktionen mit Bestätigung) weiter oben.
PF03	Exit	Beenden. Diese Taste bewirkt, dass eine bestimmte Verarbeitungsebene beendet und der Bildschirm der nächsthöheren Verarbeitungsebene angezeigt wird. Standardmäßig werden die Änderungen, die Sie vor dem Verlassen einer Funktion mit PF3 vorgenommen haben, gespeichert; siehe auch die allgemeine Option **Exit Functions with Confirmation** (Beenden von Funktionen mit Bestätigung) weiter oben.
PF04	Additional Options	Zusätzliche Optionen. Auf einem Sicherheitsprofilbildschirm können Sie diese Taste drücken (anstatt das Feld **Additional Options** auf dem Bildschirm mit Y zu markieren), um das Auswahlfenster **Additional Options** für ein Sicherheitsprofil anzuzeigen.
PF05		Verschiedene Funktionen auf verschiedenen Bildschirmen (wie ggf. dort beschrieben).
PF06	Flip	PF-Tastenzeile umschalten. Die PF-Tastenzeilen am unteren Rand der Natural Security-Bildschirme zeigen entweder die PF-Tasten 1 bis 12 oder die PF-Tasten 13 bis 24 an. Durch Drücken von PF6 können Sie von einer Anzeige zur anderen umschalten.
PF07	Previous Page (-)	Vorherige Seite (-). Mit dieser Taste blättern Sie in einer angezeigten Liste eine Seite zurück.
PF08	Next Page (+)	Nächste Seite (+). Mit dieser Taste blättern Sie in einer angezeigten Liste eine Seite vorwärts.
PF12	Cancel	Abbrechen. Mit dieser Taste wird eine bestimmte Verarbeitungsebene beendet und der Bildschirm der nächsthöheren Verarbeitungsebene angezeigt. Standardmäßig werden die Änderungen, die Sie vor dem Verlassen einer Funktion mit PF12 vorgenommen haben, gespeichert; siehe auch die allgemeine

Taste	Funktion	Erläuterung
		Option **Exit Functions with Confirmation** (Beenden von Funktionen mit Bestätigung) weiter oben.
PF13	Refresh	Wiederherstellen. Diese Taste macht alle Änderungen rückgängig, die Sie auf einem Bildschirm vorgenommen haben, die aber noch nicht gespeichert wurden. Die Felder auf dem Bildschirm werden auf die Werte zurückgesetzt, die sie hatten, bevor Sie sie geändert haben.
PF14		(reserviert für zukünftige Verwendung)
PF15	Menu	Menü. Diese Taste ruft das Hauptmenü (**Main Menu**) von Natural Security auf. Standardmäßig werden die Änderungen, die Sie vor dem Verlassen einer Funktion mit PF15 vorgenommen haben, gespeichert; siehe auch die allgemeine Option **Exit Functions with Confirmation** (Beenden von Funktionen mit Bestätigung) weiter oben.
PF16 bis PF17		Verschiedene Funktionen auf verschiedenen Bildschirmen (wie ggf. dort beschrieben).
PF18		(reserviert für zukünftige Verwendung)
PF19	First Page (- -)	Erste Seite (- -). Diese Taste blättert in einer angezeigten Liste an deren Anfang.
PF20 bis PF24		(reserviert für zukünftige Verwendung)

Anmerkung: Die Taste CLR hat die gleiche Funktion wie PF12.

PF09, PF10, PF11, PA1, PA2

Sie können jeder dieser Tasten selber eine Funktion zuweisen. Die zugewiesene Funktion kann dann innerhalb von Natural Security durch Drücken der entsprechenden PF-Taste (oder PA-Taste) aufgerufen werden.

Einer PF-Taste (oder PA-Taste) kann eine der folgenden Funktionen zugewiesen werden:

- ein Natural-Systemkommando,
- ein Natural-Terminalkommando,
- ein Natural-Programm.

Um einer Taste eine Funktion zuzuweisen, geben Sie in der Spalte **Function** des Bildschirms **Set PF-Keys** (PF-Tasten belegen) neben einer Tastennummer ein Kommando oder einen Programmnamen ein.

PF-Tastennamen

Sie können allen PF-Tasten einen Namen zuordnen, auch denjenigen, deren Funktionsbelegung Sie nicht ändern können. Die Namen dürfen bis zu 5 Zeichen lang sein und können in der Spalte **Name** des Bildschirms **Set PF-Keys** eingegeben werden.

Die zugewiesenen Namen erscheinen in den PF-Tasten-Zeilen, die am unteren Rand eines jeden Natural Security-Bildschirms angezeigt werden:

```
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help  PrevM Exit  AddOp       Flip  -     +                     Canc
```

Wenn bei einer PF-Taste kein Name angezeigt wird, bedeutet dies, dass die Funktion, die dieser Taste zugewiesen ist, bei dem angezeigten Bildschirm nicht anwendbar ist.

Die Zeilen zeigen entweder die Tasten PF1 bis PF12 oder die Tasten PF13 bis PF24. Durch Drücken von PF6 können Sie zwischen den beiden Anzeigen umschalten.

Anmelde-/Gegenzeichnungsfehler - Logon/Countersign Errors

Die Funktionen **Logon/Countersign Errors** (Anmelde-/Gegenzeichnungsfehler) dienen zwei Zwecken:

- Sie können damit *Anmeldefehler* (Logon Errors) anzeigen, d. h. erfolglose Versuche, sich bei Natural anzumelden.
- Sie können damit *gesperrte Benutzer* (Locked Users) anzeigen und entsperren, d. h. Benutzer, deren Benutzerkennungen aufgrund von Anmelde- oder Gegenzeichnungsfehlern ungültig geworden sind (wenn die **Lock User Option** aktiviert ist).

Anmeldefehler - Logon Errors

Unter **General Options** können Sie im Feld **Maximum number of logon attempts** die maximale Anzahl der Anmeldeversuche festlegen, indem Sie eine Zahl *n* im Bereich von 1 bis 9 eingeben (die Standardeinstellung ist 5). Jedes Mal, wenn ein Benutzer *n* aufeinanderfolgende erfolglose Anmeldeversuche unternimmt, wird der Benutzer "rausgeworfen" und Natural Security schreibt einen Datensatz, der in dieser Dokumentation als *Anmeldefehlersatz* bezeichnet wird.

Ein Anmeldefehlersatz enthält detaillierte Informationen zu jedem der *n* Anmeldeversuche, die zum Schreiben des Datensatzes geführt haben (z. B. welche Benutzer- und Bibliothekskennungen vom Benutzer eingegeben wurden). Sie können diese Datensätze mit den Funktionen zur Bearbeitung von Anmeldefehlern (**Logon Error Processing**) anzeigen. Dies dient den folgenden Zwecken:

- Sie können sehen, ob Unbefugte versucht haben, sich Zugang zu Natural zu verschaffen.

- Sie können sehen, was Benutzer falsch machen, wenn sie versuchen, sich anzumelden. Die Benutzer können dann darüber informiert werden, wie sie sich korrekt anmelden können.
- Sie können sehen, ob die Benutzer die richtigen Zugriffsrechte erhalten haben. Zum Beispiel kann ein Benutzer versuchen, sich bei einer Bibliothek anzumelden, für die er nicht berechtigt ist, die er aber benutzen können sollte. Sie können dann die erforderlichen Anpassungen an den betreffenden Sicherheitsprofilen und Links vornehmen.

Die Aufzeichnung von Anmeldefehlern durch Natural Security kann nicht abgeschaltet werden.

Fehler beim Zugriff auf Dienstprogramme (Utilities)

Auch fehlgeschlagene Versuche, auf ein Natural-Dienstprogramm zuzugreifen, werden von Natural Security aufgezeichnet. Diese Utility-Zugriffsfehlerprotokolle können auch mit den **Logon/Countersign Errors**-Funktionen eingesehen werden.

Anmerkung: Der Begriff *Anmeldefehler(-sätze)*, wie er im folgenden Text verwendet wird, umfasst auch *Dienstprogramm-Zugriffsfehler(-sätze)*, sofern nicht ausdrücklich anders angegeben.

Locked Users

Wenn die Option **Lock User Option** (Benutzer sperren, siehe *Allgemeine Optionen - General Options*) aktiviert ist, können Benutzer aufgrund von Anmelde- oder Gegenzeichnungsfehlern "gesperrt" werden:

- **Anmeldefehler:**
  Wenn ein Benutzer die maximale Anzahl von Anmeldeversuchen erreicht hat, ohne dabei das richtige Passwort einzugeben, wird dieser Benutzer gesperrt.
- **Gegenzeichnungsfehler:**
  Nach Eingabe von zu vielen ungültigen Passwörtern auf einem **Countersignature**-Bildschirm wird der Benutzer, der die Funktion, für die die Gegenzeichnung erforderlich ist, aufgerufen hat, gesperrt (Informationen zu Countersignatures finden Sie im Kapitel *Gegenzeichnungen*).

Mit der Funktion **List/Unlock Locked Users** (Gesperrte Benutzer auflisten/entsperren) können Sie sehen, welche Benutzer aufgrund von Anmelde- oder Gegenzeichnungsfehlern gesperrt wurden. Sie können sie auch wieder entsperren.

Gegenzeichnungsfehler werden nur erfasst, wenn die **Lock User Option** aktiv ist, während Anmeldefehler immer erfasst werden (unabhängig von der **Lock User Option**).

Menü Logon/Countersign Errors aufrufen

Um das Menü Logon/Countersign Errors aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) den Menüeintrag **Administrator Services**.

Wenn Sie **berechtigt** sind, auf die Administrator Services zuzugreifen, wird das Menü **Administrator Services Menu 1** angezeigt.

2 Wählen Sie in diesem Menü die Option **Logon/countersign errors**.

Das zugehörige Menü wird angezeigt. Es bietet die folgenden Funktionen:

Funktion	Beschreibung siehe:
List error records	*Fehlersätze auflisten*
Delete error records	*Fehlersätze löschen*
Display individual error records	*Einzelne Fehlersätze anzeigen*
List/unlock locked users	*Gesperrte Benutzer auflisten/entsperren*

Die einzelnen Funktionen werden im Folgenden beschrieben.

Optionen im Menü Logon/Countersign Errors

Wenn Sie eine dieser Funktionen auswählen, können Sie die folgenden Optionen festlegen:

Option	Erläuterung
Order of Records	Reihenfolge der Datensätze. Diese Option bestimmt die Reihenfolge, in der die Anmeldefehlersätze aufgelistet werden:
	`T` Die Datensätze werden in der Reihenfolge der Terminalkennungen aufgeführt (wie durch die Natural-Systemvariable `*INIT-ID` definiert). Bei Anmeldefehlern im Zusammenhang mit Natural RPC und Natural Web I/O Service Requests wird `RPCSRVRQ` bzw. `NWOSRVRQ` anstelle des `*INIT-ID`-Werts verwendet.) `TY` Wie `T`, nur für Fehlersätze im Zusammenhang mit dem Zugriff auf ein Dienstprogramm (Utility). `P` Die Datensätze werden in der Reihenfolge der Benutzerkennungen (wie durch die Natural-Systemvariable `*INIT-USER` definiert) angeordnet. `PY` Wie `P`, nur für Fehlersätze im Zusammenhang mit dem Zugriff auf ein Dienstprogramm (Utility). `D` Die Datensätze werden in der Reihenfolge des Datums aufgelistet (d. h. der Daten, an denen die Fehler aufgetreten sind). `DT` Wie `D`, wobei das Feld **Start Value** (Startwert) ausgewertet wird, um die Liste auf bestimmte Terminalkennungen (`*INIT-ID`) zu beschränken.

Option	Erläuterung
	DP Wie D, wobei das Feld **Start Value** (Startwert) ausgewertet wird, um die Liste auf bestimmte Benutzerkennungen zu beschränken (*INIT-USER). Diese Option hat keinen Einfluss auf die Funktion **List/Unlock Locked Users**.
Start Value	Startwert. Wenn Sie nicht alle, sondern nur einen bestimmten Bereich von Anmeldefehlersätzen oder gesperrten Benutzern auflisten möchten, können Sie einen Startwert angeben. Mögliche Optionen können Sie durch Eingabe eines Fragezeichens (?) in diesem Feld ermitteln. Spezielle Startwerte (bei Order of Records = T): ■ RPCSRVRQ - um Anmeldefehler aufzulisten, die in Verbindung mit Natural RPC Service Requests aufgetreten sind. ■ NWOSRVRQ - um Anmeldefehler aufzulisten, die in Verbindung mit Natural Web I/O Service Requests aufgetreten sind. Dieses Feld wird bei Order of Records = D ignoriert.
Date from ... to	Datum von ... bis. Diese beiden Felder können Sie verwenden, wenn Sie nur Datensätze von Anmelde-/Gegenzeichnungsfehlern auflisten möchten, die an einem bestimmten Datum oder innerhalb eines bestimmten Datumsbereichs aufgetreten sind. Mögliche Optionen können Sie durch Eingabe eines Fragezeichens (?) in eines dieser Felder ermitteln. Wenn **Date from** einen Platzhalter (*, > oder <) enthält, gilt Folgendes: ■ **Date to** und **Time to** werden ignoriert. ■ Wenn **Time from** eine bestimmte Zeit enthält, werden nur Fehler aufgelistet, die an jedem Tag des Datumsbereichs zu dieser Zeit aufgetreten sind. Wenn dies nicht erwünscht ist, können Sie einen Platzhalter in **Time from** verwenden, um einen Zeitbereich anzugeben. Spezielle Werte für **Date from**: YEAR - Es werden nur Fehler aufgelistet, die im aktuellen Jahr aufgetreten sind. MONTH - Es werden nur Fehler aufgelistet, die im aktuellen Monat aufgetreten sind. TODAY - Es werden nur Fehler aufgelistet, die am aktuellen Tag aufgetreten sind. YESTERDAY - Es werden nur Fehler aufgelistet, die am Vortag des aktuellen Tages aufgetreten sind.
Time from ... to	Sie können diese beiden Felder verwenden, wenn Sie nur Datensätze von Anmelde-/Gegenzeichnungsfehlern auflisten möchten, die in einem bestimmten Zeitraum aufgetreten sind. Mögliche Optionen können Sie durch Eingabe eines Fragezeichens (?) in eines dieser Felder ermitteln. Wenn das Feld **Date from** ein bestimmtes Datum enthält, bezieht sich der Wert für **Time from** auf die Zeit an diesem Datum. Wenn **Date to** ein bestimmtes Datum enthält, bezieht sich der Wert für **Time to** auf die Zeit an diesem Datum. Wenn **Time from** einen Platzhalter (*, > oder <) enthält, werden **Date to** und **Time to** ignoriert.

Option	Erläuterung
FUSER DBID/FNR	Wenn Sie nur Sätze mit Anmeldefehlern auflisten möchten, die in Verbindung mit Anmeldeversuchen bei einer bestimmten FUSER-Systemdatei aufgetreten sind, können Sie in diesen Feldern deren Datenbankkennung und Dateinummer angeben.

Fehlersätze auflisten - List Error Records

Die Funktion **List Error Records** zeigt eine Liste der Anmeldefehler an.

In der Liste kann geblättert werden, siehe Kapitel *Grundlagen der Benutzung*.

Sie können den Bereich der aufgelisteten Fehlersätze ändern, indem Sie Auswahlkriterien in die Eingabefelder oberhalb der Liste eingeben. Mögliche Optionen können Sie durch Eingabe eines Fragezeichens (?) in das betreffende Feld ermitteln.

Zusätzlich sind die folgenden speziellen PF-Tasten verfügbar:

Taste	Erläuterung
PF06	Nur Dienstprogrammzugriffsfehlersätze auflisten. (Durch erneutes Drücken wird wieder die Liste aller Fehlersätze angezeigt).
PF09	Auflistung der Fehlersätze sortiert nach Terminalkennung (`*INIT-ID`).
PF10	Auflistung der Fehlersätze sortiert nach Benutzerkennung (`*INIT-USER`).
PF11	Auflistung der Fehlersätze sortiert nach Datum.

Um detaillierte Informationen zu einem Fehlersatz anzuzeigen, müssen Sie ihn mit dem Code `DI` markieren. Es wird die Fehlerhistorie des markierten Fehlers aufgerufen (wie bei der Funktion **Display Individual Error Records**; siehe unten).

Fehlersätze löschen - Delete Error Records

Die Funktion **Delete Error Records** zeigt eine Liste der Anmeldefehlersätze an, so wie die oben beschriebene Funktion **List Error Records** (Fehlersätze auflisten). Die Optionen zum Bearbeiten der Liste sind dieselben wie bei der Funktion **List Error Records**. Darüber hinaus können Sie Anmeldefehlersätze löschen.

Es wird empfohlen, Anmeldefehlersätze periodisch zu löschen, um Platz in der FSEC-Systemdatei zu sparen.

- Um einzelne Fehlersätze zu löschen, können Sie diese mit dem Code `DE` markieren.
- Um alle auf der aktuellen Seite angezeigten Fehlersätze zu löschen, müssen Sie PF4 drücken.
- Um alle vorhandenen Fehlersätze zu löschen, können Sie das Direktkommando `ERRDEL` verwenden (siehe unten).
- Um selektiv eine größere Anzahl von Fehlersätzen zu löschen, können Sie die Anwendungsprogrammierschnittstelle `NSCADM` verwenden.

Wenn ein Fehlersatz gelöscht wurde, wird dies durch ## in der ersten Spalte der Liste angezeigt.

Direktkommando ERRDEL

Um alle Anmelde-/Gegenzeichnungsfehlersätze auf einmal zu löschen, können Sie das Direktkommando ERRDEL in der Kommandozeile eingeben.

Einzelne Fehlersätze anzeigen - Display Individual Error Records

Die Funktion **Display Individual Error Records** zeigt die Fehlerhistorie (**Error History**) der Anmeldefehlersätze nacheinander an.

Um einen Fehlersatz zu löschen, müssen Sie im **Error History**-Bildschirm des Fehlersatzes PF4 drücken.

Gesperrte Benutzer auflisten/entsperren - List/Unlock Locked Users

Die Funktion **List/Unlock Locked Users** ist nur anwendbar, wenn die Option **Lock User Option** (siehe *Allgemeine Optionen*) aktiv ist. Sie zeigt eine Liste der Benutzer an, deren Sicherheitsprofile aufgrund von Anmelde- oder Gegenzeichnungsfehlern „gesperrt“ wurden. Die Liste ist in alphabetischer Reihenfolge der Benutzerkennungen geordnet. In der Liste können Sie dann einzelne Benutzer entsperren.

Wenn Sie die Funktion **List/Unlock Locked Users** aufrufen, wird der Bildschirm **List Locked Users** (Gesperrte Benutzer auflisten) angezeigt.

In der Liste kann geblättert werden, siehe Kapitel *Grundlagen der Benutzung*.

Sie können den Bereich der aufgelisteten Benutzer ändern, indem Sie Auswahlkriterien in die Eingabefelder oberhalb der Liste eingeben. Mögliche Optionen können Sie durch Eingabe eines Fragezeichens (?) in das oder die betreffenden Felder ermitteln.

Die Spalte **Lock** im Bildschirm **List Locked Users** zeigt den Typ des Fehlers an, der zur Sperrung des Benutzers geführt hat:

Fehlertyp	Bedeutung	Daneben angezeigte Informationen
C	Countersign error	Gegenzeichnungsfehler. Die Kennung des Eigentümers, dessen Kennwort falsch eingegeben wurde, und die Kennung des Objekts, das der gesperrte Benutzer zu ändern versucht hat.
L	Logon error	Anmeldefehler. Die Fehlernummern
X	Anmeldung des Benutzers, nachdem seine Benutzerkennung automatisch entsperrt wurde.	Eine der obigen Angaben, abhängig von dem ursprünglichen Fehlertyp.

Informationen zur automatischen Entsperrung finden Sie unter der Option **Automatically unlock users after** (Benutzer automatisch entsperren nach) in *User Preset Values*.

Die folgenden Funktionen sind verfügbar, wenn Sie einen Eintrag auf dem Bildschirm **List Locked Users** mit einem der folgenden Funktionscodes markieren:

Code	Funktion
DI	Ausführliche Informationen zu einem Eintrag anzeigen.
UL	Einen Benutzer entsperren. Es wird ein Fenster angezeigt, in dem Sie die Entsperrung durch Eingabe eines Y bestätigen müssen (gilt nicht für Fehler vom Typ 0).
DE	Eintrag löschen. (Gilt nur für Fehler des Typs 0.)

Anmerkung: Sie können auch die Funktion **Modify User** (siehe *Benutzer verwalten*) verwenden, um einen gesperrten Benutzer zu entsperren.

Anmeldesätze - Logon Records

Anhand der Anmeldesätze können Sie sehen, welche Benutzer welche Bibliotheken benutzt haben.

Sie können die Option **Logon recorded** im Sicherheitsprofil jeder Bibliothek und jedes Benutzers angeben (siehe Kapitel *Bibliotheken verwalten* bzw. *Benutzer verwalten*).

Natural Security schreibt einen Anmeldesatz:

- jedes Mal, wenn sich ein Benutzer bei einer Bibliothek anmeldet, in deren Sicherheitsprofil die Option **Logon recorded** auf Y gesetzt ist;
- jedes Mal, wenn sich ein Benutzer, in dessen Sicherheitsprofil die Option **Logon recorded** auf Y gesetzt ist, bei einer beliebigen Bibliothek anmeldet.

Wenn die allgemeine Option **Transition Period Logon** auf Y gesetzt ist, wird auch bei jeder Anmeldung eines nicht definierten Benutzers (unabhängig von der Einstellung der Option **Logon recorded**) und bei jeder Anmeldung eines Benutzers bei einer nicht definierten Bibliothek ein Anmeldesatz geschrieben.

Wenn der Benutzersicherheitsprofileintrag **ETID** in den **User Preset Values** auf S gesetzt ist, wird auch bei jeder Anmeldung eines Benutzers bei Natural ein Anmeldesatz - mit zeitstempelbezogener ETID - geschrieben (dies ist nur möglich, wenn die FSEC-Systemdatei nicht schreibgeschützt ist). In diesem Fall gibt der Anmeldesatz nur Auskunft darüber, welche ETID von welcher Benutzerkennung verwendet wurde, er enthält jedoch keine Bibliotheksinformationen.

In ähnlicher Weise wird von Natural Security jedes Mal ein Zugriffssatz geschrieben, wenn ein Benutzer ein Dienstprogramm (Utility) aufruft, in dessen Standardsicherheitsprofil die Option **Access recorded** auf Y gesetzt ist.

Sie können diese Anmelde-/Zugriffssätze mit den Funktionen **Logon records** einsehen.

Anmerkung: Sofern nicht ausdrücklich anders angegeben, bezeichnet der Begriff „Anmeldesätze“ im folgenden Text sowohl Anmeldedatensätze als auch Zugriffsdatensätze.

Anmeldesätze aufrufen

Um Anmeldesätze aufzurufen:

1 Wählen Sie im Hauptmenü **Main Menu**() den Menüeintrag **Administrator Services**.

Wenn Sie **berechtigt** sind, auf die Administrator Services zuzugreifen, wird das Menü **Administrator Services Menu 1** angezeigt.

2 Wählen Sie in dem Menü die Option **Logon Records**.

Das **Logon Records Menu** wird angezeigt. Es bietet die folgenden Funktionen:

Funktion	Beschreibung
List logon records	*Anmeldesätze auflisten*
Delete logon records	*Anmeldesätze löschen*
Delete logon records but last	*Anmeldesätze löschen, außer dem letzten*

Die einzelnen Funktionen werden im Folgenden beschrieben.

Optionen im Menü Logon Records

Wenn Sie eine dieser Funktionen auswählen, können Sie die folgenden Auswahloptionen festlegen:

Option	Erläuterung	
Order of Records	U	Auflistung der Anmeldesätze in alphabetischer Reihenfolge der Benutzerkennungen.
	UX	Wie U, jedoch werden nur die Anmeldesätze von nicht definierten Benutzern aufgelistet.
	L	Auflistung der Anmeldesätze in alphabetischer Reihenfolge der Bibliothekskennungen.
	LX	Wie L, jedoch werden nur Anmeldesätze zu nicht definierten Bibliotheken aufgelistet.
	Y	Auflistung der Dienstprogramm-Zugriffssätze in alphabetischer Reihenfolge der Dienstprogramm-Namen.
	UY	Auflistung der Dienstprogramm-Zugriffssätze in alphabetischer Reihenfolge der Benutzerkennungen.

Option	Erläuterung	
	LY	Auflistung der Dienstprogramm-Zugriffssätze in alphabetischer Reihenfolge der Bibliothekskennungen.
	UE	Liste der ETID-bezogenen Anmeldesätze in alphabetischer Reihenfolge der Benutzerkennungen.
	EU	Auflistung der ETID-bezogenen Anmeldesätze in aufsteigender Reihenfolge der ETIDs.
	D	Auflistung der Anmeldedatensätze in chronologischer Reihenfolge des Datums/der Uhrzeit, zu der die Anmeldungen erfolgten.
Start Value	Startwert. Wenn Sie nicht alle, sondern nur einen bestimmten Bereich von Anmeldesätzen auflisten möchten, können Sie einen Startwert angeben. Mögliche Optionen können Sie durch Eingabe eines Fragezeichens (?) in diesem Feld ermitteln.	
ETID Start Value	ETID-Startwert In diesem Feld können Sie einen Startwert im hexadezimalen Format angeben (nur bei Order of Records (Satzreihenfolge) = UE und EU= UE und EU).	
Date from ... to	Datum von ... bis. Diese beiden Felder können Sie verwenden, wenn Sie nur Anmeldesätze von Anmeldungen auflisten möchten, die an einem bestimmten Datum oder innerhalb eines bestimmten Datumsbereichs stattgefunden haben. Mögliche Optionen können Sie durch Eingabe eines Fragezeichens (?) in eines der Felder ermitteln. Wenn **Date from ... to** einen Platzhalter (*, > oder <) enthält, gilt Folgendes: ■ **Date to** und **Time to** werden ignoriert. ■ Wenn **Time from** eine bestimmte Uhrzeit enthält, werden nur Anmeldungen aufgelistet, die an jedem Tag des Datumsbereichs zu dieser Uhrzeit stattfanden. Wenn dies nicht erwünscht ist, müssen Sie einen Platzhalter in **Time from** verwenden, um einen Zeitbereich anzugeben. Spezielle Werte für **Date from**: YEAR - Es werden nur Anmeldungen aufgelistet, die im aktuellen Jahr stattgefunden haben. MONTH - Es werden nur Anmeldungen aufgelistet, die im aktuellen Monat stattgefunden haben. TODAY - Es werden nur Anmeldungen aufgelistet, die am aktuellen Tag stattgefunden haben. YESTERDAY - Es werden nur Anmeldungen aufgelistet, die am Vortag des aktuellen Tages stattgefunden haben.	
Time from ... to	Zeit von ... bis. Diese beiden Felder können Sie verwenden, wenn Sie nur Anmeldesätze von Anmeldungen auflisten möchten, die innerhalb einer bestimmten Zeitspanne stattgefunden haben. Mögliche Optionen können Sie durch Eingabe eines Fragezeichens (?) in eines der Felder ermitteln. Wenn das Feld **Date from** ein bestimmtes Datum enthält, bezieht sich der Wert in **Time from** auf die Uhrzeit an diesem Datum. Wenn **Date to** ein bestimmtes Datum enthält, bezieht sich der Wert in **Time to** auf die Uhrzeit an diesem Datum. Wenn **Time from** einen Platzhalter (*, > oder <) enthält, werden **Date to** und **Time to** ignoriert.	

Option	Erläuterung
FUSER DBID/FNR	Wenn Sie nur Anmeldesätze von Anmeldungen bei einer bestimmten FUSER-Systemdatei auflisten möchten, müssen Sie in diesen Feldern deren Datenbankkennung und Dateinummer angeben.

Anmeldesätze auflisten - List Logon Records

Die Funktion **List Logon Records** zeigt eine Liste der Anmeldesätze an.

In der Liste kann geblättert werden, siehe Kapitel *Grundlagen der Benutzung*.

Sie können den Bereich der aufgelisteten Anmeldesätze ändern, indem Sie Auswahlkriterien in die Eingabefelder oberhalb der Liste eingeben. Für mögliche Optionen können Sie ein Fragezeichen (?) in das/die jeweilige(n) Eingabefeld(er) eingeben.

Darüber hinaus stehen Ihnen die folgenden speziellen PF-Tastenfunktionen zur Verfügung:

Taste	Erläuterung
PF06	Nur Dienstprogramm-Zugriffssätze auflisten. (Durch erneutes Drücken wird wieder die Liste aller Anmeldesätze angezeigt.)
PF09	Anmeldesätze nach Benutzerkennung sortiert auflisten.
PF10	Anmeldesätze nach Bibliothekskennung sortiert auflisten.
PF11	Anmeldesätze nach Datum sortiert auflisten.

Anmeldesätze löschen - Delete Logon Records

Die Funktion **Delete Logon Records** zeigt eine Liste von Anmeldesätzen an, so wie die oben beschriebene Funktion **List Logon Records**. Die Optionen zum Bearbeiten der Liste sind dieselben wie bei der genannten Funktion. Darüber hinaus können Sie Anmeldesätze löschen.

Es wird empfohlen, die Anmeldesätze regelmäßig zu löschen, um Platz in der FSEC-Systemdatei zu sparen.

- Um einzelne Anmeldesätze zu löschen, müssen Sie diese mit dem Code `DE` markieren.
- Um alle auf der aktuellen Seite angezeigten Anmeldesätze zu löschen, müssen Sie PF4 drücken.

  Wenn Sie im Menü **Logon Records** die Funktion **Delete Logon Records** durch Drücken von PF4 (Del+) anstelle von ENTER aufgerufen haben, wird durch Drücken von PF4 in der Liste sofort nach dem Löschen automatisch zur nächsten Seite geblättert, ohne dass Sie PF8 drücken müssen.
- Um alle vorhandenen Anmeldesätze zu löschen, können Sie das Direktkommando `LOGDEL` verwenden (siehe unten).
- Um selektiv eine größere Anzahl von Anmeldesätzen zu löschen, können Sie die Anwendungsprogrammierschnittstelle `NSCADM` verwenden.

Wurde ein Anmeldesatz gelöscht, so wird dies durch ## in der ersten Spalte der Liste angezeigt (außer bei PF4 (Del+)).

Direktkommando LOGDEL

Um alle Anmeldesätze auf einmal zu löschen, können Sie das Direktkommando LOGDEL in der Kommandozeile eingeben.

Anmeldesätze löschen, außer dem letzten

Die Funktion **Delete Logon Records But Last** entspricht der oben beschriebenen Funktion **Delete Logon Records**. Die einzige Löschmöglichkeit besteht jedoch darin, PF4 zu drücken. In diesem Fall werden alle auf der aktuellen Seite angezeigten Anmeldesätze gelöscht - mit Ausnahme des letzten Eintrags für jede Benutzerkennung auf der aktuellen Seite.

Verwaltungsprotokollsätze verwalten - Maintenance Log Records

Die Funktionen unter **Maintenance Log Records** können nur verwendet werden, wenn die allgemeine Option **Logging of Maintenance Functions** aktiviert wurde. Wenn diese Option aktiviert ist, werden Protokollsätze geschrieben, wenn Sicherheitsprofile und Administrator Services-Einstellungen geändert werden. Durch das Schreiben von Protokollsätzen können Sie feststellen, wer welche Sicherheitsprofile und Administrator Services-Einstellungen geändert hat. „Ändern“ umfasst in diesem Zusammenhang alle Verwaltungsfunktionen, die auf ein Sicherheitsprofil angewandt werden (einschließlich Anlegen, Kopieren, Löschen, Verlinken usw.). Dazu gehört auch die Übertragung eines Sicherheitsprofils mit den Programmen SECULD2 und SECLOAD.

Um die Protokollsätze einzusehen, können Sie die Funktionen unter **Maintenance Log Records** verwenden.

Um diese Funktionen aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) den Eintrag **Administrator Services**.

Wenn Sie **berechtigt** sind, auf die Administrator Services zuzugreifen, wird das Menü **Administrator Services Menu 1** angezeigt.

2 Wählen Sie in diesem Menü die Option **Maintenance Log Records**.

Es wird ein Menü angezeigt, in dem Sie die in den folgenden Abschnitten beschriebenen Funktionen auswählen können:

- Status der Protokollierungsfunktion anzeigen - Display Status of Logging Function
- Verwaltungsprotokolle der Administrator Services auflisten - List Administrator Services Maintenance Logs
- Sicherheitsprofil-Verwaltungsprotokolle auflisten - List Security Profile Maintenance Logs

- Protokolldateien verwalten - Log File Maintenance
- Letzte Anmeldesätze auflisten - List Last Logon Records

Status der Protokollierungsfunktion anzeigen - Display Status of Logging Function

Die Funktion **Display Status of Logging Function** zeigt die folgenden Informationen an:

- für welche Objekttypen Protokollsätze geschrieben werden,
- die Anzahl der Protokollsätze, die zu jedem Objekttyp geschrieben wurden,
- ob die Option **Logging even if no actual modification** (Protokollierung auch ohne tatsächliche Änderung)" gesetzt ist oder nicht.

Anmerkung: Bei dieser Funktion brauchen Sie nur den Funktionscode einzugeben, die anderen Optionen des Menüs haben keine Auswirkung.

Verwaltungsprotokolle der Administrator Services auflisten - List Administrator Services Maintenance Logs

Die Funktion **List Administrator Services Maintenance Logs** zeigt eine Liste der Protokollsätze an, die bei Änderungen an den Einstellungen der Administrator Services geschrieben wurden.

Menüoptionen bei dieser Funktion	Erläuterung
Modifier	Änderer. Um nur die Änderungen aufzulisten, die von einem bestimmten Administrator durchgeführt wurden, können Sie in diesem Feld seine Benutzerkennung angeben.
Date from/to	Datum von/bis. Standardmäßig enthalten diese Felder beide das aktuelle Datum, d.h. es werden nur die heute geschriebenen Protokollsätze aufgelistet. Um ältere Protokollsätze aufzulisten, können Sie die Datumswerte in diesen Feldern wie gewünscht ändern.
Time from/to	Zeit von/bis. Um nur Protokollsätze aufzulisten, die innerhalb einer bestimmten Zeitspanne geschrieben wurden, können Sie in diesen Feldern die gewünschte Zeitspanne angeben (Format Stunden:Minuten:Sekunden).
Ascending/Descending	Aufsteigend/Absteigend. Sie können wählen, ob die Protokolleinträge in aufsteigender oder absteigender chronologischer Reihenfolge aufgelistet werden sollen.

Anmerkung: Die anderen im Menü angebotenen Optionen sind bei dieser Funktion nicht anwendbar. Sie haben keine Wirkung, wenn sie angegeben werden.

In der angezeigten Liste werden zu jedem Protokolleintrag folgende Informationen angezeigt: die ausgeführte Administrator Services-Funktion, die Kennung des Benutzers, der die Änderung vorgenommen hat, sowie das Datum und die Uhrzeit der Änderung.

In der Liste können Sie einen Protokollsatz mit einem beliebigen Zeichen markieren: Der Bildschirm, auf dem die Änderung vorgenommen wurde, wird dann angezeigt; auf diesem Bildschirm werden die Felder, deren Werte geändert wurden, hervorgehoben dargestellt. Auf dem Bildschirm werden auch die Natural Security-Version und die FSEC-Systemdatei angezeigt, mit/in der die Änderung vorgenommen wurde.

Sicherheitsprofil-Verwaltungsprotokolle auflisten - List Security Profile Maintenance Logs

Die Funktion **List Security Profile Maintenance Logs** zeigt die Protokollsätze an, die bei Änderungen an Sicherheitsprofilen geschrieben wurden.

Menu Options for this Function	Erläuterung
Object type	Objekttyp. In diesem Feld können Sie den Typ des Objekts (USer, LIbrary usw.) angeben, dessen geänderte Sicherheitsprofile aufgelistet werden sollen. Wenn Sie das Feld leer lassen oder ein Fragezeichen (?) eingeben, wird ein Fenster angezeigt, in dem Sie den gewünschten Objekttyp auswählen können. Wenn Sie einen Stern (*) eingeben, werden alle Protokollsätze für alle Sicherheitsprofile aufgelistet.
Start value	Startwert. In diesem Feld können Sie eine Objektkennung als Startwert für die anzuzeigende Liste eingeben.
Modifier	Änderer. Um nur die Änderungen aufzulisten, die ein bestimmter Administrator vorgenommen hat, können Sie in diesem Feld seine Benutzerkennung angeben.
Date from/to	Datum von/bis. Standardmäßig enthalten diese Felder beide das aktuelle Datum, d.h. es werden nur die heute geschriebenen Protokollsätze aufgelistet. Um ältere Protokollsätze aufzulisten, ändern Sie die Datumswerte in diesen Feldern wie gewünscht.
Time from/to	Zeit von/bis. Um nur Protokolleinträge aufzulisten, die innerhalb eines bestimmten Zeitraums geschrieben wurden, können Sie in diesen Feldern die gewünschte Zeitspanne angeben (Format Stunden:Minuten:Sekunden).
Function	Funktion. Standardmäßig werden die für alle durchgeführten Verwaltungsfunktionen geschriebenen Protokollsätze aufgelistet. Um nur Protokollsätze aufzulisten, die für eine bestimmte Funktion geschrieben wurden (z.B. Ändern, Löschen, Umbenennen), können Sie die gewünschte Funktion in diesem Feld angeben. Die Funktionen können mit den ersten beiden Buchstaben abgekürzt werden (z.B. MO für Modify/Ändern). Um eine Auswahlliste der verfügbaren Funktionen zu erhalten, können Sie in diesem Feld ein Fragezeichen (?) eingeben.
Ascending/Descending	Aufsteigend/Absteigend. Sie können wählen, ob Sie die Protokollsätze in aufsteigender oder absteigender chronologischer Reihenfolge aufgelistet haben möchten.
Display modification	Änderung anzeigen. Mit dieser Option können Sie sich die tatsächlichen Änderungen, die in den Sicherheitsprofilen vorgenommen wurden, hervorgehoben anzeigen lassen; analog zu PF2 im Sicherheitsprofil-Bildschirm (siehe unten).

In der angezeigten Liste werden zu jedem Protokollsatz folgende Informationen angezeigt: die Funktion, die an dem Sicherheitsprofil ausgeführt wurde, die Kennung des Sicherheitsprofils, die Kennung des Benutzers, der die Änderung vorgenommen hat, sowie das Datum und die Uhrzeit der Änderung.

In der Liste können Sie einen Protokolleintrag mit einem beliebigen Zeichen markieren: Das Sicherheitsprofil, in dem die Änderung vorgenommen wurde, wird dann angezeigt. Wenn Sie auf dem Bild des Sicherheitsprofils PF2 drücken, werden die Felder, deren Werte geändert wurden, hervorgehoben angezeigt (und ggf. wird in einer Meldung angegeben, ob tatsächlich eine Änderung vorgenommen wurde oder nicht). Auf dem Bildschirm werden auch die Natural Security-Version und die FSEC-Systemdatei angezeigt, mit/in der die Änderung vorgenommen wurde.

Protokolldateien verwalten - Log File Maintenance

Auf z/OS und Open Systems kann diese Funktion nur im Batch-Modus verwendet werden.

Mit der Funktion **Log File Maintenance** können Sie den Inhalt der Protokolldatei in eine Arbeitsdatei (Work File) schreiben bzw. aus dieser lesen.

Protokollsätze müssen in eine Arbeitsdatei geschrieben werden, wenn die Protokolldatei voll ist. Die Arbeitsdatei dient also als „Archiv“ für die Protokollsätze.

Die zu verwendenden Arbeitsdateien sind Work File 1 und Work File 5. Unter Linux und Windows muss die Arbeitsdatei 5 eine Datei mit der Erweiterung `.sag` sein.

Die Ausgabereports werden in die Druckdateien `CMPRT01` und `CMPRT02` geschrieben.

Wenn Sie diese Funktion aufrufen, werden Sie aufgefordert, die Datenbankkennung und die Dateinummer der Protokolldatei anzugeben. Wenn Sie später eine andere Protokolldatei angeben möchten, können Sie PF5 im Menü **Log File Maintenance** drücken.

Wenn Sie diese Funktion aufrufen, wird das Menü **Logfile Maintenance** angezeigt, in dem Sie die folgenden Funktionen auswählen können:

Code	Funktion	Erläuterung
`LI`	List Log Records	Mit dieser Funktion wird der Inhalt der Protokolldatei aufgelistet. Die Ausgabe enthält die gleichen Informationen wie die Funktion **List Security Profile Maintenance Logs**: eine Liste aller geänderten Profile/Einstellungen sowie jedes betroffene Profil (mit Angabe der Profilbestandteile, die geändert wurden). Die Ausgabe besteht aus zwei Reports: ■ der Report **List of History Log Entries** wird in die Druckdatei `CMPRT01` geschrieben, ■ der Report **Detail History Log Entries** wird in die Druckdatei `CMPRT02` geschrieben.

Code	Funktion	Erläuterung
LX	List Log Records Extended	Wie **List Log Records** - zusätzlich zeigt diese Funktion die zusätzlichen Daten an, die protokolliert werden, wenn die erweiterte Protokollierung für Benutzer- oder Bibliothekssicherheitsprofile aktiviert ist; siehe *Erweiterte Protokollierung - Extended Logging* unter ***Verwaltungsfunktionen protokollieren - Logging of Maintenance Functions***.
WR	Write Log Records to Work File	Mit dieser Funktion werden Protokollsätze aus der Protokolldatei in die Arbeitsdatei 5 geschrieben (ohne sie aus der Protokolldatei zu löschen).
WD	Write Log Records to Work File and Delete	Mit dieser Funktion werden Protokollsätze aus der Protokolldatei in die Arbeitsdatei 5 geschrieben und aus der Protokolldatei gelöscht.
RA	Read Log Records from Work File	Mit dieser Funktion werden Protokollsätze aus Arbeitsdatei 5 in die Protokolldatei gelesen.
SA	Scan Work File	Mit dieser Funktion wird der Inhalt von Arbeitsdatei 5 gescannt.

Die Funktion **Log File Maintenance** kann auch mit dem Direktkommando LOGFILE aufgerufen werden.

Mögliche Objekttypen, die im Menü **Log File Maintenance** eingegeben werden können:

Code	Objekttyp
*	Alle.
AD	Administrationsfunktionen
AA	Alle (Basis- und Verbund-)Anwendungen
AB	Basisanwendungen
AC	Verbundanwendungen
DD oder FI	DDMs/Dateien
LI	Bibliotheken
MA	Mailboxen
US	Benutzer

Objekttypcodes für externe Objekte finden Sie unter ***Externe Objekttypen - Types of External Objects***.

Weitere Parameter, die im Menü **Log File Maintenance** angegeben werden können:

Parameter	Erläuterung
Start value	Sie können einen Startwert für die zu schreibenden/lesenden Objekte angeben.
Date from/to	Datum von/bis. Wenn Sie nur Protokollsätze verarbeiten möchten, die in einem bestimmten Zeitraum erstellt wurden, können Sie in diesen Feldern einen Datumsbereich angeben.
Work File 1	Der Name der Arbeitsdatei 1.
Work File 5	Der Name der Arbeitsdatei 5.

Beispiel:

Um Protokollsätze aus der Protokolldatei in die Arbeitsdatei 5 zu schreiben, würde die Batch-Eingabedatei `CMSYNIN` die folgenden Kommandos enthalten:

```
LOGFILE
FIN
```

Batch-Eingabedatei `CMSYNIN` könnte die folgenden Angaben enthalten:

```
SYSSEC,DBA,PASSWORD
22,241
WR,US,,2002-07-01,2002-07-25
```

Die erste Zeile muss die Bibliothekskennung `SYSSEC` sowie die Benutzerkennung und das Passwort des jeweiligen Natural Security-Administrators enthalten.

Die zweite Zeile muss die Datenbankkennung (DBID) und die Dateinummer (FNR) der Protokolldatei enthalten, aus der die Datensätze gelesen werden.

Die dritte Zeile muss den Funktionscode und den Objekttyp enthalten (mögliche Werte sind die gleichen wie im Menü **Logfile Maintenance**) - optional gefolgt von verschiedenen Parametern (deren Reihenfolge und mögliche Werte denen der entsprechenden Felder im Menü **Logfile Maintenance** entsprechen).

Wenn Sie die Arbeitsdatei scannen oder lesen, müssen Sie den folgenden Parameter in der JCL angeben:

```
WORK=((5),OPEN=ACC)
```

Beispiel Batch Job 1 für Großrechner - Protokollsätze in die Arbeitsdatei schreiben:

```
//DBA       JOB DBA,CLASS=K,MSGCLASS=X
//**
//** WRITE LOGGING OF MAINTENANCE DATA TO WORK FILE 5
//** DELETE RECORDS FROM LOG FILE
//**

//NSCnnBAT EXEC PGM=NATBATnn,REGION=2400K,
// PARM=('IM=D,FNAT=(22,210),INTENS=1,FSEC=(22,240),',
//       'MT=0,MAXCL=0,MADIO=0,AUTO=OFF,WORK=((5),OPEN=ACC)')
//STEPLIB DD   DSN=PRODNAT.LOAD,DISP=SHR
//DDCARD   DD  DISP=SHR,DSN=PRD.NATnn.JOBS(ADADB22)
//CMPRINT  DD  SYSOUT=X
//CMWKF05   DD DSN=NSC.LOG.WKF05,
```

```
//    DISP=(NEW,CATLG),DCB=(RECFM=VB,LRECL=4624,BLKSIZE=4628),
//    SPACE=(TRK,(5,2))
//CMSYNIN   DD *
SYSSEC,DBA,password
LOGFILE
22,241
WD,US,,2002-07-01,2002-07-25
.
FIN
/*
//*
```

Im obigen Beispiel werden die Protokollsätze aller Benutzersicherheitsprofile, die zwischen dem 1. und 25. Juli 2002 geändert wurden, in die Arbeitsdatei 5 geschrieben und dann aus der Protokolldatei gelöscht.

Beispiel Batch Job 2 für Großrechner - Protokollsatz-Reports auf Drucker schreiben:

```
//DBA       JOB DBA,CLASS=K,MSGCLASS=X
//**
//** LIST LOG RECORDS-WRITE REPORTS OF MAINTENANCE DATA TO PRINTER
//**
//NSCnnBAT EXEC PGM=NATBATnn,REGION=2400K,
// PARM=('IM=D,FNAT=(22,210),INTENS=1,FSEC=(22,240),',
//       'MT=0,MAXCL=0,MADIO=0,AUTO=OFF')
//STEPLIB  DD  DSN=PRODNAT.LOAD,DISP=SHR
//DDCARD   DD  DISP=SHR,DSN=PRD.NATnn.JOBS(ADADB22)
//** CMWKF01   DD DISP=SHR,DSN=NSC.LOG.WKF01
//** CMWKF05   DD DISP=SHR,DSN=NSC.LOG.WKF05
//CMPRINT  DD SYSOUT=X
//CMPRT01  DD SYSOUT=X
//CMPRT02  DD SYSOUT=X
//CMSYNIN  DD *
LOGFILE
FIN
/*
//CMOBJIN  DD *
SYSSEC,DBA,password
22,241
LI,AD,,2002-06-06,2002-06-06
LI,US,MILL*,2002-05-01,2002-05-31
.
/*
//*
```

Im obigen Beispiel werden die Protokollsätze aller am 6. Juni 2002 geänderten Administrator Services-Einstellungen und aller im Mai 2002 geänderten Benutzersicherheitsprofile in die Druckdateien `CMPRT01` (Liste der Protokollsätze) und `CMPRT02` (ausführliche Protokollsatzinformationen) geschrieben.

Beispiel Batch Job 3 für Großrechner - Protokollsätze aus der Arbeitsdatei lesen:

```
//DBA       JOB DBA,CLASS=K,MSGCLASS=X
//**
//** READ LOGGING OF MAINTENANCE DATA FROM WORK FILE 5
//** INTO LOG FILE
//**
//NSCnnBAT EXEC PGM=NATBATnn,REGION=2400K,
// PARM=('IM=D,FNAT=(22,210),INTENS=1,FSEC=(22,240),',
//       'MT=0,MAXCL=0,MADIO=0,AUTO=OFF,WORK=((5),OPEN=ACC)')
//STEPLIB DD   DSN=PRODNAT.LOAD,DISP=SHR
//DDCARD   DD  DISP=SHR,DSN=PRD.NATnn.JOBS(ADADB22)
//CMPRINT  DD  SYSOUT=X
//CMWKF05  DD  DSN=NSC.LOG.WKF05,DISP=(SHR)
//CMSYNIN   DD *
SYSSEC,DBA,password
LOGFILE
22,241
RA,US,,2002-07-01,2002-07-25
.
FIN
/*
//*
```

Im obigen Beispiel werden die Protokollsätze aller Benutzersicherheitsprofile, die zwischen dem 1. und 25. Juli 2002 geändert wurden, aus der Arbeitsdatei 5 gelesen und somit in der Protokolldatei wiederhergestellt.

Siehe auch Kapitel *Natural Security im Batch-Modus*.

Letzte Anmeldesätze auflisten - List Last Logon Records

Anmerkung: Diese Funktion ist unabhängig von der Protokollierung der Verwaltungsfunktionen. Intern verwendet sie jedoch die gleiche Protokolldatei.

Die Funktion **List Last Logon Records** wertet die von Natural Security geschriebenen Anmeldesätze aus (siehe *Anmeldesätze - Logon Records*). Damit können Sie feststellen:

- wann sich die einzelnen Benutzer zuletzt angemeldet haben,
- welche Benutzer sich in den letzten *n* Tagen nicht angemeldet haben.

Wenn Sie die Funktion aufrufen, wird ein Fenster angezeigt, in dem Sie eine Anzahl von Tagen eingeben können:

- Wenn Sie eine `0` eingeben, erhalten Sie eine Liste der Anmeldesätze, die den letzten zu jedem Benutzer geschriebenen Anmeldesatz enthält.

- Wenn Sie einen anderen Wert als *n* eingeben, erhalten Sie eine Liste der Anmeldesätze derjenigen Benutzer, die sich in den letzten *n* Tagen nicht angemeldet haben, wobei zu jedem dieser Benutzer der letzte vor dem angegebenen Zeitintervall geschriebene Anmeldesatz angezeigt wird.

Die Anmeldesätze werden in chronologischer Reihenfolge aufgelistet.



Anmerkung: Bei dieser Funktion haben die Felder **Object Type**, **Start Value** und **Date from/to** keine Wirkung im Menü.

SAF Online Services

Die **SAF Online Services** bieten verschiedene Funktionen zur Überwachung des SAF-Servers.

Die SAF Online Services sind nur auf Großrechnern verfügbar, und zwar wenn Natural SAF Security (oder ein anderes SAF-bezogenes Produkt) installiert ist.

Bevor Sie die SAF Online Services nutzen können, müssen Sie ein Dienstprogramm-(Utility-)Sicherheitsprofil für das Dienstprogramm `SYSSAFOS` (das die SAF Online Services enthält) definieren.

Um die SAF Online Services aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) den Eintrag **Administrator Services**.

Wenn Sie **berechtigt** sind, auf die Administrator Services zuzugreifen, wird das Menü **Administrator Services Menu 1** angezeigt.

2 Wählen Sie in diesem Menü den Eintrag **SAF Online Services**.

Es wird das Menü **Online Services** angezeigt, das folgende Funktionen bietet:

- Systemparameter - System Parameters
- System-Statistikinformationen - System Statistics
- Benutzer-Statistikinformationen - User Statistics
- Zap-Verwaltung - Zap Maintenance
- Speicheranzeige - Storage Display
- System Tracing

- Server neu starten - Refresh Server

Systemparameter - System Parameters

Die Funktion **System Parameters** zeigt die im Systemparametermodul definierten Parametereinstellungen an. Die folgenden Informationen werden angezeigt:

Feld	Erläuterung
Authorization	Zeigt die verschiedenen Ressourcen-Autorisierungsprüfungen an, die vom SAF-Server durchgeführt werden und sich auf Natural auf Großrechnern, EntireX Communicator, Adabas, Entire Net-Work und Adabas SQL Server beziehen.
Class/Type	Zeigt die Namen der verschiedenen allgemeinen SAF-Ressourcen-Klassen oder -Typen. Diese enthalten entweder die Standard- oder die Überschreibungswerte, die im Systemparametermodul definiert wurden.
Universal	Zeigt an, dass eine bestimmte Prüfung als universal bezeichnet wird. Wenn diese Option ausgewählt ist, haben alle Benutzer Zugriff auf ein bestimmtes Ressourcenprofil, wenn es nicht definiert ist. Die Berechtigung zur Ausführung eines Natural-Programms kann nicht als universell bezeichnet werden.
Buffered	Zeigt bei jeder Art von Prüfung die maximale Anzahl positiver Prüfungen an, die der SAF-Server für jeden Benutzer puffern kann.
Logging	Hier wird die SMF-Protokollierungsstufe angegeben, die bei der Durchführung von Sicherheitsüberprüfungen erforderlich ist. "0" bedeutet, dass ASIS protokolliert wird, d. h. gemäß der Vorgabe für die Sicherheitsklasse/den Sicherheitstyp; "1" bedeutet eine Überschreibungseinstellung von `NONE`.
Active	Gibt an, welche Berechtigungsprüfungen aktiv sind. Dies gilt nur für die vom Großrechner-Natural durchgeführten Prüfungen, da alle anderen Prüfungen durch den Installationsvorgang aktiviert werden.
Env (Environment)	Gibt an, dass ein auf den Natural-Systemdateien basierender Umgebungscode verwendet wird, um bestimmten Ressourcenprofilen ein Präfix zu geben. Gilt nur für Berechtigungsprüfungen, die von Großrechner-Natural durchgeführt werden.
Storage (k)	Die Größe des Puffers in Kilobyte, der für die Zwischenspeicherung positiver Sicherheitsüberprüfungen im Adressraum des SAF-Servers verwendet werden kann.
Server DBID	Zeigt die vom SAF-Server verwendete Datenbankkennung an.
Encrypt Req.	Gibt an, ob Sicherheitsanfragen, die zwischen verschiedenen SAF-Server-Komponenten übermittelt werden, verschlüsselt kommuniziert werden.
Encrypt Stg.	Zeigt an, ob der in der Natural-Umgebung verwaltete Speicher in einem verschlüsselten Zustand gehalten wird.
Messages	SAF-Server-Meldungsebene: Level `0` gibt nur Fehlermeldungen aus, `1` meldet Sicherheitsverletzungen, und `3` erzeugt einen Audit Trail (Prüfpfad, Belegbestand) aller Prüfungen.
Cmd Log	Gibt an, ob die Kommandoprotokollierung eingeschaltet ist.
Buffer	Zeigt an, ob Sicherheitsprüfungen vom SAF-Server zwischengespeichert werden sollen.

Feld	Erläuterung
JCL check	Gibt an, ob die Verarbeitung von CA-JCL-Checks in der Natural-Umgebung verfügbar ist.
Prefix Prog	Gibt an, ob Natural-Programmnamen bei der Durchführung von Berechtigungsprüfungen der Name der aktuellen Anwendungsbibliothek vorangestellt wird. *Gilt nicht für Natural SAF Security.*
Protect Obj	Zeigt an, ob Programmobjekte in der Natural-Umgebung geschützt sind. Benutzer benötigen ALTER-Zugriff auf eine bestimmte Anwendung, um deren Programmobjekte ändern zu können. *Gilt nicht für Natural SAF Security.*
Log SYSMAIN	Gibt an, ob eine Protokollierung aller SYSMAIN-Aktivitäten erforderlich ist. *Gilt nicht für Natural SAF Security.*
SYSMAIN/Lib	Gibt an, ob die Berechtigungsprüfung für SYSMAIN-Funktionen den Zugriff auf die entsprechenden Natural-Anwendungsbibliotheken einschließt. *Gilt nicht für Natural SAF Security.*
Cmd Line	Kommandozeile. Zeigt an, ob die Natural-Kommandozeile geschützt ist. Benutzer benötigen CONTROL-Zugriff, um Kommandos in der Natural-Kommandozeile einzugeben.
ETID	Zeigt an, ob Natural eine eindeutige ETID generieren soll.
Edit/Lib	Zeigt an, ob Natural die Bearbeitung von Objekten in einer anderen Natural-Anwendungsbibliothek verhindert. Gilt nicht für Natural SAF Security. *Gilt nicht für Natural SAF Security.*
Clear/Ed	Zeigt an, ob Natural den Bearbeitungsbereich bei der Anmeldung bei einer anderen Natural-Anwendungsbibliothek löschen soll. *Gilt nicht für Natural SAF Security.*
Ext Name	Gibt an, ob Natural den Benutzernamen aus SAF übernehmen soll. Insbesondere das Feld `*USER-NAME` wird aus RACF oder CA-ACF2 übernommen.
Ext Group	Zeigt an, ob Natural den Gruppennamen aus SAF übernimmt. Das heißt, das Feld `*GROUP` wird aus RACF, CA Top Secret, CA-ACF2 übernommen.
Log API	Gibt an, ob beim Ausführen der Natural-API eine SMF-Protokollierung durchgeführt wird.
Env API	Gibt an, ob den von der Natural-API durchgeführten Berechtigungsprüfungen ein Umgebungscode vorangestellt wird, der auf den Natural-Systemdateien basiert.

System-Statistikinformationen - System Statistics

Diese Funktion **System Statistics** zeigt Statistikinformationen über den SAF-Server an. Die folgenden Informationen werden angezeigt:

Feld	Erläuterung
Authorization	Zeigt die verschiedenen Ressourcen-Autorisierungsprüfungen an, die der SAF-Server in Bezug auf Natural auf Großrechnern, EntireX Communicator, Adabas, Entire Net-Work und Adabas SQL Server durchgeführt hat.
Check (+ve)	Zeigt die Anzahl der Berechtigungsprüfungen an, die gegen das Sicherheitssystem für jeden Prüftyp durchgeführt wurden. Die Anzahl gibt an, für welche Berechtigungen der Zugriff erlaubt wurde, und kann universelle Prüfungen beinhalten.
Check (-ve)	Zeigt die Anzahl der Berechtigungsprüfungen an, die für das Sicherheitssystem durchgeführt wurden und für die der Zugriff verweigert wurde.
Check saved	Zeigt die Anzahl der Berechtigungsprüfungen an, die vom SAF-Server optimiert wurden, weil das Ergebnis bereits bekannt war.
Overwritten	Überschrieben. Anzahl der Fälle, in denen positive Berechtigungsergebnisse im Zwischenspeicher des SAF-Servers überschrieben wurden, weil neuere Informationen den Platz im Puffer eingenommen haben. Erhöhen Sie die Anzahl der gepufferten Elemente, wenn diese Zahl für einen bestimmten Prüftyp zu hoch ist.
Lngth	Länge. Anzahl der Bytes, die für die Zwischenspeicherung von Ressourcenprofilen reserviert sind, die zu jeder Art von Berechtigungsprüfung gehören. Dieser Wert wird automatisch vom System generiert.
Active Users	Anzahl der derzeit auf dem SAF-Server aktiven Benutzer.
High Watermark	Höchstwertmarke bei der Anzahl der auf dem SAF-Server vorhandenen Benutzer.
Max Users	Maximale Anzahl von Benutzern, die untergebracht werden können.
Overwritten	Überschrieben. Anzahl der Fälle, in denen ein Benutzerbereich zurückgewonnen und einem anderen Benutzer zugewiesen wurde.
Authenticated	Authentifiziert. Die Gesamtzahl der erfolgreich durchgeführten Authentifizierungsprüfungen.
Denied	Verweigert. Die Anzahl der erfolglosen Authentifizierungsprüfungen.

Benutzer-Statistikinformationen - User Statistics

Die Funktion **User Statistics** liefert statistische Informationen über die derzeit aktiven Benutzer. Die Funktion zeigt eine Liste der Benutzer an. Wenn Sie einen Benutzer aus der Liste auswählen, werden die statistischen Informationen zu diesem Benutzer angezeigt. Die einzelnen Punkte entsprechen den gleichnamigen Punkten, die oben bei der Funktion **System Statistics** beschrieben wurden.

Zap-Verwaltung - Zap Maintenance

Die Funktion **Zap Maintenance** zeigt eine Liste der beim SAF-Server angewendeten ZAPs an.

Speicheranzeige - Storage Display

Die Funktion **Storage Display** zeigt den Adressraum des SAF-Servers an.

System Tracing

Diese Funktion zeigt eine Liste der 256 letzten Trace-Ereignisse an.

Server neu starten - Refresh Server

Die Funktion **Refresh Server** dient dem Neustart des SAF-Servers. Sie sorgt dafür, dass alle Daten im SAF-Server-eigenen Puffer geleert werden, einschließlich der Einstellungen der **NSF-Optionen**, der **System Statistics**, zwischengespeicherter Sicherheitsprüfungen und Benutzerinformationen. Außerdem werden alle Daten, die vom Sicherheitssystem selbst im Adressraum des SAF-Servers gehalten werden, bei der Ausführung dieser Funktion geleert.

Benutzer-Standardprofile - User Default Profiles

Bevor Sie Standardprofile verwenden, sollten Sie mit der normalen Art der Benutzerdefinition vertraut sein, die im Kapitel *Benutzer verwalten* erläutert wird.

Wenn Sie neue Benutzer hinzufügen, können Sie entweder jedes Element jedes Benutzersicherheitsprofils von Hand eintippen, oder Sie können ein vordefiniertes Benutzer-Standardprofil als Vorlage für die Erstellung eines Benutzersicherheitsprofils verwenden. Wenn Sie zahlreiche Benutzer definieren müssen, deren Sicherheitsprofile einander sehr ähnlich sein sollen, können Sie in einem Standardprofil die Elemente definieren, die für viele Benutzer gleich sein sollen, und dieses Standardprofil dann als Grundlage für die einzelnen Sicherheitsprofile verwenden. Durch die Verwendung von Standardprofilen können Sie so den Arbeitsaufwand für die Definition von Benutzern in Natural Security reduzieren.

Sie können ein Standardprofil wie unten beschrieben anlegen und können es dann als Vorlage für ein Benutzersicherheitsprofil verwenden, siehe *Benutzer verwalten*.

Benutzer-Standardprofil anlegen

Um ein Benutzer-Standardprofil anzulegen:

1 Wählen Sie im Hauptmenü (**Main Menu**) die Option **Administrator Services**.

Wenn Sie **berechtigt** sind, auf die Administrator Services zuzugreifen, wird das Menü **Administrator Services Menu 1** angezeigt.

2 Drücken Sie PF8.

3 Wählen Sie im **Administrator Services Menu 2** die Option **User Default Profiles**.

Die Auswahlliste **Default User Profiles** wird angezeigt.

4 Geben Sie in der Kommandozeile dieses Bildschirms das Kommando `ADD` ein.

Das Fenster **Add User Default Profile** wird angezeigt.

5 Geben Sie in diesem Fenster die *Benutzerkennung* und den *Benutzertyp* des Standardprofils ein.

Informationen zu Benutzerkennungen und Benutzertypen finden Sie im Kapitel ***Benutzer verwalten***.

Der Bildschirm **Add User Default Profile** (Standardprofil anlegen) wird eingeblendet.

6 In diesem Bildschirm können Sie ein Benutzer-Standardprofil für einen Benutzer definieren.

Der Bildschirm **Add User Default Profile** entspricht in etwa dem Bildschirm **Add User** für denselben Benutzertyp. Die einzelnen Bestandteile, die Sie als Teil eines Benutzersicherheitsprofils definieren können, sind unter ***Bestandteile eines Benutzersicherheitsprofils*** beschrieben. Beachten Sie jedoch, dass Sie einige Bestandteile nur in einem individuellen Sicherheitsprofil, nicht aber in einem Standardprofil definieren können.

Standardprofile werden wie individuelle Benutzersicherheitsprofile gepflegt (wie im Kapitel ***Benutzer verwalten*** beschrieben).

Benutzer-Standardprofil verwenden

Wenn Sie einen neuen Benutzer anlegen, können Sie die Kennung eines Standardprofils angeben, das als Vorlage für das von Ihnen erstellte Benutzersicherheitsprofil verwendet werden soll.

Der Benutzertyp des Standardprofils muss derselbe sein wie der des Sicherheitsprofils, für das Sie es verwenden.

Wenn Sie ein Standardprofil zum Anlegen eines neuen Benutzers verwenden, werden die Bestandteile aus dem Standardprofil in das Benutzersicherheitsprofil kopiert - mit Ausnahme der Benutzerkennung, des Benutzernamens und der Eigentümer.

Im Benutzersicherheitsprofil können Sie die aus dem Standardprofil kopierten Bestandteile überschreiben und weitere Bestandteile angeben.

Anmerkung: Um mehrere Benutzer zu definieren, die identische Sicherheitsprofile haben sollen, können Sie auch die Funktion **Multiple Add User** verwenden (die im Kapitel *Benutzer verwalten* beschrieben wird).

Standardprofile für Bibliotheken - Library Default Profiles

Bevor Sie Standard-Bibliothekssicherheitsprofile verwenden, sollten Sie mit der "normalen" Art der Definition von Bibliotheken vertraut sein, wie sie im Kapitel ***Bibliotheken verwalten*** erklärt wird

Wenn Sie neue Bibliotheken hinzufügen, können Sie entweder jedes Bestandteil jedes Bibliothekssicherheitsprofils von Hand eingeben, oder Sie können ein vordefiniertes Standard-Bibliothekssicherheitsprofil als Vorlage für die Erstellung eines Bibliothekssicherheitsprofils verwenden. Wenn Sie zahlreiche Bibliotheken definieren müssen, deren Sicherheitsprofile einander sehr ähnlich sein sollen, können Sie in einem Standardprofil die Bestandteile definieren, die für viele Bibliotheken gleich sein sollen, und dieses Standardprofil dann als Grundlage für die einzelnen Sicherheitsprofile verwenden. Durch die Verwendung von Standardprofilen für Bibliotheken können Sie so den Arbeitsaufwand für die Definition von Bibliotheken für Natural Security reduzieren.

Erstellen Sie ein Standardprofil wie unten beschrieben, und verwenden Sie es dann als Vorlage für ein Bibliothekssicherheitsprofil, wie im Kapitel ***Bibliotheken verwalten*** beschrieben.

Standard-Bibliothekssicherheitsprofil anlegen

Um ein Standard-Bibliothekssicherheitsprofil anzulegen:

1. Wählen Sie im Hauptmenü (**Main Menu**) die Option **Administrator Services**.

   Wenn Sie **berechtigt** sind, auf die Administrator Services zuzugreifen, wird das Menü **Administrator Services Menu 1** angezeigt.
2. Drücken Sie PF8.
3. Wählen Sie im **Administrator Services Menu 2** die Option **Library Default Profiles**.

   Die Auswahlliste **Default Library Profiles** wird angezeigt.
4. Geben Sie in der Kommandozeile dieses Bildschirms das Kommando `ADD` ein.

   Das Fenster **Add Default Library Profile** wird angezeigt.
5. Geben Sie in diesem Fenster die *`Bibliothekskennung`* des Standardprofils ein (Informationen zu **Bibliothekskennungen** finden Sie im Kapitel ***Bibliotheken verwalten***).

Der Bildschirm **Add Default Library Profile** wird angezeigt.

6 Auf diesem Bildschirm können Sie ein Standardprofil für eine Bibliothek definieren.

Der Bildschirm **Add Default Library Profile** entspricht in etwa dem Bildschirm **Add Library**. Die einzelnen Bestandteile, die Sie als Teil eines Bibliothekssicherheitsprofils definieren können, sind unter *Bestandteile eines Bibliothekssicherheitsprofils* beschrieben. Beachten Sie jedoch, dass Sie einige Bestandteile nur in einem individuellen Sicherheitsprofil, nicht aber in einem Standardprofil definieren können.

Standardprofile werden wie individuelle Bibliothekssicherheitsprofile verwaltet (wie im Kapitel *Bibliotheken verwalten* beschrieben).

Standard-Bibliothekssicherheitsprofil verwenden

Wenn Sie eine neue Bibliothek anlegen, können Sie die Kennung eines Standardprofils angeben, das als Vorlage für das von Ihnen erstellte Bibliothekssicherheitsprofil verwendet werden soll.

Wenn Sie ein Standardprofil zum Anlegen einer neuen Bibliothek verwenden, werden die Bestandteile aus dem Standardprofil in das Bibliothekssicherheitsprofil kopiert - mit Ausnahme der Bibliothekskennung, des Bibliotheksnamens und der Eigentümer.

Im Bibliothekssicherheitsprofil können Sie die aus dem Standardprofil kopierten Bestandteile überschreiben und weitere Bestandteile angeben.

Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values

Bevor Sie mit der Definition von Benutzern in Natural Security beginnen, können Sie mit dieser Funktion die Werte mehrerer Bestandteile, die Teil eines Benutzersicherheitsprofils sind, vordefinieren. Wenn Sie dann ein Benutzersicherheitsprofil erstellen, sind die Bestandteile in dem Profil, das Sie anlegen, bereits mit diesen Werten vorbelegt.

Um die Funktion User Preset Values aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) die Option **Administrator Services**.

Wenn Sie **berechtigt** sind, auf die Administrator Services zuzugreifen, wird das Menü **Administrator Services Menu 1** angezeigt.

2 Drücken Sie PF8.

3 Wählen Sie im **Administrator Services Menu 2** die Option **User Preset Values**.

Der erste Bildschirm **User Preset Values** wird angezeigt.

Die Funktion **Preset User Values** umfasst drei Bildschirme:

- Allgemeine Benutzersicherheitsprofiloptionen - General User Profile Options
- Optionen für Passwörter - Password Options
- Optionen für Passphrasen - Passphrase Options

Um zwischen ihnen zu navigieren, können Sie PF7 (Allgemeine Optionen - General options), PF8 (Passwortoptionen - Password options) und PF9 (Passphrasenoptionen - Passphrase options) drücken.

Alle Optionen werden im Folgenden erklärt.

Einige der Optionen erscheinen auch im Sicherheitsprofil jedes Benutzers, wo deren Werte auf die Werte voreingestellt werden, die Sie auf dem Bildschirm **Preset User Values** angeben. Wenn die allgemeine Option **Overwriting of defaults possible** (Überschreiben von Standardwerten möglich) auf `Y` gesetzt ist, können Sie diese Werte in individuellen Benutzersicherheitsprofilen überschreiben. Andere Optionen beziehen sich nicht direkt auf Benutzersicherheitsprofilfelder, sondern gelten für Benutzersicherheitsprofile im Allgemeinen.

Anmerkung: Um festzustellen, in welchen Benutzersicherheitsprofilen der Wert einer bestimmten Komponente vom entsprechenden voreingestellten Wert abweicht, können Sie die Anwendungsprogrammierschnittstelle `NSCADM` verwenden.

Allgemeine Benutzersicherheitsprofiloptionen - General User Profile Options

Option	Erläuterung	
ETID	Sie können angeben, welcher Wert als Kennung (ETID) für die End-of-Transaction-Daten verwendet werden soll. Damit Natural Security ETIDs liefern kann, muss beim Start der Natural-Sitzung der Natural-Profilparameter `ETID` auf `OFF` gesetzt sein.	
	`S`	Diese Einstellung gilt für alle Benutzer. Sie kann in individuellen Benutzersicherheitsprofilen nicht geändert werden. Eine ETID für jeden Benutzer wird von Natural Security zu Beginn der Natural-Sitzung des Benutzers generiert. Eine solche ETID besteht aus `S`, gefolgt von einem Zeitstempel (die am weitesten rechtsstehenden 7 Bytes des Werts der Natural-Systemvariablen `*TIMESTMP` beim Sitzungsstart) und identifiziert die Benutzersitzung eindeutig. Sie bleibt so lange bestehen, bis der Benutzer seine Natural-Sitzung beendet. In den individuellen Benutzersicherheitsprofilen wird dies dadurch angezeigt, dass dem Feld **Default ETID** ein `S>` vorangestellt wird. Jeder nicht

Option	Erläuterung	
		zeitstempelbezogene ETID-Wert in diesem Feld wird dann nicht verwendet. Um eine zeitstempelbezogene ETID nur für einen einzelnen Benutzer zu verwenden, müssen Sie `*TIMSTMP` im Feld **Default ETID** des individuellen Benutzersicherheitsprofils angeben. Wenn zeitstempelbezogene ETIDs verwendet werden, schreibt Natural Security bei jeder Anmeldung eines Benutzers bei Natural einen Anmeldesatz, der die ETID enthält. Um festzustellen, welche ETID von welcher Benutzerkennung verwendet wurde, können Sie die Anmeldesätze einsehen oder die Anwendungsprogrammierschnittstelle `NSCADM` verwenden. Siehe auch *Anmeldesätze - Logon Records*. Für Service Requests in einer RPC-Client/Server-Umgebung können Sie auch zeitstempelbezogene ETIDs verwenden; siehe *Bestandteile eines RPC-Serverprofils*. **Anmerkung:** Wenn ETID auf `S` gesetzt ist, enthält die Natural-Systemvariable `*ETID` binäre, nicht druckbare Daten. Dies kann Auswirkungen auf Ihre Anwendungen haben, wenn diese den `*ETID`-Wert auswerten. Für die Anzeige können Sie die Verwendung einer Editiermaske in Betracht ziehen, z. B. `EM=(H(8))`.
	`F`	Wie "S", nur dass keine Anmeldesätze geschrieben werden.
	`G`	ETIDs werden von Natural Security während des Anmeldevorgangs aus den folgenden Komponenten generiert: ■ Das erste Byte ist ein einzelnes Zeichen, das die Umgebung angibt, aus der Natural aufgerufen wird (B=Batch, C=Color, P=PC, T=TTY, V=Video, X=BTX). ■ Das 2. bis 5. Byte ist eine eindeutige alphanumerische Zeichenfolge, die den Benutzer identifiziert (diese Zeichenfolge wird generiert, wenn ein Benutzer in Natural Security definiert wird). Nur diese 4 Bytes werden im Sicherheitsprofil des Benutzers angezeigt.

Option	Erläuterung	
		■ Das 6. bis 8. Byte ist eine eindeutige alphanumerische Zeichenkette, die die Bibliothek identifiziert (diese Zeichenkette wird generiert, wenn eine Bibliothek in Natural Security definiert wird).
	U	Die Kennung (ID), mit der ein Benutzer in Natural Security definiert ist, d. h. der Wert der Natural-Systemvariablen *USER, wird als ETID verwendet. Wenn die Funktion **Automatic Logon** (beschrieben im Kapitel *Anmeldung*) verwendet wird, ist der Wert von *USER identisch mit dem Wert von *INIT-USER.
	I	Der Wert der Natural-Systemvariable *INIT-USER wird als ETID verwendet.
	T	Der Wert der Natural-Systemvariablen *INIT-ID wird als ETID verwendet.
	N	ETIDs werden nicht verwendet.
	Wenn Sie sich nicht an die möglichen Werte erinnern, die Sie angeben können, können Sie ein Fragezeichen (?) oder einen Stern (*) in das Feld eingeben. Es wird ein Fenster angezeigt. Markieren Sie in dem Fenster den gewünschten Wert mit einem Zeichen oder mit dem Cursor, der Wert wird dann in das Feld **ETID** geschrieben. Einzelheiten zu den oben genannten Systemvariablen finden Sie in der Natural-*Systemvariablen*-Dokumentation.	
Private library for administrator/person	Private Bibliothek für Administrator/Person. Legt fest, ob der Benutzer, wenn er vom Typ Person oder Administrator ist, eine persönliche (private) Bibliothek haben darf.	
Password phrases active	Passphrasen aktiv. Diese Option gilt für Benutzersicherheitsprofile im Allgemeinen. *Passphrasen* sind Passwörter, die länger als 8 Zeichen sind. Mit dieser Option wird die Verwendung von Passphrasen aktiviert. ■ N = Passphrasen können nicht verwendet werden. Es können nur "normale" Passwörter (bis zu 8 Zeichen) verwendet werden. ■ **A** = Es können sowohl Passphrasen als auch "normale" Passwörter verwendet werden. ■ Y = Es werden ausschließlich Passphrasen verwendet. Wenn diese Option auf A oder Y gesetzt ist, wird der anmeldebezogene User Exit LOGONEX0 anstelle von LOGONEX1 verwendet.	

Option	Erläuterung
Change password after *nnn* days	Passwort ändern nach *nnn* Tagen. Sie können ein Zeitintervall (Anzahl der Tage) festlegen, nach dem die Benutzer gezwungen werden, ihr Passwort während des Anmeldevorgangs zu ändern. Der Höchstwert ist 365 Tage. Mit der Option **Message before password expiration** (Nachricht vor Ablauf des Passworts) können Sie den Benutzern eine Nachricht übermitteln, die sie vor dem Ablauf ihres Passworts warnt (siehe unten).
Message before password expiration	Nachricht vor Ablauf des Passworts. Diese Option gilt für Benutzersicherheitsprofile im Allgemeinen. Sie können sie verwenden, um Benutzern, deren Passwort in Kürze abläuft, eine Nachricht zukommen zu lassen. Die Zahl, die Sie hier angeben, bestimmt, wie viele Tage (mögliche Werte sind 1 bis 10) vor Ablauf des Passworts ein Benutzer eine Nachricht erhält, die ihn darauf hinweist, dass sein Passwort abläuft. Die Meldung (NAT1691) wird nach der Erstanmeldung bei Natural angezeigt. Dies gilt nur für Benutzer, in deren Sicherheitsprofilen ein Zeitintervall für die Änderung des Passworts festgelegt ist (Option **Change after** *nnn* **days** in einem **Benutzersicherheitsprofil**.)
Password change possible after	Passwortänderung möglich nach. Diese Option gilt für Benutzersicherheitsprofile im Allgemeinen.
Automatically unlock users after	Benutzer automatisch entsperren nach. Diese Option gilt für Benutzersicherheitsprofile im Allgemeinen. Wenn die Option **Lock User Option** aktiviert ist, können Benutzer aufgrund von Anmelde- oder Gegenzeichnungsfehlern gesperrt werden. Um einen gesperrten Benutzer manuell zu entsperren, können Sie die Funktion **List/Unlock Locked Users** verwenden. Mit dieser Option können Sie ein Zeitintervall festlegen, nach dem ein gesperrter Benutzer *automatisch* entsperrt wird. In diesem Fall wird eine gesperrte Benutzerkennung *nn* Stunden und *nn* Minuten nach dem Auftreten der Sperrung entsperrt.

Optionen für Passwörter - Password Options

Diese Optionen gelten für normale Passwörter mit bis zu 8 Zeichen. Für Passwörter, die länger als 8 Zeichen sind, siehe **Passphrase Options** unten.

Option	Erläuterung
Minimum password length	Mindestlänge des Passworts. Diese Option gilt für Benutzersicherheitsprofile im Allgemeinen. Das Passwort eines Benutzers darf nicht weniger als die hier angegebene Anzahl von Zeichen enthalten. Mögliche Werte: 1 - 8. Beachten Sie bei der Festlegung dieser Länge, dass Passwörter standardmäßig mit den Benutzerkennungen identisch sind (siehe Kapitel *Benutzer verwalten*).
Password case-sensitive	Passwort unter Berücksichtigung der Groß- und Kleinschreibung. Diese Option gilt für Benutzersicherheitsprofile im Allgemeinen. Sie legt fest, ob Natural Security zwischen Klein- und Großbuchstaben in Benutzerpasswörtern unterscheiden soll oder nicht: ■ `N` = Natural Security wandelt intern alle alphabetischen Zeichen in Passwörtern in Großbuchstaben um. ■ `Y` = Natural Security unterscheidet zwischen Klein- und Großbuchstaben in Passwörtern. **Anmerkung:** Wenn Sie diese Option auf `Y` setzen, müssen Sie sicherstellen, dass alle verwendeten Eingabefelder für Passwörter ebenfalls zwischen Klein- und Großbuchstaben unterscheiden. Dies kann Auswirkungen auf den Anmeldebildschirm, den User Exit `LOGONEX1`, alle mit der Anmeldung verbundenen Programmierschnittstellen von Natural Security oder die mit der Anmeldung verbundenen RPC-Programmierschnittstellen von Natural haben.
User password history	Historie der Benutzerpasswörter. Mit dieser Option können Sie die Verwendung von Passwörtern tiefergehend kontrollieren. ■ `N` = Die Passwort-Historie ist für keinen Benutzer aktiv. ■ `*` = Die Passwort-Historie ist generell nicht aktiv. Sie kann für einzelne Benutzer aktiviert werden, indem das Feld **Password History** in den einzelnen Benutzersicherheitsprofilen auf `Y` gesetzt wird. ■ `Y` = Die Passwort-Historie ist für alle Benutzer aktiv. Die Aktivierung der Passwort-Historie hat folgende Auswirkungen: ■ Wenn Sie diese Option auf `Y` oder `*` setzen, wird sie in **User Preset Values** auf schreingeschützt gesetzt. ■ Die letzten *nn* von einem Benutzer verwendeten Passwörter werden von Natural Security aufgezeichnet. Sie können vom Benutzer nicht mehr verwendet werden. Die

Option	Erläuterung
	Anzahl der aufzuzeichnenden Passwörter können Sie in dem Fenster einstellen, das angezeigt wird, wenn Sie diese Option aktivieren. Mögliche Werte: `1 - 10`. ■ Ein Benutzer wird gezwungen, sein Passwort bei der Anmeldung zu ändern, wenn es von einem Administrator im Sicherheitsprofil des Benutzers geändert wurde. ■ Mit den nachstehenden Optionen können Sie bestimmte Regeln festlegen, denen die Passwörter entsprechen müssen.
Die folgenden Optionen können nur verwendet werden, wenn die **User Password / Passphrase History** auf `Y` oder `*` gesetzt ist.	
Maximum number of stored passwords	Maximale Anzahl gespeicherter Passwörter. Dies entspricht dem Feld im Aktivierungsfenster **User Password History**: Die letzten *nn* von einem Benutzer verwendeten Passwörter werden von Natural Security gespeichert. Sie können vom Benutzer nicht erneut verwendet werden. Mögliche Werte: `1 - 10`.
Password mask	Passwort-Maske. Sie können eine Maske definieren, der die Passwörter entsprechen müssen, d. h. Sie können zu jeder Position in einem Passwort festlegen, woraus es bestehen muss: `A` An dieser Stelle muss ein alphabetisches Zeichen (wenn Groß-/Kleinschreibung im Passwort auf `N` eingestellt ist) oder ein Großbuchstabe (wenn **Password case-sensitive** auf `Y` gesetzt ist) angegeben werden. `a` An dieser Stelle muss ein Kleinbuchstabe angegeben werden (nur möglich, wenn **Password case-sensitive** auf `Y` eingestellt ist). `N` An dieser Stelle muss eine Zahl (ein numerisches Zeichen) angegeben werden. `E` An dieser Stelle muss ein Sonderzeichen (d. h. weder ein alphabetisches Zeichen noch eine Zahl) angegeben werden. `*` An dieser Stelle kann ein beliebiges Zeichen angegeben werden. Zum Beispiel bedeutet `***NNN`, dass die ersten drei Zeichen beliebige Zeichen sein können, während die zweiten drei Zeichen numerische Zeichen (Ziffern) sein müssen. Die Länge der Maske muss der Mindestlänge des Passworts entsprechen (siehe **Minimum Password Length** oben).
Each character only once	Jedes Zeichen nur einmal. Wenn dieser Wert auf `Y` gesetzt ist, dürfen Passwörter ein Zeichen nicht zweimal enthalten. Zum Beispiel wäre `THIRST` als Passwort nicht zulässig, da es zwei Mal den Buchstaben T enthält.
Disallow double characters	Doppelte Zeichen nicht zulassen. Wenn dieser Wert auf `Y` gesetzt ist, dürfen Passwörter keine doppelten Zeichen enthalten. Zum Beispiel wäre `LITTLE` wegen des doppelten T nicht zulässig.
Check password for pattern	Passwort auf Muster prüfen. Wenn dieser Wert auf `Y` gesetzt ist, darf ein Passwort nicht mit dem aktuellen Wert der Natural-Systemvariablen `*USER` übereinstimmen. Außerdem darf ein neues Passwort dem alten nicht zu ähnlich sein: Ein neues Passwort wird abgelehnt, wenn seine letzten drei Zeichen mit denen des alten Passworts identisch sind.

Option	Erläuterung
PF5 (PHist) key	Sie können die Taste PF5 (PHist) drücken, um das Kennzeichen für den Passwortverlauf zu ändern. Mit PF5 können nur die Werte der Kennzeichen „Y“ und „*“ geändert werden. Die maximale Anzahl der gespeicherten Passwörter (**Maximum number of stored passwords**) kann mit PF5 nicht geändert werden.
Die folgenden Optionen sind nur verfügbar, wenn im Passwort Groß- und Kleinschreibung berücksichtigt wird (**Password case-sensitive** = Y, siehe oben). Die Summe dieser vier Werte muss der Angabe in **Minimum Password Length** entsprechen, siehe oben.	
Minimum no. of upper-case letters	Mindestanzahl an Großbuchstaben. In diesem Feld können Sie angeben, wie viele Großbuchstaben ein Passwort mindestens enthalten muss.
Minimum no. of lower-case letters	Mindestanzahl an Kleinbuchstaben. In diesem Feld können Sie angeben, wie viele Kleinbuchstaben ein Passwort mindestens enthalten muss.
Minimum no. of numeric characters	Mindestanzahl an numerischen Zeichen In diesem Feld können Sie angeben, wie viele numerische Zeichen ein Passwort mindestens enthalten muss.
Minimum no. of special characters	Mindestanzahl an Sonderzeichen. In diesem Feld können Sie angeben, wie viele Sonderzeichen ein Passwort mindestens enthalten muss.

Optionen für Passphrasen - Passphrase Options

Diese Optionen sind nur verfügbar, wenn die allgemeine Benutzersicherheitsprofiloption **Passphrases active** (siehe oben) auf Y oder A gesetzt ist. Sie gelten für Passphrasen, d.h. für Passwörter, die länger als 8 Zeichen sind.

Anmerkung: Bei Passphrasen wird immer zwischen Groß- und Kleinschreibung unterschieden.

Option	Erläuterung
Minimum passphrase length	Mindestlänge der Passphrase. Diese Option gilt für Benutzersicherheitsprofile im Allgemeinen. Eine Passphrase darf nicht aus weniger Zeichen bestehen als die hier angegebene Anzahl. Mögliche Werte: 9 - 128.
User passphrase history	Historie der Benutzerpassphrasen. Mit dieser Option können Sie die Verwendung von Passphrasen besser steuern. N Die Historie der Passphrasen ist für keinen Benutzer aktiv. * Die Historie der Passphrasen ist generell nicht aktiv. Sie kann für einzelne Benutzer aktiviert werden, indem das Feld **Password History** in individuellen Benutzersicherheitsprofilen auf Y gesetzt wird. Y Die Passphrasen-Historie ist für alle Benutzer aktiv. Die Aktivierung der Passphrasen-Historie hat folgende Auswirkungen:

Option	Erläuterung
	■ Die letzten *nn* von einem Benutzer verwendeten Passphrasen werden von Natural Security aufgezeichnet. Sie können vom Benutzer nicht mehr verwendet werden. Die Anzahl der aufzuzeichnenden Passphrasen können Sie in dem Fenster einstellen, das angezeigt wird, wenn Sie diese Option aktivieren. Mögliche Werte: 1 - 10. ■ Ein Benutzer wird gezwungen, seine Passphrase bei der Anmeldung zu ändern, wenn sie von einem Administrator im Sicherheitsprofil des Benutzers geändert wurde. ■ Mit den nachstehenden Optionen können Sie bestimmte Regeln festlegen, denen die Passphrasen entsprechen müssen.
Die folgenden Optionen können nur verwendet werden, wenn die Benutzerpassphrasenverlauf (siehe **User Passphrase History** oben) auf Y oder * eingestellt ist.	
Maximum number of stored passphrases	Maximale Anzahl der gespeicherten Passphrasen. Dies entspricht dem Feld im **User Passphrase History**-Aktivierungsfenster: Die letzten *nn* von einem Benutzer verwendeten Passphrasen werden von Natural Security gespeichert. Sie können vom Benutzer nicht erneut verwendet werden. Mögliche Werte: 1 - 10.
Blanks allowed within passphrase	Leerzeichen in der Passphrase erlaubt. Wenn dieser Wert auf Y gesetzt ist, dürfen Passphrasen Leerzeichen enthalten.
Check passphrase for pattern	Passphrase auf Muster prüfen. Wenn dieser Wert auf Y gesetzt ist, darf eine Passphrase nicht den aktuellen Wert der Natural-Systemvariablen *USER enthalten. Außerdem darf eine neue Passphrase der alten nicht zu ähnlich sein: Sie wird abgelehnt, wenn ihre letzten drei Zeichen mit denen der alten identisch sind.
Minimum no. of upper-case letters	Mindestanzahl an Großbuchstaben. In diesem Feld können Sie angeben, wie viele Großbuchstaben eine Passphrase mindestens enthalten muss.
Minimum no. of lower-case letters	Mindestanzahl an Kleinbuchstaben. In diesem Feld können Sie angeben, wie viele Kleinbuchstaben eine Passphrase mindestens enthalten muss.
Minimum no. of numeric characters	Minimale Anzahl an numerischen Zeichen. In diesem Feld können Sie angeben, wie viele numerische Zeichen eine Passphrase mindestens enthalten muss.
Minimum no. of special characters	Mindestanzahl an Sonderzeichen. In diesem Feld können Sie angeben, wie viele Sonderzeichen eine Passphrase mindestens enthalten muss.
PF5 (PHist)	Sie können die Taste PF5 (PHist) drücken, um das Kennzeichen für den Passwortverlauf zu ändern. Mit PF5 können nur die Werte der Kennzeichen Y und * geändert werden. Die maximale Anzahl der gespeicherten Passwörter (**Maximum number of stored passphrases**) kann mit PF5 nicht geändert werden.

Voreingestellte Werte für Bibliothekssicherheitsprofile - Library Preset Values

Bevor Sie mit der Definition von Bibliotheken in Natural Security beginnen, können Sie mit dieser Funktion die Werte mehrerer Elemente, die Teil eines Bibliothekssicherheitsprofils sind, vordefinieren. Wenn Sie dann ein Bibliothekssicherheitsprofil erstellen, sind die Elemente in dem Profil, das Sie erstellen, bereits auf diese Werte voreingestellt.

Um die Funktion Library Preset Values aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) die Option **Administrator Services**.

Wenn Sie **berechtigt** sind, auf die Administrator Services zuzugreifen, wird das Menü **Administrator Services Menu 1** angezeigt.

2 Drücken Sie PF8.

3 Wählen Sie im **Administrator Services Menu 2** die Option **Library Preset Values**.

Es wird der Bildschirm **Preset Library Values** (Voreingestellte Werte für Bibliothekssicherheitsprofile) angezeigt, der die Bestandteile des Bibliothekssicherheitsprofils enthält.

Mit PF5 können Sie einen weiteren Bildschirm mit **weiteren Bibliotheksoptionen** aufrufen.

Diese Optionen werden im Folgenden beschrieben.

Bibliothekssicherheitsprofilbestandteile - Library Profile Items

Einige dieser Profilbestandteile erscheinen auch im Sicherheitsprofil jeder Bibliothek, wo ihre Werte auf die Werte voreingestellt werden, die Sie auf dem Bildschirm **Preset Library Values** angeben. Wenn die allgemeine Option **Overwriting of defaults possible** auf `Y` gesetzt ist, können Sie diese Werte in den einzelnen Bibliothekssicherheitsprofilen überschreiben. Andere Einträge entsprechen nicht direkt den Feldern von Bibliothekssicherheitsprofilen, sondern sind Optionen, die für Bibliothekssicherheitsprofile im Allgemeinen gelten.

Option	Erläuterung
Active cross-reference for Predict	Aktive Cross-Referenz für Predict. Legt fest, ob für eine Bibliothek eine aktive Cross-Referenz in Predict erzeugt wird. Wenn Sie hier einen Stern (*) angeben, gilt dies für alle Bibliotheken: Die Erzeugung aktiver Cross-Referenzen wird durch den Wert des Natural-Profilparameters `XREF` bestimmt, unabhängig von der **Cross-Reference**-Einstellung in individuellen Bibliothekssicherheitsprofilen.
Logon recorded	Anmeldung aufgezeichnet. Legt fest, ob Anmeldungen bei einer Bibliothek aufgezeichnet werden.

Option	Erläuterung
Natural programming mode	Natural-Programmiermodus. Legt fest, ob der Programmiermodus mit dem Natural-Profilparameter/Session-Parameter SM geändert werden kann. Wenn Sie hier einen Stern (*) angeben, gilt dies für alle Bibliotheken: Der Programmiermodus wird durch den Wert des Natural-Profilparameters SM bestimmt, unabhängig von der Einstellung des Programmiermodus in den individuellen Bibliothekssicherheitsprofilen.
Restart	Neustart. Legt fest, ob während des Anmeldevorgangs ein Adabas-OPEN-Kommando mit oder ohne End of Transaction ID (ETID) ausgeführt wird.
Maintenance with Natural utilities	Verwaltung mit Natural Utilities. Legt fest, wer den Inhalt der Bibliothek mit Natural-Dienstprogrammen (Utilities) verwalten darf.
Clear source area by logon	Quellcodebereich bei Anmeldung löschen. Legt fest, ob der Quellcode-Arbeitsbereich des Editors automatisch geleert wird, wenn sich ein Benutzer der Bibliothek bei einer anderen Bibliothek anmeldet.
Execute startup transaction in batch	Startup-Transaktion im Batch ausführen. Legt fest, ob die im Bibliothekssicherheitsprofil angegebene Startup-Transaktion im Batch-Modus ausgeführt wird.
Steplibs	Steplibs. Ermöglicht es Ihnen, die Bibliotheken anzugeben, die als Steplib-Bibliotheken für die Bibliothek dienen sollen. Sie können den Namen der ersten Steplib im Feld **Steplibs** auf dem Bildschirm **Preset Library Values** angeben. Wenn Sie mehr als eine Steplib angeben möchten, geben Sie einen Stern (*) in das Feld ein oder drücken Sie PF4: Es wird ein Fenster angezeigt, in dem Sie bis zu 9 Steplibs angeben können.
Profile parameters for undefined libraries	Profilparameter für nicht definierte Bibliotheken. Diese Option gilt für nicht definierte Bibliotheken generell. Für Bibliotheken, für die noch keine Sicherheitsprofile definiert wurden, werden die folgenden Einstellungen durch die entsprechenden Natural-Profilparameter bestimmt: NC = Verwendung von Natural-Systemkommandos erlauben.
RPC-Server-Sitzungsoptionen (Natural RPC-Einschränkungen)	
Close all databases	Alle Datenbanken schließen. Steuert das anmelde- und abmeldeabhängige Schließen von Datenbanken, die von entfernten Subprogrammen in einer Bibliothek geöffnet wurden.
Logon option	Anmeldeoption. Legt fest, welche Anmeldedaten beim Zugriff auf eine Bibliothek über einen Natural RPC Service Call ausgewertet werden.
Logon recorded	Anmeldung aufgezeichnet. Dies ist nicht nur ein voreingestellter Wert. Er gilt auch als Standardwert, wenn das entsprechende Feld im Bibliothekssicherheitsprofil auf * gesetzt ist. In diesem Fall bestimmt er, ob der Zugriff auf eine Bibliothek beim Zugriff über einen Natural RPC Service Call aufgezeichnet werden soll oder nicht.

Option	Erläuterung
Lock user option	Option Benutzer sperren. Einzelheiten zu dieser Funktion finden Sie auch in der **Lock User Option** unter *Allgemeine Optionen*. Dies ist nicht nur ein voreingestellter Wert. Er gilt auch als Standardwert, wenn die Option **Lock User** im Sicherheitsprofil des Natural RPC-Servers auf * gesetzt ist. In diesem Fall steuert sie die Sperrung von Benutzern, wenn diese versuchen, über einen Natural RPC Service Call auf eine Bibliothek auf diesem Server zuzugreifen: N Es wird keine Sperrung von Benutzern vorgenommen. X Sobald ein Benutzer die maximale Anzahl von Anmeldeversuchen erreicht hat, ohne das richtige Passwort einzugeben, wird er gesperrt, d.h. die Benutzerkennung wird ungültig gemacht. Natural Security „merkt“ sich erfolglose Versuche über mehrere Sitzungen hinweg: Die Fehlerzähler für die Client-Benutzerkennungen, die erfolglos ausprobiert wurden, werden für Zugriffsversuche in nachfolgenden Sitzungen aufbewahrt, wodurch die Anzahl der nachfolgenden Versuche mit diesen Kennungen reduziert wird. Der Fehlerzähler für eine Benutzerkennung wird erst nach einer erfolgreichen Anmeldung zurückgesetzt. * Das Sperren von Benutzern wird durch die **Lock User Option** im Abschnitt *Allgemeine Optionen - General Options* der Administrator Services gesteuert.

Weitere Bibliotheksoptionen

Mit PF5 auf dem Bildschirm für die Bibliothekssicherheitsprofilbestandteile können Sie einen weiteren Bildschirm mit zusätzlichen Bibliotheksoptionen aufrufen:

- Modulschutz-Modus - Module Protection Mode
- Umbenennen und Löschen von Bibliotheksknoten deaktivieren - Disable Rename and Delete of Library Node
- NDV Startup Inactive
- Entwicklungsmodus - Development Mode
- Natural Client-Zugang - Natural Client Access
- Bibliotheks-FDIC-Zuweisung aktiviert - Library FDIC Assignment Enabled
- Natural-Benutzerkennung (*USER) an Adabas übergeben - Pass Natural User ID (*USER) to Adabas

- INIT-LIB für nicht definierte Benutzerkennung(en) - INIT-LIB for undefined user ID(s)

Modulschutz-Modus - Module Protection Mode

Die Option **Module Protection Mode** gilt für alle Bibliotheken. Sie wirkt sich auf die Art und Weise aus, in der die Einstellungen **Disallow/Allow Modules** in den Sicherheitsprofilen der Bibliotheken ausgewertet werden. Mögliche Werte:

Wert	Erläuterung
*	Die Auswertung der Einstellungen **Disallowed/Allowed** hängt von der Plattform ab: ■ **Auf Großrechnern:** Wenn ein Modul zur Ausführung aufgerufen wird, wird die Einstellung **Disallowed/Allowed** für dieses Modul im Sicherheitsprofil der aktuellen Bibliothek nur ausgewertet, wenn das Modul in dieser Bibliothek enthalten ist. ■ **Auf anderen Plattformen:** Wenn ein Modul zur Ausführung aufgerufen wird, wird die Einstellung **Disallowed/Allowed** für dieses Modul im Sicherheitsprofil der aktuellen Bibliothek immer ausgewertet, unabhängig davon, ob das Modul in der aktuellen Bibliothek oder einer anderen Bibliothek (Steplib) enthalten ist.
L	Die Auswertung der Einstellung **Disallowed/Allowed** ist auf allen Plattformen gleich: Wenn ein Modul zur Ausführung aufgerufen wird, wird die Einstellung von **Disallowed/Allowed** für dieses Modul im Sicherheitsprofil der aktuellen Bibliothek nur ausgewertet, wenn das Modul in dieser Bibliothek enthalten ist. Die Einstellung dieser Option auf L kann nützlich sein, wenn Sie eine Natural-Anwendung von einer Großrechner- auf eine Nicht-Großrechner-Plattform übertragen und den Modulschutz unverändert lassen möchten.

Umbenennen und Löschen von Bibliotheksknoten deaktivieren - Disable Rename and Delete of Library Node

Mit der Option **Disable Rename and Delete of Library Node** können Sie das versehentliche Löschen/Umbenennen einer Bibliothek in der gemappten Umgebung des Natural Development Server verhindern. Sie gilt für die Aktionen Umbenennen und Löschen im Kontextmenü des Bibliotheksknotens in der gemappten Umgebung. Siehe ***Baumansicht-Aktionen - Tree-View Actions*** im Kapitel *Natural Development Server-Umgebung und -Anwendungen schützen*.

Wert	Erläuterung
Y	Die Aktionen **Rename** (Umbenennen) und **Delete** (Löschen) sind deaktiviert. Sie können nicht über das Kontextmenü des Bibliotheksknotens ausgewählt werden.
N	Die Aktionen **Rename** (Umbenennen) und **Delete** (Löschen) sind im Kontextmenü des Bibliotheksknotens verfügbar.

Anmerkung: Die Einstellung dieser Option auf Y kann nicht verhindern, dass eine Bibliothek aus der Baumansicht verschwindet, wenn die darin enthaltenen Objekte gelöscht werden

(entweder innerhalb der Bibliothek oder mit Dienstprogrammen (Utilities) von außerhalb der Bibliothek).

NDV Startup Inactive

Mit der Option **NDV Startup Inactive** können Sie die Ausführung von **Startup-Transaktionen** bei Anmeldungen bei Bibliotheken in einer gemappten Umgebung auf einem Natural Development Server-Client unterdrücken (siehe auch ***Map-Umgebung und Bibliotheksauswahl - Map Environment und Bibliotheksauswahl*** im Kapitel *Natural Development Server-Umgebung und -Anwendungen schützen*.

Wert	Erläuterung
Y	Startup-Transaktionen werden in einer gemappten Umgebung nicht ausgeführt. Der Name der Startup-Transaktion, wie er im Sicherheitsprofil der Bibliothek, bei der eine Anmeldung durchgeführt wird, angegeben ist, wird nicht in die Natural-Systemvariable *STARTUP geschrieben.
N	Die Ausführung von Startup-Transaktionen in einer gemappten Umgebung ist nicht eingeschränkt.

Diese Option ist nur in gemappten Umgebungen bei Natural Development Server Clients wirksam.

Entwicklungsmodus - Development Mode

NaturalONE unterstützt zwei Entwicklungsmodi für Natural-Projekte: Shared Mode und Private Mode. Die Option Development Mode legt fest, wie Natural Security die Natural-Server-Aktionen steuert, die durch die von den Natural-Projekten verwendeten Eclipse-Navigator-Ansicht-Aktionen ausgelöst werden.

Wert	Erläuterung
*	Die NaturalONE-Entwicklungsmodi werden von Natural Security nicht unterstützt. Die Aktionen werden durch eine Reihe von Einstellungen im Bibliothekssicherheitsprofil und im Utility-Profil gesteuert.
Y	NaturalONE-Entwicklungsmodi werden von Natural Security unterstützt. Die Aktionen werden durch die Entwicklungsmodus-Optionen gesteuert, die Sie einstellen können, wenn Sie in diesem Feld ein Y eingeben und dann PF5 drücken. Einzelheiten finden Sie unter ***Navigator-Ansicht schützen*** im Kapitel *Natural-Entwicklungsumgebung in Eclipse schützen* .

Natural Client-Zugang - Natural Client Access

Die Option **Natural Client Access** legt fest, welche Client-Typen eine Verbindung zum Natural Development Server herstellen dürfen:

Wert	Erläuterung
N	Nur Natural for Windows Clients (Natural Studio) dürfen eine Verbindung zum Server herstellen.
O	Nur NaturalONE Clients dürfen eine Verbindung zum Server herstellen.
A	Sowohl Natural for Windows Clients (Natural Studio) als auch NaturalONE Clients dürfen eine Verbindung zum Server herstellen. Dies ist die Standardeinstellung.
P	Natural for Windows Clients (Natural Studio) und NaturalONE-Clients dürfen sich *nicht* mit dem Server verbinden.

Siehe auch *Starting the Natural Development Server* in den umgebungsspezifischen Kapiteln der *Natural Development Server*-Dokumentation.

Bibliotheks-FDIC-Zuweisung aktiviert - Library FDIC Assignment Enabled

Diese Option bestimmt, ob die FDIC-Systemdatei in Bibliothekssicherheitsprofilen und Special-Link-Profilen gesetzt werden kann. Sie besitimmt außerdem, ob die FUSER-Systemdatei und die **Cross-reference**-Option in Special-Link-Profilen gesetzt werden kann.

Wert	Erläuterung
N	Bei dieser Einstellung gilt Folgendes: ■ Die FDIC-Datei kann nicht in Bibliothekssicherheitsprofilen und Special-Link-Profilen eingestellt werden. ■ Die FUSER-Datei kann nur in Bibliothekssicherheitsprofilen, nicht aber in Special-Link-Profilen eingestellt werden. ■ Die Option **Cross-Reference** kann nur in Bibliothekssicherheitsprofilen, nicht aber in Special-Link-Profilen eingestellt werden.
Y	Bei dieser Einstellung gilt Folgendes: Die FDIC-Datei, die FUSER-Datei und die **Cross-reference**-Option können sowohl in Bibliothekssicherheitsprofilen als auch in Special-Link-Profilen eingestellt werden.

Die Anzeige der entsprechenden Felder in Bibliothekssicherheitsprofilen und Special-Link-Profilen hängt davon ab, wie diese Option eingestellt ist.

Wenn Sie diese Option auf `Y` gesetzt haben, können Sie sie nur dann auf `N` zurücksetzen, wenn keine FDIC-Spezifikation in einer Bibliothek oder einem Special-Link-Profil und keine FUSER-Spezifikation in einem Special-Link-Profil vorhanden ist.

Einzelheiten zum Einstellen der FUSER- und FDIC-Dateien sowie der **Cross-reference**-Option finden Sie unter *Bibliotheksdatei - Library File* und *Allgemeine Optionen* unter ***Bestandteile eines Bibliothekssicherheitsprofils***.

Natural-Benutzerkennung (*USER) an Adabas übergeben - Pass Natural User ID (*USER) to Adabas

Die Option **Pass Natural User ID (*USER) to Adabas** legt fest, welche Benutzerkennung an Adabas übergeben wird, um zur Anmeldung bei Adabas verwendet zu werden.

Wert	Erläuterung
N	Die in der Natural-Systemvariablen *INIT-USER enthaltene Benutzerkennung.
Y	Die Benutzerkennung, die in der Natural-Systemvariablen *USER enthalten ist.

Diese Option ist nur in Nicht-Großrechnerumgebungen wirksam. In Großrechnerumgebungen wird immer der *USER-Wert zur Anmeldung bei Adabas verwendet.

Anmerkung: *USER wird dem Adabas-Kommando Open zugewiesen. Wenn die Benutzerkennung während des Anmeldevorgangs geändert werden kann, ist es erforderlich, **NSC Library Profile** > **Security Options** > **Close Database by Logon** für Nicht-RPC-Sitzungen auf Y und die Option **Close All Databases** für Natural RPC-Sitzungen auf Y oder F (Force) zu setzen.

INIT-LIB für nicht definierte Benutzerkennung(en) - INIT-LIB for undefined user ID(s)

Mit der Option **INIT-LIB for undefined user ID(s)** wird die NSC-Bibliothekskennung als Standard-Bibliothekskennung für eine nicht definierte Benutzerkennung zugewiesen, die nicht mit der Namenskonvention für Natural-Bibliothekskennungen übereinstimmt. Ein NSC-Bibliothekssicherheitsprofil, das als öffentliche Bibliothek definiert ist, und eine auf Y gesetzte Übergangszeitanmeldeoption sind erforderlich, bevor Sie diese Option setzen.

```
Value = library ID (A8)
```

Systembibliotheken definieren - Definition of System Libraries

Die Funktion **Definition of System Libraries** wird im Rahmen der Erstinstallation von Natural Security verwendet. Mit ihr können Sie automatisch Bibliothekssicherheitsprofile für Systembibliotheken (d.h. Bibliotheken, deren Namen mit SYS beginnen) von Natural und seinen Subprodukten erstellen.

Wenn Sie diese Funktion verwenden, müssen Sie den Natural-Profilparameter MADIO auf einen Wert von mindestens 2000 setzen.

Sie sollten diese Funktion nicht bei SYS-Bibliotheken anwenden, die Natural-Dienstprogramme (Utilities) enthalten, da empfohlen wird, Dienstprogramme zu schützen. Siehe *Dienstprogramme (Utilities) schützen*.

Um Systembibliotheken zu definieren:

1 Wählen Sie im Hauptmenü (**Main Menu**) die Option **Administrator Services**.

Wenn Sie **berechtigt** sind, auf die Administrator Services zuzugreifen, wird das Menü **Administrator Services Menu 1** angezeigt.

2 Drücken Sie PF8.

3 Wählen Sie im **Administrator Services Menu 2** die Option **Definition of System Libraries**.

Es wird eine Liste der Systembibliotheken von Natural und allen Natural-Subprodukten angezeigt, die an Ihrem Standort installiert sind. Für jede Systembibliothek wird ein bibliotheksspezifisches Sicherheitsprofil bereitgestellt, in dem alle erforderlichen Bestandteile bereits entsprechend definiert sind.

4 In der Liste können Sie entweder einzelne Bibliotheken mit AD markieren, auf die die vordefinierten Profile nacheinander angewendet werden sollen, oder Sie können die vordefinierten Profile auf alle Produkt-Systembibliotheken gleichzeitig anwenden, indem Sie das entsprechende Produkt mit AD markieren.

Weitere Informationen zur Installation von Natural Security finden Sie in der Natural-*Installation*-Dokumentation.

Nicht definierte Bibliotheken definieren - Definition of Undefined Libraries

Mit der Funktion **Definition of Undefined Libraries** können Sie Bibliothekssicherheitsprofile für nicht definierte Bibliotheken erstellen, d.h. für Bibliotheken, die in der aktuellen FUSER-Systemdatei vorhanden sind, für die aber noch keine Bibliothekssicherheitsprofile erstellt wurden.

Diese Funktion entspricht derjenigen des SHOW-Kommandos, die unter *Nicht definierte Bibliotheken auflisten - Listing Undefined Libraries* im Kapitel *Bibliotheken verwalten* beschrieben ist.

Um nicht definierte Bibliotheken zu definieren:

1 Wählen Sie im Hauptmenü (**Main Menu**) die Option **Administrator Services**.

Wenn Sie **berechtigt** sind, auf die Administrator Services zuzugreifen, wird das Menü **Administrator Services Menu 1** angezeigt.

2 Drücken Sie PF8.

3 Wählen Sie im **Administrator Services Menu 2** die Option **Definition of Undefined Libraries**.

Es wird eine Liste aller nicht definierten Bibliotheken angezeigt. Sie entspricht der Liste, die Sie erhalten, wenn Sie in der **Library Maintenance**-Auswahlliste das Kommando SHOW UNDF eingeben.

4 Gehen Sie vor wie unter ***Nicht definierte Bibliotheken auflisten - Listing Undefined Libraries*** im Kapitel *Bibliotheken verwalten* beschrieben.

8 Benutzer verwalten

- Vorbereitungen treffen 130
- Bestandteile eines Benutzersicherheitsprofils 130
- Benutzersicherheitsprofile anlegen und verwalten 142

In diesem Kapitel wird beschrieben, wie Sie *Benutzersicherheitsprofile* erstellen und verwalten. Folgenden Themen werden behandelt:

Vorbereitungen treffen

Bevor Sie damit beginnen, Benutzer in Natural Security zu definieren, empfiehlt es sich, einige Vorbereitungen zu treffen:

- Erstellen Sie eine Liste aller Personen in Ihrem Unternehmen, die Natural verwenden.
- Teilen Sie sie entsprechend ihrer Tätigkeit und im Hinblick auf die Natural-Bibliotheken, die sie verwenden sollen, in Gruppen ein. Die Einteilung Ihres Unternehmens in Abteilungen kann dabei als Richtschnur dienen. Personen, die dieselben Bibliotheken verwenden, sollten in dieselben Gruppen eingeteilt werden. (Personen können in mehr als einer Gruppe sein.)

Es wird empfohlen, so oft wie möglich Gruppen zu verwenden, da dies nicht nur den Verwaltungsaufwand für Natural Security erheblich reduziert, sondern auch für eine konsistentere Schutzstruktur sorgt.

Die Definition von Benutzern in Natural Security und die Zuordnung von Benutzern zu Gruppen erfolgt am besten in der folgenden Reihenfolge:

1. Erstellen Sie ein Gruppensicherheitsprofil, d.h. definieren Sie einen Benutzer vom Typ Gruppe (Group).
2. Erstellen Sie individuelle Benutzersicherheitsprofile, d.h. definieren Sie Benutzer, typischerweise vom Typ Mitglied (Member).
3. Weisen Sie der Gruppe Mitglieder zu, d. h. ändern Sie das Gruppensicherheitsprofil.

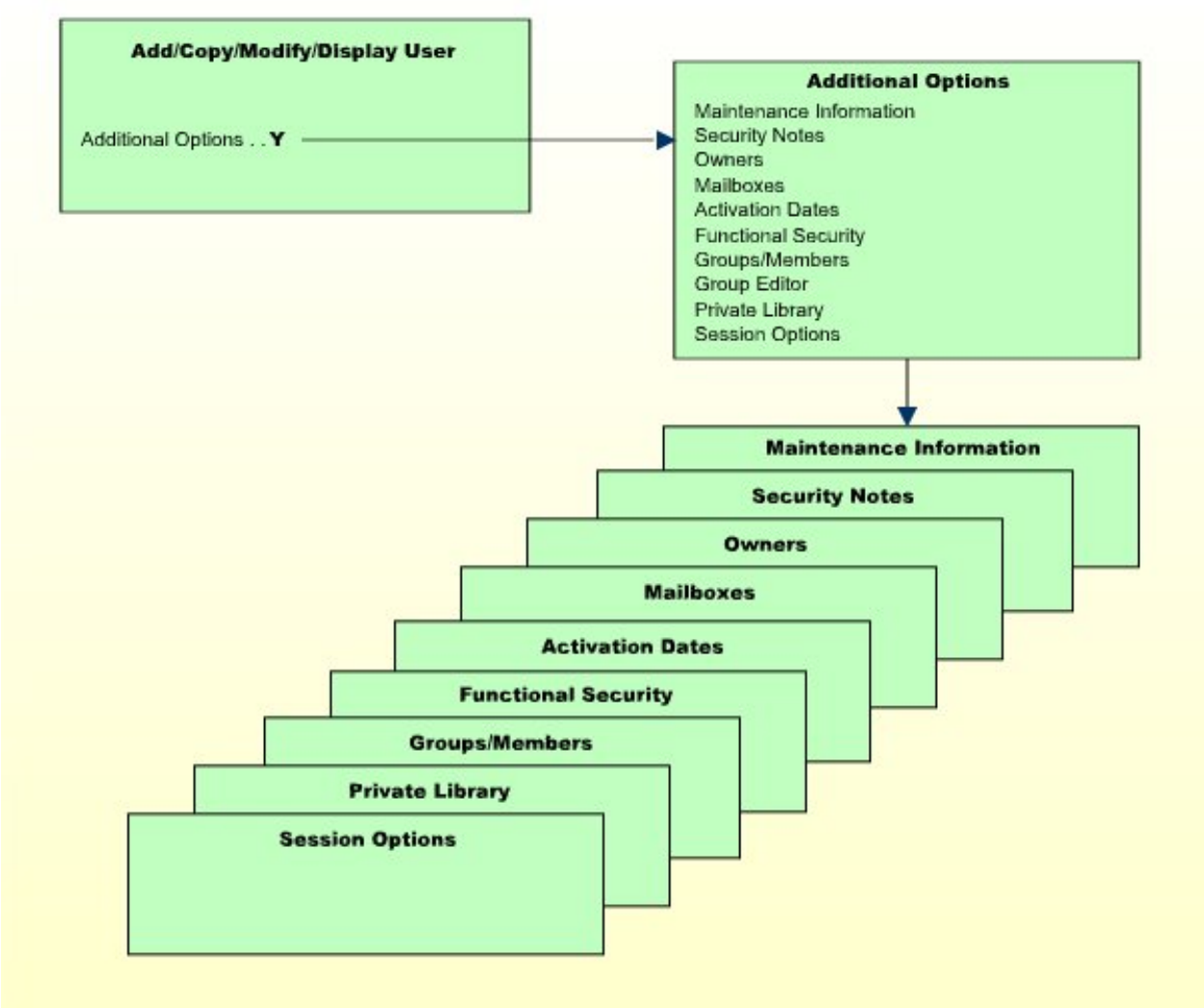
Bestandteile eines Benutzersicherheitsprofils

Dieser Abschnitt behandelt die folgenden Themen:

- Übersicht über die Bestandteile eines Benutzersicherheitsprofils
- Bestandteile des Hauptbildschirms eines Benutzersicherheitsprofils

- Zusätzliche Optionen eines Benutzersicherheitsprofils

Übersicht über die Bestandteile eines Benutzersicherheitsprofils



Bestandteile des Hauptbildschirms eines Benutzersicherheitsprofils

Der folgende Bildschirmtyp ist der zugrunde liegende Benutzersicherheitsprofilbildschirm („Basis-Bildschirm“), der angezeigt wird, wenn Sie eine der Funktionen Add/Anlegen, Copy/Kopieren, Modify/Ändern, Display/Anzeigen bei einem Benutzersicherheitsprofil aufrufen:

```
15:27:08                    *** NATURAL SECURITY ***               2022-08-08
                                - Modify User -

                                                Modified ..          by
User ID ...... AD
User Name .... ARTHUR DENT_____________________
User Type .... A (A=Administrator, P=Person, M=Member)

Privil. Groups          Libraries                 Password
--------------      -------------------      ----------------------
DOC_____            Default .. SYSSEC__      New Password ________
________            Last .....               Change after 666 days
________            Private Library ... Y    Password History .. N
________                                     Individual Lock ... F
________
                           ETID                  Characteristics
No. groups   3      -------------------      --------------------------------
                    Default ..  AR1R  G      Logon recorded .... N
                    Last .....               Batch User ID ..... ________
                                             Language .......... _0
                    Batch ....               Time Differential   + __ h __ min
                                             Time Zone
                                             _________________________________


Additional Options ... N

Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help  PrevM Exit  AddOp PrLib Flip                                 Canc
```

Die einzelnen Bestandteile, die Sie als Teil eines Benutzersicherheitsprofils definieren können, werden im Folgenden erläutert.

Die Bestandteile eines Benutzersicherheitsprofils können je nach Benutzertyp variieren. Bei jedem im Folgenden erläuterten Bestandteil sind die betreffenden Benutzertypen in Klammern angegeben. Wenn keine Benutzertypen angegeben sind, gilt der Bestandteil für alle Benutzertypen.

Feld	Erläuterung
User ID (nur Anzeige)	Benutzerkennung. Die Kennung des Benutzers, wie sie bei der Erstellung des Benutzersicherheitsprofils angegeben wurde.
User Name	Name des Benutzers. Kann bis zu 32 Zeichen lang sein. Dieser Name sollte mit dem entsprechenden Eintrag in Predict (falls installiert) identisch sein.
User Type	Benutzertyp: `G` = Group `M` = Member `A` = Administrator

Feld	Erläuterung
	P = Person, T = Terminal B = Batch User E = External User
Privileged Groups (alle außer G)	Privilegierte Gruppen. Sie können die Kennungen von bis zu fünf Gruppen eingeben, denen der Benutzer angehört. Damit können Sie die Reihenfolge beeinflussen, in der Natural Security nach einem Link zu einer Bibliothek sucht: ■ Für Benutzer des Typs Mitglied gilt Folgendes: Wenn der Benutzer versucht, sich bei einer geschützten Bibliothek anzumelden, werden die in seinem Sicherheitsprofil eingetragenen privilegierten Gruppen (in der Reihenfolge ihres Eintrags) auf einen Link zu der Bibliothek geprüft, bevor die anderen Gruppen, denen der Benutzer angehört, (in alphabetischer Reihenfolge) auf einen Link zu der Bibliothek geprüft werden. ■ Für Benutzer des Typs Administrator und Person gilt Folgendes: Wenn der Benutzer versucht, sich bei einer geschützten Bibliothek anzumelden, mit der er nicht direkt verlinkt ist, werden die in seinem Sicherheitsprofil eingetragenen privilegierten Gruppen (in der Reihenfolge ihres Eintrags) auf einen Link zu der der Bibliothek geprüft, bevor die anderen Gruppen, denen der Benutzer angehört, (in alphabetischer Reihenfolge) auf einen Link zu der Bibliothek geprüft werden. ■ Für Terminals gilt Folgendes: Wenn ein Benutzer versucht, sich mit der Terminalkennung bei einer geschützten Bibliothek anzumelden (d. h. ohne Eingabe einer Benutzerkennung), werden die privilegierten Gruppen im Sicherheitsprofil des Terminals (in der Reihenfolge ihres Eintrags) auf einen Link zu der Bibliothek geprüft, bevor die anderen Gruppen, zu denen das Terminal gehört, (in alphabetischer Reihenfolge) auf einen Link zu der geprüft werden. Die privilegierten Gruppen können auch dazu verwendet werden, die Reihenfolge zu beeinflussen, in der Natural Security nach anzuwendenden Dienstprogrammprofilen (Utility-Profilen) sucht; weitere Informationen finden Sie unter ***Welches Dienstprogramm-Profil wird angewendet?*** im Kapitel *Dienstprogramme (Utilities) schützen*. Sie können eine Gruppe erst in die Liste **Privileged Groups** (Privilegierte Gruppen) eintragen, nachdem der Benutzer zu der Gruppe hinzugefügt wurde. Wenn Sie eine Gruppe aus der Liste **Privileged Groups** (Privilegierte Gruppen) des Benutzers entfernen, wird der Benutzer *nicht* als Mitglied dieser Gruppe gelöscht.
Members (G)	Mitglieder. Sie können die Benutzerkennungen der ersten fünf Benutzer eingeben, die zu dieser Gruppe gehören. Wenn mehr als fünf Benutzer zu der Gruppe gehören, müssen Sie die Funktion **Edit Group Members** (Gruppenmitglieder bearbeiten) verwenden. Sie können Benutzer erst dann zu einer Gruppe zuweisen, wenn sie in Natural Security definiert worden sind.

Feld	Erläuterung
	Nach der Eingabe einer Benutzerkennung wird der zugehörige Benutzertyp angezeigt.
No. groups (alle außer G; nur Anzeige)	Anzahl Gruppen. Die Gesamtzahl der Gruppen, denen der Benutzer angehört (einschließlich der privilegierten Gruppen). Unter **Additional Options** (siehe unten) erhalten Sie eine Liste aller dieser Gruppen.
No. members (G; nur Anzeige)	Anzahl Mitglieder. Die Anzahl der Benutzer, die zu dieser Gruppe gehören. Unter **Additional Options** (siehe unten) erhalten Sie eine Liste all dieser Benutzer.
Sum members (G; nur Anzeige)	Summe Mitglieder. Dieses Feld wird nur angezeigt, wenn die Gruppe eine andere Gruppe enthält. Es zeigt die Summe aller in der Gruppe enthaltenen Benutzer an. Dazu gehören auch Benutzer, die selbst Mitglied der Gruppe sind.
Libraries (Bibliotheken)	
Default	In dieses Feld können Sie die Kennung einer Standardbibliothek eingeben. ■ Für Benutzer des Typs Administrator, Person oder Mitglied gilt Folgendes: Für Benutzer des Typs Administrator, Person oder Mitglied gilt Folgendes: Die im Sicherheitsprofil eines Benutzers angegebene Standardbibliothek wird automatisch aufgerufen, wenn sich der Benutzer bei Natural anmeldet, ohne eine Bibliothekskennung einzugeben. ■ Für Terminals gilt Folgendes: Die im Sicherheitsprofil eines Terminals angegebene Standardbibliothek wird automatisch aufgerufen, wenn sich ein Benutzer über das Terminal bei Natural anmeldet, ohne eine Bibliothekskennung einzugeben. ■ Für Gruppen gilt Folgendes: Die im Sicherheitsprofil einer Gruppe angegebene Bibliothek wird automatisch aufgerufen, wenn sich ein Benutzer bei Natural anmeldet, ohne eine Bibliothekskennung einzugeben, wenn der Benutzer keine Standardbibliothek in seinem eigenen Sicherheitsprofil angegeben hat und wenn die Gruppe zu den privilegierten Gruppen gehört, die im Sicherheitsprofil des Benutzers aufgeführt sind.
Last (alle außer G und E; nur Anzeige)	Letzte. Die letzte neustartfähige Bibliothek, bei der der Benutzer angemeldet war. (Die Option **Restart** (Neustart) in einem Bibliothekssicherheitsprofil bestimmt, ob eine Bibliothek neustartfähig ist).
Private Library (A, P, E)	Private Bibliothek. Diese Option bestimmt, ob der Benutzer eine private Bibliothek haben darf (siehe unten).
ETID	
Default (alle außer G)	Standard. In diesem Feld wird die Kennung zur Identifizierung der End-of-Transaction-Daten (ETID) angezeigt. ■ Wenn diesem Feld ein `S>` vorangestellt ist, bedeutet dies, dass zeitstempelbezogene ETIDs für alle Benutzer von Natural Security beim Sitzungsstart generiert werden. In diesem Fall wird der tatsächliche ETID-Wert, der im Benutzersicherheitsprofil angegeben ist, nicht verwendet. Weitere Informationen finden Sie unter `ETID=S` unter

Feld	Erläuterung
	Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values im Kapitel *Administrator Services*. ■ Wenn die angezeigte ETID von einem `G` gefolgt wird, bedeutet dies, dass sie von Natural Security generiert wurde, wie für ETID=G unter *Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values* beschrieben. Wenn die ETID nicht generiert wurde und Sie dies wünschen, geben Sie ein Fragezeichen (?) in das Feld **Default ETID** ein. ■ Andere mögliche ETID-Werte (Benutzerkennung, TP-Benutzerkennung oder Terminalkennung) sind unter *Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values* beschrieben. **Anmerkung:** ETIDs können nur von Natural Security geliefert werden, wenn die Natural-Sitzung mit dem Natural-Profilparameter `ETID` auf `OFF` oder den Standardwert gesetzt ist.
Last (alle außer G und E; nur Anzeige)	Letzte. Die ETID, die zuletzt für den Benutzer erzeugt/eingestellt wurde. **Anmerkung:** Wenn das Feld **Batch** (siehe unten) einen Wert enthält, wird das Feld **Last** in einer Batch-Modus-Umgebung nicht aktualisiert.
Batch (A, P, M, E)	Wenn die Natural-Sitzung des Benutzers im Batch-Modus läuft, bestimmt dieses Feld die ETID, die für die Sitzung verwendet wird. Mögliche Werte für dieses Feld: ■ `*INIT-US(ER)`, `*USER`, `*INIT-ID`, `*INITPGM` (= `*INIT-PROGRAM`). Der Wert der entsprechenden Natural-Systemvariablen wird als ETID verwendet. Dieser Wert wird für die gesamte Batch-Sitzung verwendet, auch bei Bibliotheken, die mit `Restart=N` definiert sind. Eine zeitstempelbezogene ETID wird nicht verwendet, auch wenn das Feld **ETID** in *Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values* auf `S` gesetzt ist. ■ Wenn dieses Feld leer ist, wird die ETID im Feld **Default** (siehe oben) auch im Batch-Modus verwendet.
Password	
New Password (A, P, M)	Neues Passwort. Sie können ein Passwort für den Benutzer eingeben, das er bei der Anmeldung verwenden soll. Dieses Passwort kann vom Benutzer (während des Anmeldevorgangs) oder von einem Eigentümer des Sicherheitsprofils des Benutzers (im Sicherheitsprofil) geändert werden. Wird hier kein Passwort eingegeben, geht Natural Security davon aus, dass das Passwort mit der Benutzerkennung identisch ist. Die Mindestlänge (Minimum Length) des Passworts wird im Abschnitt *Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values* der *Administrator Services* festgelegt.

Feld	Erläuterung
Change after *nnn* days (A, P, M)	Änderung nach *nnn* Tagen. In diesem Feld können Sie ein Zeitintervall angeben, nach dem der Benutzer gezwungen wird, sein Kennwort während des Anmeldevorgangs zu ändern. Wenn Sie das Zeitintervall z. B. auf `007` einstellen, muss der Benutzer alle 7 Tage ein neues Passwort auf dem Anmeldebildschirm eingeben. Andernfalls kann sich der Benutzer nicht anmelden. Wenn Sie verhindern wollen, dass der Benutzer das Passwort ändert, setzen Sie dieses Feld auf `999`. Der Benutzer kann dann sein Passwort bei der Anmeldung nicht ändern. Wenn Sie dieses Feld leer lassen, kann der Benutzer sein Kennwort so oft ändern, wie er möchte. Sie können den Benutzern eine Nachricht anzeigen lassen, die sie vor dem Ablauf ihres Passworts warnt, siehe die Option **Message before password expiration** (Nachricht vor Ablauf des Passworts) im Abschnitt ***Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values*** (**User Preset Values**) der *Administrator Services*.
Password History	Passwort-Historie. Dieses Feld steht nur zur Verfügung, wenn in ***Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values*** (**User Preset Values**) * bei **User Password History** angegeben ist. In diesem Fall können Sie dieses Feld verwenden, um die Funktion **User Password History** für einen einzelnen Benutzer zu aktivieren. Mögliche Werte: ■ `N` = Die Passwort-Historie ist für diesen Benutzer nicht aktiv. ■ `Y` = Die Passwort-Historie ist für diesen Benutzer aktiv. Weitere Informationen finden Sie bei den entsprechenden Werten des Feldes **User Password History** (beschrieben im Abschnitt ***Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values*** (**User Preset Values**) unter *Administrator Services*.
Individual Lock	Individuelle Sperre. Dieses Feld ist nur verfügbar, wenn in *Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values* der Wert * für **User Password History** angegeben ist. In diesem Fall können Sie dieses Feld verwenden, um die Option **Lock User** für einen einzelnen Benutzer zu aktivieren. Mögliche Werte: ■ `N` = Die Funktion **Lock User** ist für diesen Benutzer nicht aktiv. ■ `F` = Die Funktion **Lock User** ist für diesen Benutzer aktiv. Weitere Informationen finden Sie unter den entsprechenden Werten der Option **Lock User**, die im Abschnitt *Allgemeine Optionen* der *Administrator Services* beschrieben ist.
Characteristics (Besondere Merkmale)	

Feld	Erläuterung
Logon recorded	Anmeldung aufgezeichnet. Alle Anmeldungen des Benutzers bei einer beliebigen Bibliothek werden aufgezeichnet. Informationen zu den Anmeldesätzen (***Anmeldesätze - Logon Records***) finden Sie im Kapitel *Administrator Services*.
Batch User ID (alle außer `T` und `B`)	Batch-Benutzerkennung. Wenn die Natural-Systemvariable `*DEVICE` auf `BATCH` gesetzt ist, gilt Folgendes: Sie können die Kennung eines Batch-Benutzersicherheitsprofils eingeben. Bevor Sie eine Batch-Benutzerkennung eingeben können, muss ein Sicherheitsprofil für diese Batch-Benutzerkennung definiert worden sein. Im Batch-Modus meldet sich ein Benutzer mit seiner normalen Benutzerkennung und seinem Passwort an. Natural Security verwendet dann die im Sicherheitsprofil des Benutzers angegebene Batch-Benutzerkennung, und es gelten die für diese Batch-Benutzerkennung definierten Nutzungsbedingungen. Wenn im Sicherheitsprofil des Benutzers keine Batch-Benutzerkennung angegeben ist, werden die im Sicherheitsprofil des Benutzers angegebenen Privileged Groups (in der Reihenfolge ihrer Eintragung) auf eine Batch-Benutzerkennung überprüft. Wenn auch keine der privilegierten Gruppen eine Batch-Benutzerkennung hat, wird die eigene Benutzerkennung des Benutzers verwendet. **Anmerkung:** Diese Option gilt nur, wenn die Natural-Systemvariable `*DEVICE` auf `BATCH` gesetzt ist; andernfalls hat diese Option keine Wirkung.
Language (alle außer `T`)	Sprache. Dies entspricht der Natural-Systemvariablen `*LANGUAGE` und steuert die Verwendung von Natural-Fehlermeldungen. Sie können einen numerischen Wert von `1` bis `60` eingeben. Jeder Wert steht für eine Sprache (z. B. steht `1` für Englisch). Wenn Sie den Wert auf `0` setzen, gilt der Wert des Natural-Profilparameters `ULANG`. Weitere Informationen finden Sie unter der Systemvariablen `*LANGUAGE` und dem Profilparameter `ULANG` (in der Natural *Systemvariablen-* bzw. *Parameter-Referenz*-Dokumentation).
Time Differential (alle außer `B` und `E`)	Zeitdifferenz.Dies gilt nur für eine Umgebung, in der entfernte Knoten in einem Rechnernetzwerk verwendet werden. Er entspricht dem Natural-Profilparameter `TD` (siehe Natural-*Parameter-Referenz*-Dokumentation). Sie können einen Wert von `-23` bis `+23` für Stunden und `00` oder `59` für Minuten eingeben. Die Werte geben die Anzahl der Stunden/Minuten an, die zur Rechenzentrumszeit addiert bzw. von dieser subtrahiert werden, um die Ortszeit zu erhalten. Der Standardwert ist `0` (was bedeutet, dass die Zeit des Rechenzentrums verwendet wird). Wenn die Zeit Ihres Standorts beispielsweise 5 Stunden vor der Zeit des Rechenzentrums liegt, können Sie den Wert auf `+5` setzen, wenn Sie die tatsächliche Ortszeit anstelle der Zeit des Rechenzentrums verwenden möchten.

Feld	Erläuterung
	Sie können auch einen Stern (*) angeben. Dies hat die gleiche Wirkung wie die Profilparametereinstellung TD=AUTO (d. h. die Zeitdifferenz wird automatisch durch den Vergleich der physischen und logischen Maschinenzeiten berechnet). Sie können entweder **Time Differential** oder **Time Zone** (siehe unten) verwenden, aber nicht beides.
Time Zone (alle außer B und E)	Zeitzone. Dies gilt nur für eine Umgebung, in der entfernte Knoten in einem Rechnernetzwerk verwendet werden. Sie können den Namen einer Zeitzone eingeben. Eine Zeitzone mit diesem Namen muss im NTTZ-Makro des NATCONFG-Konfigurationsmoduls definiert werden. Die Definition im NTTZ-Makro bestimmt die Anzahl der Stunden/Minuten, die zur Rechenzentrumszeit addiert bzw. von ihr subtrahiert werden, um die Ortszeit zu erhalten. Sie können entweder **Time Zone** oder **Time Differential** (siehe unten) verwenden, aber nicht beides.

Zusätzliche Optionen eines Benutzersicherheitsprofils

Wenn Sie das Feld **Additional Options** im Basis-Bildschirm des Sicherheitsprofils mit Y markieren, wird ein Fenster angezeigt, in dem Sie die folgenden Optionen auswählen können:

- **Maintenance Information**
- **Security Notes**
- **Owners**
- **Mailboxes**
- **Activation Dates**
- **Functional Security**
- **Groups/Members**
- **Group Editor**
- **Private Library**
- **Session Options**
- **Development Mode**

Die Optionen, bei denen schon etwas angegeben oder definiert wurde, sind mit einem Pluszeichen (+) gekennzeichnet.

Einige Optionen sind nur für bestimmte Benutzertypen verfügbar.

Sie können ein oder mehrere Optionen aus dem Fenster auswählen, indem Sie sie mit einem beliebigen Zeichen markieren. Für jede ausgewählte Option wird ein weiteres Fenster oder Bildschirm angezeigt (in der Reihenfolge der Optionen im Auswahlfenster).

Der Bildschirm **Private Library** kann auch direkt durch Drücken von PF5 auf dem Basis-Bildschirm des Sicherheitsprofils aufgerufen werden.

Die einzelnen Optionen werden im Folgenden erläutert.

Zusätzliche Optionen (Benutzer) - Additional Options (User)	Erläuterung
Maintenance Information (nur Anzeige)	Verwaltungsinformationen. In diesem Fenster werden die folgenden Informationen angezeigt: ■ das Datum und die Uhrzeit, zu der das Sicherheitsprofil erstellt wurde, die Kennung des Administrators, der es erstellt hat, und (falls zutreffend) die Kennungen der Miteigentümer, die für die Erstellung gegengezeichnet haben; ■ das Datum und die Uhrzeit der letzten Änderung des Sicherheitsprofils, die Kennung des Administrators, der die letzte Änderung vorgenommen hat, und (falls zutreffend) die Kennungen der Miteigentümer, die für die Änderung gegengezeichnet haben.
Security Notes	Sicherheitsvermerke. In diesem Fenster können Sie Vermerke zum Sicherheitsprofil eingeben.
Owners	Eigentümer. In diesem Fenster können Sie bis zu acht Kennungen von Administratoren eingeben. Nur die hier angegebenen Administratoren sind berechtigt, das Sicherheitsprofil des Benutzers zu verwalten. Wird kein Besitzer angegeben, kann jeder Benutzer vom Typ Administrator das Sicherheitsprofil verwalten. Zu jedem Eigentümer kann optional die Anzahl der Miteigentümer, deren Gegenzeichnung für die Verwaltungserlaubnis erforderlich ist, im Feld hinter der Kennung angegeben werden. Informationen zu Eigentümern und Miteigentümern finden Sie im Kapitel *Gegenzeichnungen*.
Mailboxes	Mailboxen. In diesem Fenster können Sie bis zu fünf Mailbox-Kennungen eingeben. Informationen zu Mailboxen finden Sie im Kapitel *Mailboxen*.
Activation Dates (alle außer T und B)	Aktivierungsdatum. In diesem Fenster können Sie das Datum festlegen, ab dem oder bis zu dem das Sicherheitsprofil gültig sein soll. Die Meldung „This security profile is currently not active.“ (Dieses Sicherheitsprofil ist derzeit nicht aktiv.) wird angezeigt, wenn das Sicherheitsprofil noch nicht oder nicht mehr oder vorübergehend nicht gültig ist, d. h. die entsprechende Benutzerkennung kann nicht vor oder nach einem bestimmten Datum oder innerhalb eines bestimmten Zeitraums verwendet werden.

Zusätzliche Optionen (Benutzer) - Additional Options (User)	Erläuterung
Functional Security (alle außer T und E)	Funktionssicherheit. In diesem Fenster können Sie die Funktionssicherheit für den Benutzer in Bezug auf die Kommandoprozessoren definieren, die in den Bibliotheken definiert sind, auf die der Benutzer Zugriff hat. Dies ist nur relevant, wenn die Kommandoprozessoren mit dem Natural-Dienstprogramm `SYSNCP` erstellt wurden. Weitere Informationen finden Sie im Kapitel ***Funktionssicherheit***.
Groups/Members (nur Anzeige)	Gruppen/Mitglieder. Wenn Sie dieses Feld markieren, wird eine Liste aller Gruppen angezeigt, denen der Benutzer angehört. Wenn der Benutzer eine Gruppe ist, wird eine Liste aller Benutzer angezeigt, die zu dieser Gruppe gehören.
Group Editor (G)	Gruppen-Editor. Wenn Sie dieses Feld markieren, wird die Funktion **Edit Group Members** aufgerufen. Diese Funktion wird unter ***Gruppenmitglieder editieren - Editing Group Members*** weiter unten erklärt.
Private Library (A, P, E)	Private Bibliothek. Ein Benutzer kann eine "persönliche" Bibliothek haben, deren Kennung mit seiner Benutzerkennung identisch ist. Eine solche Bibliothek wird als *private Bibliothek* bezeichnet. Private Bibliotheken können in zwei Modi zur Verfügung gestellt werden: ■ **Public Mode:** Im öffentlichen Modus werden private Bibliotheken wie alle anderen Bibliotheken behandelt, d. h. ihre Nutzung kann auf die gleiche Weise kontrolliert werden wie die "normaler" Bibliotheken. Der einzige Unterschied besteht darin, dass, wenn eine private Bibliothek geschützt ist (was die Standardeinstellung ist), der Benutzer mit der gleichen Kennung auf sie zugreifen kann, ohne mit ihr verlinkt sein zu müssen, während andere Benutzer einen Link zu ihr benötigen (siehe ***Private Bibliothek schützen - Protecting a Private Library*** im Kapitel *Bibliotheken schützen*). ■ **Private Mode:** Im privaten Modus kann nur der Benutzer auf eine private Bibliothek zugreifen, der direkt mit ihr verlinkt ist, d. h. dessen Benutzerkennung mit der Bibliothekskennung identisch ist. Nicht einmal ein Natural Security-Administrator hat Zugriff auf die Bibliothek. (Die einzige Möglichkeit für einen Administrator, Zugang zu einer privaten Bibliothek zu erhalten, besteht darin, das Kennwort des Benutzers im Sicherheitsprofil des Benutzers zu ändern und sich dann mit der Benutzerkennung des Benutzers und dem neuen Kennwort bei der privaten Bibliothek anzumelden.) Eine solche private Bibliothek bietet also ein gewisses Maß an Privatsphäre für den Benutzer. Ein möglicher Missbrauch dieser Privatsphäre lässt sich nur schwer ausschließen. Es wird daher empfohlen, diesen Modus *nicht* zu verwenden. Der Modus wird mit der allgemeinen Option **Private libraries in public mode** (beschrieben im Kapitel *Administrator Services*) gesetzt und gilt für alle privaten Bibliotheken.

Zusätzliche Optionen (Benutzer) - Additional Options (User)	Erläuterung
	Informationen zum Anlegen und Verwalten einer privaten Bibliothek finden Sie unter ***Private Bibliothek anlegen und verwalten*** im Kapitel *Bibliotheken verwalten*. Hinsichtlich des Zugriffs auf DDMs/Dateien gibt es keinen Unterschied zwischen privaten Bibliotheken und "normalen" Bibliotheken. **Anmerkung:** Wenn nicht ausdrücklich anders angegeben, gilt das, was in der *Natural Security*-Dokumentation über Bibliotheken gesagt wird, auch für private Bibliotheken.
Session Options (A, P, G, E)	Sitzungsoptionen. **Siehe unten.**
Development Mode (A, P, G, E)	Entwicklungsmodus. Siehe ***User Development Mode Options*** im Kapitel *Natural-Entwicklungsumgebung in Eclipse schützen* .

Optionen für Sitzungen - Session Options

Option	Erläuterung
Unlock Objects	Objekte entsperren. Diese Option steuert die Verwendung des Natural-Systemkommandos `UNLOCK`, das in Verbindung mit dem Natural Development Server verwendet wird. Sie können einen der folgenden Werte angeben: ■ `N` = Der Benutzer kann das `UNLOCK`-Kommando nicht verwenden. ■ `Y` = Der Benutzer kann das `UNLOCK`-Kommando verwenden, allerdings nur für seine eigenen Programmierobjekte (d.h. Objekte, die unter seiner Benutzerkennung gesperrt sind). Dies ist der Standardwert. ■ **F** = Der Benutzer kann das `UNLOCK`-Kommando für jedes gesperrte Programmierobjekt verwenden.
Environment Protection (nur Anzeige)	Schutz der Umgebung. Dieses Feld ist nur relevant, wenn der Umgebungsschutz aktiv ist (d.h. wenn die allgemeine Option **Environment Protection** auf `Y` gesetzt ist). Es zeigt an, ob es Umgebungen gibt, auf die der Benutzer nicht zugreifen darf: ■ `N` = Der Benutzer kann auf jede Umgebung zugreifen, für die ein Sicherheitsprofil definiert ist. ■ `Y` = Dem Benutzer ist der Zugriff auf mindestens eine definierte Umgebung nicht erlaubt. Einzelheiten zum Umgebungsschutz finden Sie im Kapitel ***Umgebungen schützen***.
Suspend Line Protection	Zeilenschutz aufheben. In diesem Feld wird festgelegt, ob der Benutzer die Funktion **Suspend Line Protection** des Natural Studio-Programmeditors verwenden darf oder nicht: ■ `Y` = Der Benutzer darf die Funktion verwenden. ■ `N` = Der Benutzer darf die Funktion nicht verwenden.

Option	Erläuterung
Profile Maintenance	Profilverwaltung. Dieses Feld steuert die Berechtigung zur Verwaltung der Profile, die vom Natural-Systemkommando `LIST` und dem Natural Object Handler-Dienstprogramm verwendet werden: ■ `U` = Der Benutzer darf nur seine eigenen benutzerspezifischen Parameter der beiden Profile ändern (dies ist die Standardeinstellung).. ■ `G` = Der Benutzer darf sowohl die allgemeinen Parameter der beiden Profile als auch seine eigenen benutzerspezifischen Parameter ändern. ■ `N` = Der Benutzer kann keinen der Parameter der beiden Profile ändern. Das LIST-Profil wird unter *Individuelles LIST-Profil erstellen* beim Kommando `LIST` in der Natural-*Systemkommandos*-Dokumentation beschrieben. Das Object Handler-Profil wird unter *Profileinstellungen (Profile Settings)* im Kapitel *Object Handler* in der Natural-*Debugger- und Dienstleistungsprogramme (Utilities)*-Dokumentation beschrieben.
Natural Client Access	Zugang für Natural Clients. Dieses Feld legt fest, welche Client-Typen eine Verbindung mit dem Natural Development Server herstellen dürfen: ■ `N` = Nur Natural for Windows-Clients (Natural Studio) dürfen eine Verbindung zum Server herstellen. ■ `O` = Nur NaturalONE-Clients dürfen eine Verbindung zum Server herstellen. ■ `A` = Sowohl Natural for Windows (Natural Studio) als auch NaturalONE-Clients dürfen sich mit dem Server verbinden. Dies ist die Standardeinstellung. ■ `P` = Natural for Windows (Natural Studio) und NaturalONE-Clients dürfen sich nicht mit dem Server verbinden. Siehe auch *Starting the Natural Development Server* in den umgebungsspezifischen Kapiteln der *Natural Development Server*-Dokumentation.

Benutzersicherheitsprofile anlegen und verwalten

In diesem Abschnitt werden die Funktionen zum Anlegen und Verwalten von Benutzersicherheitsprofilen beschrieben.

Folgende Themen werden behandelt:

- Benutzerverwaltung aufrufen
- Neuen Benutzer anlegen
- Mehrere neue Benutzer anlegen
- Vorhandene Benutzer zur Bearbeitung auswählen
- Benutzer kopieren - Copy User
- Benutzer ändern - Modify User
- Benutzer umbenennen - Rename User
- Benutzer löschen - Delete User

- Benutzer anzeigen - Display User
- Gruppenmitglieder editieren - Editing Group Members
- Verlinkungen eines Benutzers kopieren - Copy User's Links

Benutzerverwaltung aufrufen

Um die Benutzerverwaltung aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) die Option **Maintenance**.

Es wird ein Fenster angezeigt.

2 Markieren Sie in dem Fenster den Objekttyp **User** mit einem Zeichen oder mit dem Cursor.

Es wird die **User Maintenance**-Auswahlliste angezeigt.

3 Von dieser Auswahlliste aus können Sie alle Funktionen der Benutzerverwaltung wie unten beschrieben aufrufen.

Neuen Benutzer anlegen

Mit der Funktion **Add User** können Sie neue Benutzer in Natural Security definieren, d. h. Sicherheitsprofile für Benutzer anlegen.

Wenn Sie einen neuen Benutzer anlegen, müssen Sie Folgendes angeben:

- eine Benutzerkennung,
- einen Benutzertyp,
- die Kennung eines Standardprofils (optional).

Benutzerkennung

Die Benutzerkennung wird von Natural Security zur Identifizierung des Benutzers verwendet. Sie kann 1 bis 8 Zeichen lang sein. Die Kennung muss unter allen in Natural Security definierten Benutzer- und Bibliothekskennungen eindeutig sein. Für Benutzerkennungen gelten dieselben Namenskonventionen wie für Bibliothekskennungen (siehe Kapitel *Bibliotheken verwalten*).

- Handelt es sich bei dem Benutzer um eine Einzelperson, wird in der Regel eine Kennung gewählt, die einen Bezug zum Namen des Benutzers hat.
- Handelt es sich bei dem Benutzer um ein Terminal, muss die Kennung mit der Terminalkennung identisch sein, über die das Terminal dem Rechner gegenüber definiert ist (fragen Sie Ihren Systemprogrammierer).
- Handelt es sich bei dem Benutzer um eine Gruppe, können Sie eine beliebige Kennung wählen.

Benutzertyp

Wenn Sie einen Benutzer anlegen, müssen Sie den Code für einen der folgenden Benutzertypen angeben:

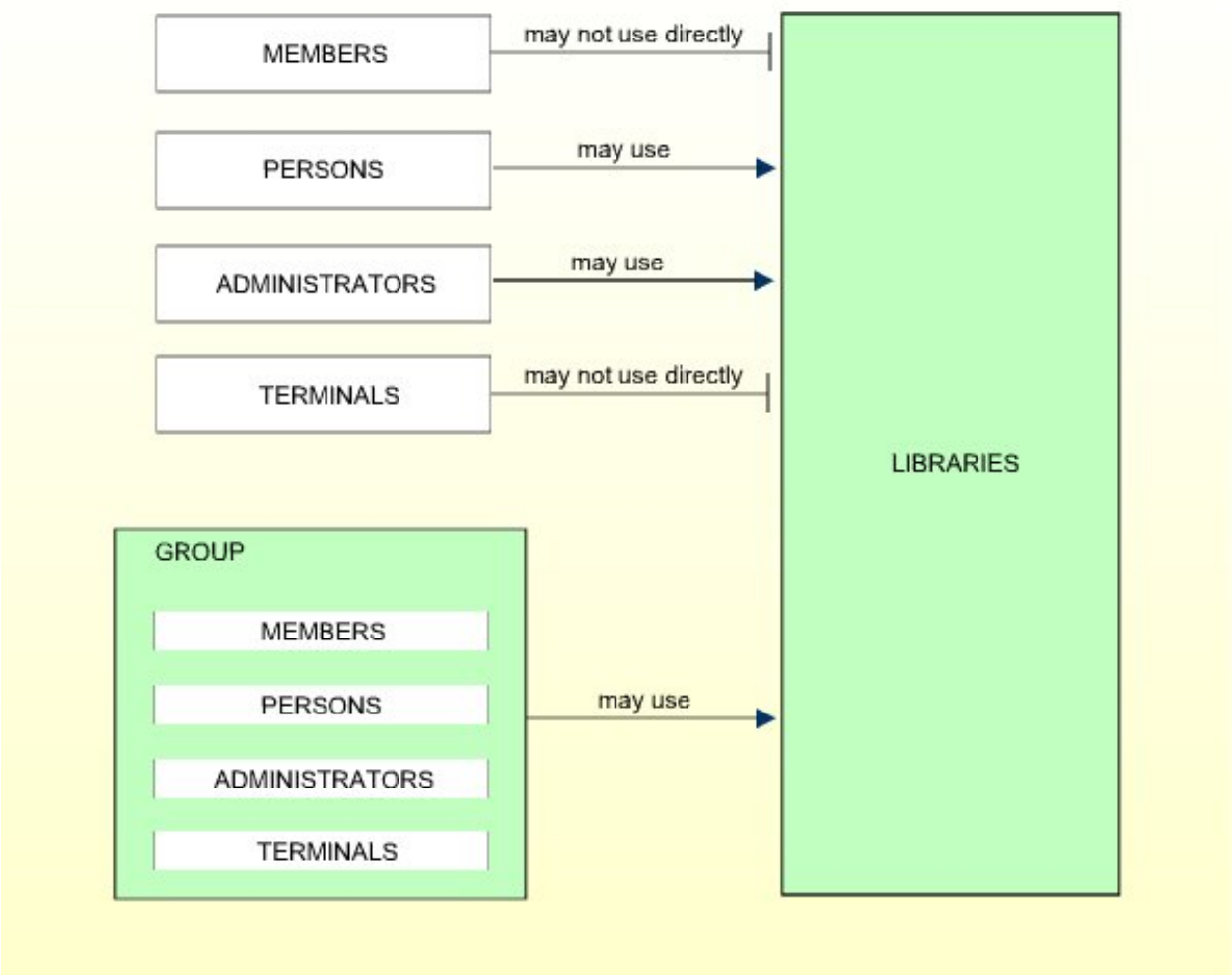
Code	Benutzertyp
G	Group
M	Member
P	Person
A	Administrator
T	Terminal
Spezielle Benutzertypen:	
B	Batch-Benutzer (siehe ***Batch-Benutzersicherheitsprofile*** im Kapitel *Natural Security im Batch-Modus*).
E	Externer Benutzer (dieser Benutzertyp kann nicht explizit angegeben werden; siehe das Feld **NSC user ID** unter ***Bestandteile eines LDAP-Sicherheitsprofils*** im Abschnitt *Authentifizierungsoptionen (LDAP)*).

Handelt es sich bei dem zu definierenden Benutzer um eine Gruppe, muss der Benutzertyp `G` sein.

Handelt es sich bei dem zu definierenden Benutzer um ein Terminal, muss der Benutzertyp `T` lauten.

Handelt es sich bei dem zu definierenden Benutzer um eine Einzelperson, muss der Benutzertyp `M` sein (mit Ausnahme von Einzelpersonen, die Natural Security-Administratoren sind und den Benutzertyp `A` haben müssen).

Die Zugriffsrechte der verschiedenen Benutzertypen auf Bibliotheken sind in der folgenden Abbildung zusammengefasst:



Sollten Sie Zweifel an der korrekten Angabe des Benutzertyps haben, sollten Sie den Abschnitt *Benutzer* im Kapitel *Struktur und Terminologie von Natural Security* lesen.

Nachdem Sie eine Person definiert haben, können Sie später die Klassifizierung ihres Benutzertyps (wie unter *Herauf- und Herabstufung von Benutzern* weiter unten erklärt).

Standardprofil

Wenn Sie einen neuen Benutzer hinzufügen, können Sie entweder jedes Bestandteil des Benutzersicherheitsprofils von Hand eingeben oder ein vordefiniertes Standardprofil als Vorlage für das anzulegende Sicherheitsprofil verwenden.

Bevor Sie Standardprofile verwenden, sollten Sie mit der normalen Art der Benutzerdefinition (d.h. ohne Standardprofil) vertraut sein.

Standardprofile werden im Administrator Services-Subsystem angelegt und verwaltet.

Der *Benutzertyp* des von Ihnen angegebenen Standardprofils muss mit dem des anzulegenden Benutzersicherheitsprofils identisch sein.

Wenn Sie im Fenster **Add User** die Kennung eines Standardprofils angeben, werden die Bestandteile aus dem Standardprofil in das Benutzersicherheitsprofil kopiert - mit Ausnahme der Benutzerkennung, des Benutzernamens und der Eigentümer.

Auf dem Bildschirm **Add User** können Sie dann die in das Benutzersicherheitsprofil kopierten Bestandteile überschreiben und weitere Bestandteile angeben.

Weitere Informationen finden Sie unter ***Benutzer-Standardprofile - User Default Profiles*** im Kapitel *Administrator Services*.

Anmerkung: Um eine größere Anzahl von Benutzern mit identischen Sicherheitsprofilen zu definieren, können Sie auch die Funktion **Multiple Add User** verwenden (siehe ***Mehrere neue Benutzer anlegen***).

Neuen Benutzer anlegen

Geben Sie in der Kommandozeile der **User Maintenance**-Auswahlliste das Kommando `ADD` ein.

Es wird ein Fenster angezeigt. In diesem Fenster geben Sie Folgendes ein:

- eine Benutzerkennung,
- einen Benutzertyp,
- die Kennung eines Standardprofils (optional).

Der Bildschirm **Add User** für den angegebenen Benutzertyp wird angezeigt. In diesem Fenster können Sie ein Sicherheitsprofil für den Benutzer definieren.

Der Bildschirm **Add User** und die nachfolgenden Bildschirme/Fenster, die Teil eines Benutzersicherheitsprofils sind, sowie die einzelnen Bestandteile, die Sie definieren können, werden unter ***Bestandteile eines Benutzersicherheitsprofils*** beschrieben.

Wenn Sie einen neuen Benutzer anlegen, werden die in Ihrem eigenen Benutzersicherheitsprofil angegebenen Eigentümer automatisch in das von Ihnen anzulegende Benutzersicherheitsprofil kopiert.

Mehrere neue Benutzer anlegen

Bevor Sie die Funktion **Multiple Add User** verwenden, sollten Sie mit dem "normalen" Weg der Benutzerdefinition vertraut sein (wie oben unter *Neuen Benutzer anlegen* beschrieben).

Mit der Funktion **Multiple Add User** können Sie schnell und einfach eine große Anzahl von Benutzern in Natural Security definieren. Mit dieser Funktion können Sie zahlreiche Benutzer definieren, die identische Sicherheitsprofile haben sollen.

Geben Sie in der Kommandozeile der **User Maintenance**-Auswahlliste das Kommando `ADDM` ein.

Es wird ein Fenster angezeigt. In diesem Fenster geben Sie eine *Benutzerkennung* und einen *Benutzertyp* ein (und optional die Kennung eines *Standardprofils*).

Es wird der Bildschirm **Multiple Add User** für den angegebenen Benutzertyp angezeigt. Auf diesem Bildschirm können Sie ein Sicherheitsprofil für den Benutzer definieren.

Der Bildschirm **Multiple Add User** und die nachfolgenden Bildschirme/Fenster, die Teil eines Benutzersicherheitsprofils sind, sowie die einzelnen Bestandteile, die Sie definieren können, sind unter *Bestandteile eines Benutzersicherheitsprofils* beschrieben.

Wenn Sie einen neuen Benutzer anlegen, werden die in Ihrem eigenen Benutzersicherheitsprofil angegebenen Eigentümer automatisch in das von Ihnen anzulegende Benutzersicherheitsprofil kopiert.

Um mehrere Benutzersicherheitsprofile zu anzulegen

1. Definieren Sie auf dem ersten Bildschirm (und allen weiteren Bildschirmen/Fenstern) ein Sicherheitsprofil für einen einzigen Benutzer.
2. Wenn Sie die Eingabe der zu definierenden Bestandteile abgeschlossen haben und sich wieder auf dem Bildschirm **Multiple Add User** befinden, ohne dass weitere Bildschirme/Fenster aktiv sind, müssen Sie ENTER drücken. Der erste Benutzer ist nun definiert.
3. Drücken Sie dann PF5 - das gleiche Sicherheitsprofil wird erneut angezeigt, wobei die Einträge für die Benutzerkennung und den Benutzernamen weggelassen werden. Geben Sie eine Benutzerkennung und den Namen des nächsten Benutzers ein und drücken Sie ENTER. Der zweite Benutzer ist nun definiert.
4. Drücken Sie danach PF5 - das gleiche Sicherheitsprofil wird erneut angezeigt, wobei die Einträge für die Benutzerkennung und den Benutzernamen weggelassen werden. Auf diese Weise können Sie weitere Benutzer mit identischen Sicherheitsprofilen definieren.
5. Um die Funktion **Multiple Add User** zu verlassen, müssen Sie PF3 drücken.

Vorhandene Benutzer zur Bearbeitung auswählen

Wenn Sie die Funktion **User Maintenance** aufrufen, wird eine Liste aller Benutzer angezeigt, die in Natural Security definiert wurden.

Wenn Sie nicht eine Liste aller vorhandenen Benutzer, sondern sich nur bestimmte Benutzer anzeigen lassen möchten, können Sie die Optionen **Start Value** (Startwert) und **Type/Status** (Typ/Status) verwenden, siehe *Grundlagen der Benutzung*.

Wählen Sie im Hauptmenü (**Main Menu**) die Option **Maintenance**. Es wird ein Fenster angezeigt.

Markieren Sie in dem Fenster den Objekttyp **User** mit einem Zeichen oder mit dem Cursor (und geben Sie, falls gewünscht, einen Startwert und/oder einen Benutzertyp ein).

Die Auswahlliste **User Maintenance** wird angezeigt:

```
11:11:11                  *** NATURAL SECURITY ***                2022-08-31
                            - User Maintenance -

 Co User ID  User Name                          Type Message
 __ ________ _____________________________ ____ ________________________
 __ AAZ      ABDUL ALHAZRED                    A
 __ AD       ARTHUR DENT                       A
 __ CDW      CHARLES DEXTER WARD               A
 __ CZ       CODY ZAMORA                       P
 __ DI       DAVID INNES                       A
 __ EW       ESMERALDA WEATHERWAX              M
 __ HC       HAGBARD CELINE                    A
 __ HW       HENRY WILT                        A
 __ IW       IRENE WILDE                       M
 __ LL       LOCKE LAMORA                      M
 __ PE       PALMER ELDRITCH                   M
 __ PR       PRECIOUS RAMOTSWE                 M
 __ SV       SAM VIMES                         M
 __ TN       THURSDAY NEXT                     P
 __ VV       VINCENT VEGA                      M

 Command ===>
 Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
       Help        Exit             Flip  -     +                     Canc
```

Zu jedem Benutzer werden die Benutzerkennung, der Benutzername und der Benutzertyp angezeigt.

In der Liste kann geblättert werden, wie im Kapitel *Grundlagen der Benutzung* beschrieben.

Die folgenden Funktionen zur Benutzerverwaltung sind verfügbar (mögliche Code-Kürzel sind unterstrichen):

Code	Funktion	Beschreibung siehe
CO	Copy user	**Benutzer kopieren**
MO	Modify user	**Benutzer ändern**
RE	Rename user	**Benutzer umbenennen**
DE	Delete user	**Benutzer löschen**
DI	Display user	**Benutzer anzeigen**
EG	Edit group members	**Gruppenmitglieder editieren**
LA	Link user to applications	**Benutzer mit Anwendungen verlinken**
LL	Link user to libraries	**Benutzer mit Bibliotheken verlinken**
LO	Link user to external objects	**Benutzer mit externen Objekten verlinken**
LR	Link user to RPC servers	**Benutzer mit RPC-Servern verlinken**
CP	Copy user's links	**Verlinkungen des Benutzers kopieren**
EP	Protect environments for user	**Umgebungen für Benutzer schützen**
MD	Modify DDM restrictions in user's private library	**DDM-Beschränkungen in der privaten Bibliothek des Benutzers ändern** (diese Funktion ist auf Großrechnern nicht verfügbar)

Um eine bestimmte Funktion für einen Benutzer aufzurufen, müssen Sie den Benutzer mit dem entsprechenden Funktionscode in Spalte **Co** markieren.

Sie können mehrere Benutzer gleichzeitig für verschiedene Funktionen auswählen, d.h. Sie können mehrere Benutzer auf dem Bildschirm mit einem Funktionscode markieren. Für jeden markierten Benutzer wird dann der entsprechende Bearbeitungsbildschirm angezeigt. Sie können dann für einen Benutzer nach dem anderen die ausgewählten Funktionen ausführen.

Benutzer kopieren - Copy User

Mit der Funktion **Copy User** können Sie einen neuen Benutzer für Natural Security definieren, indem Sie ein Sicherheitsprofil erstellen, das mit einem bereits vorhandenen Sicherheitsprofil eines Benutzers identisch ist.

- Was wird kopiert?
- Vorgehensweise beim Kopieren
- Kopieren ohne Verlinkungen

- Kopieren mit Verlinkungen

Was wird kopiert?

Alle Bestandteile des bestehenden Sicherheitsprofils werden in das neue Sicherheitsprofil kopiert - *außer*:

- der Benutzername (siehe *Vorgehensweise beim Kopieren* unten),
- das Passwort,
- die ETID (die die End-of-Transaction-Daten identifiziert),
- die Eigentümer (diese werden aus Ihrem eigenen Sicherheitsprofil in das neue Sicherheitsprofil kopiert, das Sie anlegen).

Ob die in der Spalte **Privileged Groups** (Privilegierte Gruppen) eingegebenen Gruppen und etwaige Verlinkungen zu Bibliotheken kopiert werden, hängt davon ab, ob Sie mit oder ohne Verlinkungen kopieren (siehe ***Kopieren mit Verlinkungen*** bzw. ***Kopieren ohne Verlinkungen***).

Vorgehensweise beim Kopieren

1. Markieren Sie in der Auswahlliste der Funktion **User Maintenance** den Benutzer, dessen Sicherheitsprofil Sie duplizieren möchten, mit dem Funktionscode `CO`.
2. Es wird ein Fenster angezeigt, in dem Sie folgende Angaben machen können:

Feld	Erläuterung
To user	Nach Benutzer. Geben Sie die Kennung des "neuen" Benutzers ein.
User name	Benutzername. In diesem Feld wird der Name des bestehenden Benutzers angezeigt. Überschreiben Sie ihn mit dem Namen des "neuen" Benutzers.
With links	Mit Verlinkungen. Mit dieser Option können Sie zusätzlich zum Benutzersicherheitsprofil auch dessen Verlinkungen, Utility-Profile und Gruppen kopieren. `N` = Siehe ***Kopieren ohne Verlinkungen*** unten. `Y` = Siehe ***Kopieren mit Verlinkungen*** unten.

3. Der Bildschirm **Copy User** wird angezeigt. Er zeigt das neue Sicherheitsprofil.

   Die Bestandteile, die Sie definieren können, sind unter ***Bestandteile eines Benutzersicherheitsprofils*** beschrieben.

Kopieren ohne Verlinkungen

Wenn Sie **With links = N** wählen:

- Die Gruppen, die in der Spalte **Privileged Groups** (Privilegierte Gruppen) des bestehenden Benutzers eingetragen sind, werden *nicht* in das Sicherheitsprofil des neuen Benutzers kopiert.
- Jegliche für den vorhandenen Benutzer definierten Verlinkungen werden *nicht* auf den neuen Benutzer angewendet.
- Benutzerspezifische und benutzerbibliotheksspezifische Utility-Profile des bestehenden Benutzers werden *nicht* auf den neuen Benutzer übertragen.

Kopieren mit Verlinkungen

Wenn Sie **With links = Y** wählen:

- Verlinkungen, die für den bestehenden Benutzer existierten, werden für den neuen Benutzer kopiert, und Sie haben die Möglichkeit, die Verlinkungen, die nicht für den neuen Benutzer gelten sollen, löschen.
- Der neue Benutzer wird zu allen Gruppen hinzugefügt, in denen der existierende Benutzer enthalten ist (und alle Zugriffsrechte der Gruppen auf Bibliotheken gelten dann auch für den neuen Benutzer), und Sie haben die Möglichkeit, den neuen Benutzer aus jeder dieser Gruppen zu löschen.
- Benutzerspezifische und benutzerbibliotheksspezifische Utility-Profile, die für den bestehenden Benutzer existierten, werden für den neuen Benutzer kopiert.

Vorgehensweise:

1. Nachdem Sie Änderungen am kopierten Sicherheitsprofil vorgenommen und den Bildschirm **Copy User** durch Drücken von PF3 verlassen haben, wird eine Liste mit Bibliotheken angezeigt: Die Liste enthält alle Bibliotheken, mit denen der bestehende Benutzer direkt verlinkt ist.
2. In der Liste können Sie einzelne Bibliotheken mit CL (Cancel) markieren, um Verlinkungen aufzuheben, die Sie für den neuen Benutzer nicht gelten lassen wollen. Mit allen Bibliotheken, die Sie nicht markieren, wird der neue Benutzer automatisch auf die gleiche Weise - normale oder spezielle Verlinkung - verlinkt wie der bestehende Benutzer.
3. Wenn Sie alle direkten Verlinkungen hergestellt haben und dann die Liste der Bibliotheken durch Drücken von PF3 verlassen, wird eine Liste mit Gruppen angezeigt: Sie enthält alle Gruppen, in denen der bestehende Benutzer enthalten ist.
4. In der Liste können Sie mit CL die Gruppen markieren, zu denen der neue Benutzer nicht hinzugefügt werden soll. Der neue Benutzer wird automatisch zu allen Gruppen hinzugefügt, die Sie nicht markiert haben. Wenn eine der Gruppen, zu denen der neue Benutzer hinzugefügt wird, im Sicherheitsprofil des bestehenden Benutzers als privilegierte Gruppe (**Privileged Groups**) eingetragen ist, wird sie automatisch auch im Sicherheitsprofil des neuen Benutzers als privilegierte Gruppe eingetragen.

Benutzer ändern - Modify User

Die Funktion **Modify User** wird verwendet, um ein bestehendes Benutzersicherheitsprofil zu ändern.

Dazu:

1 Markieren Sie in der Auswahlliste der Funktion **User Maintenance** den Benutzer, dessen Sicherheitsprofil Sie ändern möchten, mit dem Funktionscode `MO`.

2 Es erscheint der Bildschirm **Modify User**, der das Sicherheitsprofil anzeigt.

Die Bestandteile, die Sie definieren oder ändern können, sind unter *Bestandteile eines Benutzersicherheitsprofils* beschrieben.

Herauf- und Herabstufung von Benutzern

Bei Bedarf können Sie die Einstufung des Benutzertyps einer Einzelperson ändern.

Um den Benutzertyp zu ändern, müssen Sie zuerst den neuen Benutzertyp eingeben und ENTER drücken, um den entsprechenden Bildschirm **Modify User** (Benutzer ändern) zu erhalten, bevor Sie das Sicherheitsprofil weiter ändern, da die **Modify User**-Bildschirme für die verschiedenen Benutzertypen nicht identisch sind.

Benutzertyp eines Benutzers heraufstufen

Sie können ein MITGLIED zu einer PERSON oder einem ADMINISTRATOR heraufstufen und Sie können eine PERSON zu einem ADMINISTRATOR heraufstufen.

Benutzertyp eines Benutzers herabstufen

Sie können einen ADMINISTRATOR zu einer PERSON oder einem MEMBER herunterstufen und Sie können eine PERSON zu einem MEMBER herunterstufen.

- Bevor Sie einen Benutzer vom Benutzertyp ADMINISTRATOR zum Benutzertyp PERSON herunterstufen können, müssen Sie ihn als Eigentümer aus jedem Sicherheitsprofil entfernen, in dem er als Eigentümer angegeben ist.

  Solange ein ADMINISTRATOR noch Eigentümer eines Sicherheitsprofils ist, kann er nicht heruntergestuft werden.
- Bevor Sie einen Benutzer von ADMINISTRATOR auf MEMBER herunterstufen können, müssen Sie Folgendes tun:
  - Entfernen Sie ihn als Eigentümer aus jedem Sicherheitsprofil, in dem er als Eigentümer angegeben ist. Solange ein ADMINISTRATOR noch Eigentümer eines Sicherheitsprofils ist, kann er nicht heruntergestuft werden.

- Entfernen Sie alle direkten Verlinkungen von dem Benutzer zu Bibliotheken/externen Objekten. Solange der Benutzer mit einer Bibliothek oder einem externen Objekt verlinkt ist, kann er nicht MEMBER werden.
- Löschen Sie die private Bibliothek des ADMINISTRATORs (falls definiert). Solange der Benutzer über eine private Bibliothek verfügt, kann er kein Member werden.

- Bevor Sie einen Benutzer von PERSON zu MEMBER herunterstufen können, müssen Sie alle direkten Verknüpfungen vom Benutzer zu Bibliotheken/externen Objekten entfernen. Solange der Benutzer mit einer Bibliothek oder einem externen Objekt verlinkt ist, kann er kein Member werden. Darüber hinaus müssen Sie die private Bibliothek der PERSON löschen (falls definiert). Solange der Benutzer eine private Bibliothek hat, kann er kein Member werden.

Benutzer gesperrt?

Wenn die **Lock User Option** (siehe *Administrator Services*) aktiv ist, kann es vorkommen, dass das Sicherheitsprofil des Benutzers gesperrt wurde.

Wenn das Sicherheitsprofil gesperrt ist, wird dies auf dem Bildschirm **Modify User** durch die Meldung angezeigt:

```
This user is currently locked due to logon/countersign error!
```

(Dieser Benutzer ist derzeit aufgrund eines Anmelde-/Gegenzeichnungsfehlers gesperrt!)

Wenn Sie in das Feld **Unlock? (Y/N)** ein `Y` eingeben, wird ein Fenster angezeigt, das ausführliche Informationen darüber enthält, wie und wann die Sperrung erfolgte. In diesem Fenster können Sie auch das Sicherheitsprofil entsperren.

Anmerkung: Sie können gesperrte Benutzer auch mit der Funktion **List/Unlock Locked Users** (Gesperrte Benutzer auflisten/entsperren) anzeigen und entsperren (siehe *Administrator Services*).

Benutzer umbenennen - Rename User

Mit der Funktion **Rename User** können Sie die Benutzerkennung eines bestehenden Benutzersicherheitsprofils ändern.

Dazu:

1 On the **User Maintenance** selection list, mark the user whose ID you wish to change with function code `RE`.

Markieren Sie in der Auswahlliste **User Maintenance** den Benutzer, dessen Kennung Sie ändern möchten, mit dem Funktionscode `RE`.

2 Es wird ein Fenster angezeigt, in dem Sie eine neue Kennung für den Benutzer eingeben (und optional den Namen des Benutzers ändern) können.

Die folgenden Benutzer können nicht umbenannt werden:

- ein Administrator, der Eigentümer eines oder mehrerer Sicherheitsprofile ist,
- ein Benutzer, der in einem oder mehreren DDM-/Datei-Sicherheitsprofilen als DDM-Änderer (Modifier) angegeben ist.

Benutzer löschen - Delete User

Die Funktion **Delete User** wird verwendet, um ein bestehendes Benutzersicherheitsprofil zu löschen.

Dazu:

1 Markieren Sie in der Auswahlliste **User Maintenance** den Benutzer, dessen Kennung Sie ändern möchten, mit dem Funktionscode `RE`.

2 Das Fenster **Delete User** wird angezeigt.

- Wenn Sie sich gegen das Löschen des Benutzersicherheitsprofils entscheiden, können Sie das Fenster, indem Sie ENTER drücken, verlassen, ohne etwas eingegeben zu haben.
- Um das Benutzersicherheitsprofil zu löschen, müssen Sie die Kennung des Benutzers in das Fenster eingeben, um die Löschung zu bestätigen.

Abhängig von der Einstellung der allgemeinen Option **Allow Deletion of Users Who Are Owners/DDM Modifiers** (Löschen von Benutzern, die Eigentümer/DDM-Änderer sind, zulassen) (siehe *Administrator Services*), ist es nicht möglich, ein Benutzersicherheitsprofil zu löschen, wenn der Benutzer in einem Sicherheitsprofil als Eigentümer oder in einem DDM-/Datei-Sicherheitsprofil als DDM-Änderer angegeben ist.

Wenn Sie mehr als einen Benutzer mit `DE` markieren, wird ein Fenster angezeigt, in dem Sie gefragt werden, ob Sie die Löschung jedes einzelnen Benutzersicherheitsprofils durch Eingabe der Kennung des Benutzers bestätigen möchten oder ob alle zum Löschen ausgewählten Benutzer ohne diese Einzelbestätigung gelöscht werden sollen. Achten Sie darauf, dass Sie nicht versehentlich einen Benutzer löschen.

Anmerkung: Wenn Sie ein Gruppensicherheitsprofil löschen, werden die einzelnen Sicherheitsprofile der dieser Gruppe zugeordneten Benutzer nicht gelöscht.

Benutzer anzeigen - Display User

Die Funktion **Display User** wird verwendet, um ein bestehendes Benutzersicherheitsprofil anzuzeigen.

Dazu:

1 Markieren Sie in der Auswahlliste **User Maintenance** den Benutzer, dessen Sicherheitsprofil Sie anzeigen möchten, mit dem Funktionscode `DI`.

2 Sie gelangen auf den Bildschirm **Display User**, der das Sicherheitsprofil anzeigt.

Seine Bestandteile werden unter *Bestandteile eines Benutzersicherheitsprofils* erläutert.

Benutzer gesperrt?

Wenn die **Lock User Option** (beschrieben im Kapitel *Administrator Services*) aktiv ist, kann es vorkommen, dass das Sicherheitsprofil des Benutzers gesperrt wurde.

Wenn das Sicherheitsprofil gesperrt ist, wird dies auf dem Bildschirm **Display User** durch die Meldung angezeigt:

```
This user is currently locked due to logon/countersign error!
```

(Dieser Benutzer ist derzeit aufgrund eines Anmelde-/Gegenzeichnungsfehlers gesperrt!)

Wenn Sie in das Feld **Lock Info (Y/N)** ein `Y` eingeben, wird ein Fenster angezeigt, das ausführliche Informationen darüber enthält, wie und wann die Sperrung erfolgte.

Gruppenmitglieder editieren - Editing Group Members

Die Funktion **Edit Group Members** wird verwendet, um Benutzer zu einer Gruppe zuzuweisen oder aus ihr zu löschen.

Solange die Anzahl der einer Gruppe zugewiesenen Benutzer nicht mehr als 5 beträgt, können die Gruppenmitglieder in der Spalte Members des Sicherheitsprofils der Gruppe mit der Funktion **Modify User** verwaltet werden. Bei größeren Gruppen muss die Mitgliederverwaltung mittels der Funktion **Edit Group Members** durchgeführt werden.

Anmerkung: Die Anzahl der Gruppenmitglieder, die Sie mit der Funktion **Edit Group Members** (Gruppenmitglieder editieren) verwalten können, ist durch interne Speicherbeschränkungen begrenzt, die durch den Natural-Profilparameter `ESIZE` festgelegt werden. Um eine größere Anzahl von Gruppenmitgliedern zu verwalten, können Sie die Anwendungsprogrammierschnittstelle `NSCUS` verwenden. Mit `NSCUS` können Sie Gruppen mit bis zu 99.999 Mitgliedern verwalten.

Um die Funktion Edit Group Members aufzurufen:

Sie können die Funktion **Edit Group Members** auf zwei Arten aufrufen:

- Markieren Sie in der Auswahlliste **User Maintenance** die Gruppe, die Sie editieren möchten, mit dem Funktionscode `EG`.
- Markieren Sie im Sicherheitsprofil einer Gruppe im Fenster **Additional Options** die Option **Group Editor** mit einem beliebigen Zeichen. Der Bildschirm **Edit Group Members** wird angezeigt:

Der Bildschirm **Edit Group Members** wird angezeigt:

```
>                     > +   Gr ELGRUPO                  Size 7    Line 1
  ALL  User ID             User Name                Type        Status
       -------- -------------------------------- ---- --------------------
       AD       ARTHUR DENT                      A
       AT       TIFFANY ACHING                   M
       MT       MERCY THOMPSON                   M
       RM       RACHEL MORGAN                    P
       TAK      THE ANALOG KID                   M
       TW2112   WEINRIB'S TERMINAL               T
       UBG      UNBEARABLE BOY GROUP             G
```

Der Bildschirm **Edit Group Members** ist ein modifizierter Natural-Programm-Editor. Wenn Sie ihn aufrufen, werden die Benutzer, die bereits in der angegebenen Gruppe enthalten sind, in den Quellcodebereich eingelesen. Die Liste der Gruppenmitglieder ist in alphabetischer Reihenfolge der Benutzerkennungen sortiert. Für jeden Benutzer werden die Benutzerkennung, der Benutzername und der Benutzertyp angezeigt.

Liste der Gruppenmitglieder editieren

Um die Liste zu editieren, können Sie die Blätter-, Zeilen- und Editorkommandos des Natural-Programm-Editors verwenden (wie in der Dokumentation der Natural-Editoren beschrieben).

Um einen Benutzer zur Gruppe hinzuzufügen, müssen Sie die Benutzerkennung in die Liste aufnehmen. Um einen Benutzer aus der Gruppe zu entfernen, müssen Sie die Benutzerkennung aus der Liste löschen.

Denken Sie daran, dass Benutzer erst in Natural Security definiert werden müssen, bevor sie einer Gruppe hinzugefügt werden können.

Es ist nicht wichtig, in welcher Reihenfolge Sie neue Benutzerkennungen angeben: Wenn Sie die Liste der Gruppenmitglieder katalogisieren (siehe unten), werden sie automatisch alphabetisch sortiert.

Um alle Benutzer, die in einer Gruppe enthalten sind, zu der Gruppe, die Sie editieren, hinzuzufügen, können Sie das Kommando `INCLUDE` *`group-ID`* in der Kommandozeile des Bildschirms

Edit Group Members eingeben. Alle Benutzer, die in der Gruppe enthalten sind, deren Kennung Sie mit dem INCLUDE-Kommando angeben, werden dann in die Liste aufgenommen. Sie werden vor dem Benutzer aufgeführt, der in der obersten Zeile des Bildschirms angezeigt wird.

Alternativ können Sie eine Gruppe innerhalb einer Gruppe haben, d.h. Sie fügen die Gruppenkennung zu der Liste der Gruppenmitglieder hinzu, die Sie bearbeiten.

Änderungen speichern

Änderungen werden nur im Quellcodebereich bearbeitet, bis Sie sie katalogisieren. Dazu müssen Sie in der Kommandozeile das Kommando CATALOG eingeben, oder PF3 drücken. Dieses Kommando ruft zunächst eine Prozedur auf, die auf doppelte Kennungen prüft. Wenn alle Kennungen eindeutig sind, wird die bearbeitete Liste der Mitglieder in das Sicherheitsprofil der Gruppe eingetragen.

Um nur den Prüfvorgang aufzurufen, können Sie das Kommando CHECK verwenden.

Wenn Sie die Liste der Gruppenmitglieder katalogisieren, wird der User Exit NSCUSEX2 aufgerufen. Er zeigt eine Liste der Gruppenmitglieder an, die angibt, welche Mitglieder der Gruppe hinzugefügt und welche aus ihr entfernt wurden.

Um den Bildschirm **Edit Group Members** zu verlassen, müssen Sie in der Kommandozeile einen Punkt (.) eingeben.

Verlinkungen eines Benutzers kopieren - Copy User's Links

Mit der Funktion **Copy User's Links** können Sie Verlinkungen aus einem bestehenden Benutzersicherheitsprofil in ein anderes des gleichen Benutzertyps kopieren.

Sie können die zu kopierenden Links einzeln auswählen. Zusätzlich zu den Links können Sie auch Gruppenmitgliedschaften (einschließlich der Angaben zu privilegierten Gruppen) und Funktionssicherheitsdefinitionen kopieren.

Dazu:

1. Markieren Sie in der Auswahlliste **User Maintenance** den Benutzer, dessen Links Sie kopieren möchten, mit dem Funktionscode CP.
2. Es erscheint ein Fenster, in dem Sie die Kennung des Benutzers eingeben können, zu dem Sie Links kopieren möchten.

   Außerdem können Sie in dem Fenster die Auswahl der Linktypen einschränken:

Linktyp	Bedeutung
Library links	Bibliotheksverlinkungen
Groups/Members	Gruppen/Mitglieder
Utility links	Dienstprogramm-(Utility-)Verlinkungen
Functional security	Funktionssicherheit
File links	Dateiverlinkungen (wenn der Benutzer eine private Bibliothek hat)
Environment links	Umgebungsverlinkungen
External object links	Externe Objektverlinkungen

Standardmäßig sind alle oben genannten Linktypen ausgewählt. Um die Auswahl eines Typs aufzuheben, müssen Sie das `O` entfernen.

3 Es wird eine Liste aller bestehenden Links des ersten Benutzers (mit den ausgewählten Typen) angezeigt.

Die aufgelisteten Links sind nicht automatisch zum Kopieren vorausgewählt. In der Spalte **Co** der Liste müssen Sie mit dem Funktionscode `CO` jede Verlinkung markieren, die Sie von dem einen auf den anderen Benutzer kopieren möchten.

Sie können einen oder mehrere Links pro Bildschirm markieren. Für jeden markierten Link wird eine Meldung angezeigt, die angibt, ob er kopiert wurde. Wenn ein Link nicht kopiert werden kann, wird dies ebenfalls angezeigt. Wenn zum Beispiel ein Benutzer bereits einen Link zu einem bestimmten Objekt hat, kann dieser nicht durch einen vom anderen Benutzer kopierten Link ersetzt werden.

9 Bibliotheken verwalten

- Bestandteile eines Bibliothekssicherheitsprofils 160
- Bibliothekssicherheitsprofile anlegen und verwalten 191

Eine Bibliothek (*Library*) wird in Natural Security definiert, indem ein *Bibliothekssicherheitsprofil* erstellt wird. Das Bibliothekssicherheitsprofil bestimmt die Bedingungen, unter denen die Bibliothek verwendet werden darf.

In diesem Kapitel werden die folgenden Themen behandelt:

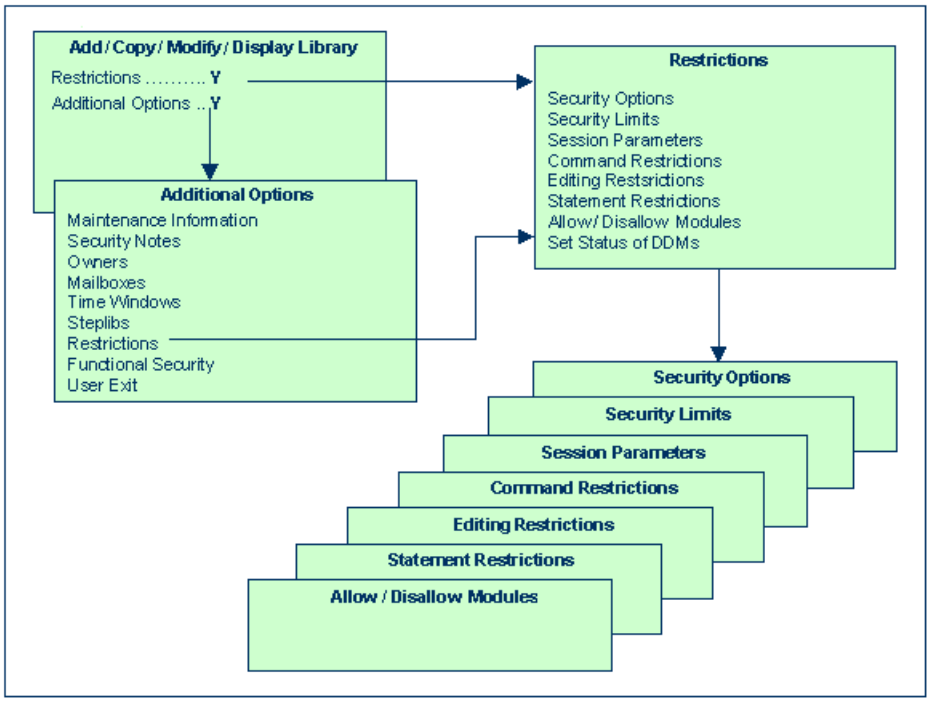
Bestandteile eines Bibliothekssicherheitsprofils

In diesem Abschnitt werden die folgenden Themen behandelt:

- Übersicht über die Bestandteile eines Bibliothekssicherheitsprofils
- Bestandteile eines typischen Basisbildschirms eines Bibliothekssicherheitsprofils
- Allgemeine Optionen (Bibliothek) - General Options (Library)
- Bibliotheksdatei - Library File
- Bibliotheks-ETID - Library ETID
- Transaktionen - Transactions

- Zusätzliche Optionen (Bibliothek) - Additional Options (Libraries)

Übersicht über die Bestandteile eines Bibliothekssicherheitsprofils



Bestandteile eines typischen Basisbildschirms eines Bibliothekssicherheitsprofils

Der folgende Bildschirm ist der typische Basisnildschirm, der angezeigt wird, wenn Sie eine der Funktionen Add/Anlegen, Copy/Kopieren, Modify/Ändern, Display/Anzeigen für ein Bibliotheks-sicherheitsprofil aufrufen, hier für die Funktion „Modify Library“:

```
15:52:08                    *** NATURAL SECURITY ***                 2021-12-31
                               - Modify Library -

                                                Modified .. 2021-12-12 by SAG
Library ID ..... TESTLIB
Library Name ... ____________________________________

    General Options            Library File               Transactions
-----------------------   -----------------------   ---------------------------
People-protected .... N   DBID ........ _____       Startup .......... ________
Terminal-protected .. N   FNR ......... _____       Batch execution .. Y
Restrictions ........ Y   Password .... ________    Restart .......... ________
Logon recorded ...... N   Ciphercode .. ________    Error ............ ________
Utilities ........... O   Read Only ... _
Programming mode .... R                             User exit ........ ________
Cross-reference ..... N
Restart ............. N


Additional Options ... N




Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help  PrevM Exit  AddOp Restr Flip                                 Canc
```

Die einzelnen Bestandteile, die Sie als Teile eines Bibliothekssicherheitsprofils definieren können, werden im Folgenden erläutert.

Feld	Erläuterung
Library ID (nur Anzeige)	Bibliothekskennung. Die Kennung der Bibliothek, wie sie beim Anlegen des Bibliothekssicherheitsprofils angegeben wurde.
Library Name	Bibliotheksname. Sie können einen Namen für die Bibliothek eingeben, der bis zu 32 Zeichen lang sein kann.

Allgemeine Optionen (Bibliothek) - General Options (Library)

Feld	Erläuterung
People-protected/Terminal-protected	Personengeschützt/Terminalgeschützt. Sie können angeben, ob die Bibliothek *people-protected* und/oder *terminal-protected* sein soll, um die Nutzung der Bibliothek einzuschränken. Die möglichen Schutzkombinationen sind unter ***Geschützte Bibliotheken*** im Kapitel *Bibliotheken schützen* beschrieben.
Restrictions	Einschränkungen. Für die Bibliothek können spezielle Einschränkungen definiert werden, wie unter ***Zusätzliche Optionen***

Feld	Erläuterung	
	(Bibliothek) - Additional Options (Libraries) weiter unten beschrieben. ■ Wenn keine Einschränkungen definiert sind, gilt das im Natural-Parametermodul definierte Systemprofil. ■ Wenn Einschränkungen definiert sind, wird der Wert dieses Feldes automatisch auf `Y` gesetzt. Wenn Sie es wieder auf `N` setzen, werden alle Angaben, die Sie in den Einschränkungen gemacht haben, automatisch gelöscht!	
Logon recorded	Anmeldung aufgezeichnet. Diese Option legt fest, ob Anmeldungen bei der Bibliothek aufgezeichnet werden sollen oder nicht.	
	Y	Jedes Mal, wenn sich ein Benutzer bei der Bibliothek anmeldet, wird von Natural Security ein Anmeldesatz geschrieben. Sie können die Aktivitäten der Benutzer überprüfen, indem Sie diese Anmeldesätze einsehen (weitere Informationen finden Sie unter *Anmeldesätze - Logon Records* im Kapitel *Administrator Services*).
	N	Anmeldungen bei der Bibliothek werden nicht aufgezeichnet.
Utilities	Dienstprogramme. Für eine konsistente Steuerung der Nutzung von Natural-Dienstprogrammen sollten Utility-Profile verwendet werden. Sie werden im Kapitel *Dienstprogramme (Utilities) schützen* beschrieben. Diese Option gilt für die folgenden Natural-Dienstprogramme: ■ SYSERR - wenn für dieses Dienstprogramm kein Utility-Profil definiert ist. ■ SYSMAIN - wenn kein Utility-Profil für SYSMAIN definiert ist; oder wenn die Session Option **Utilities Option** im Standardsicherheitsprofil des SYSMAIN-Dienstprogramms auf `Y` oder `O` gesetzt ist. ■ SYSOBJH (Natural Object Handler) - wenn die Session-Option **Utilities Option** im Standardsicherheitsprofil des Dienstprogramms auf `Y` oder `O` gesetzt ist. Unter dieser Bedingung bestimmt diese Option, wer das Dienstprogramm verwenden darf, um den Inhalt der Bibliothek zu bearbeiten. Mögliche Werte:	
	N	Kein Schutz - Der Inhalt der Bibliothek kann von jedem Benutzer bearbeitet werden.

Feld	Erläuterung	
	O	Berechtigung für Eigentümer - Der Inhalt der Bibliothek kann nur von den *Eigentümern* (Owners) des Bibliothekssicherheitsprofils bearbeitet werden. Wenn kein Eigentümer angegeben ist, kann jeder Benutzer vom Typ Administrator den Inhalt bearbeiten. Im Falle einer privaten Bibliothek darf neben den Eigentümern auch der Benutzer mit der gleichen Kennung wie die Bibliothekskennung den Inhalt der Bibliothek bearbeiten. Im Batch-Modus kann ein Eigentümer, der die Gegenzeichnung eines Miteigentümers benötigt, den Inhalt der Bibliothek nicht bearbeiten (da Gegenzeichnungen im Batch-Modus nicht möglich sind). Im Online-Modus: Wenn die Session Option **Utilities Option** im Standardsicherheitsprofil von SYSMAIN oder SYSOBJH auf `0` gesetzt ist und ein Eigentümer eine Gegenzeichnung anfordert, wird die Aufforderung zur Gegenzeichnung unterdrückt und die Bibliothek von der Verarbeitung in SYSMAIN/SYSOBJH ausgeschlossen.
	P	Berechtigung unter Schutzregeln - Der Inhalt der Bibliothek kann unter *Schutzregeln* verarbeitet werden, d. h. nur von Benutzern, die sich bei der Bibliothek anmelden dürfen. Für private Bibliotheken im privaten Modus gilt Folgendes: Der Benutzer mit der gleichen Kennung wie die Bibliothekskennung darf den Inhalt der Bibliothek bearbeiten. Alle anderen dürfen ihn nur nach Eingabe des Passworts dieses Benutzers (auf einem dafür vorgesehenen Bildschirm zur Gegenzeichnung) bearbeiten. Beachten Sie, dass ein Benutzer im Batch-Modus den Inhalt der privaten Bibliothek eines anderen Benutzers nicht bearbeiten kann (da im Batch-Modus kein Passwort eingegeben werden kann).
	Wenn das Natural-Systemkommando `SCAN` für die Bibliothek erlaubt ist (siehe ***Kommandoeinschränkungen - Command Restrictions*** unten), gilt diese Option auch für das Kommando SCAN.	

Feld	Erläuterung	
Programming mode	Natural-Programmiermodus:	
	S	(= Structured mode) - Der zu verwendende Programmiermodus kann *nicht* mit dem Natural-Profil-/Session-Parameter SM geändert werden, es gilt immer der Structured Mode.
	R	(= Reporting mode) - Die Einstellung des Natural-Profil-/Session-Parameters SM (siehe Natural-*Parameter-Referenz*-Dokumentation) bestimmt den zu verwendenden Modus.
	Siehe auch **Natural programming mode** in *Voreingestellte Werte für Bibliothekssicherheitsprofile - Library Preset Values*.	
Cross-reference	Diese Option bestimmt, ob eine aktive Cross-Referenz in Predict (falls installiert) für die Bibliothek generiert wird.	
	Y	Yes - Es wird eine aktiver Cross-Referenz generiert.
	N	No - Es wird keine aktive Cross-Referenz generiert.
	F	Force - Es wird eine aktive Cross-Referenz erzwungen.
	D	Doc - Die zu katalogisierenden Objekte müssen in Predict dokumentiert sein. Es wird jedoch keine aktive Cross-Referenz generiert.
	Einzelheiten zu aktiven Cross-Referenzen finden Sie in der *Predict*-Dokumentation.	
Restart	Y	Die Bibliothek kann durch Eingabe von RESTART als Bibliothekskennung auf dem Anmeldebildschirm neu aufgerufen werden. Während des Anmeldevorgangs wird ein Adabas-OPEN-Kommando mit End of Transaction-Kennung (ETID) ausgeführt.
	N	Die Bibliothek kann nicht durch Eingabe von RESTART neu aufgerufen werden. Die in Natural Security angegebene ETID wird nicht für das Adabas-OPEN-Kommando verwendet.
Version control (nur Anzeige)	Dieses Feld gilt nur auf Großrechnern und wenn die Bibliothek unter der Kontrolle von Predict Application Control steht. In diesem Feld wird der Versionskontrollstatus der Bibliothek angezeigt. Wenn die Bibliothek von Predict Application Control gesteuert wird, werden auch die Datenbankkennung (DBID) und die Dateinummer (FNR) der FDIC-Systemdatei, in der die Predict-Daten der Bibliothek gespeichert sind, angezeigt.	

Bibliotheksdatei - Library File

Diese Teile betreffen:

- die Datenbankdatei, in der die in der Bibliothek enthaltenen Quellcodeprogramme und Objektmodule gespeichert werden sollen (FUSER).
- die Datenbankdatei, in der die aktiven Predict-Cross-Referenzen, die sich auf die Bibliothek beziehen, gespeichert werden sollen (FDIC).

Die FDIC-Einstellungen können nur festgelegt werden, wenn die Option **Library FDIC Assignment Enabled** in **Administrator Services > Library Preset Values** auf `Y` gesetzt ist.

Die hier im Bibliothekssicherheitsprofil angegebenen `FUSER`- und `FDIC`-Werte haben Vorrang vor den entsprechenden Werten der Natural-Profilparameter `FUSER` und `FDIC`, die zu Beginn der Natural-Sitzung gelten. Für Werte, die hier im Bibliothekssicherheitsprofil nicht angegeben sind, gelten die entsprechenden Werte der Profilparameter `FUSER` und `FDIC`.

Für Natural-Systembibliotheken, d.h. alle Bibliotheken, deren Kennung mit `SYS` beginnt (außer der Bibliothek `SYSTEM`), können Sie hier keine Angaben machen. Für diese Bibliotheken gelten die Angaben des Natural-Profilparameters `FNAT`.

Für Bibliotheken, die unter der Kontrolle von Predict Application Control stehen, können Sie hier keine FDIC-Angaben machen. Für diese Bibliotheken gelten die Angaben des Natural-Profilparameters `FDIC`.

Feld	Erläuterung
FUSER	
DBID/FNR	Die Datenbankkennung und Dateinummer der FUSER-Datei.
Password ([1])	Passwort. Wenn die Bibliotheksdatei passwortgeschützt ist, muss das Adabas-Passwort (bei VSAM-Dateien der VSAM-DD-Name) in dieses Feld eingegeben werden, damit Natural auf die Datei zugreifen kann.
Cipher code ([1])	Chiffriercode. Wenn die Bibliotheksdatei verschlüsselt ist, muss der Adabas-Chiffriercode (bei VSAM-Dateien das VSAM-Passwort) in dieses Feld eingegeben werden, damit Natural auf die Datei zugreifen kann.
Read-only	Nur lesen. Wenn Sie möchten, dass die Bibliotheksdatei schreibgeschützt ist, müssen Sie dieses Feld mit einem `O` markieren (dies entspricht der Option `RO` des Profilparameters `FUSER`).
FDIC	
DBID/FNR	Die Datenbankkennung und Dateinummer der FDIC-Datei. Wenn Sie hier `0` als Datenbankkennung angeben, gilt der DBID-Wert des Profilparameters `FDIC`.
Password ([1])	Passwort. Wenn die FDIC-Datei passwortgeschützt ist, muss das Adabas-Passwort (bei VSAM-Dateien der VSAM-DD-Name) in dieses Feld eingegeben werden, damit Natural auf die Datei zugreifen kann.

Feld	Erläuterung
Cipher code ([1])	Chiffriercode. Wenn die FDIC-Datei verschlüsselt ist, muss der Adabas-Chiffriercode (bei VSAM-Dateien das VSAM-Passwort) in dieses Feld eingegeben werden, damit Natural auf die Datei zugreifen kann.
Read-only	Nur lesen. Wenn Sie möchten, dass die FDIC-Datei schreibgeschützt ist, müssen Sie dieses Feld mit einem `O` markieren (dies entspricht der Option `RO` des Profilparameters `FDIC`).

([1]) Die Felder **Password** und **Cipher code** gelten nur für Großrechner, unter Linux und Windows haben sie keine Funktion. Um unbefugten Zugriff oder die Preisgabe sensibler Informationen zu verhindern, wird jeder eingegebene Wert mit einem Stern (*) maskiert.

Bezüglich der Natural Development Server-Umgebung und der in Eclipse verwendeten Natural-Server siehe auch die folgenden Abschnitte:

- ***Map Environment und Bibliotheksauswahl*** unter *Natural Development Server-Umgebung und -Anwendungen schützen*
- ***Map Environment und Bibliotheksauswahl*** unter *Natural-Entwicklungsumgebung in Eclipse schützen*

Anmerkung: Für die Verwendung des Natural-Dienstprogramms SYSMAIN gilt Folgendes: Wenn im Sicherheitsprofil einer Bibliothek FDIC-Werte angegeben sind und die Bibliothek in einer SYSMAIN-Funktion als Quell- oder Zielbibliothek ausgewählt wird, können in SYSMAIN keine anderen FDIC-Werte für diese Bibliothek verwendet werden.

Bibliotheks-ETID - Library ETID

Feld	Erläuterung
ETID (nur Anzeige)	Dieses Feld enthält den bibliotheksspezifischen Bestandteil der Kennung für End of Transaction-Daten. Weitere Informationen zu ETIDs finden Sie unter ***Bestandteile eines Benutzersicherheitsprofils***.

Transaktionen - Transactions

Feld	Erläuterung
Startup	Sie können den Namen einer Startup-Transaktion eingeben; diese Transaktion wird immer unmittelbar nach einer erfolgreichen Anmeldung bei der Bibliothek aufgerufen. Siehe auch die Natural-Systemvariable `*STARTUP`. Der Name der Startup-Transaktion wird in der Natural-Systemvariablen `*STARTUP` abgelegt. Wenn sie auch im Batch-Modus ausgeführt wird, wird ihr Name nur dann in `*STARTUP` eingetragen, wenn **Batch Execution** (siehe unten) auf "S" gesetzt ist.

Feld	Erläuterung	
Batch execution	Ausführung im Batch-Modus. Dieses Feld gilt nur, wenn die Natural-Systemvariable *DEVICE auf BATCH gesetzt ist (andernfalls hat ihr Wert keine Wirkung). Es bestimmt, ob die im Bibliothekssicherheitsprofil angegebene Startup-Transaktion (siehe oben) auch im Batch-Modus ausgeführt wird. Sie können einen der folgenden Werte angeben:	
	Y	Die Startup-Transaktion wird auch (einmal) im Batch-Modus ausgeführt.
	S	Die Startup-Transaktion wird auch im Batch-Modus ausgeführt; zusätzlich wird ihr Name in die Natural-Systemvariable *STARTUP gestellt.
	N	Wenn die NEXT/MORE-Zeile für die Bibliothek erlaubt ist (siehe *Security Options* unten), wird die Startup-Transaktion *nicht* im Batch-Modus ausgeführt. Wenn die NEXT/MORE-Zeile *nicht* erlaubt ist, wird die Startup-Transaktion auch (einmal) im Batch-Modus ausgeführt.
	Siehe auch ***Natural Security im Batch-Modus***.	
Restart	Neustart. Sie können den Namen einer Neustart-Transaktion eingeben. Diese Transaktion wird immer aufgerufen, wenn die Bibliothek durch Eingabe von RESTART als Bibliothekskennung auf dem Anmeldebildschirm erneut aufgerufen wird.	
Error	Fehler Sie können den Namen einer Fehlertransaktion eingeben. Diese Transaktion wird nach dem Auftreten eines Ausführungszeitfehlers aufgerufen (wenn das Programm kein ON ERROR-Statement enthält oder wenn es einen ON ERROR-Block enthält, der nicht mit einem FETCH-, STOP-, TERMINATE- oder RETRY-Statement verlassen wird); wenn der Natural-Profilparameter SYNERR auf ON gesetzt ist, kann die Fehlertransaktion auch Syntaxfehler behandeln. Weitere Informationen zu Fehlertransaktionen finden Sie unter *Fehlertransaktionsprogramm verwenden* in the Natural *Programming Guide*. **Anmerkung:** Wenn hier keine Fehlertransaktion angegeben wird, erhält das mit dem Natural-Profilparameter ETA (beschrieben in der Natural-*Parameter-Referenz*-Dokumentation) angegebene Programm die Kontrolle, wenn ein Fehler auftritt. Tritt ein Fehler bei einer Erstanmeldung auf, erhält das mit dem Profilparameter ETA angegebene Programm ebenfalls die Kontrolle (bei anderen Anmeldefehlern gilt die Fehlertransaktion, die in der Bibliothek angegeben ist, *von der aus* Sie sich bei einer anderen Bibliothek anmelden).	

User Exit

Zu jedem Bibliothekssicherheitsprofil und Special-Link-Profil können Sie 250 Byte Zusatzdaten Ihrer Wahl hinterlegen.

Diese zusätzlichen Daten können mit Hilfe eines User Exit-Subprogramms gespeichert/gelesen werden, das ein `CALLNAT`-Statement (mit fünf Parametern wie unten beschrieben) enthalten muss, das wiederum eines der folgenden Subprogramme aufruft:

Subprogramm	Funktion
`SNAASEXT`	Zusätzliche Bibliotheksdaten speichern.
`SNAAREXT`	Zusätzliche Bibliotheksdaten lesen.
`SNAUSEXT`	Zusätzliche Special-Link-Daten speichern.
`SNAUREXT`	Zusätzliche Special-Link-Daten lesen.

Diese vier Subprogramme sind in der Natural-Security-Bibliothek `SYSSEC` enthalten.

Geben Sie im Feld **User Exit** des Bibliothekssicherheitsprofils oder des Special-Link-Profils den Namen des User Exits ein, der eines der oben genannten Subprogramme aufruft.

Um den User Exit aufzurufen, müssen Sie im Fenster **Additional Options** die Option **User Exit** mit `Y` markieren (siehe unten).

Wenn Sie die Zusatzdaten aus einer Bibliothek heraus bearbeiten wollen, können Sie die oben genannten Subprogramme auch über einen User Exit aus einer Bibliothek selbst aufrufen. In diesem Fall müssen Sie die Subprogramme in diese Bibliothek kopieren (mit Hilfe des Dienstprogramms `SYSMAIN`). Beim Aufruf aus einer Bibliothek prüft jedes Subprogramm und stellt sicher, dass nur Daten, die diese Bibliothek oder den angegebenen Link betreffen, gelesen/gespeichert werden.

In den Sicherheitsprofilen der Natural-Systembibliotheken, d.h. aller Bibliotheken, deren Kennung mit "SYS" beginnt (außer der Bibliothek `SYSTEM`), können Sie keinen User Exit angeben.

SNAASEXT

Das Subprogramm `SNAASEXT` wird verwendet, um zusätzliche Bibliotheksdaten zu speichern. Es muss mit den folgenden fünf Parametern aufgerufen werden:

Parameter	Format/Länge	Inhalt, der an SNAASEXT übergeben wird	Inhalt, der von SNAASEXT zurückgegeben wird
1.	A8	keiner	Bibliothekskennung
2.	A32	keiner	Bibliotheksname
3.	D	keiner	Datum der letzten Änderung
4.	A250	**Zu speichernde Daten**	wie die übergebenen
5.	B2	keiner	Rückgabecode

SNAAREXT

Das Subprogramm SNAAREXT wird zum Lesen zusätzlicher Bibliotheksdaten verwendet. Es muss mit den folgenden fünf Parametern aufgerufen werden:

Parameter	Format/Länge	Inhalt, der an SNAAREXT übergeben wird	Inhalt, der von SNAAREXT zurückgegeben wird
1.	A8	keiner	Bibliothekskennung
2.	A32	keiner	Bibliotheksname
3.	D	keiner	Datum der letzten Änderung
4.	A250	keiner	**Gelesene Daten**
5.	B2	keiner	Rückgabecode

Wenn Sie SNAAREXT oder SNAASEXT aus einem Bibliothekssicherheitsprofil in SYSSEC aufrufen, beziehen sich die Daten auf die Bibliothek, die Sie gerade verwalten. Wenn Sie sie von außerhalb von SYSSEC aufrufen, beziehen sich die Daten auf die Bibliothek, aus der Sie das Subprogramm aufrufen.

SNAUSEXT

Das Subprogramm SNAUSEXT wird verwendet, um zusätzliche Special-Link-Daten zu speichern. Es muss mit den folgenden fünf Parametern aufgerufen werden:

Parameter	Format/Länge	Inhalt, der an SNAUSEXT übergeben wird	Inhalt, der von SNAUSEXT zurückgegeben wird
1.	A8	keiner	Bibliothekskennung
2.	A8	Benutzerkennung (muss nur angegeben werden, wenn SNAUSEXT von außerhalb von SYSSEC aufgerufen wird)	Bibliotheksname
3.	D	keiner	Datum der letzten Änderung
4.	A250	**Zu speichernde Daten**	wie die übergebenen
5.	B2	keiner	Rückgabecode

SNAUREXT

Das Subprogramm SNAUREXT wird verwendet, um zusätzliche Special-Link-Daten zu lesen. Es muss mit den folgenden fünf Parametern aufgerufen werden:

Parameter	Format/Länge	Inhalt, der an SNAUREXT übergeben wird	Inhalt, der von SNAUREXT zurückgegeben wird
1.	A8	keiner	Bibliothekskennung
2.	A8	Benutzerkennung (muss nur angegeben werden, wenn SNAUREXT von außerhalb von SYSSEC aufgerufen wird)	Bibliotheksname
3.	D	keiner	Datum der letzten Änderung
4.	A250	keiner	**Gelesene Daten**
5.	A2/B2	*	Rückgabecode *

* Wenn Sie SNAUREXT von außerhalb von SYSSEC aufrufen, können Sie mehrere Special-Links zur Bibliothek lesen, indem Sie den 2. Parameter als Startwert verwenden und einen der folgenden Operatoren im 5. Parameter (A2) angeben: „EQ“, „=“, „GT“, „>“, „LT“, „<“, „GE“, „>=“, „LE“, „<=“. Diese Operatoren bestimmen die Lesebedingung im Vergleich zum zweiten Parameter. Der Rückgabecode (B2) „0“ bedeutet, dass der angegebene Special-Link gefunden wurde. Jeder andere Wert bedeutet, dass kein solcher Link gefunden wurde.

Wenn Sie SNAUREXT oder SNAUSEXT aus einem Special-Link-Profil in SYSSEC aufrufen, beziehen sich die Daten auf den Link, den Sie gerade verwalten. Wenn Sie sie von außerhalb von SYSSEC aufrufen, beziehen sich die Daten auf den Link zwischen der angegebenen Benutzerkennung und der Bibliothek, aus der Sie das Subprogramm aufrufen.

Zusätzliche Optionen (Bibliothek) - Additional Options (Libraries)

Wenn Sie das Feld **Additional Options** auf dem Basisbildschirm des Sicherheitsprofils mit Y markieren, wird ein Fenster angezeigt, in dem Sie die folgenden Optionen auswählen können:

Option	Beschreibung siehe
Maintenance Information	**Verwaltungsinformationen**
Security Notes	**Security-Vermerke**
Owners	**Eigentümer**
Mailboxes	**Mailboxen**
Time Windows	**Zeitfenster**
Steplibs	**Steplibs**
Restrictions	**Einschränkungen**
Functional Security	**Funktionssicherheit**
User Exit	**User Exit**

Die Optionen, zu denen bereits etwas angegeben oder definiert wurde, sind mit einem Pluszeichen (+) gekennzeichnet.

Sie können einen oder mehrere Einträge aus dem Fenster auswählen, indem Sie sie mit einem beliebigen Zeichen markieren. Für jeden ausgewählten Eintrag wird ein weiteres Fenster oder ein weiterer Bildschirm angezeigt (in der Reihenfolge der Einträge im Auswahlfenster).

Das Fenster **Restrictions** kann auch direkt durch Drücken von PF5 auf dem Basisbildschirm des Sicherheitsprofils aufgerufen werden.

Die einzelnen Optionen werden im Folgenden erläutert.

Zusätzliche Option (Bibliothek)	Erläuterung
Maintenance Information (nur Anzeige)	Verwaltungsinformationen. In diesem Fenster werden die folgenden Informationen angezeigt: ■ Das Datum und die Uhrzeit, zu der das Sicherheitsprofil erstellt wurde, die Kennung des Administrators, der es erstellt hat, und (falls zutreffend) die Kennungen der Miteigentümer, die für die Erstellung gegengezeichnet haben. ■ Das Datum und die Uhrzeit der letzten Änderung des Sicherheitsprofils, die Kennung des Administrators, der die letzte Änderung vorgenommen hat, und (falls zutreffend) die Kennungen der Miteigentümer, die für die Änderung gegengezeichnet haben.
Security Notes	Sicherheitsvermerke In diesem Fenster können Sie Vermerke zum Sicherheitsprofil eingeben.
Owners	Eigentümer. In diesem Fenster können Sie bis zu acht Kennungen von Administratoren eingeben. Nur die hier angegebenen Administratoren sind berechtigt, dieses Sicherheitsprofil zu verwalten. Wenn kein Eigentümer angegeben wird, kann jeder Benutzer vom Typ "Administrator" die Bibliothek verwalten. Für jeden Eigentümer kann optional im Feld hinter der Kennung die Anzahl der Miteigentümer angegeben werden, deren Gegenzeichnung für die Verwaltungserlaubnis erforderlich ist. Erläuterungen zu Eigentümern und Miteigentümern finden Sie im Kapitel *Gegenzeichnungen*.
Mailboxes	Mailboxen. In diesem Fenster können Sie bis zu fünf Kennungen für Mailboxen eingeben. Informationen zu Mailboxen finden Sie im Kapitel *Mailboxen*.
Time Windows	Zeitfenster. In diesem Fenster können Sie bis zu fünf Zeitfenster angeben, außerhalb derer die Bibliothek nicht verwendet werden kann. Wenn das Ende eines Zeitfensters erreicht ist, wird die in der Bibliothek enthaltene Anwendung automatisch beendet und Natural Security führt eine Abmeldung durch. Abhängig von der allgemeinen Option **Enable Error Transaction Before NAT1700/1701 Logoff** kann die `ON ERROR`-Behandlung und/oder Fehlertransaktion der Anwendung vor der Abmeldung ausgeführt werden. Wenn beispielsweise ein Zeitfenster auf `0815 - 1300` eingestellt ist, kann sich ein Benutzer nur zwischen 08:15 und 13:00 Uhr bei der Bibliothek anmelden. Wenn ein Benutzer um 13:00 Uhr noch bei der Bibliothek angemeldet ist, wird die in der Bibliothek enthaltene Anwendung beendet.

Zusätzliche Option (Bibliothek)	Erläuterung
Steplibs	Im Fenster **Steplibs** können Sie die Kennungen der Bibliotheken eingeben, die als Steplib-Bibliotheken (verkettete Bibliotheken) für die Bibliothek dienen sollen. Die Bibliotheken, deren Kennungen Sie angeben, müssen in Natural Security definiert sein. Mit mehreren Steplibs können Sie verschiedenen Bibliotheken unterschiedliche Module zur Verfügung stellen und auch die allgemeine Verfügbarkeit von Modulen einschränken, ohne dass mehrere Kopien desselben Moduls in mehreren Bibliotheken vorhanden sein müssen, d.h. jedes Modul muss nur einmal vorhanden sein, Sie können es aber dennoch mehreren Bibliotheken zur Verfügung stellen, anderen aber nicht. Beispielsweise können die Module, die allen Bibliotheken zur Verfügung stehen sollen, in einer allgemeinen Steplib enthalten sein, die in allen Bibliothekssicherheitsprofilen angegeben ist, während Module, die nur einigen Bibliotheken zur Verfügung stehen sollen, in einer anderen Steplib enthalten sein können, die nur in einigen Bibliothekssicherheitsprofilen angegeben ist. Darüber hinaus können Sie durch die Angabe verschiedener Special-Links zu einer Bibliothek (siehe ***Benutzer mit Bibliotheken verlinken*** im Kapitel *Bibliotheken schützen*) verschiedenen Benutzern derselben Bibliothek die Verwendung verschiedener Steplibs erlauben. Sie können bis zu 8 Steplibs angeben, plus einen Wert für die Natural-Systemvariable `*STEPLIB`: Wenn ein Programmierobjekt in der Bibliothek angefordert, aber nicht gefunden wird, werden die 8 Steplibs - in der Reihenfolge, in der sie im Bibliothekssicherheitsprofil angegeben sind - nach diesem Objekt durchsucht. Wenn das angeforderte Objekt in keiner der 8 Steplibs gefunden werden kann, wird die `*STEPLIB`-Bibliothek danach durchsucht. Kann es auch in dieser Bibliothek nicht gefunden werden, wird in der Bibliothek `SYSTEM` danach gesucht (ohne dass `SYSTEM` als Steplib in einem Bibliothekssicherheitsprofil angegeben werden muss). Wenn in einem der 8 Steplib-Felder im Bibliothekssicherheitsprofil kein Wert angegeben ist, werden stattdessen die 8 mit dem Natural-Profilparameter `STEPLIB` angegebenen Steplibs verwendet. Wenn `*STEPLIB` im Bibliothekssicherheitsprofil kein Wert zugewiesen wird, wird stattdessen der `*STEPLIB`-Wert des Natural-Profilparameters `STEPLIB` verwendet. **Anmerkung:** 1. Für die Angabe einer Steplib gilt die Eigentümerlogik, d.h. wenn in einem Bibliothekssicherheitsprofil Eigentümer angegeben sind (siehe oben), dürfen nur diese Eigentümer die Bibliothek als Steplib in das Profil einer anderen Bibliothek eintragen. 2. Für Natural-Systembibliotheken (d.h. Bibliotheken, deren Kennung mit "SYS" beginnt) - außer der Bibliothek `SYSTEM` - können Sie keine `*STEPLIB`-Bibliothek angeben. Für diese Bibliotheken wird eine interne System-Steplib als `*STEPLIB`-Bibliothek verwendet. 3. Wenn Sie nur die Bibliothek `SYSTEM` als Steplib verwenden, braucht `SYSTEM` selbst nicht als Bibliothek für Natural Security definiert zu werden. **Dynamische Änderung der Steplib-Tabelle zur Laufzeit**

Zusätzliche Option (Bibliothek)	Erläuterung
	Die oben beschriebene Tabelle der Steplibs ist fest und kann von der Anwendung selbst nicht geändert werden. Das bedeutet, dass für alle Benutzer, die die Bibliothek verwenden, dieselbe Steplib-Tabelle gilt. Über die Natural-Anwendungsprogrammierschnittstelle (API) `USR4025N` (enthalten in der Bibliothek `SYSEXT`) ist es jedoch möglich, einzelne Einträge in der Steplib-Tabelle dynamisch zu verändern. Um von dieser Möglichkeit Gebrauch zu machen, müssen Sie die Steplib-Tabelle wie folgt anpassen: Geben Sie in einem Feld des Steplib-Fensters anstelle der eigentlichen Kennung der Steplib die Kennung ******** (8 Sterne) an. Zur Laufzeit wird dann die eigentliche Kennung der Steplib für diese Position von der Anwendung über die API geliefert. Sie können ******** in einem oder mehreren Feldern der Steplib-Tabelle angeben. Die API überschreibt nur die Felder in der Steplib-Tabelle, die ******** enthalten; alle Felder, die tatsächliche Steplib-Kennungen (oder Leerzeichen) enthalten, werden von der API nicht beeinflusst. Eine dynamische Steplib-Zuweisung ist nur bei Steplibs möglich, die in der Reihenfolge der Steplibs an letzter Stelle stehen. Das bedeutet, dass in der Steplib-Tabelle nach einem oder mehreren Feldern, die ******** enthalten, kein Feld vorhanden sein darf, das eine tatsächliche Steplib-Kennung enthält. So ist es zum Beispiel möglich, eine Aufstellung zu haben, bei der die 1. bis 4. Steplibs fest sind, wie im Bibliothekssicherheitsprofil angegeben, und die 5. und 6. Steplib werden dynamisch durch die API geliefert. **DBID, FNR, Passwort und Chiffriercode** Neben jedem Steplib-Namen können Sie im Steplib-Fenster eines Bibliotheksfensters eine Datenbankkennung (DBID), eine Dateinummer (FNR), ein Passwort und einen Chiffriercode eingeben. Wenn Sie im Steplib-Fenster eines Bibliothekssicherheitsprofils `99999` als DBID-Wert für eine Steplib vergeben, wird der im Bibliothekssicherheitsprofil der Steplib angegebene DBID-Wert verwendet. Das Gleiche gilt für FNR-, Passwort- und Chiffriercode-Werte. Wenn Sie für eine Steplib im Fenster Steplib eines Bibliothekssicherheitsprofils keinen DBID-Wert (oder `0`) angeben, wird der DBID-Wert der betreffenden Bibliothek verwendet. Das Gleiche gilt für FNR-, Passwort- und Chiffriercode-Werte. Sie können die aktuellen Werte von DBID, FNR, Passwort und Chiffriercode aus dem Steplib-Profil in das Steplib-Fenster übernehmen, indem Sie einen Steplib-Namen mit dem Cursor markieren und `PF5` im Steplib-Fenster eines Bibliothekssicherheitsprofils drücken. Für die in einem Bibliothekssicherheitsprofil angegebene `*STEPLIB`-Bibliothek gelten die DBID-, FNR-, Passwort- und Chiffriercode-Werte dieses Bibliothekssicherheitsprofils.
Restrictions	Einschränkungen. Sie können die folgenden Einschränkungen festlegen: ■ **Security Options** ■ **Security Limits** ■ **Session Parameters** (including RPC Restrictions)

Zusätzliche Option (Bibliothek)	Erläuterung
	■ **Command Restrictions** ■ **Editing Restrictions** ■ **Statement Restrictions** ■ **Allow/Disallow modules** ■ **Set Status of DDMs** ■ **Development Mode** Diese Einschränkungen werden in den folgenden Abschnitten beschrieben.
Functional Security	Funktionssicherheit. In diesem Fenster können Sie die Funktionssicherheit für die Kommandoprozessoren der Bibliothek definieren. Dies ist nur relevant, wenn die Kommandoprozessoren mit dem Natural-Dienstprogramm `SYSNCP` erstellt wurden. Weitere Informationen finden Sie im Kapitel ***Funktionssicherheit***.
User Exit	User Exit. Wenn in der Spalte **Transactions** im Basisbildschirm des Bibliothekssicherheitsprofils ein User Exit angegeben ist, können Sie diesen User Exit aktivieren, indem Sie dieses Feld markieren.

Als Teil der Einschränkungen können Sie definieren:

- Sicherheitsoptionen - Security Options
- Sicherheitslimits - Security Limits
- Session-Parameter
- Kommandoeinschränkungen - Command Restrictions
- Editiereinschränkungen
- Statement-Einschränkungen
- Module nicht erlauben/erlauben
- Status von DDMs festlegen - Set Status of DDMs
- Entwicklungsmodus - Development Mode

Sicherheitsoptionen - Security Options

Wenn Sie **Security Options** im Auswahlfenster **Restrictions** mit einem beliebigen Zeichen markieren, wird das Fenster **Security Options** angezeigt. In diesem Fenster können Sie die folgenden Optionen einstellen:

Option	Erläuterung	
Allow NEXT/MORE line	Y	`NEXT/MORE`-Zeile zulassen. Erlaubt die Verwendung des Natural-Hauptmenüs.
	N	Unterdrückt das Natural-Hauptmenü. Wenn sich ein Benutzer bei der Bibliothek anmeldet, wird stattdessen die für die Bibliothek angegebene Starttransaktion aufgerufen (wenn keine

Option	Erläuterung	
		Starttransaktion angegeben ist, wird die Anmeldeprozedur aufgerufen; siehe auch die Natural-Systemvariable *STARTUP).
Allow system commands	Y	Systemkommandos zulassen. Erlaubt die Verwendung von Natural-Systemkommandos in der Bibliothek. Um einzelne Kommandos zu verbieten, können Sie den Abschnitt **Command Restrictions** des Bibliothekssicherheitsprofils verwenden (siehe unten).
	N	Verbietet die Verwendung aller Systemkommandos in der Bibliothek. (Dies betrifft nicht die Systemkommandos FIN, LAST, LASTMSG, LOGOFF, LOGON, MAINMENU, RENUMBER, RETURN, SETUP und TECH. Diese können immer verwendet werden).
Execution of update programs	Y	Ausführung von Datenaktualisierungsprogrammen. Programme, die die Datenbank ändern, können in der Bibliothek ausgeführt werden.
	N	Programme, die die Datenbank ändern, können nicht in der Bibliothek ausgeführt werden.
Device	Gerät. Wenn Sie dieses Feld leer lassen, ist die Verwendung der Bibliothek nicht auf eine Betriebsart oder ein Gerät beschränkt. Wenn Sie einen Wert eingeben, wird die Verwendung der Bibliothek auf ein bestimmtes Gerät oder eine bestimmte Betriebsart beschränkt. Die möglichen Werte für diese Option entsprechen denen der Natural-Systemvariablen *DEVICE. Diese sind auf Großrechner- und Nicht-Großrechner-Plattformen unterschiedlich (wie in der Natural-*Systemvariablen*-Dokumentation beschrieben).	
Clear source area by logon	N	Quellcodebereich bei Anmeldung löschen. Der Quellcode-Arbeitsbereich des Editors wird nicht gelöscht, wenn sich ein Benutzer von der Bibliothek aus bei einer anderen Bibliothek anmeldet.
	Y	Der Arbeitsbereich des Editors wird automatisch geleert, wenn sich ein Benutzer von der Bibliothek aus bei einer anderen Bibliothek anmeldet.
PC download/ PC upload	Y	PC-Download/ PC-Upload. Die in der Bibliothek enthaltenen Module können vom Großrechner auf einen PC heruntergeladen bzw. von einem PC auf den Großrechner hochgeladen werden.
	N	Das Herunterladen und Hochladen von Modulen ist nicht möglich.
	Diese Option gilt nur für Großrechner; unter Linux und Windows hat sie keine Auswirkungen.	
Close databases by logon	Y	Datenbanken schließen bei Anmeldung. Alle Datenbanken, auf die während der aktuellen Natural-Sitzung zugegriffen wurde, werden automatisch geschlossen, wenn sich ein Benutzer von der Bibliothek aus bei einer anderen anmeldet.

Option	Erläuterung	
	N	Es werden keine Datenbanken geschlossen, wenn sich ein Benutzer von der Bibliothek aus bei einer anderen anmeldet.
	Wenn Sie diese Option wählen, sollten Sie auch die Einstellung des Natural-Profilparameters `DBCLOSE` überprüfen. Die Verwendung dieser Option erfordert, dass entweder ein von Leerzeichen verschiedener ETID-Wert verwendet wird oder die Natural-Sitzung mit dem Profilparameter `DBOPEN=ON` gestartet wird.	

Sicherheitslimits - Security Limits

Wenn Sie im Auswahlfenster **Restrictions** die Option **Security Limits** mit einem beliebigen Zeichen markieren, wird das Fenster **Security Limits** angezeigt. In diesem Fenster können Sie die folgenden Einschränkungen festlegen:

Limit	Erläuterung
Non-activity logoff limit	Limit für die Abmeldung bei Nichtbenutzung. Die maximale Zeit (in Sekunden), die nach der letzten Terminalkommunikation verstreichen darf. Wird diese Zeit überschritten, wird eine neue Anmeldeprozedur aufgerufen, sobald die nächste Eingabe vom Terminal empfangen wird. Abhängig von der allgemeinen Option **Enable Error Transaction Before NAT1700/1701 Logoff** kann die `ON ERROR`-Behandlung und/oder die Fehlertransaktion der Anwendung verarbeitet werden, bevor Natural Security die Abmeldung durchführt. Mögliche Werte: `0 - 99999`. Wenn Sie kein Limit wünschen, müssen Sie dieses Feld auf `0` setzen.
Maximum transaction duration	Maximale Transaktionsdauer. Die maximale Zeit (in Sekunden), die für eine einzelne Adabas-Transaktion zulässig ist. Diese Funktion kann verwendet werden, um zu verhindern, dass Ressourcen für eine zu lange Zeit blockiert werden. Wird die Zeit überschritten, wird die aktuelle Transaktion per Back-out abgebrochen. Mögliche Werte: `0 - 99999`. Wenn Sie kein Limit wünschen, müssen Sie dieses Feld auf `0` setzen. Die Natural-Systemvariable `*TIME-OUT` enthält die verbleibende Zeit, bevor eine Zeitüberschreitung entsteht. (Der Adabas TT-Parameter (Adabas-Transaktionszeitlimit) wird separat geprüft).
Maximum number of source lines	Maximale Anzahl an Quellcodezeilen. Die maximal zulässige Anzahl an Quellcodezeilen für ein vom Benutzer geschriebenes Natural-Programm. Wird das Zeilenlimit überschritten, gibt der Natural-Syntax-Checker eine entsprechende Fehlermeldung aus. Mögliche Werte: `0 - 99999`.

Limit	Erläuterung
Maximum amount of CPU time (MT)	Maximale CPU-Zeit (MT). Die maximale CPU-Zeit (in Sekunden), die verwendet werden soll (wie im Natural- Profilparameter MT beschrieben; siehe Natural-*Parameter-Referenz*-Dokumentation). Wenn Sie dieses Feld auf 0 setzen, wird das Limit durch den Wert des Natural-Profilparameters MT bestimmt. Wenn Sie möchten, dass das höchstmögliche Limit wirksam ist, müssen Sie dieses Feld auf den Maximalwert (9999999) setzen. Wenn kein Limit gelten soll, müssen Sie dieses Feld auf 9999999999 setzen. Dieses Feld gilt nur für Großrechner. Unter Linux und Windows hat es keine Auswirkungen.
Maximum number of Adabas calls (MADIO)	Maximale Anzahl der Adabas-Aufrufe (MADIO). Die maximale Anzahl der Adabas-Aufrufe, die zwischen zwei Bildschirm-E/A-Operationen erlaubt sind (wie beim Natural-Profilparameter MADIO in der Natural-*Parameter-Referenz*-Dokumentation beschrieben). Wird die angegebene Anzahl überschritten, wird das Natural-Programm unterbrochen und eine entsprechende Fehlermeldung angezeigt. Wenn Sie dieses Feld auf 0 setzen, wird das Limit durch den Wert des Natural-Profilparameters MADIO bestimmt. Wenn das höchstmögliche Limit gelten soll, müssen Sie dieses Feld auf den Maximalwert setzen (65534 für Großrechner, 32767 für andere Plattformen). Wenn kein Limit gelten soll, müssen Sie dieses Feld auf 99999 setzen.
Maximum number of program calls (MAXCL)	Maximale Anzahl von Programmaufrufen (MAXCL). Die maximale Anzahl von Programmaufrufen, die zwischen zwei Bildschirm-E/A-Operationen zulässig sind (wie im Natural-Profilparameter MAXCL in der Natural-*Parameter-Referenz*-Dokumentation beschrieben). Wird die angegebene Anzahl überschritten, wird das Natural-Programm unterbrochen und eine entsprechende Fehlermeldung angezeigt. Wenn Sie dieses Feld auf 0 setzen, wird das Limit durch den Wert des Natural-Profilparameters MAXCL bestimmt. Wenn das höchstmögliche Limit gelten soll, müssen Sie dieses Feld auf den Maximalwert setzen (65534 für Großrechner, 32767 für andere Plattformen). Wenn kein Limit gelten soll, müssen Sie dieses Feld auf 99999 setzen.
Processing loop limit (LT)	Limit für Verarbeitungsschleifen (LT). Die maximale Anzahl an Datensätzen, die in einer gegebenen Verarbeitungsschleife der Bibliothek gelesen werden können (wie im Natural-Profilparameter LT in der Natural-*Parameter-Referenz*-Dokumentation beschrieben). Wenn Sie dieses Feld auf 0 setzen, wird das Limit durch den Wert des Natural-Profilparameters LT bestimmt.

Limit	Erläuterung
	Wenn Sie das höchstmögliche Limit wünschen, müssen Sie dieses Feld auf den Maximalwert setzen (2147483647). Wenn kein Limit gelten soll, müssen Sie dieses Feld auf 9999999999 setzen. **Anmerkung:** Wenn das Limit innerhalb der Natural-Sitzung geändert wird (mit einem SET GLOBALS-Statement oder dem Systemkommando GLOBALS), darf es den Wert des Natural-Profilparameters LT nicht überschreiten.

Session-Parameter

Wenn Sie die Option **Session Parameters** im Auswahlfenster **Restrictions** mit einem beliebigen Zeichen markieren, wird der Bildschirm **Session Parameters** angezeigt.

Auf diesem Bildschirm können Sie Werte für die folgenden Natural-Session-Parameter angeben. Diese Werte überschreiben dann die bei der Natural-Installation eingestellten Standardparameterwerte:

Parameter	Kurzbeschreibung
DC	Dezimalstellenzeichen
CF	Steuerzeichen für Terminalkommandos
CLEAR	Verarbeitung der CLEAR-Taste im NEXT-Modus
IA	Input-Zuweisungszeichen
IM	Input-Modus
ID	Input-Begrenzungszeichen
SA	Terminal-Warnton
DU	Dump-Erstellung
EJ	Seitenvorschub
FS	Format-Spezifikation für Benutzervariablen
WH	Warten auf Datensatz im Hold-Status
ZD	Division durch Null
LS	Zeilenlänge
PS	Länge einer Reportseite
SL	Quellcode-Zeilenlänge (nur auf Großrechnern)
SF	Spaltenabstand

Wenn ein Parameterwert leer ist (oder 0 bei einem Parameter, der numerische Werte annimmt), gilt der entsprechende Standardwert.

Informationen zu den einzelnen Session-/Profilparametern finden Sie in der Natural-*Parameter-Referenz*-Dokumentation.

Außerdem enthält der Bildschirm die folgenden Felder:

Feld	Erläuterung
Adabas open (OPRB)	Adabas Open-Anforderung (OPRB). Sie können den Inhalt des Datensatzpuffers (Record Buffer) angeben, der mit dem Adabas OPEN-Kommando verwendet wird. In diesem Fall wird ein eingeschränktes OPEN ausgeführt, d.h. es können nur Dateien referenziert werden, die im Datensatzpuffer enthalten sind. Wird kein Inhalt des Datensatzpuffers angegeben, können alle zugänglichen Dateien referenziert werden (siehe auch die Adabas *Command Reference*-Dokumentation). Wenn dieses Feld auf NOOPEN gesetzt ist, wird kein Adabas-OPEN-Kommando ausgeführt. Wird dieses Feld leer gelassen, gilt für diese Bibliothek ein beim Aufruf von Natural dynamisch angegebener OPRB-Parameter (Informationen zum Profilparameter OPRB finden Sie in der Natural-*Parameter-Referenz*-Dokumentation).
Spool profile	Spoolprofil. Sie können den Namen des Spoolprofils angeben. Dies ist nur möglich, wenn Natural Advanced Facilities installiert ist. Weitere Informationen finden Sie in der *Natural Advanced Facilities*-Dokumentation.
Adabas password	Adabas-Passwort. Sie können das Adabas-Passwort angeben, das für den Zugriff auf die Adabas-Datendateien (nicht Systemdateien) verwendet wird, auf die die Bibliothek verweist. Dies ist nur relevant, wenn die entsprechenden Dateien unter Adabas Security passwortgeschützt sind. Das im Sicherheitsprofil angegebene Passwort gilt für alle Datenbankzugriff-Statements, für die weder ein individuelles Passwort angegeben ist, noch ein PASSW-Statement gilt. Es gilt innerhalb der Bibliothek, in deren Sicherheitsprofil es angegeben ist, und bleibt auch in anderen Bibliotheken in Kraft, bei denen Sie sich später anmelden und in deren Sicherheitsprofil kein Kennwort angegeben ist. Siehe auch das Statement PASSW in der Natural-*Statements*-Dokumentation.
SLOCK	Source-Sperrung. Dieses Feld gilt nur für Großrechner. Auf anderen Plattformen wird seine Einstellung ignoriert. Dieses Feld steuert die Quellcodesperrung (Source Locking) und legt fest, wie konkurrierende Änderungen (Updates) von Natural-Quellcode-Members in der Bibliothek behandelt werden sollen. Die möglichen Werte PRE, SPOD, POST und OFF entsprechen denjenigen des Natural-Profilparameters SLOCK. Wenn Sie dieses Feld leer lassen, gilt für diese Bibliothek der Profilparameter SLOCK, der für die aktuelle Natural-Sitzung eingestellt ist. Weitere Informationen zum Parameter SLOCK finden Sie in der Natural-*Parameter-Referenz*-Dokumentation.

Natural RPC-Einschränkungen

Wenn Sie auf dem Bildschirm **Session Parameters** die Taste PF8 benutzen, wird ein weiterer Bildschirm angezeigt, auf dem Sie verschiedene Einschränkungen festlegen können, die gelten, wenn in der Bibliothek enthaltene Subprogramme mittels Natural RPC in einer Client/Server-Umgebung ausgeführt werden.

Feld	Erläuterung	
Expiration Criteria	Verfallskriterien. Die folgenden Kriterien bestimmen, wie oft bzw. wie lange Subprogramme in der Bibliothek mit Natural RPC ausgeführt werden können. Wenn eines der Kriterien erreicht ist, kann das Kriterium entweder über die Natural-Anwendungsprogrammierschnittstelle `USR1071N` oder durch die Neuanmeldung des Benutzers bei der Bibliothek zurückgesetzt werden.	
Use Count	Anzahl Verwendungen. Legt fest, wie oft Remote-Subprogramme ausgeführt werden können. Der Wert „0“ bedeutet, dass kein solches Limit wirksam ist.	
Number of Days	Anzahl der Tage. Legt fest, für wie viele Tage Remote-Subprogramme ausgeführt werden können. Die Tage werden beginnend mit der Anmeldung bei der Bibliothek gezählt. Der Wert „0“ bedeutet, dass kein solches Limit wirksam ist.	
Number of Hours/Minutes	Anzahl der Stunden/Minuten. Gibt an, wie viele Stunden/Minuten lang Remote-Subprogramme ausgeführt werden können. Die Zeit zählt ab der Anmeldung bei der Bibliothek. Der Wert „0“ bedeutet, dass kein solches Limit wirksam ist.	
Allow Overwriting by User Exit USR1071N	Y	Überschreiben durch User Exit `USR1071N` zulassen. Die obigen Verfallskriterien im Sicherheitsprofil der Bibliothek sowie die Kennung und das Passwort aus der Client-Anmeldung können durch Kriterien überschrieben werden, die mit der Natural-Anwendungsprogrammierschnittstelle USR1071N angegeben werden.
	N	Es können keine Daten über die Natural-Anwendungsprogrammierschnittstelle `USR1071N` gesetzt/überschrieben werden.
Server Session Options - Optionen für Server-Sitzungen:		
Close All Databases	Mit dieser Option können Sie das anmelde- und abmeldeabhängige Schließen von Datenbanken steuern. Sie wirkt sich auf alle Datenbanken aus, die von in der Bibliothek enthaltenen Remote-Subprogrammen geöffnet wurden:	
	N	Die Datenbanken werden *nicht* geschlossen, wenn eine Anmeldung/Abmeldung bei oder von der Bibliothek durchgeführt wird.
	Y	Die Datenbanken werden geschlossen, wenn eine *Anmeldung* (Logon) bei der Bibliothek durchgeführt wird. Wenn **Impersonation** im RPC-Serverprofil aktiviert ist, hat `Y` die gleiche Wirkung wie `F` (siehe unten).

Feld	Erläuterung	
	F	Die Datenbanken werden geschlossen, wenn eine *Anmeldung* bei der Bibliothek erfolgt, und wenn eine *Abmeldung* von der Bibliothek erfolgt.
	Diese Option ist nur relevant, wenn die Option `LOGONRQ=ON` im Natural-Profilparameter `RPC` oder im `NTRPC`-Makro gesetzt ist. Wenn Sie für jede Datenbank, auf die der RPC-Server zugreift, ein Benutzer-Warteschlangenelement pro Client-Sitzung haben möchten, empfiehlt es sich, `LOGONRQ=ON` und **Close All Databases** auf `Y` oder `F` zu setzen. Die Verwendung dieser Option erfordert, dass ein von Leerzeichen verschiedener `ETID`-Wert verwendet wird oder die Natural-Sitzung mit dem Profilparameter `DBOPEN=ON` gestartet wird.	
Logon Option	Anmeldeoption. Diese Option legt fest, welche Anmeldedaten von Natural Security ausgewertet werden, wenn der Zugriff auf die Bibliothek über eine RPC-Dienstanforderung (Service Request) erfolgt:	
	N	Natural RPC-Benutzerkennung und -Passwort werden ausgewertet. (*)
	E	Natural RPC-Benutzerkennung und -Passwort werden ausgewertet. (*) Zusätzlich wird geprüft, ob die Natural RPC-Benutzerkennung mit der EntireX-Benutzerkennung identisch ist.
	A	Nur die Natural RPC-Kennung wird ausgewertet (ähnlich wie bei Natural-Profilparameter `AUTO=ON`, aber nur für diese Bibliothek).
	S	Nur die Natural RPC-Kennung wird ausgewertet (ähnlich wie bei Natural-Profilparameter `AUTO=ON`, aber nur für diese Bibliothek). Zusätzlich wird geprüft, ob die Natural RPC-Benutzerkennung mit der EntireX-Benutzerkennung identisch ist.
	(*) Wenn Impersonation für den Natural RPC-Server aktiv ist, wird das Passwort nicht ausgewertet (da dies von einem externen Sicherheitssystem durchgeführt wird). Weitere Informationen finden Sie unter ***Validierung einer RPC-Dienstanforderung (Service Request)*** in the section *Natural RPC Server und Services schützen* .	
Logon Recorded	Anmeldung aufgezeichnet. Mit dieser Option wird festgelegt, ob Anmeldungen bei der Bibliothek aufgezeichnet werden, wenn der Zugriff auf die Bibliothek über Natural RPC-Dienstanforderungen (Service Requests) erfolgt:	
	N	Anmeldungen bei der Bibliothek über Natural RPC-Dienstanforderungen (Service Requests) werden nicht aufgezeichnet.
	Y	Anmeldungen bei der Bibliothek über Natural RPC-Dienstanforderungen (Service Requests) werden

Feld	Erläuterung	
		aufgezeichnet. Jedes Mal, wenn ein Benutzer über eine Natural RPC-Dienstanforderung auf die Bibliothek zugreift, wird von Natural Security ein Anmeldesatz (Logon Record) geschrieben. Sie können die Aktivitäten der Benutzer überprüfen, indem Sie diese Anmeldesätze einsehen (weitere Informationen finden Sie unter ***Anmeldesätze - Logon Records*** im Kapitel *Administrator Services*).
	L	Der Wert der Option **Logon recorded** im Abschnitt **General Options** des Bibliothekssicherheitsprofils legt fest, ob Anmeldungen bei der Bibliothek über Natural RPC-Dienstanforderungen (Service Requests) aufgezeichnet werden sollen oder nicht.
	*	Der Wert der Option **Logon recorded** in den **Library Preset Values** der Administrator Services legt fest, ob Anmeldungen an Bibliotheken über Natural RPC-Dienstanforderungen (Service Requests) aufgezeichnet werden sollen oder nicht.
Lock User Option	Diese Option legt fest, ob die Funktion **Lock User** beim Zugriff auf die Bibliothek über Natural RPC-Dienstanforderungen (Service Requests) aktiv sein soll:	
	N	Die Funktion **Lock User** ist bei Zugriffsversuchen auf die Bibliothek über Natural RPC-Dienstanforderungen nicht aktiv.
	X	Die Funktion **Lock User** ist für Zugriffsversuche auf die Bibliothek über Natural RPC-Dienstanforderungen aktiv. Sobald ein Benutzer die maximale Anzahl von Anmeldeversuchen erreicht hat, ohne das korrekte Kennwort einzugeben, wird er gesperrt, d. h. die Benutzerkennung wird „ungültig“ gemacht. Natural Security „merkt“ sich erfolglose Anmeldeversuche über mehrere Sitzungen hinweg: Die Fehlerzähler für Client-Benutzerkennungen, die erfolglos ausprobiert wurden, werden für Zugriffsversuche in nachfolgenden Sitzungen gespeichert, wodurch die Anzahl der nachfolgenden Versuche mit diesen Kennungen reduziert wird. Der Fehlerzähler für eine Benutzerkennung wird erst nach einer erfolgreichen Anmeldung zurückgesetzt.
	*	Der Wert der Lock User-Option im Sicherheitsprofil des Natural RPC-Servers bestimmt, ob die Funktion **Lock User** für Zugriffsversuche auf Bibliotheken auf diesem Server über Natural RPC Service Requests aktiv ist oder nicht. Siehe ***Bestandteile eines Serverprofils*** im Kapitel *Natural RPC Server und Services schützen* .
	Weitere Informationen zur Funktion **Lock User** finden Sie auch unter **Lock User Option** im Abschnitt **General Options** der *Administrator Services*.	

Die oben erwähnte Natural-Anwendungsprogrammierschnittstelle USR1071N ist in der Bibliothek SYSEXT enthalten.

Weitere Informationen zu Natural RPC mit Natural Security finden Sie im Kapitel *Natural RPC Server und Services schützen* in der *Natural Security*-Dokumentation und in den Abschnitten *Natural RPC mit Natural Security verwenden* und *Anmeldung bei einer Server Library* in der Natural RPC-Dokumentation.

Kommandoeinschränkungen - Command Restrictions

Wenn Sie **Command Restrictions** im Auswahlfenster **Restrictions** mit einem beliebigen Zeichen markieren, wird der Bildschirm **Command Restrictions** angezeigt. Auf diesem Bildschirm können Sie die Benutzung einzelner Natural-Systemkommandos erlauben oder nicht erlauben.

Standardmäßig sind alle Kommandos, die auf dem Bildschirm **Command Restrictions** angezeigt werden, mit Y markiert, was bedeutet, dass alle Kommandos erlaubt sind.

- Markieren Sie jedes Kommando, das Sie in der Bibliothek verfügbar machen möchten, mit „Y“.
- Markieren Sie jedes Kommando, das *nicht* in der Bibliothek verwendet werden soll, mit „N“.

Für das Kommando SCAN können Sie die folgenden Einstellungen vornehmen:

- „Y“ - Das Kommando ist erlaubt.
- „N“ - Das Kommando ist *nicht* erlaubt.
- „R“- Das Kommando ist erlaubt, die Kommando-Option **Replace** ist jedoch *nicht* erlaubt.
- „B“ - Das Kommando ist erlaubt, die **Replace**-Option ist jedoch nur im Batch-Modus erlaubt (d.h. wenn die Natural-Systemvariable *DEVICE auf BATCH gesetzt ist).
- „O“ - Das Kommando ist erlaubt, die **Replace**-Option ist jedoch nur online erlaubt (d.h. wenn *DEVICE auf einen anderen Wert als BATCH gesetzt ist).

Anmerkung: Die Einstellungen R, B und O sind nur auf Großrechnern verfügbar.

Informationen zu den einzelnen Kommandos finden Sie in der Natural-*Systemkommandos*-Dokumentation.

Bei Kommandos, die auf dem Bildschirm **Command Restrictions** hervorgehoben angezeigt werden, wird Natural-Syntaxprüfung angewendet, und folglich werden Natural-Statements verwendet (die auch einzeln erlaubt/nicht erlaubt werden können. Siehe *Statement-Einschränkungen* unten).

Verwendung des SCAN-Kommandos einschränken

Sie können das Systemkommando SCAN für eine Bibliothek entweder über die Kommandoeinschränkungen (wie oben beschrieben) ganz unterbinden, oder Sie können seine Verwendung über die Option **Utilities** steuern:

- Wenn **SCAN** auf dem Bildschirm **Command Restrictions** mit `N` markiert ist, kann das Kommando `SCAN` in der Bibliothek nicht verwendet werden (unabhängig von der Option **Utilities**).
- Wenn **SCAN** auf dem Bildschirm **Command Restrictions** mit `Y` markiert ist, bestimmt die Option **Utilities** (im Abschnitt **General Options** des Bibliothekssicherheitsprofils), wer das Kommando `SCAN` in der Bibliothek verwenden darf. Die Option **Utilities** kann einen der folgenden Werte annehmen:

Wert	Erläuterung
N	Kein Schutz - Das Kommando `SCAN` kann in der Bibliothek von jedem Benutzer verwendet werden.
O	Erlaubnis für Eigentümer (Owners) - Nur die Eigentümer der Bibliothek dürfen das `SCAN`-Kommando verwenden. Wenn kein Eigentümer angegeben ist, darf es jeder Benutzer vom Typ „Administrator“ verwenden. In einer privaten Bibliothek im privaten Modus darf neben den Eigentümern auch der Benutzer mit der gleichen Kennung wie die Bibliothekskennung das `SCAN`-Kommando verwenden. Im Batch-Modus ist zu beachten, dass ein Eigentümer, der eine Gegenzeichnung von einem Miteigentümer benötigt, das `SCAN`-Kommando nicht verwenden kann (da Gegenzeichnungen im Batch-Modus nicht möglich sind).
P	Erlaubnis unter Schutzregeln - Es gilt der Personen-/Terminalschutz der Bibliothek: Nur Benutzer, die die Bibliothek benutzen dürfen - und nur unter den Bedingungen, unter denen sie sie benutzen dürfen - dürfen das `SCAN`-Kommando benutzen. Für eine private Bibliothek im privaten Modus gilt Folgendes: Der Benutzer mit der gleichen Kennung wie die Bibliothekskennung darf das `SCAN`-Kommando verwenden. Alle anderen dürfen es nur nach Eingabe des Passworts des betreffenden Benutzers (auf einem dafür vorgesehenen Gegenzeichnungsbildschirm) verwenden. Im Batch-Modus ist zu beachten, dass ein Benutzer das `SCAN`-Kommando in der privaten Bibliothek eines anderen Benutzers im privaten Modus nicht verwenden kann (da im Batch-Modus kein Passwort eingegeben werden kann).

Linux Shell-Kommandos

Sie können auch die Ausführung von Linux Shell-Kommandos innerhalb eines Natural-Programms erlauben oder nicht erlauben. Diese Kommandos werden aus einem Natural-Programm heraus ausgeführt, indem der Natural User Exit `SHCMD` über das Statement `CALL SHCMD` aufgerufen wird, das vom Programm ausgegeben wird.

Um die Ausführung von Shell-Kommandos aus einem Programm der Bibliothek heraus zu erlauben/nicht zu erlauben, müssen Sie `CALL SHCMD` auf dem Bildschirm **Command Restrictions** wie folgt markieren:

- `Y` = Shell-Kommandos können ausgeführt werden.
- N = Shell-Kommandos *können nicht* ausgeführt werden.

Editiereinschränkungen

Wenn Sie im Auswahlfenster **Restrictions** die Option **Editing Restrictions** mit einem beliebigen Zeichen markieren, wird das Fenster **Editing Restrictions** angezeigt. In diesem Fenster können Sie die Bearbeitung von Natural-Objekten bestimmter Objekttypen erlauben oder nicht erlauben.

Standardmäßig sind alle im Fenster **Editing Restrictions** angezeigten Objekttypen mit `Y` markiert, was bedeutet, dass Objekte aller Typen bearbeitet werden dürfen.

- Markieren Sie jeden Objekttyp, dessen Bearbeitung Sie in der Bibliothek zulassen möchten, mit `Y`
- Markieren Sie mit `N` jeden Objekttyp, dessen Bearbeitung in der Bibliothek *nicht* erlaubt sein soll.

Informationen zu den Natural-Objekttypen finden Sie im Natural-*Leitfaden zur Programmierung*. Informationen zu den Natural-Editoren finden Sie in der Dokumentation zu den Natural-*Editoren*.

Um die Bearbeitung komplett zu unterbinden, können Sie die Verwendung des Kommandos `EDIT` sperren (siehe ***Kommandoeinschränkungen - Command Restrictions***). Wenn Sie das Kommando `EDIT` nicht zulassen, werden alle Objekttypen im Fenster **Editing Restrictions** automatisch mit `N` markiert. Wenn Sie das Kommando `EDIT` wieder zulassen, werden alle Objekttypen im Fenster Editing Restrictions automatisch wieder mit `Y` markiert.

Statement-Einschränkungen

Wenn Sie im Auswahlfenster **Restrictions** die Option **Statement Restrictions** mit einem beliebigen Zeichen markieren, wird der Bildschirm **Statement Restrictions** angezeigt. Auf diesem und dem nächsten Bildschirm können Sie die Verwendung einzelner Natural-Statements erlauben oder nicht erlauben. Um von diesem Bildschirm zum nächsten und wieder zurück zu gelangen, können Sie `PF7` bzw. `PF8` drücken.

Standardmäßig sind alle Statements, die auf dem Bildschirm **Statement Restrictions** angezeigt werden, mit „Y“ markiert, was bedeutet, dass alle Statements erlaubt sind.

- Markieren Sie die Natural-Statements, deren Verwendung Sie in der Bibliothek zulassen wollen, mit „Y“.
- Markieren Sie mit `N` die Natural-Statements, deren Verwendung in der Bibliothek Sie *nicht* zulassen wollen

Beim `FIND`-Statement und andere Statements für den Datenbankzugriff können Sie auch einzelne Klauseln erlauben oder nicht erlauben.

Alle Natural-Statements, die nicht auf dem Bildschirm **Statements Restrictions** aufgeführt sind, sind immer erlaubt (z.B. das Statement `END`).

Die Statement-Einschränkungen werden wirksam, wenn ein Programmierobjekt bei der Kompilierung einer Syntaxprüfung unterzogen wird.

Module nicht erlauben/erlauben

Mit der Option **Disallow/Allow Modules** können Sie die Verwendung von Modulen (Programmierobjekten) in einer Bibliothek einschränken, d. h. Sie können deren Ausführung bzw. den Aufruf zur Ausführung nicht erlauben bzw. erlauben.

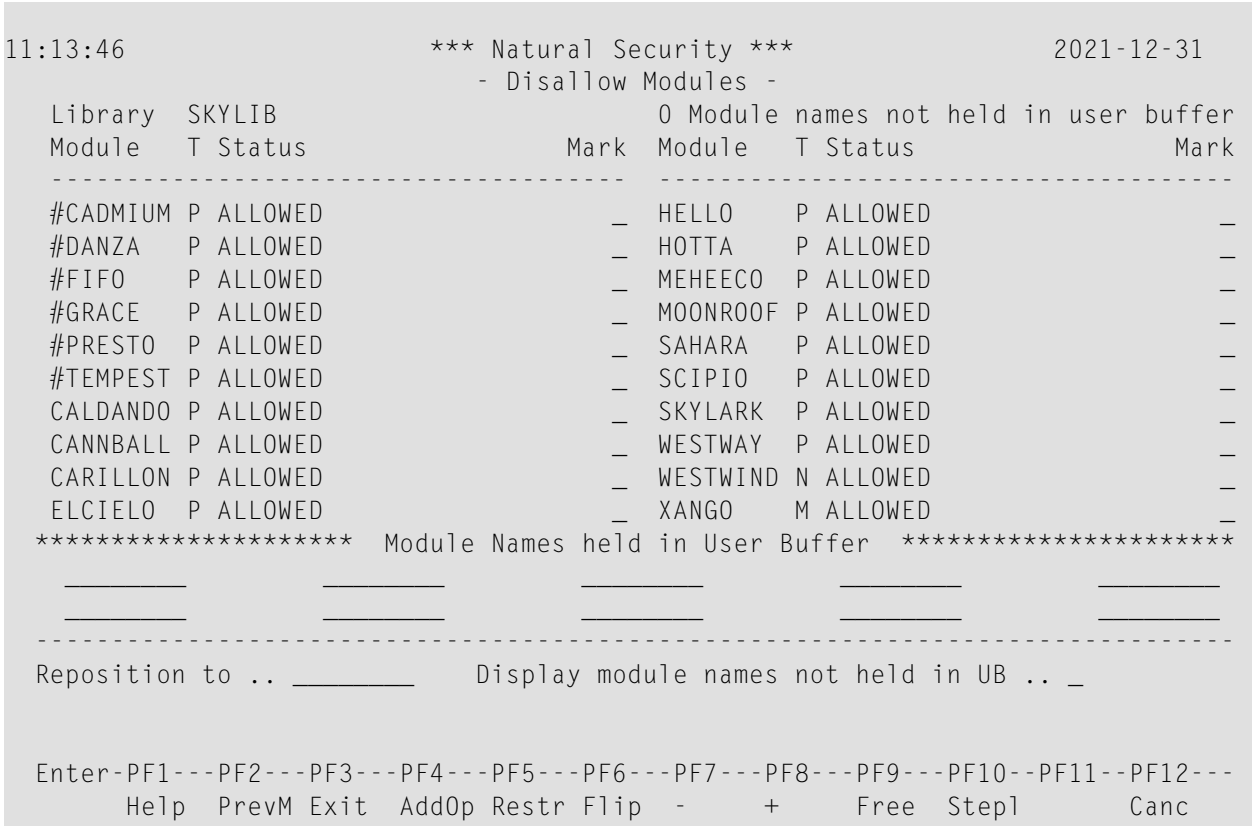
Diese Option kann auf verschiedenen Plattformen unterschiedlich ausgewertet werden, abhängig von der Option **Module Protection Mode**, wie im Kapitel *Administrator Services* beschrieben.

Im Auswahlfenster **Restrictions** gibt es neben dem Feld, das Sie zur Auswahl der Option D**isallow/Allow Modules** markieren, ein zweites Feld, in das Sie eine der folgenden Angaben machen können:

Wert	Erläuterung
X	Ein `X` bewirkt, dass *alle* Module erlaubt sind. Einzelne Module können nicht untersagt werden (der Bildschirm **Disallow/Allow Modules** wird nicht aufgerufen). Wenn Sie ein `X` eingeben, dürfen Sie nicht gleichzeitig das Auswahlfeld markieren.
D	Alle Module sind zunächst erlaubt, und Sie können einzelne Module als nicht erlaubt markieren.
A	Alle Module sind zunächst *nicht* erlaubt, und Sie können einzelne Module als erlaubt markieren.

Anmerkung: Bei der Funktion **Display** können Sie nur das Auswahlfeld markieren. Unabhängig von der Einstellung des zweiten Feldes wird der Bildschirm **Disallow/Allow Modules** mit der Liste der erlaubten/nicht erlaubten Module angezeigt.

Wenn Sie im Auswahlfenster **Restrictions** die Option **Disallow/Allow Modules** mit einem beliebigen Zeichen markieren und im zweiten Feld ein `D` oder `A` eingeben, wird der Bildschirm **Disallow Modules** bzw. **Allow Modules** angezeigt (Beispiel):



In der Spalte **T** (Typ) des Bildschirms **Disallow/Allow Modules** werden die Objekttypen der Module angezeigt:

Typ	Objekttyp
P	Programm
N	Subprogramm
S	Subroutine
H	Helproutine
G	Globaler Datenbereich (Global Data Area)
L	Lokaler Datenbereich (Local Data Area)
A	Parameter-Datenbereich (Parameter Data Area)
M	Maske (Map)
C	Copycode
3	Dialog
4	Klasse (Class)
7	Funktion (Function)
8	Adapter

Markieren Sie auf dem Bildschirm **Disallow/Allow Modules** die in der Bibliothek enthaltenen Module, die Sie nicht erlauben möchten, mit `D` und die in der Bibliothek enthaltenen Module, die

Sie erlauben möchten, mit A. Die ersten zehn markierten Modulnamen werden im Benutzerpuffer (User Buffer) gespeichert.

Darüber hinaus sind die folgenden Unterfunktionen verfügbar:

Module Names Held in User Buffer	Im Benutzerpuffer vorgehaltene Modulnamen. Wenn Sie Module nicht erlauben/erlauben und deren Namen im Benutzerpuffer speichern möchten, geben Sie diese Modulnamen in die zehn Felder auf dem Bildschirm **Disallow/Allow Modules** ein. Wenn Sie einen Wert gefolgt von einem Stern (*) eingeben, werden alle Modulnamen, die mit diesem Wert beginnen, nicht erlaubt bzw. erlaubt und im Benutzerpuffer gespeichert. Die Namen der nicht erlaubten/erlaubten Module, die sich nicht im Benutzerpuffer befinden, können angezeigt werden, indem Sie das Feld **Display module names not held in User Buffer** mit einem beliebigen Zeichen markieren. Entfernen Sie die Markierung, um zum Bildschirm **Disallow/Allow Modules** zurückzukehren. Wenn möglich, sollte die Anzahl der erlaubten/nicht erlaubten Module 10 nicht überschreiten, d.h. alle erlaubten/nicht erlaubten Modulnamen sollten im Benutzerpuffer enthalten sein. Modulnamen, die nicht im Benutzerpuffer enthalten sind, führen zu Leistungseinbußen, da zusätzlich auf die Datendatei von Natural Security zugegriffen werden muss, um zu prüfen, ob ein Modul, dessen Name nicht im Benutzerpuffer enthalten ist, erlaubt ist oder nicht.
Allowing/Disallowing "Non-Existent" Modules(PF9)	Nicht existierende Module erlauben/nicht erlauben (PF9). Der Bildschirm **Disallow/Allow Modules** eines Bibliothekssicherheitsprofils zeigt eine Liste aller in der entsprechenden Bibliothek enthaltenen Module an. Es kann jedoch Module geben, die derzeit physisch nicht verfügbar sind (z.B. weil die entsprechende Datenbank nicht aktiv ist oder die Module noch nicht geschrieben wurden) und die daher nicht in der Liste der Module erscheinen. Oder in einer heterogenen Produktionsumgebung mit einer zentralen Großrechner-FUSER-Systemdatei existiert die Bibliothek möglicherweise nicht in der Großrechner-FUSER-Systemdatei, sondern im Dateisystem einer anderen Plattform. Wenn Sie ein Bibliothekssicherheitsprofil für eine solche Bibliothek definieren würden, würde Natural Security auf dem Großrechner diese Bibliothek nicht kennen, und die Liste der Module wäre daher leer. Um solche „nicht existierenden“ Module nicht erlauben/erlauben zu können, bietet die Funktion **Allow/Disallow Modules** die Unterfunktion **Free List of Modules**. Mit dieser Unterfunktion können Sie Module vordefinieren, die in der aktuellen FUSER-Systemdatei nicht physisch vorhanden sind. Um die Unterfunktion aufzurufen, müssen Sie auf dem Bildschirm **Disallow/Allow Modules** PF9 drücken. Daraufhin wird das Fenster **Free List of Modules** angezeigt. In diesem Fenster können Sie die Namen der Module manuell angeben und sie erlauben oder nicht erlauben.

Steplibs (PF10)	Die Unterfunktion **Steplibs** gilt nicht auf Großrechnern. Mit dieser Unterfunktion können Sie Module in den Steplibs der Bibliothek nicht erlauben/erlauben. Um die Unterfunktion aufzurufen, müssen Sie im Bildschirm **Disallow/Allow Modules** PF10 drücken. Es wird eine Liste mit allen Steplibs der Bibliothek angezeigt. In der Liste können Sie die Bibliothek auswählen, deren Module Sie nicht erlauben/erlauben möchten. Anschließend wird die Liste der in der ausgewählten Steplib enthaltenen Module angezeigt, die Sie dann einzeln nicht erlauben/erlauben können. Wenn Sie auf diese Weise Module in einer Steplib nicht erlauben/erlauben, bedeutet dies nicht, dass Sie diese Module tatsächlich im Bibliothekssicherheitsprofil der Steplib nicht erlauben/erlauben. Die Steplib-Module werden nur in Bezug auf die Verwendung durch die Bibliothek, deren Profil Sie gerade verwalten (d.h. die Bibliothek, aus deren Bibliothekssicherheitsprofil Sie die Unterfunktion aufgerufen haben), nicht erlaubt/erlaubt.

Status von DDMs festlegen - Set Status of DDMs

Die Option **Set Status of DDMs** betrifft nur DDMs, für die noch keine Sicherheitsprofile definiert wurden. Sie ermöglicht es Ihnen, den Status aller neuen DDMs auf PUBLIC zu setzen. Auf Großrechnern gilt dies für den Dateistatus, unter Linux und Windows gilt dies sowohl für den internen als auch für den externen Status von DDMs.

Im Fenster **Restrictions** können Sie einen der folgenden Werte für diese Option angeben:

Wert	Erläuterung
UNDF	Der Status aller DDMs ohne Sicherheitsprofil ist nicht definiert.
PUBL	Der Status aller DDMs ohne Sicherheitsprofile ist PUBLIC.

Standardmäßig ist diese Option auf UNDF gesetzt, was bedeutet, dass DDMs, für die keine Sicherheitsprofile definiert wurden, nicht verwendet werden können.

Wenn Sie diese Option auf PUBL setzen, wird der Status aller DDMs, für die keine Sicherheitsprofile definiert wurden, als PUBLIC angenommen, was bedeutet, dass diese DDMs verwendet werden können. Damit können Sie diese DDMs verwenden, ohne Sicherheitsprofile für sie definieren zu müssen.

Weitere Informationen finden Sie in den Kapiteln *DDMs unter z/OS schützen* und *DDMs unter Linux und Windows schützen* .

Entwicklungsmodus - Development Mode

Siehe *Optionen für den Entwicklungsmodus der Bibliothek - Library Development Mode Options* im Kapitel *Natural-Entwicklungsumgebung in Eclipse schützen*.

Bibliothekssicherheitsprofile anlegen und verwalten

Dieser Abschnitt beschreibt die Funktionen zum Anlegen und Verwalten von Bibliothekssicherheitsprofilen. Die folgenden Themen werden behandelt:

- Bibliotheksverwaltung aufrufen
- Neue Bibliothek in Natural Security anlegen
- Nicht definierte Bibliotheken auflisten
- Vorhandene Bibliotheken zur Bearbeitung auswählen
- Bibliothek kopieren - Copy Library
- Bibliothek ändern - Modify Library
- Bibliothek umbenennen - Rename Library
- Bibliothek löschen - Delete Library
- Bibliothek anzeigen - Display Library
- Private Bibliothek anlegen und verwalten

Bibliotheksverwaltung aufrufen

Um die Bibliotheksverwaltung aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) die Option **Maintenance**.

2 Es wird ein Fenster angezeigt, in dem Sie den Objekttyp **Library** mit einem Zeichen oder mit dem Cursor markieren können.

Es wird die Auswahlliste **Library Maintenance** angezeigt.

3 Aus dieser Auswahlliste können Sie alle Funktionen der Bibliotheksverwaltung wie unten beschrieben aufrufen.

Neue Bibliothek in Natural Security anlegen

Die Funktion **Add Library** wird verwendet, um neue Bibliotheken in Natural Security zu definieren, d.h. *um Sicherheitsprofile für Bibliotheken anzulegen*.

Anmerkung: Um das Anlegen von Bibliothekssicherheitsprofile für Systembibliotheken von Natural und seinen Unterprodukten einfacher zu erledigen, können Sie die Funktion **Definition of System Libraries** in den **Administrator Services** verwenden, die vordefinierte Sicherheitsprofile für die meisten Systembibliotheken bereitstellt.

Um ein neues Bibliothekssicherheitsprofil anzulegen:

1 Geben Sie in der Kommandozeile der Auswahlliste **Library Maintenance** das Kommando `ADD` ein.

2 Es wird ein Fenster angezeigt, in dem Sie eine Bibliothekskennung und, optional, die Kennung eines Standardprofils eingeben müssen:

Feld	Beschreibung
Library ID	Bibliothekskennung. Bibliothekskennungen werden von Natural Security verwendet, um Bibliotheken und ihre Sicherheitsprofile zu identifizieren. Eine Bibliothekskennung kann 1 bis 8 Zeichen lang sein, muss mit einem Großbuchstaben beginnen und muss eindeutig sein. Sie kann aus den folgenden Zeichen bestehen: Großbuchstaben, Ziffern, Bindestrich (-) und Unterstrich (_). Sie darf keine Leerzeichen enthalten. Bevor Sie mit der Definition von Bibliotheken beginnen, ist es ratsam, ein logisches System von Bibliothekskennungen zu entwerfen, die mit den Bibliotheksnamen in Beziehung stehen. So können Sie die Bibliotheken bei der Verwaltung in Natural Security leichter identifizieren.
Default Profile	Standardprofil. Wenn Sie eine neue Bibliothek anlegen, können Sie entweder jeden Bestandteil des Bibliothekssicherheitsprofils von Hand eingeben oder ein vordefiniertes Standardbibliotheksprofil als Ausgangsbasis für das Sicherheitsprofil verwenden, das Sie erstellen. Bevor Sie Standardbibliotheksprofile verwenden, sollten Sie mit der „normalen“ Art der Definition von Bibliotheken (d. h. ohne Standardprofil) vertraut sein. Standardprofile werden im Subsystem **Administrator Services** angelegt und verwaltet. Wenn Sie im Fenster **Add Library** die Kennung eines Standardprofils angeben, werden die Bestandteile aus dem Standardprofil in das Bibliothekssicherheitsprofil kopiert. Auf dem Bildschirm **Add Library** können Sie die aus dem Standardprofil kopierten Bestandteile überschreiben und weitere Bestandteile angeben. Weitere Informationen zu Standardbibliotheksprofilen finden Sie unter ***Standardprofile für Bibliotheken - Library Default Profiles*** im Kapitel *Administrator Services*.

3 Der Bildschirm **Add Library** wird angezeigt. Auf diesem Bildschirm können Sie ein Sicherheitsprofil für die Bibliothek definieren.

Der Bildschirm **Add Library** und die nachfolgenden Bildschirme/Fenster, die Teil eines Bibliothekssicherheitsprofils sein können, sowie die einzelnen Bestandteile, die Sie definieren können, werden unter ***Bestandteile eines Bibliothekssicherheitsprofils*** beschrieben.

Wenn Sie eine neue Bibliothek anlegen, werden die in Ihrem eigenen Benutzersicherheitsprofil angegebenen Eigentümer automatisch in das Sicherheitsprofil der Bibliothek kopiert.

Nicht definierte Bibliotheken auflisten



Anmerkung: In einer Nicht-Großrechnerumgebung erfordert die Verwendung des Kommandos `SHOW`, dass die Arbeitsdatei 3 in Ihrem Natural-Parametermodul definiert wurde, da das Kommando intern die entsprechende Funktion des Dienstprogramms *Natural Object Handler* verwendet.

Eine nicht definierte Bibliothek ist eine Bibliothek, die zwar in der Systemdatei vorhanden ist, für die jedoch kein Bibliothekssicherheitsprofil in Natural Security angelegt wurde.

Um festzustellen, welche Bibliotheken nicht definiert sind, können Sie das Kommando `SHOW` benutzen. Dadurch wird die **Library Maintenance**-Auswahlliste so erweitert, dass sie auch nicht definierte Bibliotheken enthält.

Die Syntax für das `SHOW`-Kommando lautet wie folgt:

```
SHOW ALL [FILE=(database-id,file-number,password,ciphercode)]
```

oder

```
SHOW + [FILE=(database-id,file-number,password,ciphercode)]
```

Mit `FILE` geben Sie die Systemdatei an, deren nicht definierte Bibliotheken aufgelistet werden sollen. Wenn Sie die `FILE`-Angabe weglassen, werden die nicht definierten Bibliotheken der aktuellen FUSER-Systemdatei aufgelistet.

Die Systemdatei, auf die sich die erweiterte **Library Maintenance**-Auswahlliste bezieht, wird oben in der Auswahlliste der Bibliotheksverwaltung angezeigt. In der Spalte Message der Auswahlliste wird angezeigt, welche der aufgelisteten Bibliotheken nicht definiert sind.

Anstatt das Kommando `SHOW ALL` (ohne `FILE`-Angabe) in die Kommandozeile der **Library Maintenance**-Auswahlliste einzugeben, können Sie auch `PF16` drücken.

Wenn Sie nur die nicht definierten Bibliotheken auflisten wollen, können Sie entweder das Kommando `SHOW UNDF` (mit oder ohne `FILE`-Angabe) in die Kommandozeile eingeben, oder `UNDF` in das Schutzstatusfeld (**Prot.**) eingeben.

Um die **Library Maintenance**-Auswahlliste wieder auf die Standardanzeige der definierten Bibliotheken zurückzusetzen, können Sie erneut PF16 drücken oder das folgende Kommando in die Kommandozeile eingeben:

```
SHOW -
```

Anmerkung: Um nicht definierte Bibliotheken aufzulisten, können Sie auch die Anwendungsprogrammierschnittstelle NSCXR (mit Objekttypcode SF (System File) verwenden.

Um ein Sicherheitsprofil für eine einzige, nicht definierte Bibliothek anzulegen:

1 Markieren Sie in der **Library Maintenance**-Auswahlliste die betreffende Bibliothek mit dem Funktionscode AD oder AP.

2 Bei Eingabe von AP wird ein Fenster angezeigt, in dem Sie die Kennung eines Standardprofils angeben können (siehe **oben**). Bei Eingabe von AD wird dieses Fenster übersprungen und kein Standardprofil verwendet.

3 Der Bildschirm **Add Library** wird angezeigt - wie bei Schritt 3 oben.

Um Sicherheitsprofile für mehrere nicht definierte Bibliotheken anzulegen:

- Markieren Sie in der **Library Maintenance**-Auswahlliste entweder jede der Bibliotheken mit dem Funktionscode AD oder AP oder drücken Sie PF10, um alle nicht definierten Bibliotheken auf der aktuell angezeigten Seite der **Library Maintenance**-Auswahlliste gleichzeitig auszuwählen (entspricht der Markierung aller Bibliotheken mit AP).

  Die Schritte 2 und 3 werden dann für die markierten/selektierten Bibliotheken der Reihe nach wiederholt.

Anmerkung: Um nicht definierte Bibliotheken zu definieren, können Sie auch die **Administrator Services**-Funktion **Definition of Undefined Libraries** verwenden.

Vorhandene Bibliotheken zur Bearbeitung auswählen

Wenn Sie die Bibliotheksverwaltung (**Library Maintenance**) aufrufen, wird eine Liste aller Bibliotheken angezeigt, die in Natural Security definiert wurden.

Wenn Sie keine Liste aller vorhandenen Bibliotheken wünschen, sondern nur bestimmte Bibliotheken aufgelistet haben möchten, können Sie die Optionen **Start Value** (Startwert) und **Type/Status** (Typ/Status) verwenden, siehe *Grundlagen der Benutzung*.

Wählen Sie im Hauptmenü (**Main Menu**) die Option **Maintenance**. Es wird ein Fenster angezeigt.

Markieren Sie in dem Fenster den Objekttyp **Library** mit einem Zeichen oder mit dem Cursor (und geben Sie, falls gewünscht, einen Startwert und/oder einen Schutzstatus ein).

Die **Library Maintence**-Auswahlliste wird angezeigt:

```
12:47:45                  *** NATURAL SECURITY ***                2021-12-31
                            - Library Maintenance -

 Co Library ID Library Name                        Prot. Message
 __ __________ ___________________________________ _____ ________________________
 __ KETEST                                        YN
 __ KEX        TEST APPL-KE                       YN
 __ KE1        KETEST                             NN
 __ KJH                                           NN
 __ KK-APPL                                       NN
 __ KKAPP                                         NN
 __ KKAPPC                                        NN
 __ KKAPP1                                        NN
 __ KKAPP2                                        NN
 __ KKAPP3                                        NN
 __ KKAPP4                                        YN
 __ KKAPP7                                        NN
 __ KKITEST                                       NN
 __ KKPAC                                         NN
 __ KKPROD                                        NN

 Command ===>
 Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
       Help        Exit              Flip  -     +                       Canc
```

Zu jeder Bibliothek werden die Bibliothekskennung (**Library ID**), der Name (**Library Name**) und der Schutzstatus (**Prot.**) angezeigt.

In der Liste kann geblättert werden, wie im Kapitel *Grundlagen der Benutzung* beschrieben.

Die Liste kann auch um nicht definierte Bibliotheken erweitert werden, wie im Abschnitt *Nicht definierte Bibliotheken auflisten* weiter oben beschrieben.

Die folgenden Bibliotheksverwaltungsfunktionen stehen zur Verfügung (mögliche Codekürzel sind unterstrichen):

Code	Funktion
AD	Add Library. Bibliothek anlegen, ohne Standardprofil (nur möglich, wenn die Auswahlliste erweitert wurde; siehe *Nicht definierte Bibliotheken auflisten*).
AP	Add Library. Bibliothek anlegen, optional mit Standardprofil (nur möglich, wenn die Auswahlliste erweitert wurde; siehe *Nicht definierte Bibliotheken auflisten*).
CO	**Copy library**. Bibliothek kopieren.
MO	**Modify library**. Bibliothek ändern.
RE	**Rename library**. Bibliothek umbenennen.
DE	**Delete library**. Bibliothek löschen.

Code	Funktion
DI	**Display library**. Bibliothek anzeigen.
LU	**Link users to library**. Bibliothek mit Benutzern verlinken.
LF	**Link library to files** Bibliothek mit Dateien verlinken. (Diese Funktion ist nur auf Großrechnern verfügbar.)
MD	**Modify DDM restrictions in library**. DDM-relevante Einschränkungen in Bibliothek ändern. (Diese Funktion ist nur auf Großrechnern verfügbar.)
EP	**Protect environments**. Umgebungen schützen.
RA	**Restrict access to Natural RPC services**. Zugang zu Natural RPC-Diensten einschränken.

Um eine Funktion für eine Bibliothek aufzurufen, müssen Sie die Bibliothek in der Spalte **Co** mit dem entsprechenden Funktionscode markieren.

Sie können verschiedene Bibliotheken für verschiedene Funktionen gleichzeitig auswählen, d.h. Sie können mehrere Bibliotheken auf dem Bildschirm mit einem Funktionscode markieren. Für jede markierte Bibliothek wird der entsprechende Bearbeitungsbildschirm angezeigt. Sie können dann für eine Bibliothek nach der anderen die ausgewählten Funktionen ausführen.

Bibliothek kopieren - Copy Library

Mit der Funktion **Copy Library** können Sie eine neue Bibliothek in Natural Security definieren, indem Sie ein Sicherheitsprofil anlegen, das mit einem bestehenden Bibliothekssicherheitsprofil identisch ist.

- Was wird kopiert?
- Wie wird kopiert?
- Mit Verlinkungen kopieren

Was wird kopiert?

Alle Bestandteile des bestehenden Sicherheitsprofils werden in das neue Sicherheitsprofil kopiert - jedoch *nicht* die Eigentümer (diese werden aus Ihrem eigenen Benutzersicherheitsprofil in das neue Bibliothekssicherheitsprofil kopiert).

Zusätzlich zum Duplizieren eines Bibliothekssicherheitsprofils können Sie wählen, ob Sie auch die Verlinkungen (Links) und Dienstprogramm-(Utility-)Profile sowie die Bibliothek selbst kopieren möchten; dies hängt von den unten beschriebenen Optionen ab.

Wie wird kopiert?

1. Markieren Sie in der **Library Maintenance**-Auswahlliste die Bibliothek, deren Sicherheitsprofil Sie duplizieren möchten, mit dem Funktionscode `CO`.
2. Es wird ein Fenster angezeigt, in dem Sie folgende Angaben machen müssen bzw. können:

Feld	Erläuterung
To library	Nach Bibliothek. Geben Sie die Kennung der „neuen“ Bibliothek ein.
Library name	Bibliotheksname. In diesem Feld wird der Name der vorhandenen Bibliothek angezeigt. Überschreiben Sie ihn mit dem Namen der „neuen“ Bibliothek.
With links	Mit Verlinkungen. Geben Sie `Y` oder `N` ein. Mit dieser Option können Sie zusätzlich zum Bibliothekssicherheitsprofil auch dessen Verlinkungen, Dienstprogramm-(Utility-)Profile und Dateien/DDMs kopieren; siehe *Mit Verlinkungen kopieren* unten.
With Natural objects	Mit Natural-Objekten. Geben Sie `Y` oder `N` ein. Mit dieser Option können Sie die bestehende Bibliothek selbst duplizieren. Das bedeutet, dass eine neue Bibliothek in der FUSER-Systemdatei erstellt wird und alle Natural-Programmierobjekte, die in der bestehenden Bibliothek enthalten sind, in diese neue Bibliothek kopiert werden. (Intern verwendet diese Option die Anwendungsprogrammierschnittstelle `MAINUSER` des Natural-Dienstprogramms `SYSMAIN`).

3. Der Bildschirm **Copy Library** wird angezeigt. Er zeigt das neue Bibliothekssicherheitsprofil.

   Bestandteile, die Sie definieren können, sind unter *Bestandteile eines Bibliothekssicherheitsprofils* beschrieben.

Mit Verlinkungen kopieren

Wenn Sie **With links = N** wählen:

- Für die bereits bestehende Bibliothek definierte Verlinkungen werden nicht zu der neuen Bibliothek übertragen.
- Bibliotheksspezifische und benutzerbibliotheksspezifische Dienstprogramm-Profile der bestehenden Bibliothek werden nicht auf die neue Bibliothek übertragen.

Wenn Sie **With links = Y** wählen:

- Für die bestehende Bibliothek vorhandene Verlinkungen werden auf die neue Bibliothek kopiert, und Sie können die Verlinkungen, die Sie nicht auf die neue Bibliothek übertragen möchten, abwählen.
- Bibliotheksspezifische und benutzerbibliotheksspezifische Dienstprogramm-Profile, die für die bestehende Bibliothek existieren, werden auf die neue Bibliothek kopiert.

Die Vorgehensweise bei **With links = Y** ist wie folgt:

1. Nachdem Sie alle Änderungen am kopierten Sicherheitsprofil vorgenommen und den Bildschirm **Copy Library** durch Drücken von PF3 verlassen haben, wird eine Liste der Benutzer angezeigt: Sie enthält alle Benutzer, die mit der bestehenden Bibliothek verlinkt sind.
2. In der Liste können Sie einzelne Benutzer mit CL markieren, um Verlinkungen aufzuheben, die Sie nicht auf die neue Bibliothek kopieren möchten. Alle Benutzer, die Sie nicht markieren, werden automatisch mit der neuen Bibliothek auf dieselbe Weise verlinkt - normale oder spezielle Verlinkung - wie die bestehende Bibliothek.
3. Wenn Sie alle Benutzerverlinkungen hergestellt haben und die Benutzerliste durch Drücken von PF3 verlassen, wird eine Liste mit Dateien angezeigt: Sie enthält alle Dateien/DDMs, mit denen die bestehende Bibliothek verlinkt ist.
4. In der Liste können Sie einzelne Dateien/DDMs mit CL markieren, um die Verlinkungen aufzuheben, die Sie nicht auf die neue Bibliothek kopieren möchten. Mit allen Dateien/DDMs, die Sie nicht markieren, wird die neue Bibliothek automatisch auf die gleiche Weise verlinkt - Lese- (Read) oder Änderungsverlinkung (Update) - wie die bestehende Bibliothek.

Bibliothek ändern - Modify Library

Mit der Funktion **Modify Library** können Sie ein bestehendes Sicherheitsprofil einer Bibliothek ändern.

Dazu:

1 Markieren Sie in der **Library Maintenance**-Auswahlliste die Bibliothek, deren Sicherheitsprofil Sie ändern möchten, mit dem Funktionscode MO.

2 Es wird das Sicherheitsprofil der ausgewählten Bibliothek angezeigt.

Bestandteile, die Sie definieren oder ändern können, sind unter *Bestandteile eines Bibliothekssicherheitsprofils* beschrieben.

Bibliothek umbenennen - Rename Library

Mit der Funktion **Rename Library** können Sie die Bibliothekskennung eines bestehenden Bibliothekssicherheitsprofils ändern.

Dazu:

1 Markieren Sie in der **Library Maintenance**-Auswahlliste die Bibliothek, deren Bibliothekskennung Sie ändern möchten, mit dem Funktionscode RE.

2 Es wird ein Fenster angezeigt, in dem Sie eine neue Kennung für die Bibliothek eingeben (und optional den Namen ändern) können.

Je nach Einstellung der allgemeinen Option **Deletion of non-empty libraries allowed** (siehe *Administrator Services*) kann es sein, dass die Umbenennung eines Bibliothekssicherheitsprofils nicht möglich ist, wenn die Bibliothek Quellcode- oder Objektmodule enthält.

Mit Natural-Objekten

Wenn Sie ein Bibliothekssicherheitsprofil umbenennen, können Sie mit der Option **With Natural Objects** auch den Namen der zugehörigen Bibliothek ändern. Das bedeutet, dass die Bibliothek in der FUSER-Systemdatei umbenannt wird und alle Natural-Programmierobjekte, die in der Bibliothek enthalten sind, unter dem neuen Bibliotheksnamen gespeichert werden. (Intern verwendet diese Option die Anwendungsprogrammierschnittstelle `MAINUSER` des Natural-Dienstprogramms `SYSMAIN`).

Bibliothek löschen - Delete Library

Mit der Funktion **Delete Library** können Sie ein bestehendes Bibliothekssicherheitsprofil löschen.

Dazu:

1. Markieren Sie in der **Library Maintenance**-Auswahlliste die Bibliothek, die Sie löschen möchten, mit dem Funktionscode `DE`.
2. Das Fenster **Delete Library** wird angezeigt.

   - Wenn Sie sich gegen das Löschen des Bibliothekssicherheitsprofils entscheiden, können Sie das Fenster verlassen, indem Sie ENTER drücken, ohne etwas eingegeben zu haben.
   - Um das Bibliothekssicherheitsprofil zu löschen, müssen Sie die Kennung der Bibliothek in dem Fenster eingeben, um den Löschvorgang zu bestätigen.

Wenn Sie eine Bibliothek löschen, werden auch alle bestehenden Verlinkungen zu dieser Bibliothek gelöscht.

Je nach Einstellung der allgemeinen Option **Deletion of Non-empty Libraries Allowed** (siehe *Administrator Services*) kann es sein, dass das Löschen eines Bibliothekssicherheitsprofils nicht möglich ist, wenn die Bibliothek noch Quellcode- oder Objektmodule enthält.

Wenn Sie mehrere Bibliotheken mit `DE` markieren, wird ein Fenster angezeigt, in dem Sie gefragt werden, ob Sie die Löschung jedes einzelnen Bibliothekssicherheitsprofils durch Eingabe der Bibliothekskennung bestätigen möchten, oder ob alle zum Löschen ausgewählten Bibliotheken ohne Einzelbestätigung gelöscht werden sollen. Achten Sie darauf, dass Sie nicht versehentlich eine Bibliothek löschen.

Mit Natural-Objekten

Wenn Sie ein Bibliothekssicherheitsprofil löschen, können Sie mit der Option **With Natural Objects** auch die zugehörige Bibliothek selbst löschen. Das bedeutet, dass die Bibliothek - und alle darin enthaltenen Natural-Programmierobjekte - aus der Systemdatei FUSER gelöscht werden. (Intern verwendet diese Option die Anwendungsprogrammierschnittstelle `MAINUSER` des Natural-Dienstprogramms `SYSMAIN`).

Bibliothek anzeigen - Display Library

Mit der Funktion **Display Library** können Sie ein vorhandenes Bibliothekssicherheitsprofil anzeigen.

Dazu:

- Markieren Sie in der **Library Maintenance**-Auswahlliste die Bibliothek, deren Sicherheitsprofil Sie anzeigen möchten, mit dem Funktionscode `DI`.

  Es wird das Sicherheitsprofil der ausgewählten Bibliothek angezeigt. Seine Bestandteile sind unter *Bestandteile eines Bibliothekssicherheitsprofils* beschrieben.

Private Bibliothek anlegen und verwalten

- Private Bibliothek definieren
- Private Bibliothek verwalten
- Private Bibliothek löschen

Private Bibliothek definieren

Die Bibliothekskennung, mit der eine private Bibliothek in Natural Security definiert wird, ist identisch mit der jeweiligen Benutzerkennung. Daher können private Bibliotheken nur für Benutzer erstellt werden, deren Benutzerkennungen mit den Namenskonventionen für Bibliothekskennungen übereinstimmen.

Um eine private Bibliothek in Natural Security zu definieren:

1. Markieren Sie im Sicherheitsprofil des Benutzers das Feld **Private Library** mit `Y` (auf dem Bildschirm **Add User**, **Copy User** oder **Modify User**) (das Markieren dieses Feldes bewirkt nicht, dass ein Standardprofil für private Bibliotheken angelegt wird).
2. Wählen Sie im Fenster **Additional Options** (Zusätzliche Optionen) die Option **Private Library** oder drücken Sie `PF5` im Hauptbildschirm für das Benutzersicherheitsprofil.

   Es wird der Bildschirm **Private Library** angezeigt. Er ist identisch mit einem „normalen“ Bibliothekssicherheitsprofilbildschirm (außer wenn private Bibliotheken im privaten Modus verwendet werden, in diesem Fall enthält der Bildschirm nicht die Felder **People-protected**

und **Terminal-protected**). In diesem Bildschirm und in den folgenden Bildschirmen/Fenstern können Sie das Sicherheitsprofil für die private Bibliothek definieren.

Private Bibliothek verwalten

Im privaten Modus erfolgt die Verwaltung der vorhandenen privaten Bibliothekssicherheitsprofile über die Benutzerverwaltung (**User Maintenance**).

Im Public-Modus erscheinen auch private Bibliotheken in der **Library Maintenance**-Auswahlliste zusammen mit den anderen Bibliotheken, d.h. sie können wie „normale“ Bibliotheken mit den oben beschriebenen Bibliotheksverwaltungsfunktionen verwaltet werden.

Private Bibliothek löschen

Wenn private Bibliotheken im Modus **Public** verwendet werden, können Sie eine private Bibliothek wie jede andere Bibliothek löschen (siehe ***Bibliothek löschen - Delete Library***).

Wenn private Bibliotheken im Modus **Private** verwendet werden, können Sie eine private Bibliothek löschen, indem Sie das Feld **Private Library** im Sicherheitsprofil des Benutzers mit `N` markieren. Es wird ein Fenster aufgerufen, in dem Sie das Löschen durch Eingabe der Bibliothekskennung bestätigen müssen.

Abhängig von der Einstellung der allgemeinen Option **Deletion of Non-empty Libraries Allowed** (siehe *Administrator Services*) kann es sein, dass eine private Bibliothek nicht gelöscht werden kann, wenn sie noch Quellcode- oder Objektmodule enthält.

10 Bibliotheken schützen

- Geschützte Bibliotheken - Protected Libraries 204
- Benutzer mit Bibliotheken verlinken 206
- Welche Benutzungsbedingungen sind in Kraft? 212

In diesem Kapitel wird beschrieben, wie Sie den Zugriff von Benutzern auf geschützte Bibliotheken verwalten können.

Folgende Themen werden behandelt:

Geschützte Bibliotheken - Protected Libraries

Eine Bibliothek kann geschützt werden, indem in der Spalte **General Options** des Sicherheitsprofils der Bibliothek die Werte für **People-protected** und **Terminal-protected** angegeben werden.

Schutzkombinationen

Die möglichen Kombinationen von **People-protected** und **Terminal-protected** sind im Folgenden aufgeführt:

Schutz (Protection)	Erläuterung
People: N, Terminal: N	Die Bibliothek ist nicht geschützt. Sie kann von jeder Person von jedem Terminal aus benutzt werden. Das Terminal braucht nicht in Natural Security definiert zu sein. Der Benutzer muss in Natural Security definiert sein. Die Benutzerkennung muss auf dem Anmeldebildschirm eingegeben werden, um sich bei der Bibliothek anmelden zu können.
People: L, Terminal: N	Diese Kombination ist identisch mit der obigen Kombination - mit dem folgenden Zusatz: Obwohl die Bibliothek nicht geschützt ist, ist es möglich, eine Gruppe mit der Bibliothek zu verlinken. Es kann nur eine einzige Gruppe mit der Bibliothek verlinkt werden, und die Verlinkung muss eine spezielle Verlinkung (Special Link) sein. Diese spezielle Verlinkung gilt nur für Benutzer des Typs „Administrator“, die in der Gruppe enthalten sind. Diese Funktion ist nur dafür gedacht, Administratoren zu Verwaltungszwecken einen anderen Zugriff auf eine ungeschützte Bibliothek zu ermöglichen. (Die spezielle Verlinkung zu einer solchen Bibliothek kann nur über die Funktion **Link users to library** hergestellt werden, die über die **Library Maintenance**-Auswahlliste aufgerufen wird). **Anmerkung:** Wenn ein Administrator den Inhalt der Bibliothek mit einem Natural-Dienstprogramm unter einer Bedingung bearbeitet, unter der die **Utilities**-Option im Bibliothekssicherheitsprofil gelten würde, reagiert Natural Security so, als ob diese Option auf `N` gesetzt wäre.
People: Y, Terminal: N	Die Bibliothek kann nur von Personen verwendet werden, die mit der Bibliothek verlinkt sind oder einer Gruppe angehören, die mit der Bibliothek verlinkt ist. Sie kann von jedem Terminal aus benutzt werden. Das Terminal muss nicht in Natural Security definiert sein. Der Benutzer (und ggf. die Gruppe) muss in Natural Security definiert sein. Die Benutzerkennung muss auf dem Anmeldebildschirm eingegeben werden, um sich bei der Bibliothek anmelden zu können.
People: N, Terminal: Y	Die Bibliothek kann von jeder Person genutzt werden, aber nur von einem Terminal aus, das in Natural Security definiert ist und zu einer Gruppe gehört, die mit der

Schutz (Protection)	Erläuterung
	Bibliothek verlinkt ist. Auf dem Anmeldebildschirm ist keine Benutzerkennung erforderlich, um sich bei der Bibliothek anzumelden.
People: Y, Terminal: Y	Die Bibliothek kann entweder von Personen genutzt werden, die mit der Bibliothek verlinkt sind, oder von einem Terminal, das in einer Gruppe enthalten ist, die mit der Bibliothek verlinkt ist. Mit anderen Worten: Eine verlinkte Person kann durch Eingabe ihrer Benutzerkennung auf dem Anmeldebildschirm die Bibliothek von einem beliebigen Terminal aus nutzen. Personen, die nicht mit der Bibliothek verlinkt sind, können die Bibliothek nur von einem verlinkten Terminal aus nutzen.
People: Y, Terminal: A	Die Bibliothek kann nur von Personen über verlinkte Terminals genutzt werden: Die Person muss in Natural Security definiert sein und muss sich in einer Gruppe befinden, die mit der Bibliothek verlinkt ist (oder kann direkt verlinkt sein, wenn ihr Benutzertyp „Administrator“ oder „Person“ ist). Das Terminal muss ebenfalls in Natural Security definiert sein und muss sich in einer Gruppe befinden, die mit der Bibliothek verlinkt ist. Die Benutzerkennung und die Bibliothekskennung müssen auf dem Anmeldebildschirm eingegeben werden, um sich bei der Bibliothek anmelden zu können.
People: P, Terminal: N	Diese Kombination gilt nur für **private Bibliotheken** im Public-Modus. Der Benutzer mit der gleichen Benutzerkennung wie die Bibliothekskennung kann die Bibliothek nutzen, ohne dass eine Verlinkung mit ihr erforderlich ist. Ansonsten ist diese Kombination identisch mit People: Y, Terminal: N (siehe oben).
People: P, Terminal: Y	Diese Kombination gilt nur für **private Bibliotheken** im Public-Modus. Der Benutzer mit der gleichen Benutzerkennung wie die Bibliothekskennung kann die Bibliothek nutzen, ohne dass eine Verlinkung mit ihr erforderlich ist. Ansonsten ist diese Kombination identisch mit People: Y, Terminal: Y(siehe oben).
People: P, Terminal: A	Diese Kombination gilt nur für **private Bibliotheken** im Public-Modus. Der Benutzer mit der gleichen Benutzerkennung wie die Bibliothekskennung kann die Bibliothek nutzen, ohne dass eine Verlinkung mit ihr erforderlich ist. Ansonsten ist diese Kombination identisch mit People: Y, Terminal: A(siehe oben).
People: N, Terminal: A	Diese Kombination ist nicht möglich!
People: L, Terminal: Y	Diese Kombination ist nicht möglich!
People: L, Terminal: A	Diese Kombination ist nicht möglich!

Schutzkombination ändern

Vorsicht ist geboten, wenn Sie eine bestehende Kombination aus **People-protected** und **Terminal-protected** ändern. Wenn die Änderung zu einer „niedrigeren“ Schutzstufe führt, werden bestimmte Links automatisch von Natural Security gemäß den folgenden Regeln gelöscht:

Änderung von	nach	Auswirkung auf Links
beliebige Schutzkombination	People: N, Terminal: N	Alle bestehenden Links zur Bibliothek werden gelöscht.
	People: N, Terminal: Y	Alle direkten Links von „Administrator(en)“ und „Person(en)“ werden gelöscht. Verlinkungen von „Gruppen“ mit der Bibliothek bleiben erhalten.
	People: Y, Terminal: N	Es werden keine Links gelöscht.
	People: Y, Terminal: Y	Es werden keine Links gelöscht.
People: N, Terminal: Y	People: Y, Terminal: Y	Es werden keine Links gelöscht. Allerdings können sich alle Personen, die in „Gruppen“ enthalten sind, die mit der Bibliothek verlinkt sind, nun auch in der Bibliothek anmelden!

Private Bibliothek schützen

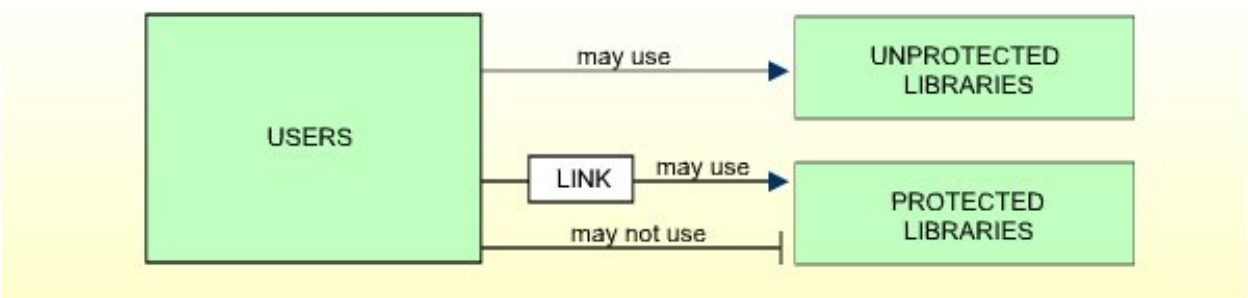
Der Benutzer mit der gleichen Benutzerkennung wie die Bibliothekskennung hat immer Zugriff auf seine **private Bibliothek**.

Im Public-Modus wird der Zugriff anderer Benutzer auf jemandes private Bibliothek durch die Einstellungen der Felder **People-protected** und **Terminal-protected** im Sicherheitsprofil der privaten Bibliothek bestimmt. Mögliche Werte für das Feld **People-protected** sind `P` (dies ist der Standardwert und entspricht `Y` in anderen Bibliothekssicherheitsprofilen) und `N` (dies ist derselbe Wert wie in anderen Bibliothekssicherheitsprofilen). Die möglichen Werte für das Feld **Terminal-protected** sind die gleichen wie für andere Bibliotheken (`Y`, `N` oder `A`). Die möglichen **Schutzkombinationen** sind oben beschrieben.

Im Private-Modus hat kein anderer Benutzer Zugriff auf die private Bibliothek eines anderen Benutzers.

Benutzer mit Bibliotheken verlinken

Um einem Benutzer den Zugriff auf eine geschützte Bibliothek zu ermöglichen, muss ein *Link* zwischen dem Benutzer und der Bibliothek hergestellt werden.



Nur Benutzer der Typen „Administrator“, „Person“ und „Group“ (Gruppe) können mit einer Bibliothek verlinkt werden.

Benutzer der Typen „Administrator“ und „Person“ können entweder direkt oder über eine „Group“ (Gruppe) mit einer Bibliothek verlinkt werden.

Benutzer der Typen „Member“ (Mitglied) und „Terminal“ können nur über eine „Group“ (Gruppe) mit einer Bibliothek verlinkt werden, d.h. sie müssen einer Gruppe zugeordnet werden und die Gruppe muss mit der Bibliothek verlinkt sein.

Es gibt zwei Funktionen, um Links zwischen Benutzern und Bibliotheken herzustellen und zu verwalten:

- eine Benutzerverwaltungsfunktion (**User Maintenance**-Funktion), um *einen Benutzer* mit *einer oder mehreren Bibliotheken* zu verlinken,
- eine Bibliotheksverwaltungsfunktion (**Library Maintenance**-Funktion), um *einen oder mehrere Benutzer* mit *einer Bibliothek* zu verlinken.

Diese beiden Funktionen werden im Folgenden beschrieben.

Einzelnen Benutzer mit Bibliotheken verlinken

Um einen Benutzer mit einer oder mehreren Bibliotheken zu verlinken:

1 Markieren Sie in der **User Maintenance**-Auswahlliste den Benutzer, den Sie verlinken möchten, mit dem Funktionscode `LL`. Es erscheint ein Fenster mit den folgenden Optionen:

2 Es erscheint ein Fenster mit den folgenden Optionen:

- **Start value**
  Sie können einen Startwert für die Liste der anzuzeigenden Bibliotheken eingeben (wie im Kapitel *Grundlagen der Benutzung* beschrieben).

- **Selection criterion**
  N = None/kein Selektionskriterium: Es werden alle Bibliotheken aufgelistet.

  L = Linked: Es werden nur Bibliotheken aufgelistet, mit denen der Benutzer bereits verlinkt ist (normale und spezielle Links, einschließlich vorübergehend gesperrter).

  U = Unlinked: Es werden nur Bibliotheken aufgelistet, mit denen der Benutzer noch nicht verlinkt ist.

3 Dann wird die Auswahlliste **Link User To Libraries** angezeigt, die die Liste der Bibliotheken anzeigt. Sie enthält alle geschützten Bibliotheken, d. h. wenn Sie einen Benutzer vom Typ „Person“ oder „Administrator“ verlinken, enthält sie alle Bibliotheken, bei denen **People-protected** auf Y gesetzt ist. Wenn Sie einen Benutzer vom Typ „Group“ verlinken, enthält sie alle Bibliotheken, bei denen mindestens einer der beiden Schutzwerte auf Y gesetzt ist.

In der Liste kann geblättert werden, wie im Kapitel *Grundlagen der Benutzung* beschrieben.

Markieren Sie in der Liste die Bibliotheken, mit denen Sie den ausgewählten Benutzer verlinken möchten.

In der Spalte **Co** können Sie jede Bibliothek mit einem der folgenden Funktionscodes markieren (mögliche Code-Abkürzungen sind unterstrichen):

Code	Funktion
LK	Link - Der Benutzer darf die Bibliothek benutzen, wenn das Sicherheitsprofil der Bibliothek wirksam ist.
SL	Spezieller Link - Der Benutzer kann die Bibliothek mit einem speziellen Sicherheitsprofil verwenden, das für den Link definiert werden muss. Das Linkprofil hat Vorrang vor dem Bibliothekssicherheitsprofil. Siehe *Spezielle Links* unten.
CL	Cancel - Eine bestehende Verlinkung oder ein spezieller Link wird aufgehoben.
TL	Temporarily Locked/Vorübergehend gesperrt - Eine bestehende Verlinkung oder eine spezielle Verlinkung wird ausgesetzt, bis sie wiederhergestellt wird. Eine vorübergehend gesperrte Verlinkung oder spezielle Verlinkung kann wiederhergestellt werden, indem die betreffende Bibliothek erneut mit LK oder SL markiert wird. Wenn ein spezieller Link wiederhergestellt wird, wird auch das ursprüngliche Link-Sicherheitsprofil wiederhergestellt.
DL	Display Special Link/Speziellen Link anzeigen - Das Sicherheitsprofil eines bestehenden speziellen Links zwischen dem Benutzer und der Bibliothek wird angezeigt.
DI	Display Library/Bibliothek anzeigen - Das Sicherheitsprofil der Bibliothek wird angezeigt.
LD	DDM-Einschränkungen im Special Link Profile ändern. (Diese Funktion ist auf Großrechnern nicht verfügbar. Sie entspricht der Funktion MD, wie unter *DDM-Sicherheitsprofile anlegen und verwalten* beschrieben).

Sie können auf dem Bildschirm eine oder mehrere Bibliotheken mit einem Funktionscode markieren.

4 Für jede markierte Bibliothek werden die ausgewählten Funktionen nacheinander ausgeführt. Nach Abschluss der Verarbeitung wird für jede Bibliothek eine Meldung angezeigt, in der die jetzt gültige Verlinkungssituation angegeben ist.

Mehrere Benutzer mit einer Bibliothek verlinken

Um einen oder mehrere Benutzer mit einer Bibliothek zu verlinken:

1 Markieren Sie in der **Library Maintenance**-Auswahlliste die Bibliothek, mit der Sie einen oder mehrere Benutzer verlinken möchten, mit dem Code `LU`.

2 Es wird ein Fenster mit folgenden Optionen angezeigt:

- **Start value**
  Sie können einen Startwert für die Liste der anzuzeigenden Benutzer eingeben (wie im Kapitel *Grundlagen der Benutzung* beschrieben).
- **Selection criterion**
  `N` = None/kein Selektionskriterium: Alle Benutzer werden aufgelistet.

  `L` = Linked: Nur Benutzer, die bereits mit der Bibliothek verlinkt sind (normale und spezielle Links, einschließlich vorübergehend gesperrter) werden aufgelistet.

  `U` = Unlinked: Nur Benutzer, die noch nicht mit der Bibliothek verlinkt sind, werden aufgelistet.

3 Anschließend wird die Auswahlliste **Link Users To Library** (Benutzer mit Bibliothek verlinken) angezeigt, die die Liste der Benutzer anzeigt. Sie enthält alle Benutzer der Typen „Group“ (Gruppe), „Administrator“ und „Person“.

In der Liste kann geblättert werden, wie im Kapitel *Grundlagen der Benutzung* beschrieben.

Markieren Sie in der Liste die Benutzer, die Sie mit der ausgewählten Bibliothek verlinken möchten.

In der Spalte **Co** können Sie jeden Benutzer mit einem der folgenden Funktionscodes markieren (mögliche Code-Abkürzungen sind unterstrichen):

Code	Funktion
`LK`	Link/Verlinken - Der Benutzer darf die Bibliothek mit dem für die Bibliothek definierten und wirksamen Sicherheitsprofil benutzen.
`SL`	Spezieller Link - Der Benutzer kann die Bibliothek mit einem speziellen Sicherheitsprofil verwenden, das für die Verlinkung zu definieren ist. Das Linkprofil hat Vorrang vor dem Bibliothekssicherheitsprofil. Siehe *Spezielle Links* unten.
`CL`	Cancel/Aufheben - Eine bestehende Verlinkung oder spezielle Verlinkung wird aufgehoben.

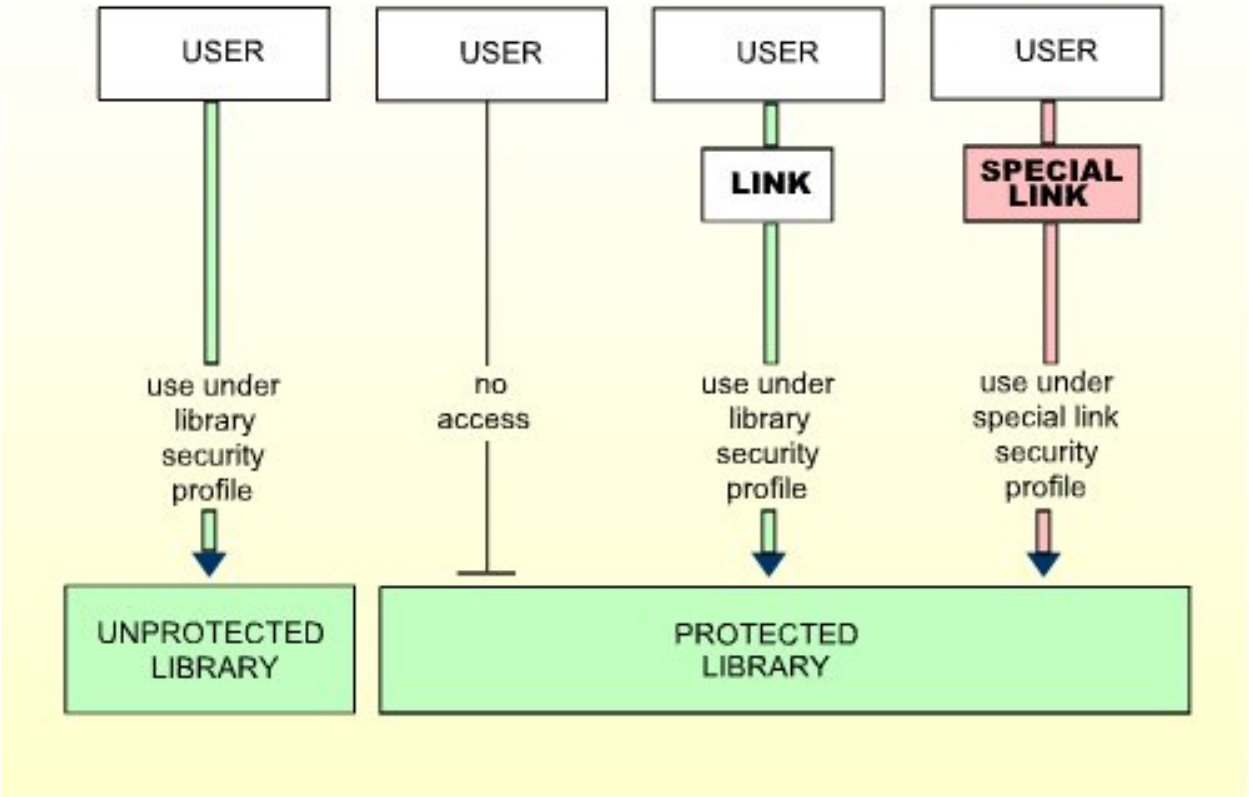
Code	Funktion
TL	Temporarily Locked/Vorübergehend gesperrt - Eine bestehende Verlinkung oder eine spezielle Verlinkung wird ausgesetzt, bis sie wiederhergestellt wird. Eine ausgesetzte Verlinkung oder spezielle Verlinkung kann wiederhergestellt werden, indem der betreffende Benutzer erneut mit LK oder SL markiert wird. Wenn eine spezielle Verlinkung wiederhergestellt wird, wird auch das ursprüngliche Link-Sicherheitsprofil wiederhergestellt.
DL	Display Special Link/Spezielle Verlinkung anzeigen - Das Sicherheitsprofil einer bestehenden speziellen Verlinkung zwischen dem Benutzer und der Bibliothek wird angezeigt.
DI	Display User/Benutzer anzeigen - Das Sicherheitsprofil des Benutzers wird angezeigt.
LD	DDM-Einschränkungen im Special Link Profile ändern (Diese Funktion ist auf Großrechnern nicht verfügbar. Sie entspricht der Funktion MD, wie unter *DDM-Sicherheitsprofile anlegen und verwalten* beschrieben).

Sie können in dem Bildschirm einen oder mehrere Benutzer mit einem Funktionscode markieren.

4 Für jeden markierten Benutzer werden die gewählten Funktionen nacheinander ausgeführt. Nach Abschluss der Verarbeitung wird eine Meldung angezeigt, die besagt, dass die Verlinkungssituation für den jeweiligen Benutzer nun in Kraft ist.

Spezielle Links - Special Links

Während ein Bibliothekssicherheitsprofil die Bedingungen festlegt, unter denen die Bibliothek allgemein benutzt werden darf, bestimmt das Sicherheitsprofil für spezielle Links die Bedingungen, unter denen der so verlinkte Benutzer (oder Gruppe von Benutzern) die Bibliothek benutzen darf. Das bedeutet, dass Sie durch die Verwendung spezieller Links für verschiedene Benutzer unterschiedliche Bedingungen für die Nutzung derselben Bibliothek festlegen können.



Die Bestandteile, die Sie in einem Profil für spezielle Verknüpfungen definieren, haben Vorrang vor den entsprechenden Bestandteilen im Bibliothekssicherheitsprofil.

Einige Bestandteile können in speziellen Verknüpfungsprofilen nicht eingestellt werden. Für diese gelten die im Bibliothekssicherheitsprofil angegebenen Einstellungen.

Speziellen Link anlegen

Wenn Sie einen Benutzer/eine Bibliothek mit `SL` markieren, können Sie auf den dann angezeigten Bildschirmen das Sicherheitsprofil für diesen speziellen Link festlegen. Die Standardeinstellungen, die auf den Bildschirmen des Sicherheitsprofils für den speziellen Link erscheinen, werden aus dem Sicherheitsprofil der Bibliothek übernommen.

Die Bestandteile eines Sicherheitsprofils für einen speziellen Link entsprechen denen, die Sie als Teil eines Bibliothekssicherheitsprofils definieren können (siehe ***Bestandteile eines Bibliothekssicherheitsprofils*** im Kapitel *Bibliotheken verwalten*).

Speziellen Link ändern - Modify Special Link

Um ein bestehendes Sicherheitsprofil für einen speziellen Link zu ändern, markieren Sie den betreffenden Benutzer/die betreffende Bibliothek erneut mit `SL` auf dem Bildschirm **Link Users To Library** oder **Link User To Libraries**: Der Bildschirm mit dem Sicherheitsprofil für einen **Special Link** wird zur Änderung aufgerufen.

Speziellen Link anzeigen

Um das Sicherheitsprofil für einen speziellen Link anzuzeigen, markieren Sie den betreffenden Benutzer/die betreffende Bibliothek auf dem Bildschirm **Link Users To Library** oder **Link User To Libraries** mit `DL`: Der Bildschirm mit dem Sicherheitsprofil für einen **Special Link** wird angezeigt.

Welche Benutzungsbedingungen sind in Kraft?

Wenn sich ein Benutzer bei einer geschützten Bibliothek anmeldet, führt Natural Security eine Reihe von Prüfungen durch, um festzustellen, unter welchen Bedingungen der Benutzer die Bibliothek benutzen darf. Wenn keine der Prüfungen positiv ausfällt, wird die Anmeldung abgelehnt.

Die folgenden Prüfungen zum Schutz der Bibliothek werden in der folgenden Reihenfolge durchgeführt:

Library Protection/Schutz der Bibliothek	Durchgeführte Prüfungen
1. People: Y Terminal: N	Prüfung, ob der Benutzer direkt mit der Bibliothek verlinkt ist. Wenn der Benutzer über einen speziellen Link verlinkt ist, gelten die im Sicherheitsprofil für einen **Special Link** definierten Bedingungen. Wenn der Benutzer über einen normalen Link verlinkt ist, gelten die im Sicherheitsprofil der Bibliothek definierten Bedingungen. Zweitens: Prüfung, ob der Benutzer einer Gruppe angehört, die mit der Bibliothek verlinkt ist. Ist der Benutzer in mehr als einer Gruppe enthalten, werden diese Gruppen in der folgenden Reihenfolge geprüft: Zuerst werden die privilegierten Gruppen im Sicherheitsprofil des Benutzers in der Reihenfolge ihres Eintrags geprüft, dann werden die anderen Gruppen in alphabetischer Reihenfolge geprüft. Die erste gefundene verlinkte Gruppe wird gewählt. Ist die Gruppe über einen speziellen Link verlinkt, gelten die im Sicherheitsprofil für einen **Special Link** definierten Bedingungen. Ist die Gruppe über einen normalen Link verlinkt, dann gelten die im Sicherheitsprofil der Bibliothek definierten Bedingungen.
2. People: N Terminal: Y	Prüfung, ob das Terminal einer Gruppe angehört, die mit der Bibliothek verlinkt ist. Ist das Terminal in mehr als einer Gruppe enthalten, werden diese Gruppen in der folgenden Reihenfolge geprüft: Zuerst werden die privilegierten Gruppen (Privileged Groups) im Sicherheitsprofil des Terminals in der Reihenfolge ihres Eintrags geprüft,

Library Protection/Schutz der Bibliothek	Durchgeführte Prüfungen
	dann die anderen Gruppen in alphabetischer Reihenfolge. Die erste gefundene verlinkte Gruppe wird ausgewählt. Ist diese Gruppe über einen speziellen Link verlinkt, gelten die im Sicherheitsprofil für einen **Special Link** definierten Bedingungen. Ist diese Gruppe über einen normalen Link verlinkt, gelten die in den Sicherheitsprofilen der Bibliothek definierten Bedingungen.
3. People: Y Terminal: Y	Wenn sich der Benutzer *mit einer Benutzerkennung* anmeldet, werden die gleichen Prüfungen wie unter 1. durchgeführt. Meldet sich der Benutzer *ohne Angabe einer Benutzerkennung* an, werden die gleichen Prüfungen wie unter 2. durchgeführt.
4. People: Y Terminal: A	Es werden die gleichen Prüfungen wie unter 1. durchgeführt.

Anmerkung: Das Terminal muss sich in einer Gruppe befinden, die mit der Bibliothek verlinkt ist, aber die Bedingungen für die Benutzung werden durch den Link des Benutzers bestimmt.

PROFILE-Kommando

Wenn ein Benutzer bei einer Bibliothek angemeldet ist, kann er das Natural-Systemkommando `PROFILE` eingeben, um festzustellen, welche Benutzungsbedingungen zurzeit in Kraft sind.

Wenn Sie das Kommando `PROFILE` eingeben, wird der **Security Profile**-Bildschirm mit den folgenden Informationen angezeigt:

User / Benutzer	
ID	Die Benutzerkennung des Benutzers.
Name	Der Name des Benutzers.
Type	Der Benutzertyp.
Link ID	Link-Kennung. Der aktuelle Wert der Natural-Systemvariablen `*GROUP`. Ein Stern (*) neben der Kennung zeigt an, dass die Verlinkung der Gruppe/des Benutzers mit der aktuellen Bibliothek ein Special Link ist.
ETID	Der aktuelle Wert der Natural-Systemvariablen `*ETID`.
Library / Bibliothek	
ID	Die Bibliothekskennung der aktuellen Bibliothek.
Name	Der Name der aktuellen Bibliothek.
Steplibs	Die Steplibs der aktuellen Bibliothek.
Transactions / Transaktionen	

User / Benutzer	
Startup	Der aktuelle Wert der Natural-Systemvariablen *STARTUP.
Restart	Der Name der Neustart-Transaktion.
Error	Der aktuelle Wert der Natural-Systemvariablen *ERROR-TA.

Zusätzliche Optionen - Additional Options

Wenn Sie im Bildschirm **Security Profile** das Feld **Additional Options** mit Y markieren oder PF4 drücken, wird ein Fenster angezeigt, in dem Sie die folgenden Informationen auswählen können:

- Security options
- Security limits
- Session parameters
- Command restrictions
- Editing restrictions
- Statement restrictions
- Time windows
- System files
- Natural version

Diejenigen Optionen, bei denen etwas für den aktuellen Benutzer definiert ist, sind mit einem Pluszeichen (+) gekennzeichnet.

Sie können einen oder mehrere Optionen aus dem Fenster auswählen, indem Sie sie mit einem beliebigen Zeichen markieren. Für jede ausgewählte Option wird ein weiteres Fenster/Bildschirm angezeigt (in der Reihenfolge der Optionen im Auswahlfenster).

Zugangsberechtigungen für Dienstprogramme - Utility Access Rights

Wenn Sie PF5 drücken, wird das Fenster **NSC Utility Access Rights** angezeigt, das einen Überblick über die Dienstprogramm-Funktionen gibt, die Sie in jeder Bibliothek verwenden dürfen.

- Wenn Sie das Systemkommando PROFILE aus einem Dienstprogramm heraus abgesetzt haben, listet das Fenster die in diesem Dienstprogramm nutzbaren Funktionen auf.
- Wenn Sie das Systemkommando PROFILE an anderer Stelle abgesetzt haben, listet das Fenster alle Dienstprogramme auf, zusammen mit der Information, ob einige oder alle Funktionen eines Dienstprogramms für eine bestimmte Bibliothek erlaubt/nicht erlaubt sind. (Die Notation <others> (sonstige) im Feld **Library** des Fensters zeigt alle Bibliotheken an, für die nichts Spezielles definiert wurde). Um ausführlichere Informationen über die für eine bestimmte Bibliothek zulässigen Dienstprogrammfunktionen zu erhalten, können Sie eine oder mehrere Bibliotheken im Fenster auswählen, indem Sie sie mit einem beliebigen Zeichen markieren.

11 Umgebungen schützen

- Konzept des Umgebungsschutzes 216
- Umgebungsschutz aktivieren 216
- Umgebungsprofile definieren 217
- Bestandteile eines Umgebungsprofils 219
- Zugriff auf Bibliotheken in Umgebungen nicht erlauben/erlauben 221
- Benutzern den Zugang zu Umgebungen nicht erlauben/erlauben 224

Folgende Themen werden behandelt:

Konzept des Umgebungsschutzes

Mit Natural Security können Sie den Zugriff der Benutzer auf eine Bibliothek umgebungsspezifisch gestalten. Eine Natural-Umgebung wird durch die Kombination der Systemdateien FNAT, FUSER, FSEC und FDIC bestimmt. Sie können für jede Umgebung (d. h. für jede Kombination von Systemdateien), die Sie schützen möchten, ein Sicherheitsprofil definieren und den Zugriff der Benutzer darauf steuern. Außerdem können Sie eine Bibliothek in einigen Umgebungen zugänglich machen, in anderen jedoch nicht.

Eine Anmeldung in einer anderen Umgebung erfolgt, wenn sich ein Benutzer bei einer Bibliothek anmeldet, die sich in einer anderen FUSER-Systemdatei befindet (wie im Bibliothekssicherheitsprofil unter **Library File** durch Datenbankkennung (DBID) und Dateinummer (FNR) angegeben).

Wenn sich ein Benutzer bei einer Bibliothek in einer anderen Umgebung anmeldet, prüft Natural Security Folgendes:

- Ob der Zugriff auf die Bibliothek in dieser Umgebung erlaubt ist und
- ob der Benutzer berechtigt ist, auf diese Umgebung zuzugreifen.

Eine solche Prüfung wird nicht nur dann durchgeführt, wenn sich ein Benutzer explizit bei einer Bibliothek anmeldet, sondern auch, wenn der Benutzer eine Funktion aufruft, die implizit auf eine andere Bibliothek zugreift oder den Inhalt einer anderen Bibliothek verarbeitet.

Umgebungsschutz aktivieren

Um den Umgebungsschutz zu aktivieren, müssen Sie die Allgemeine Option **Environment Protection** auf `Y` setzen.

Wenn der Umgebungsschutz aktiviert ist, gilt Folgendes:

- Der Zugriff auf nicht definierte Umgebungen ist nicht möglich.
- Für jede Umgebung, auf die zugegriffen werden soll, muss ein Umgebungssicherheitsprofil definiert werden.
- Standardmäßig ist der Zugriff auf eine Bibliothek in jeder definierten Umgebung erlaubt.
- Standardmäßig ist der Zugriff auf eine definierte Umgebung für alle Benutzer erlaubt.
- Für einzelne, definierte Umgebungen können Sie den Zugriff auf eine Bibliothek untersagen.
- Für einzelne Benutzer können Sie den Zugriff auf eine definierte Umgebung untersagen.

Um den Umgebungsschutz zu deaktivieren, müssen Sie die Allgemeine Option **Environment Protection** auf N setzen.

Anmerkung: Wenn der Umgebungsschutz aktiv ist, kann die Benutzerkennung DBA zur Anmeldung bei der Bibliothek SYSSEC verwendet werden, auch wenn die Umgebung nicht definiert ist. Dies ermöglicht es, neue Umgebungen zu definieren.

Umgebungsprofile definieren

Die Funktion **Environment Profiles** in den **Administrator Services** dient der Definition von Umgebungsprofilen, d.h. von Sicherheitsprofilen für die einzelnen Systemdatei-Kombinationen.

Um die Funktion aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) die Option **Administrator Services**.

Wenn Sie **berechtigt** sind, auf die Administrator Services zuzugreifen, wird das Menü **Administrator Services Menu 1** angezeigt.

2 Drücken Sie PF8.

3 Wählen Sie im **Administrator Services Menu 2** die Option **Environment Profiles**.

Die **Environment Maintenance**-Auswahlliste für die Umgebungsverwaltung wird aufgerufen.

Environment Maintenance-Auswahlliste

Die **Environment Maintenance**-Auswahlliste zeigt eine Liste aller definierten Umgebungsprofile an.

In der Liste kann geblättert werden, siehe Kapitel *Grundlagen der Benutzung*.

Zu jedem Umgebungsprofil wird entweder seine Systemdateikombination (DBID/Datenbankkennungen und FNR/Dateinummern der Systemdateien FUSER, FDIC, FSEC und FNAT) oder seine Kennung angezeigt. Mit PF4 können Sie zwischen beiden Anzeigen umschalten. Darüber hinaus werden zu jedem Umgebungsprofil der Alias (AL) und der Schutzstatus (P = Protection Status) angezeigt.

Schutzstatus - Protection Status

Möglicher Schutzstatus:

Status	Erläuterung
I	Das Umgebungsprofil ist inaktiv (sowohl **NSC Protection** = N als auch **NSF Protection** = N im Umgebungsprofil).
N	Der Zugriff auf die Umgebung wird von Natural Security ausgewertet (**NSC Protection** = Y im Umgebungsprofil).
S	Der Zugriff auf die Umgebung wird durch den SAF-Server ausgewertet (**NSF Protection** = Y im Umgebungsprofil).

Verfügbare Funktionen

Die folgenden Funktionen sind verfügbar:

Code	Funktion
AD	Add - Neues Umgebungsprofil anlegen. (Sie können diese Funktion auch durch Eingabe von AD in der Kommandozeile aufrufen).
CO	Copy - Umgebungsprofil kopieren.
MO	Modify - Umgebungsprofil ändern.
RE	Rename - Umgebungsprofil umbenennen.
DE	Delete - Umgebungsprofil löschen.
DI	Display - Umgebungsprofil anzeigen.
EP	Environment Protection - Umgebung schützen.

Um eine Funktion für eine Umgebung aufzurufen, müssen Sie die Umgebung in der Spalte **Co** mit dem entsprechenden Funktionscode markieren.

Sie können verschiedene Umgebungen für verschiedene Funktionen gleichzeitig auswählen, d.h. Sie können mehrere Umgebungen auf dem Bildschirm mit einem Funktionscode markieren. Für jede markierte Umgebung werden dann die ausgewählten Funktionen nacheinander ausgeführt.

Bestandteile eines Umgebungsprofils

Wenn Sie ein neues Umgebungsprofil anlegen oder ein bestehendes ändern, wird der Bildschirm **Define Environment Profile** angezeigt. Die Bestandteile, die Sie als Teil eines Umgebungsprofils auf diesem Bildschirm und allen nachfolgenden Bildschirmen/Fenstern definieren können, sind:

Feld	Erläuterung
Environment ID	Umgebungskennung. Geben Sie einen beschreibenden Namen für das Umgebungsprofil ein.
Alias	Sie können einen aus einem Zeichen bestehenden Alias für das Umgebungsprofil angeben. Ein Alias kann von mehreren Umgebungsprofilen gemeinsam verwendet werden. Indem Sie denselben Alias in mehreren Umgebungsprofilen angeben, können Sie Gruppen von Umgebungen bilden. Sie können zum Beispiel folgende Alias verwenden: `D` - für alle Entwicklungsumgebungen, `T` - für alle Testumgebungen, `P` - für alle Produktionsumgebungen. Dies erleichtert die Verwaltung von Umgebungsprofilen, da Sie den Alias als Selektionskriterium in der Auswahlliste **Environment Maintenance** verwenden können, um alle Profile aufzulisten, die den gleichen Alias haben. Bei Natural SAF Security gilt das Folgende: Der Alias wird im externen Sicherheitssystem verwendet, um die Ressourcen zu definieren, die sich auf die Systemdateikombination dieser Umgebung beziehen. Die für einen Alias im externen Sicherheitssystem definierten Regeln gelten für alle Systemdateikombinationen, in deren Umgebungsprofilen dieser Alias angegeben ist.
General Options	Allgemeine Optionen. Sie können angeben, durch welches System die Umgebung geschützt werden soll: ■ **NSC Protection:** Wenn diese Option auf `Y` gesetzt ist, wird die Umgebung für die Validierung durch Natural Security aktiviert, wie in dieser Dokumentation beschrieben. ■ **NSF Protection:** Wenn diese Option auf `Y` gesetzt ist, wird die Umgebung für die Validierung durch den SAF-Server aktiviert, wie in der *Natural SAF Security*-Dokumentation beschrieben. Diese Validierung setzt voraus, dass die Option **Protect Environment** in den **General NSF Options** auf `Y` gesetzt ist (siehe *Natural SAF Security*-Dokumentation). Sind beide Optionen auf `N` gesetzt, ist das Umgebungsprofil nicht aktiv, d.h. es wird so behandelt, als ob es nicht definiert wäre.
System Files	Systemdateien. Sie können die Umgebung definieren, indem Sie die DBID/Datenbankkennungen und FNR/Dateinummern der einzelnen Systemdateien (FUSER, FDIC, FSEC, FNAT) angeben. Diese Kombination von Systemdateien identifiziert die Umgebung und muss eindeutig sein.

Feld	Erläuterung
	Einmal eingegeben, können die Werte in diesen Feldern nicht mehr geändert werden. Wenn Sie auf dem Hauptbildschirm des Umgebungsprofils PF9 drücken, wird ein Fenster mit der Systemdateikombination Ihrer aktuellen Natural-Sitzung angezeigt. In diesem Fenster können Sie mit einem beliebigen Zeichen die Systemdateien markieren, die Teil der Umgebung sein sollen, deren Umgebungsprofil Sie gerade anlegen.

Zusätzliche Optionen (Umgebungen) - Additional Options (Environments)

Wenn Sie entweder das Feld **Additional Options** mit Y markieren oder PF4 drücken, wird ein Fenster angezeigt, in dem Sie die folgenden Optionen auswählen können:

- Maintenance Information - Verwaltungsinformationen
- Security Notes - Sicherheitsvermerke
- Owners - Eigentümer
- Session Options - Sitzungsoptionen

DBID/Datenbankkennungen und FNR/Dateinummern

Die Optionen, für die bereits etwas angegeben oder definiert wurde, sind mit einem Pluszeichen (+) gekennzeichnet.

Sie können ein oder mehrere Elemente aus dem Fenster auswählen, indem Sie sie mit einem beliebigen Zeichen markieren. Für jedes ausgewählte Element wird ein weiteres Fenster angezeigt:

Option	Erläuterung
Maintenance Information (nur Anzeige)	Verwaltungsinformationen. Die folgenden Informationen werden angezeigt: ■ Das Datum und die Uhrzeit, zu der das Sicherheitsprofil angelegt wurde, die Kennung des Administrators, der es angelegt hat, und (falls zutreffend) die Kennungen der Miteigentümer, die für das Anlegen gegengezeichnet haben. ■ Das Datum und die Uhrzeit der letzten Änderung des Sicherheitsprofils, die Kennung des Administrators, der die letzte Änderung vorgenommen hat, und (falls zutreffend) die Kennungen der Miteigentümer, die die Änderung gegengezeichnet haben.
Security Notes	Sicherheitsvermerke. Sie können Anmerkungen zum Sicherheitsprofil eingeben.
Owners	Eigentümer. Sie können bis zu acht Kennungen von Administratoren eingeben. Nur die hier angegebenen Administratoren sind berechtigt, das Sicherheitsprofil der Umgebung zu verwalten oder Benutzern den Zugriff darauf zu erlauben/nicht zu erlauben. Wenn kein Eigentümer angegeben wird, kann jeder Benutzer vom Typ Administrator dies tun.

Option	Erläuterung
	Bei jedem Eigentümer kann optional im Feld hinter der Kennung die Anzahl der Miteigentümer angegeben werden, deren Gegenzeichnung für die Verwaltungs-/Verlinkungserlaubnis erforderlich ist. Erläuterungen zu Eigentümern und Miteigentümern siehe *Gegenzeichnungen*.
Sitzungsoptionen - Session Options	
Session Options TEST Command	Sitzungsoptionen - TEST-Kommando. Mit dieser Option können Sie die Verwendung des Natural-Systemkommandos `TEST` in der Umgebung steuern. Mögliche Werte: ■ `Y` = Das Kommando `TEST` kann ohne Einschränkungen verwendet werden. ■ `P` = Das Kommando `TEST` kann mit folgenden Einschränkungen verwendet werden: Die Debugger-Kommandos `MODIFY VARIABLE`, `ESCAPE ROUTINE`, `ESCAPE BOTTOM` und `STOP` können nicht verwendet werden. ■ `N` = Die Verwendung des Kommandos `TEST` ist komplett untersagt. Diese Option gilt nur für Umgebungen auf Großrechnern.

Zugriff auf Bibliotheken in Umgebungen nicht erlauben/erlauben

Wenn der Umgebungsschutz aktiv ist, ist der Zugriff auf eine Bibliothek standardmäßig in jeder Umgebung erlaubt. Für einzelne Umgebungen können Sie den Zugriff auf eine Bibliothek untersagen.

Wenn der Zugriff auf eine Bibliothek in mindestens einer Umgebung nicht erlaubt ist, wird die Tatsache, dass die Bibliothek „umgebungsgeschützt“ ist, im Sicherheitsprofil der Bibliothek angezeigt.

Es stehen zwei Funktionen zur Verfügung, um den umgebungsspezifischen Zugriff auf Bibliotheken nicht zu erlauben/zu erlauben:

- Eine Environment Maintenance-Funktion, um den Zugriff auf eine oder mehrere Bibliotheken für eine Umgebung nicht zu erlauben/zu erlauben,
- Eine Library Maintenance-Funktion, um den Zugriff auf eine Bibliothek für eine oder mehrere Umgebungen nicht zu erlauben/zu erlauben.

Die beiden Funktionen werden im Folgenden beschrieben.

Einzelne Umgebung für mehrere Bibliotheken schützen

Um den Zugriff auf eine oder mehrere Bibliotheken für eine Umgebung zu erlauben/nicht zu erlauben:

1 Markieren Sie in der **Environment Maintenance**-Auswahlliste die Umgebung, die Sie schützen möchten, mit `EP`.

2 Es wird ein Fenster mit den folgenden Feldern angezeigt:

- **Protect for users/libraries**
  Geben Sie ein `L` ein.
- **Start value**
  Sie können einen Startwert für die Liste der anzuzeigenden Bibliotheken eingeben (wie im Kapitel *Grundlagen der Benutzung* beschrieben)
- **Select only disallowed ones**
  Wenn Sie diese Option wählen, enthält die Liste der anzuzeigenden Bibliotheken nur die Bibliotheken, für die der Zugriff in der Umgebung derzeit nicht erlaubt ist.

3 Der Bildschirm **Disallow/Allow Libraries** wird angezeigt. Er enthält die Liste der Bibliotheken.

In der Liste kann geblättert werden, siehe Kapitel *Grundlagen der Benutzung*.

Markieren Sie in der Liste die Bibliotheken, für die Sie den Zugriff in der Umgebung erlauben/nicht erlauben möchten. In der Spalte **Co** können Sie jede Bibliothek mit einem der folgenden Funktionscodes markieren:

Code	Funktion
`ED`	Disallow - Auf die Bibliothek kann in dieser Umgebung nicht zugegriffen werden.
`EA`	Allow - Auf die Bibliothek kann in dieser Umgebung zugegriffen werden.

Sie können eine oder mehrere Bibliotheken auf dem Bildschirm mit einem Funktionscode markieren.

4 Für jede markierte Bibliothek werden dann die ausgewählten Funktionen nacheinander ausgeführt. Wenn die Verarbeitung abgeschlossen ist, wird in einer Meldung angegeben, welche Zugriffssituation nun für jede Bibliothek gilt.

Mehrere Umgebungen für eine einzelne Bibliothek schützen

Um den Zugriff auf eine Bibliothek für eine oder mehrere Umgebungen zu erlauben/nicht zu erlauben:

1 Markieren Sie in der **Library Maintenance**-Auswahlliste die gewünschte Bibliothek mit dem Funktionscode`EP`.

2 Es wird ein Fenster mit den folgenden Optionen angezeigt:

Option	Erläuterung
Disallow/allow	**D** = Der Zugriff auf die Bibliothek ist zunächst für alle Umgebungen erlaubt, und Sie können ihn für einzelne Umgebungen untersagen. **A** = Der Zugriff auf die Bibliothek ist zunächst für alle Umgebungen nicht erlaubt, Sie können ihn für einzelne Umgebungen erlauben. Wenn Sie diese Funktion später aufrufen und den Wert dieser Option ändern, wird der Status „erlaubt/ nicht erlaubt“ aller Umgebungen für diese Bibliothek geändert.
Sorted by environment ID / Sorted by alias	Sortiert nach Umgebungskennung / Sortiert nach Alias. Indem Sie eines dieser beiden Felder mit einem Zeichen markieren, können Sie wählen, ob die Liste der anzuzeigenden Umgebungen nach Umgebungskennungen oder nach Aliasnamen sortiert werden soll. Letzteres ermöglicht es Ihnen, den Zugriff für alle Umgebungen, die denselben Alias haben, gleichzeitig zu erlauben/nicht zu erlauben (siehe unten).
Start value	Startwert. In eines dieser beiden Felder können Sie einen Startwert (wie im Kapitel *Grundlagen der Benutzung* beschrieben) für die Liste der anzuzeigenden Umgebungen eingeben. Je nachdem, wie die Liste sortiert werden soll, können Sie entweder die Datenbankkennung (DBID) / Dateinummer (FNR) der FNAT-Systemdatei der Umgebungen oder einen aus einem Zeichen bestehenden Alias als Startwert angeben.
Select only disallowed/allowed ones	Wenn Sie diese Option wählen, werden in der Liste der anzuzeigenden Umgebungen - je nach obiger Option **Disallow/allow** - entweder nur die Umgebungen angezeigt, für die der Zugriff nicht erlaubt ist oder die, für die er erlaubt ist.

3 Der Bildschirm **Disallow/Allow Environments** wird angezeigt. Er enthält die Liste der Umgebungen. Für jede Umgebung wird entweder ihre Systemdateikombination (Datenbankkennungen und Dateinummern der Systemdateien FUSER, FDIC, FSEC und FNAT) oder ihre Umgebungskennung angezeigt. Mit `PF4` können Sie zwischen den beiden Anzeigen umschalten. Außerdem werden für jedes Umgebungsprofil der Alias (`AL`) und der Schutzstatus (`P`) angezeigt.

In der Liste kann geblättert werden, siehe Kapitel *Grundlagen der Benutzung*.

In der Liste können Sie die Umgebungen markieren, für die Sie den Zugriff auf die Bibliothek erlauben oder nicht erlauben wollen. In der Spalte **Co** können Sie jede Umgebung mit einem der folgenden Funktionscodes markieren:

Code	Funktion
ED	Disallow - Der Zugriff auf die Bibliothek ist in dieser Umgebung nicht erlaubt.
EA	Allow - Auf die Bibliothek kann in dieser Umgebung zugegriffen werden.

Sie können eine oder mehrere Umgebungen mit einem Funktionscode markieren.

4 Für jede markierte Umgebung werden dann die ausgewählten Funktionen nacheinander ausgeführt. Wenn die Verarbeitung abgeschlossen ist, wird in einer Meldung angegeben, welche Zugriffssituation nun für jede Umgebung gilt.

Wenn die Liste nach Alias sortiert ist, werden keine einzelnen Umgebungen markiert. Stattdessen müssen Sie einen Alias markieren, und die ausgewählte Funktion wird auf alle Umgebungen angewendet, die diesen Alias haben.

Benutzern den Zugang zu Umgebungen nicht erlauben/erlauben

Wenn der Umgebungsschutz aktiviert ist, ist der Zugriff auf eine Umgebung standardmäßig für alle Benutzer erlaubt. Für einzelne Benutzer können Sie den Zugriff auf eine Umgebung untersagen.

Der Zugriff auf eine Umgebung kann nur für Benutzer der Typen Group, Administrator und Person erlaubt/nicht erlaubt werden. Für Benutzer der Typen Administrator und Person kann er entweder direkt oder über eine Gruppe erlaubt/nicht erlaubt werden. Für Benutzer des Typs Member (Mitglied) und Terminal kann er nur für die Gruppe, der sie zugeordnet sind, erlaubt/nicht erlaubt werden.

Wenn der Zugriff auf mindestens eine Umgebung für einen Benutzer nicht erlaubt ist, wird die Sitzungsoption **Environment Protection** im Sicherheitsprofil des Benutzers automatisch auf Y gesetzt.

Es stehen zwei Funktionen zur Verfügung, um den Benutzern den Zugang zu Umgebungen nicht zu erlauben/zu erlauben:

- Eine **Environment Maintenance-**Funktion, um einem oder mehreren Benutzern den Zugang zu einer Umgebung zu untersagen/zu erlauben.
- Eine **User Maintenance**-Funktion, um einem Benutzer den Zugang zu einer oder mehreren Umgebungen zu untersagen/zu erlauben.

Diese beiden Funktionen werden im Folgenden beschrieben.

Einzelne Umgebung für mehrere Benutzer schützen

Um eine Umgebung für einen oder mehrere Benutzer zu schützen:

1 Markieren Sie in der **Environment Maintenance**-Auswahlliste die Umgebung, die Sie schützen möchten, mit `EP`.

2 Es wird ein Fenster mit den folgenden Feldern angezeigt:

- **Protect for users/libraries**
  Geben Sie ein `U` ein.
- **Start value**
  Sie können einen Startwert für die Liste der anzuzeigenden Benutzer eingeben (wie im Kapitel *Grundlagen der Benutzung* beschrieben).
- **Select only disallowed ones**
  Wenn Sie diese Option wählen, enthält die Liste der anzuzeigenden Benutzer nur die Benutzer, denen der Zugriff auf die Umgebung derzeit untersagt ist.

3 Der Bildschirm **Disallow/Allow Users** wird angezeigt. Er enthält die Liste der Benutzer.

Standardmäßig enthält die Liste nur Benutzer des Typs Group. Um zwischen einer Liste mit Gruppen und einer Liste mit allen drei Benutzertypen umzuschalten, können Sie PF5 drücken.

In der Liste kann geblättert werden, siehe Kapitel *Grundlagen der Benutzung*.

In der Liste können Sie die Benutzer markieren, denen Sie den Zugriff auf die Umgebung nicht erlauben oder erlauben möchten. In der Spalte **Co** können Sie jeden Benutzer mit einem der folgenden Funktionscodes markieren:

Code	Funktion
`ED`	Disallow - Der Benutzer kann nicht auf die Umgebung zugreifen.
`EA`	Allow - Der Benutzer darf auf die Umgebung zugreifen.

Sie können auf dem Bildschirm einen oder mehrere Benutzer mit einem Funktionscode markieren.

4 Für jeden markierten Benutzer werden dann die ausgewählten Funktionen nacheinander ausgeführt. Nach Abschluss der Verarbeitung erscheint eine Meldung, die angibt, welche Zugriffssituation nun für den jeweiligen Benutzer gilt.

Mehrere Umgebungen für einen einzelnen Benutzer schützen

Um eine oder mehrere Umgebungen für einen Benutzer zu schützen:

1 Markieren Sie in der **User Maintenance**-Auswahlliste den Benutzer, für den Sie Umgebungen mit dem Funktionscode `EP` schützen möchten.

2 Es wird ein Fenster mit den folgenden Feldern angezeigt:

- **Start value**
  Sie können einen Startwert für die Liste der anzuzeigenden Umgebungen eingeben (wie im Kapitel *Grundlagen der Benutzung* beschrieben). Als Startwert verwenden Sie die Datenbankkennung / Dateinummer der FNAT-Systemdatei der Umgebungen.
- **Select only disallowed environments**
  Nur nicht erlaubte Umgebungen auswählen. Wenn Sie diese Option wählen, enthält die Liste der anzuzeigenden Umgebungen nur die Umgebungen, für die der Benutzer derzeit keine Zugriffsberechtigung hat.

3 Der Bildschirm **Disallow/Allow Environments** wird angezeigt. Er zeigt die Liste der Umgebungen an. Bei jeder Umgebung wird entweder ihre Systemdateikombination (Datenbankkennungen und Dateinummern der Systemdateien FUSER, FDIC, FSEC und FNAT) oder ihre Umgebungskennung angezeigt. Mit `PF4` können Sie zwischen den beiden Anzeigen umschalten. Außerdem werden bei jedem Umgebungsprofil der Alias (`AL`) und der Schutzstatus (`P`) angezeigt.

In der Liste kann geblättert werden, siehe *Grundlagen der Benutzung*.

In der Liste können Sie die Umgebungen markieren, auf die Sie dem Benutzer den Zugriff nicht erlauben/erlauben möchten. In der Spalte **Co** können Sie jede Umgebung mit einem der folgenden Funktionscodes markieren:

Code	Function
`ED`	Disallow - Der Benutzer hat keinen Zugriff auf die Umgebung
`EA`	Allow - Der Benutzer darf auf die Umgebung zugreifen.

Sie können auf dem Bildschirm eine oder mehrere Umgebungen mit einem Funktionscode markieren.

4 Für jede markierte Umgebung werden dann die ausgewählten Funktionen nacheinander ausgeführt. Wenn die Verarbeitung abgeschlossen ist, erscheint eine Meldung, die die aktuelle Zugriffssituation für jede Umgebung angibt.

12 DDMs unter z/OS schützen

- Bevor Sie beginnen: 228
- Bestandteile eines Dateiprofils (File Profile) 229
- Dateiprofile anlegen und verwalten - Creating and Maintaining File Profiles 233

Wie im Kapitel ***Natural Security auf verschiedenen Plattformen*** erläutert, unterscheidet sich der Schutz von Datendefinitionsmodulen (DDMs) mit Natural Security auf Großrechnern von dem auf anderen Plattformen. In diesem Kapitel wird beschrieben, wie Sie die Verwendung von DDMs (Dateien) auf *Großrechnern* kontrollieren können. Die Steuerung von DDMs auf anderen Plattformen wird im Abschnitt ***DDMs unter Linux und Windows schützen*** beschrieben.

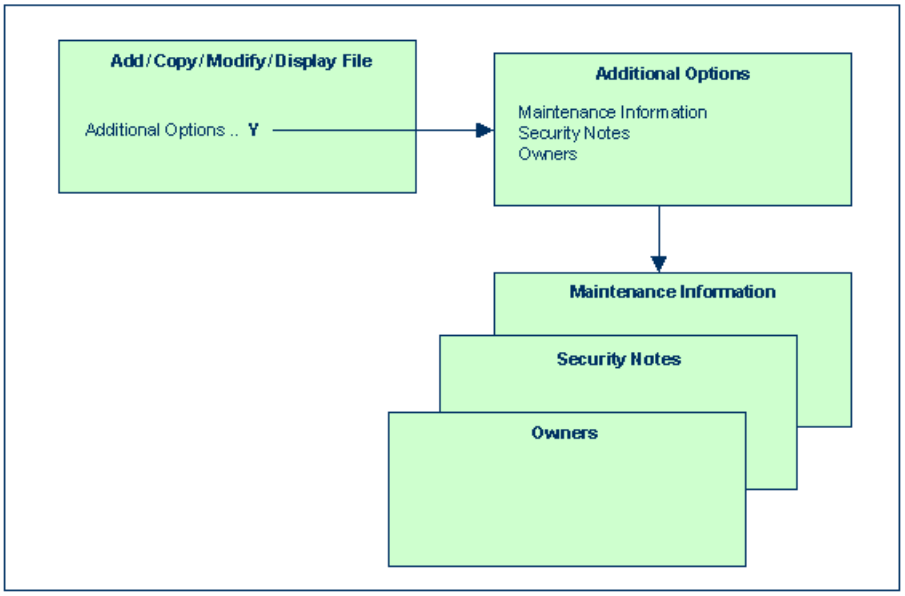
In diesem Kapitel werden die folgenden Themen behandelt:

In Natural Security auf Großrechnern werden DDMs als „Files“ (Dateien) bezeichnet. Um DDMs in Natural Security zu definieren, können Sie die Dateiverwaltungsfunktionen von Natural Security verwenden.

Bevor Sie beginnen:

Ein DDM muss generiert worden sein (in Predict oder mit dem Natural-Dienstprogramm `SYSDDM`), bevor es als Datei in Natural Security definiert werden kann.

Bestandteile eines Dateiprofils (File Profile)



Der folgende Bildschirmtyp ist der Basis-Bildschirm des Dateisicherheitsprofils. Er wird angezeigt, wenn Sie für ein Dateisicherheitsprofil eine der Funktionen Add (anlegen), Copy (kopieren), Modify (ändern), Display (anzeigen) aufrufen.

Bildschirm-Beispiel für die Modify-Funktion:

```
10:25:36                  *** Natural Security ***                 2022-09-09
                                - Modify File -

 File ID .. EMPLOYEES                          Modified .. 2022-09-09 by SAG
 DBID .....    10
 FNR ......    16
 Status ... PUBL  (PUBL, ACCE, PRIV)

 -- DDM Modifiers --
    ________   _
    ________   _
    ________   _
    ________   _
    ________   _
    ________   _
    ________   _
    ________   _

 Additional Options ... N


 Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
       Help  PrevM Exit  AddOp       Flip                              Canc
```

Die einzelnen Bestandteile, die Sie als Teil eines Dateisicherheitsprofils definieren können, werden im Folgenden erläutert.

Feld	Erläuterung
File ID (nur Anzeige)	Dateikennung. Die Kennung, unter der die Datei in Natural Security definiert ist und für die ein DDM in der Natural-Systemdatei existiert. Die Dateikennung, mit der eine Datei in Natural Security definiert ist, muss mit der des DDMs identisch sein. Eine Dateikennung kann bis zu 32 Zeichen lang sein und muss unter allen für Natural Security definierten Dateikennungen eindeutig sein.
DBID / FNR (nur Anzeige)	Die Datenbankkennung und die Dateinummer der Datenbankdatei, auf die das DDM verweist. Diese Werte werden aus dem DDM übernommen und in das Sicherheitsprofil geschrieben.
Status	Sie können den Dateistatus auf einen der folgenden Werte setzen: ■ `PUBL` = Public (nicht geschützt) ■ `ACCE` = Access (schreibgeschützt) ■ `PRIV` = Private (lese- und schreibgeschützt) Wenn Sie ein Dateisicherheitsprofil anlegen, wird der Dateistatus standardmäßig auf `PUBL` gesetzt. Weitere Informationen finden Sie unter *Dateistatus - File Status* unten.
DDM Modifiers	DDM-Änderer. Sie können bis zu acht Benutzerkennungen eingeben. Nur diese Benutzer dürfen dann das DDM in Predict (oder mit dem Natural-Dienstprogramm `SYSDDM`)

Feld	Erläuterung
	verwalten. Wenn Sie keinen DDM-Änderer angeben, dürfen die Eigentümer des Sicherheitsprofils (siehe *Zusätzliche Optionen (DDM/Datei) - Additional Options (DDM/File)* unten) das DDM pflegen. Wenn weder DDM-Änderer noch Eigentümer angegeben werden, ist die Verwaltung des DDMs nicht eingeschränkt. Neben der Benutzerkennung jedes DDM-Änderers können Sie optional eine Zahl von 1 bis 3 angeben. Diese Zahl bestimmt, wie viele der anderen angegebenen DDM-Änderer für die Verwaltungserlaubnis gegenzeichnen müssen (die Logik der Gegenzeichnung, die für die DDM-Verwaltungserlaubnis gilt, ist analog zu der von Eigentümern und Miteigentümern, wie im Abschnitt *Gegenzeichnungen - Countersignatures* beschrieben).

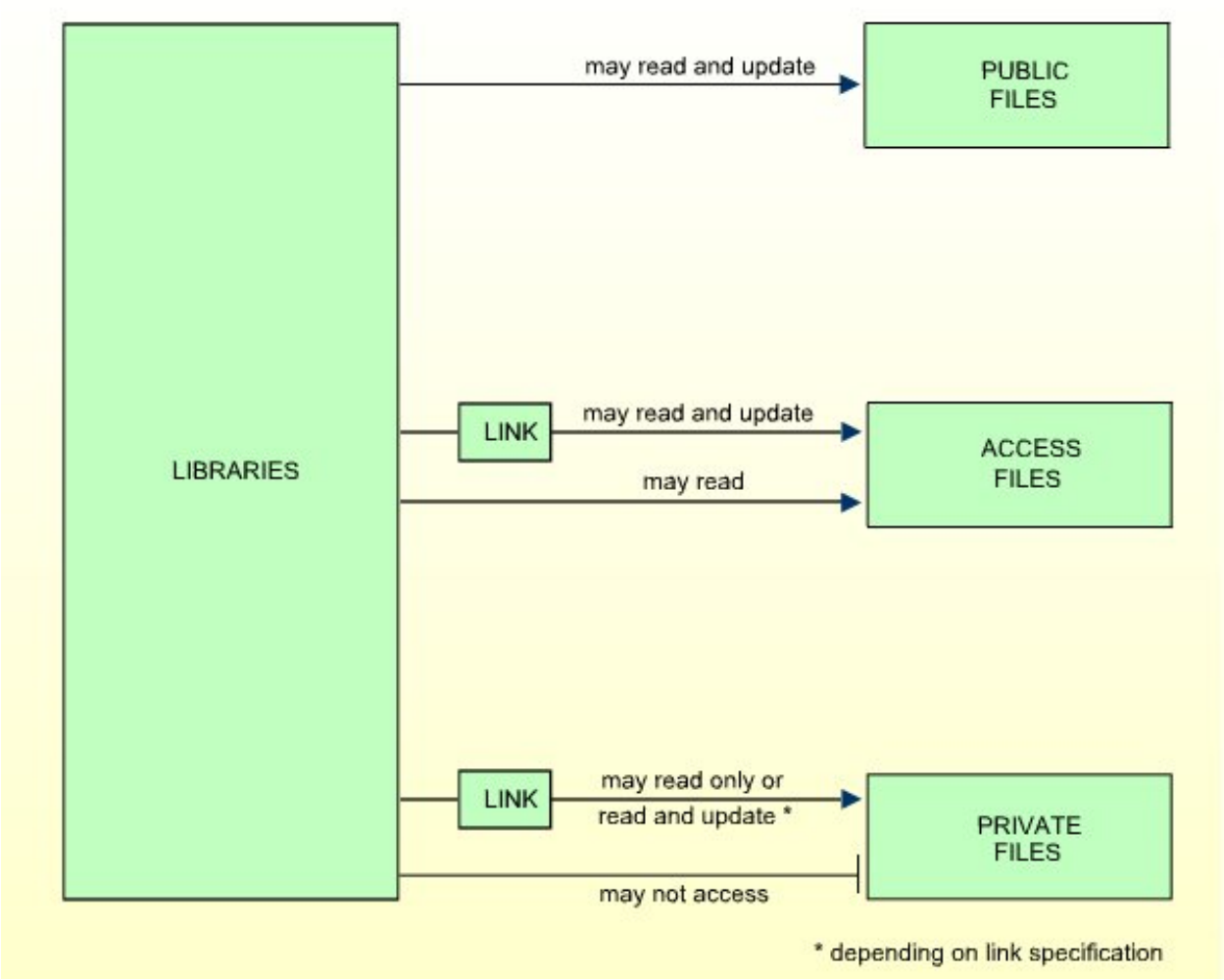
Dateistatus - File Status

Als Dateistatus einer Datei kann einer der folgenden Werte angegeben werden:

Wert	Bedeutung
PUBL	PUBLIC: Die Datei ist nicht geschützt. Sie kann von jeder Bibliothek gelesen (Read) und geändert (Update) werden.
ACCE	ACCESS: Die Datei ist schreibgeschützt. Sie kann von jeder Bibliothek gelesen werden. Sie kann jedoch nur von Bibliotheken geändert werden, die mit der Datei verlinkt worden sind.
PRIV	PRIVATE: Die Datei ist geschützt. Auf sie kann nur von Bibliotheken zugegriffen werden, die mit ihr verlinkt sind. Eine Verlinkung mit einer PRIVATE-Datei kann als „read“ (d.h. nur lesen) oder „update“ (schreiben, was lesen impliziert) angegeben werden.

Die Prüfung, ob ein Programm eine Datei verwenden darf, erfolgt beim *Kompilieren* des Programms.

Die folgende Grafik veranschaulicht die möglichen Beziehungen zwischen Bibliotheken und Dateien in Abhängigkeit vom Dateityp:



Um einer Bibliothek den Zugriff auf eine Datei mit dem Status PRIVATE oder ACCESS zu ermöglichen, muss ein Link zwischen der Bibliothek und der Datei hergestellt werden. Informationen über die Verlinkung von Bibliotheken mit Dateien finden Sie unter *Bibliotheken mit Dateien verlinken - Linking Libraries to Files* weiter unten.

Zusätzliche Optionen eines Dateiprofils (File Profile)

Wenn Sie das Feld **Additional Options** auf dem Basis-Bildschirm des Sicherheitsprofils mit `Y` markieren, wird ein Fenster angezeigt, in dem Sie die folgenden Optionen auswählen können:

- Maintenance Information - Verwaltungsinformationen
- Security Notes - Sicherheitsvermerke
- Owners - Eigentümer

Die Optionen, bei denen bereits etwas angegeben oder definiert wurde, sind mit einem Pluszeichen (+) gekennzeichnet.

Sie können ein oder mehrere Elemente aus dem Fenster auswählen, indem Sie sie mit einem beliebigen Zeichen markieren. Für jedes ausgewählte Element wird ein weiteres Fenster angezeigt:

usätzliche Optionen (DDM/Datei) - Additional Options (DDM/File)	
Maintenance Information (nur Anzeige)	Verwaltungsinformationen. Die folgenden Informationen werden angezeigt: ■ Das Datum und die Uhrzeit, zu der das Sicherheitsprofil erstellt wurde, die Kennung des Administrators, der es erstellt hat, und (falls zutreffend) die Kennungen der Miteigentümer, die für die Erstellung gegengezeichnet haben. ■ Das Datum und die Uhrzeit der letzten Änderung des Sicherheitsprofils, die Kennung des Administrators, der die letzte Änderung vorgenommen hat, und (falls zutreffend) die Kennungen der Miteigentümer, die die Änderung gegengezeichnet haben.
Security Notes	Sicherheitsvermerke. Hier können Sie Anmerkungen zum Sicherheitsprofil eingeben.
Owners	Eigentümer. Sie können bis zu acht Kennungen von Administratoren eingeben. Nur die hier angegebenen Administratoren sind berechtigt, dieses Dateisicherheitsprofil zu verwalten oder Bibliotheken damit zu verlinken. Wenn kein Eigentümer angegeben wird, kann jeder Benutzer vom Typ Administrator das Sicherheitsprofil verwalten und verlinken. Zu jedem Eigentümer kann optional im Feld hinter der Kennung die Anzahl der Miteigentümer angegeben werden, deren Gegenzeichnung für die Verwaltungs-/Verlinkungserlaubnis erforderlich ist. Eine Erläuterung der Eigentümer und Miteigentümer finden Sie im Kapitel *Gegenzeichnungen - Countersignatures* .

Dateiprofile anlegen und verwalten - Creating and Maintaining File Profiles

Dieser Abschnitt beschreibt die Funktionen zum Anlegen und Verwalten von Dateiprofilen. Er umfasst die folgenden Themen:

- Dateiverwaltung aufrufen
- Datei oder DDM zur Bearbeitung auswählen
- Datei anlegen - Add File
- Datei kopieren - Copy File
- Datei ändern - Modify File
- Datei löschen - Delete File
- Datei anzeigen - Display File

- Bibliotheken mit Dateien verlinken - Linking Libraries To Files

Dateiverwaltung aufrufen

Um die Dateiverwaltung aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) die Option **Maintenance**.

Es wird ein Fenster angezeigt.

2 Markieren Sie im Fenster den Objekttyp **File** mit einem Zeichen oder mit dem Cursor.

Es wird die **File Maintenance**-Auswahlliste angezeigt.

3 Von dieser Auswahlliste aus können Sie alle Funktionen zur Dateiverwaltung wie unten beschrieben aufrufen.

Datei oder DDM zur Bearbeitung auswählen

Wenn Sie die Option **File Maintenance** aufrufen, wird eine Liste aller Dateien angezeigt, die in Natural Security definiert wurden.

Wenn Sie nicht alle vorhandenen Dateien, sondern nur bestimmte Dateien aufgelistet haben möchten, können Sie die Optionen **Start Value** und **Type/Status** verwenden, siehe *Grundlagen der Benutzung*.

Wählen Sie im Hauptmenü (**Main Menu**) die Option **Maintenance**.

Es wird ein Fenster angezeigt.

Markieren Sie im Fenster den Objekttyp **File** mit einem Zeichen oder mit dem Cursor (und geben Sie, falls gewünscht, einen Startwert und/oder einen Dateistatus ein).

Die **File Maintenance**-Auswahlliste wird angezeigt:

```
12:50:20                  *** Natural Security ***                2022-09-09
                              - File Maintenance -

 Co File ID                              Status Message
 __ _____________________________________ ______ ____________________
 __ ANGLOFILE                            PUBL
 __ AUTOMOBILES                          PUBL
 __ CLIENTES                             PUBL
 __ DELINCUENTES                         PUBL
 __ EMPLEADOS                            PUBL
 __ FAHRZEUGE                            PRIV
 __ FINANCE                              PUBL
 __ IMPUESTOS                            PUBL
 __ INVOICE                              PUBL
 __ MITARBEITER                          PUBL
 __ NAILFILE                             PUBL
 __ NEWFILE                              PUBL
 __ OLDFILE                              PUBL
 __ OTRASCOSAS                           PUBL
 __ PRO-FILE                             PUBL

 Command ===>
 Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
       Help        Exit              Flip  -     +                       Canc
```

Zu jeder Datei werden die Dateikennung und der Dateistatus angezeigt.

In der Liste kann geblättert werden, siehe *Grundlagen der Benutzung*.

Status als Auswahlkriterium benutzen

Wenn Sie nur DDMs mit einem bestimmten Status auflisten möchten, können Sie im Feld **Status** oberhalb der Liste eines der folgenden Auswahlkriterien angeben:

Status	Auswahl
PUBL	Alle DDMs mit dem Status PUBLIC.
ACCE	Alle DDMs mit dem Status ACCESS.
PRIV	Alle DDMs mit dem Status PRIVATE.
DEFI	Definiert, d. h. alle DDMs mit dem Status PRIV, ACCE und PUBL (*).
UNDF	Nicht definiert, d. h. alle DDMs, deren Status nicht PRIV, ACCE oder PUBL ist (*).
DDM	Alle definierten und nicht definierten DDMs (*).
NDDM	DDM-Sicherheitsprofile, für die keine entsprechenden DDMs existieren (*).

* Dies ist kein tatsächlicher DDM-Status, sondern dient nur zu Auswahlzwecken.

Der Standardstatus für die Auswahl ist DDM, d.h. alle DDMs werden aufgelistet.

Funktion auswählen

Die folgenden Dateiverwaltungsfunktionen stehen zur Verfügung (mögliche Codeabkürzungen sind unterstrichen):

Code	Funktion
AD	**Add file** - Datei anlegen
CO	**Copy file** - Datei kopieren
MO	**Modify file** - Datei ändern
DE	**Delete file** - Datei löschen
DI	**Display file** - Datei anzeigen
LL	**Link libraries to file** - Bibliotheken mit Datei verlinken

Um eine bestimmte Funktion für eine Datei aufzurufen, müssen Sie die Datei mit dem entsprechenden Funktionscode in der Spalte **Co** markieren.

Sie können mehrere Dateien gleichzeitig für verschiedene Funktionen auswählen, d.h. Sie können auf dem Bildschirm mehrere Dateien mit einem Funktionscode markieren. Für jede markierte Datei wird der entsprechende Verarbeitungsbildschirm angezeigt. Sie können dann für eine Datei nach der anderen die ausgewählten Funktionen ausführen.

Datei anlegen - Add File

Mit dieser Funktion können Sie DDMs in Natural Security definieren, d.h. neue Dateisicherheitsprofile erstellen.

Dazu:

1 Wählen Sie im Hauptmenü (**Main Menu**) die Option **Maintenance**.

Es wird ein Fenster angezeigt.

2 Markieren Sie in dem Fenster den Objekttyp **File** mit einem Zeichen und geben Sie `UNDF` in das Feld **Type/Status** ein (und geben Sie, falls gewünscht, einen Startwert ein).

Die **File Maintenance**-Auswahlliste wird angezeigt. Es werden alle Dateien mit dem Dateistatus „Undefined“ aufgelistet (d.h. alle DDMs, die zwar generiert, aber noch nicht in Natural Security definiert wurden).

In der Liste kann geblättert werden, siehe *Grundlagen der Benutzung*.

3 Markieren Sie in der **File Maintenance**-Auswahlliste das DDM, für das Sie ein Dateisicherheitsprofil anlegen möchten, mit dem Funktionscode `AD`.

Der Bildschirm **Add File** wird angezeigt.

4 Die einzelnen Bestandteile, die Sie auf diesem Bild definieren können, und alle zusätzlichen Fenster, die Teil eines Dateisicherheitsprofils sein können, sind unter *Bestandteile eines Dateiprofils* beschrieben.

Wenn Sie eine Datei anlegen, werden die in Ihrem eigenen Benutzersicherheitsprofil angegebenen Eigentümer automatisch in das Dateisicherheitsprofil kopiert.

Datei kopieren - Copy File

Mit dieser Funktion können Sie eine neue Datei in Natural Security definieren, indem Sie ein Sicherheitsprofil anlegen, das mit einem bereits vorhandenen Dateisicherheitsprofil identisch ist.

- Was wird kopiert?
- Wie wird kopiert?
- Kopieren mit Links

Was wird kopiert?

Alle Bestandteile des bestehenden Dateisicherheitsprofil werden in das neue Dateisicherheitsprofil kopiert - *außer*:

- Dateinummer und Datenbankkennung (diese werden aus dem DDM übernommen).
- Eigentümer (diese werden aus Ihrem eigenen Benutzersicherheitsprofil in das neue Dateisicherheitsprofil kopiert).

Ob Links kopiert werden, hängt davon ab, ob Sie sich für das Kopieren mit oder ohne Links entscheiden (siehe unten).

Wie wird kopiert?

1. Markieren Sie in der **File Maintenance**-Auswahlliste die Datei, deren Sicherheitsprofil Sie duplizieren möchten, mit dem Funktionscode `CO`.
2. Es wird ein Fenster angezeigt, in dem Sie folgende Angaben machen können:

Feld	Erläuterung
To file	Nach Datei: Geben Sie die Kennung der „neuen“ Datei ein.
With links	Mit Links: Geben Sie `Y` oder `N` ein. Mit dieser Option können Sie zusätzlich zum Dateiprofil auch dessen Verlinkungen kopieren; siehe *Kopieren mit Links* unten.

3. Der Bildschirm **Copy File** wird angezeigt. Er zeigt das neue Dateisicherheitsprofil an.

   Die Bestandteile, die Sie definieren können, sind unter *Bestandteile eines Dateiprofils* beschrieben.

Kopieren mit Links

Wenn Sie **With Links = N** wählen, werden alle Verlinkungen von Bibliotheken mit der bestehenden Datei nicht bei der neuen Datei übernommen.

Wenn Sie **With Links = Y** wählen, werden alle Verlinkungen von Bibliotheken mit der bestehenden Datei für die neue Datei kopiert, und Sie haben die Möglichkeit, die Verlinkungen, die Sie nicht auf die neue Datei anwenden möchten, zu entfernen. Die Vorgehensweise ist wie folgt:

1. Wenn Sie Änderungen am Dateisicherheitsprofil der kopierten Datei vorgenommen haben und den Bildschirm **Copy File** durch Drücken von PF3 verlassen, wird eine Liste der Bibliotheken angezeigt: Sie enthält alle Bibliotheken, die mit der bestehenden Datei verlinkt sind.
2. In der Liste können Sie einzelne Bibliotheken mit CL (Cancel) markieren, um alle Verlinkungen zu entfernen, die Sie nicht für die neue Datei übernehmen möchten. Alle Bibliotheken, die Sie nicht markieren, werden automatisch mit der neuen Datei auf dieselbe Weise verlinkt - Lese- oder Update-Link - wie bei der bestehenden Datei.

Datei ändern - Modify File

Mit der Funktion **Modify File** können Sie ein bestehendes Dateisicherheitsprofil ändern.

Dazu:

1 Markieren Sie in der **File Maintenance**-Auswahlliste die Datei, deren Sicherheitsprofil Sie ändern möchten, mit dem Funktionscode MO.

2 Es wird das Dateisicherheitsprofil der markierten Datei angezeigt.

Die Bestandteile, die Sie definieren oder ändern können, sind unter *Bestandteile eines Dateiprofils* beschrieben.

Datei löschen - Delete File

Mit der Funktion **Delete File** können Sie ein bestehendes Dateisicherheitsprofil löschen.

Dazu:

1 Markieren Sie in der **File Maintenance**-Auswahlliste die Datei, deren Sicherheitsprofil Sie löschen möchten, mit dem Funktionscode DE.

2 Das Fenster **Delete File** wird angezeigt.

- Wenn Sie sich gegen das Löschen des Dateisicherheitsprofils entscheiden, können Sie das Fenster durch Drücken von ENTER verlassen, ohne etwas eingegeben zu haben.
- Um das Dateisicherheitsprofil zu löschen, müssen Sie die Kennung der Datei in das Fenster eingeben, um den Löschvorgang zu bestätigen.

Wenn Sie eine Datei löschen, werden auch alle bestehenden Links zu dieser Datei gelöscht.

Wenn Sie ein Dateisicherheitsprofil löschen, wird das DDM selbst nicht gelöscht. Die Dateikennung verbleibt in der **File Maintenance**-Auswahlliste, wobei der Dateistatus auf „Undefined“ gesetzt wird.

Wenn ein DDM in `SYSDDM`, in `SYSMAIN` oder in `SYSDIC` (Predict) gelöscht wird (mittels Uncatalog, Delete bzw. Scratch), wird das entsprechende Dateiprofil für Natural Security automatisch gelöscht.

Wenn Sie mehr als eine Datei mit `DE` markieren, wird ein Fenster angezeigt, in dem Sie gefragt werden, ob Sie die Löschung jedes einzelnen Dateisicherheitsprofils durch Eingabe der Dateikennung bestätigen möchten, oder ob alle zum Löschen ausgewählten Dateien ohne diese Einzelbestätigung gelöscht werden sollen. Achten Sie darauf, dass Sie nicht versehentlich eine Datei löschen.

Datei anzeigen - Display File

Mit der Funktion **Display File** können Sie ein bestehendes Dateisicherheitsprofil anzeigen.

Dazu:

1. Markieren Sie in der **File Maintenance**-Auswahlliste die Datei, deren Sicherheitsprofil Sie anzeigen möchten, mit dem Funktionscode `DI`.
2. Das Sicherheitsprofil der ausgewählten Datei wird angezeigt. Seine Bestandteile sind unter *Bestandteile eines Dateiprofils* beschrieben.

Bibliotheken mit Dateien verlinken - Linking Libraries To Files

Um für eine Bibliothek den Zugriff auf eine Datei zu ermöglichen, muss ein *Link* zwischen der Bibliothek und der Datei hergestellt werden.

Es gibt zwei Funktionen, um diese Links herzustellen und zu verwalten:

- Eine **Library Maintenance**-Funktion, um *eine Bibliothek* mit *einer oder mehreren Dateien* zu verlinken,
- Eine **File Maintenance**-Funktion, um *eine oder mehrere Bibliotheken* mit *einer Datei* zu verlinken.

Beide Funktionen werden im Folgenden beschrieben. Die möglichen Verlinkungsarten sind am Ende dieses Kapitels zusammengefasst.

Informationen über Links zu Private-Mode-Bibliotheken finden Sie unter im *Private-Mode-Bibliotheken* im Kapitel *Natural-Entwicklungsumgebung in Eclipse schützen* .

Einzelne Bibliothek mit Dateien verknüpfen

Die Bibliotheksverwaltungsfunktion **Link Library to Files** zeigt eine Liste von Dateien mit dem Dateistatus ACCESS und PRIVATE an. In der Liste können Sie die Dateien markieren, mit denen Sie die gegebene Bibliothek verlinken möchten.

Dazu:

1 Markieren Sie in der **Library Maintenance**-Auswahlliste die zu verlinkende Bibliothek mit dem Funktionscode `LF`.

2 Es erscheint ein Auswahlfenster mit folgenden Optionen:

- **Start value**
  Sie können einen Startwert für die Liste der anzuzeigenden Dateien eingeben (wie im Kapitel *Grundlagen der Benutzung* beschrieben).
- **Selection criterion**
  `N` = None: alle Dateien werden aufgelistet.

  `L` = Linked: nur Dateien, mit denen die Bibliothek bereits verlinkt ist, werden aufgelistet.

  `U` = Unlinked: nur Dateien, mit denen die Bibliothek noch nicht verlinkt ist, werden aufgelistet.

3 Anschließend wird die Auswahlliste **Link Library To Files** angezeigt. Sie enthält die Liste der Dateien.

In der Liste kann geblättert werden, siehe *Grundlagen der Benutzung*.

In der Spalte **Co** können Sie jede Datei mit einem der folgenden Funktionscodes markieren (mögliche Code-Abkürzungen sind unterstrichen):

Code	Funktion
`RE`	Read-Link - Die so verlinkte Bibliothek darf die Datei nur lesen, aber nicht ändern.
`UP`	Update-Link - Die so verknüpfte Bibliothek darf die Datei lesen und ändern.
`CL`	Cancel Link - Eine bestehende Verlinkung wird aufgehoben.
`DI`	Display File - Das Sicherheitsprofil der Datei wird angezeigt.

Sie können eine oder mehrere Dateien mit einem Funktionscode markieren.

4 Für jede markierte Datei werden die ausgewählten Funktionen nacheinander ausgeführt. Wenn die Verarbeitung abgeschlossen ist, wird eine Meldung angezeigt, in der die jetzt gültige Verlinkungssituation zwischen der Bibliothek und jeder Datei angegeben wird.

Mehrere Bibliotheken mit einer Datei verlinken

Die Dateiverwaltungsfunktion **Link Libraries to File** zeigt eine Liste der Bibliotheken an, die in Natural Security definiert wurden. Markieren Sie dort die Bibliotheken, die mit der gegebenen Datei verlinkt werden sollen.

Dazu:

1 Markieren Sie in der **File Maintenance**-Auswahlliste die mit der Bibliothek zu verlinkende Datei mit dem Funktionscode `LL`.

2 Es wird ein Fenster mit den folgenden Optionen angezeigt:

- **Start value**
  Sie können einen Startwert (wie im Kapitel *Grundlagen der Benutzung* beschrieben) für die Liste der anzuzeigenden Bibliotheken eingeben.
- **Libraries/Private libraries**
  `L` = Die Liste enthält entweder alle Bibliotheken einschließlich privater Bibliotheken (wenn private Bibliotheken im Public-Mode verwendet werden) oder alle Bibliotheken außer privaten Bibliotheken (wenn private Bibliotheken im Private-Mode verwendet werden)

  `U` = Die Liste enthält nur die privaten Bibliotheken der Benutzer.
- **Selection criterion**
  `N` = None: Alle Bibliotheken werden aufgelistet.

  `L` = Linked: Nur Bibliotheken, die bereits mit der Datei verlinkt sind, werden aufgelistet.

  `U` = Unlinked: nur Bibliotheken, die noch nicht mit der Datei verlinkt sind, werden aufgelistet.

3 Anschließend wird die Auswahlliste **Link Libraries To File** angezeigt. Sie enthält die Liste der Bibliotheken.

In der Liste kann geblättert werden, siehe *Grundlagen der Benutzung*.

In der Spalte **Co** können Sie jede Bibliothek mit einem der folgenden Funktionscodes markieren (mögliche Code-Abkürzungen sind unterstrichen):

Code	Funktion
`RE`	Read-Link - Die so verlinkte Bibliothek darf die Datei nur lesen, jedoch nicht ändern.
`UP`	Update-Link - Die so verlinkte Bibliothek darf die Datei lesen und ändern.
`CL`	Cancel Link- Eine bestehende Verlinkung wird aufgehoben.
`DI`	Display Library - Das Sicherheitsprofil der Bibliothek wird angezeigt.

Sie können eine oder mehrere Bibliotheken mit einem Funktionscode markieren.

4 Für jede markierte Bibliothek werden die ausgewählten Funktionen nacheinander ausgeführt. Nach Beendigung der Verarbeitung wird eine Meldung angezeigt, die über die nun bestehende Verlinkungssituation zwischen der Datei und jeder Bibliothek informiert.

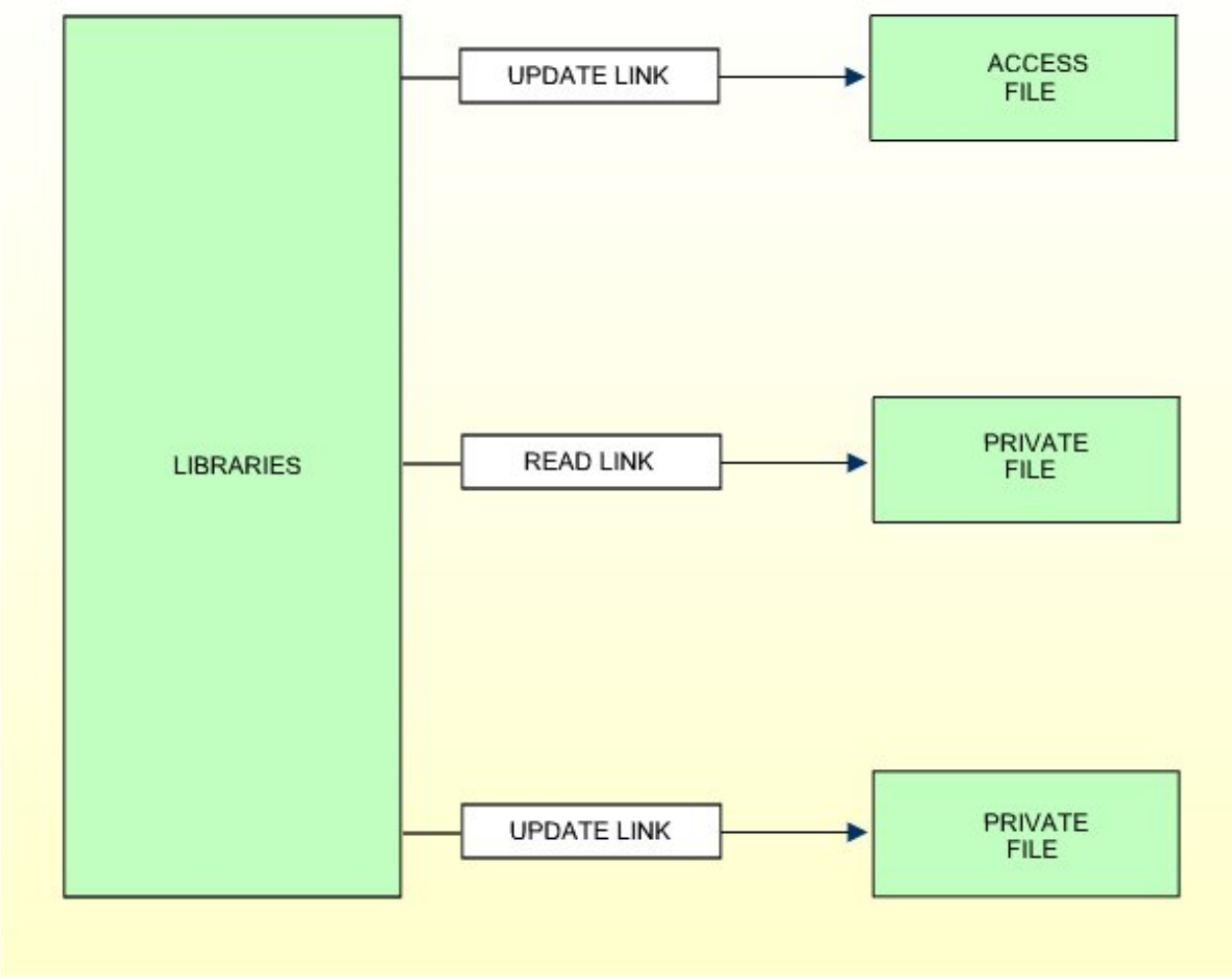
Mögliche Verlinkungsarten

Ein Link kann nur zu einer PRIVATE- oder ACCESS-Datei hergestellt werden. Zum Lesen oder Ändern einer PUBLIC-Datei ist keine Verlinkung erforderlich.

Ein Link zu einer PRIVATE-Datei kann als Read-Link (`RE`) oder Update-Link (`UP`) angegeben werden.

Ein Link zu einer ACCESS-Datei kann nur als Update-Link (`UP`) angegeben werden. Zum Lesen einer ACCESS-Datei ist kein Link erforderlich.

Die folgende Abbildung zeigt alle möglichen Verlinkungsarten:



13 DDMs unter Linux und Windows schützen

- Zentrale Systemdatei für DDMs angeben (Profilparameter FDDM) 244
- Status eines DDM 244
- DDM-Sicherheitsprofile 249
- DDM-Sicherheitsprofile anlegen und verwalten 252
- DDM-Sicherheitsprofil anlegen - Add DDM Profile 254
- DDM-Sicherheitsprofil kopieren - Copy DDM Profile 255
- DDM-Sicherheitsprofil ändern - Modify DDM Profile 256
- DDM-Sicherheitsprofil löschen - Delete DDM Profile 256
- DDM-Sicherheitsprofil anzeigen - Display DDM Profile 257
- Profil kopieren/Verlinken mit allen Special-Links - Copy Profile/Link to All Special Links 258
- Bibliothek mit einem geschützten DDM verlinken 258

Wie im Kapitel *Natural Security auf verschiedenen Plattformen* erläutert, unterscheidet sich der Schutz von Datendefinitionsmodulen (DDMs) mit Natural Security auf dem Mainframe unter z/OS von dem auf anderen Plattformen. In diesem Kapitel wird beschrieben, wie Sie die Verwendung von DDMs unter *Linux* und *Windows* steuern können. Die Steuerung von DDMs auf Großrechnern wird im Kapitel *DDMs auf Großrechnern schützen* beschrieben.

In diesem Kapitel werden die folgenden Themen behandelt:

Zentrale Systemdatei für DDMs angeben (Profilparameter FDDM)

Mit dem Natural-Profilparameter `FDDM` können Sie eine Systemdatei als zentralen Speicherort angeben, an dem DDMs (außerhalb von Bibliotheken) gespeichert werden sollen. Wenn der Parameter `FDDM` gesetzt ist, können DDM-Sicherheitsprofile nur für DDMs erstellt und verwaltet werden, die in der Bibliothek `SYSTEM` in dieser Systemdatei enthalten sind. Vorhandene Sicherheitsprofile/Einstellungen/Verlinkungen für DDMs, die in anderen Bibliotheken enthalten sind, gehen nicht verloren, sondern sind in Natural Security sichtbar und haben keine Wirkung.

Wenn mit dem Profilparameter `FDDM` eine zentrale Systemdatei für DDMs angegeben wird, erfolgt der Schutz von Linux- und Windows-DDMs und die Verwaltung ihrer Sicherheitsprofile auf die gleiche Weise wie mit den im Kapitel *DDMs unter z/OS schützen* beschriebenen Funktionen zur Dateiverwaltung für Großrechner-DDMs.

Wenn mit dem Profilparameter `FDDM` keine Systemdatei für DDMs angegeben wird, erfolgt der Schutz und die Verwaltung von DDMs wie im Folgenden beschrieben.

Status eines DDM

Bevor ein DDM unter Natural Security verwendet werden kann, muss sein Status in Natural Security definiert werden. Dieser Status bestimmt, ob das DDM verwendet werden kann, d.h. innerhalb eines Programms in einem Statement für den Datenbankzugriff (z.B. `READ`, `FIND`, `HISTOGRAM`, `STORE`, `UPDATE`, `DELETE`) referenziert werden kann.



Anmerkung: Programm bedeutet in diesem Zusammenhang jede Art von Natural-Programmierobjekt, das Datenbankzugriffs-Statements enthalten kann, d.h. Programme, Subprogramme, Subroutinen usw.

Ein DDM, dessen Status nicht definiert ist, kann nicht referenziert werden.

Bei jedem DDM, das verwendet werden soll, müssen in Natural Security zwei Statusklassifizierungen vorgenommen werden: ein **interner Status** und ein **externer Status**.

In diesem Abschnitt werden folgende Themen behandelt:

- Interner Status
- Externer Status
- Initialstatus eines DDM

Interner Status

Der interne Status steuert die Verwendung des DDMs *innerhalb* der Bibliothek, in der er enthalten ist.

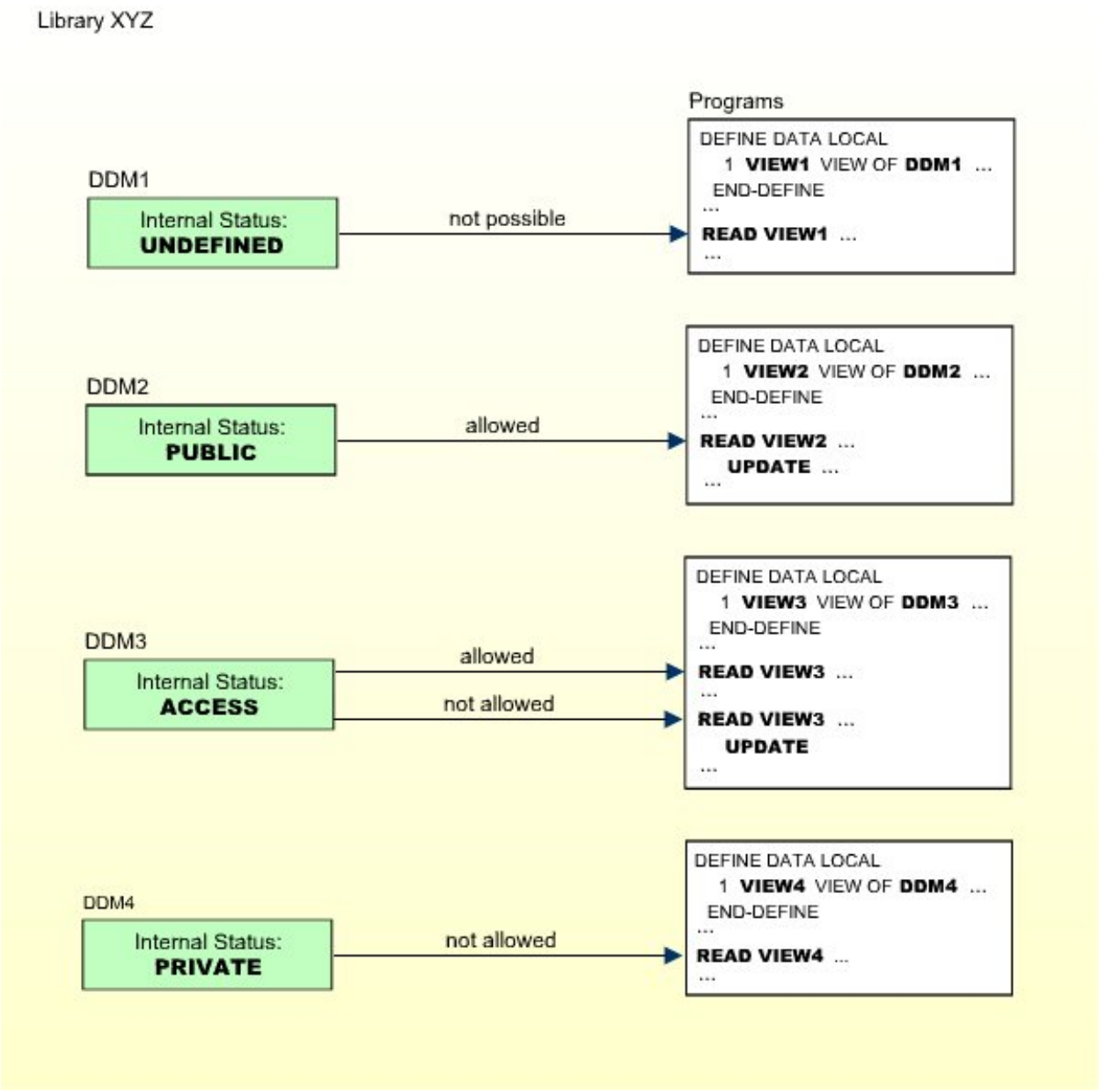
Der interne Status eines DDMs kann einer der folgenden sein:

Status	Bedeutung
PUBLIC	Das DDM kann von allen Programmen innerhalb der Bibliothek gelesen und geändert werden (Read und Update möglich).
ACCESS	Das DDM kann von allen Programmen innerhalb der Bibliothek gelesen, aber nicht geändert werden.
PRIVATE	Das DDM kann von keinem Programm innerhalb der Bibliothek verwendet werden.

Der interne Status gilt nur innerhalb der Bibliothek, in der das DDM enthalten ist.

Die Prüfung, ob ein Programm ein DDM verwenden darf, erfolgt beim *Kompilieren* des Programms.

Die folgende Abbildung zeigt, wie sich der interne Status auf die Verwendung eines DDMs innerhalb einer Bibliothek auswirkt:



Externer Status

Der externe Status steuert die Verwendung des DDM *durch andere Bibliotheken*.

Dies setzt voraus, dass die Bibliothek, die das DDM enthält, von diesen anderen Bibliotheken als Steplib verwendet wird. Bibliotheken, für die die Bibliothek, die das DDM enthält, keine Steplib ist, können das DDM ohnehin nicht verwenden.

Der externe Status eines DDMs kann einer der Folgenden sein:

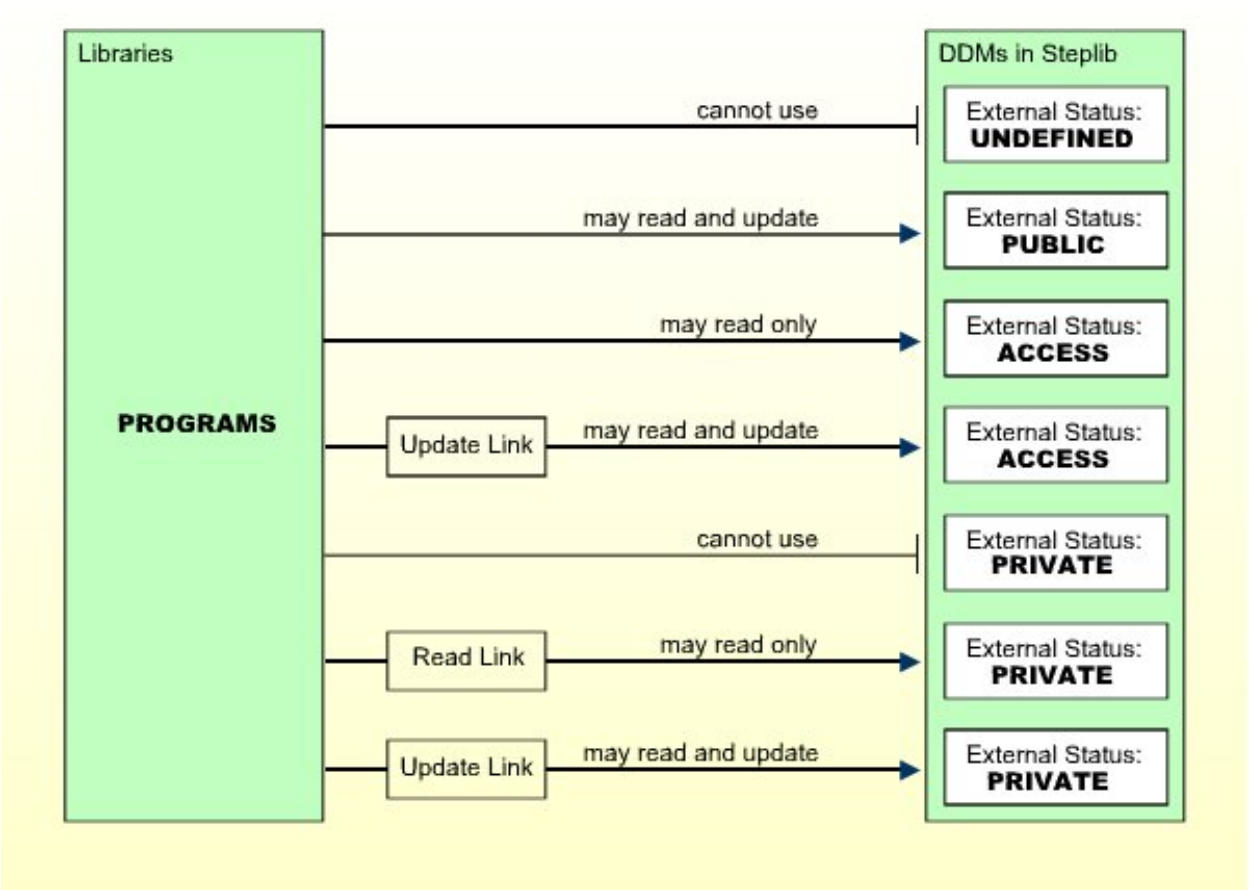
Status	Bedeutung
PUBLIC	Das DDM ist *nicht* geschützt. Es kann von jeder Bibliothek verwendet, d. h. gelesen und geändert werden (Read und Update möglich).
ACCESS	Das DDM ist geschützt, was das Ändern (Update) betrifft. Es kann von jeder Bibliothek gelesen werden. Er kann jedoch nur von Bibliotheken geändert werden, die mit ihm *verlinkt* worden sind.
PRIVATE	Das DDM ist geschützt. Er kann nur von Bibliotheken verwendet werden, die mit ihm verlinkt wurden. Dieser *Link* kann als Read-Link (d.h. nur lesen) oder Update-Link (d.h. Ändern, was lesen impliziert) definiert werden.

Der externe Status eines DDM ist nur dann relevant, wenn die Bibliothek, die das DDM enthält, von anderen Bibliotheken als Steplib verwendet wird.

Damit eine Bibliothek ein geschütztes DDM in einer der Steplibs der Bibliothek verwenden kann, müssen Sie einen *Link* zwischen der Bibliothek und dem DDM definieren.

Ein Link zu einem DDM, dessen externer Status PRIVATE ist, kann als Read-Link oder Update-Link definiert werden. Eine Verlinkung mit einem DDM, dessen externer Status ACCESS ist, kann nur als Update-Link definiert werden.

Die möglichen Beziehungen zwischen Bibliotheken und DDMs in einer Steplib sind in der folgenden Abbildung dargestellt:



Anmerkung: Ein Link kann nur zu einem DDM hergestellt werden, dessen externer Status ACCESS oder PRIVATE ist, da zum Lesen (Read) oder Ändern (Update) eines DDM, dessen externer Status PUBLIC ist, kein Link erforderlich ist.

Die Prüfung, ob ein Programm ein DDM in einer Steplib verwenden darf, erfolgt beim *Kompilieren* des Programms.

Wie Sie eine Bibliothek mit einem DDM verlinken können, erfahren Sie weiter unten unter *Bibliothek mit einem geschützten DDM verlinken*.

Initialstatus eines DDM

Der initiale interne und externe Status eines neu generierten DDMs hängt von der Option **Set Status of DDMs** ab, die im Fenster **Restrictions** des Bibliothekssicherheitsprofils eingestellt ist (siehe ***Bestandteile eines Bibliothekssicherheitsprofils*** im Kapitel *Bibliotheken verwalten*).

Diese Option betrifft alle DDMs in der Bibliothek, für die keine Sicherheitsprofile definiert wurden.

Standardmäßig ist diese Option auf `UNDF` gesetzt, d.h. sowohl der interne als auch der externe Status eines neuen DDMs sind zu Beginn nicht definiert. Bevor ein neues DDM von einem Programm verwendet werden kann, müssen Sie ein Sicherheitsprofil für es erstellen und seinen internen und externen Status in dem Profil definieren.

Wenn Sie die Option auf `PUBL` setzen, werden sowohl der interne als auch der externe Status aller neu erzeugten DDMs automatisch auf PUBLIC gesetzt. Das bedeutet, dass neue DDMs von jedem Programm innerhalb der gleichen Bibliothek und in Bibliotheken, die die Bibliothek als Steplib verwenden, verwendet werden können. Wenn Sie die Verwendung dieser DDMs nicht einschränken wollen, brauchen Sie keine Sicherheitsprofile für sie zu erstellen oder weitere Sicherheitsangaben zu machen. Wenn Sie die Verwendung eines dieser DDMs einschränken wollen, müssen Sie ein Sicherheitsprofil für es definieren und in dem Profil den internen und externen Status wie gewünscht ändern.

Wenn Sie die Option **Set Status of DDMs** von `PUBL` nach `UNDF` zurücksetzen, werden der interne und externe Status aller PUBLIC DDMs ohne Sicherheitsprofile auf nicht definiert zurückgesetzt.

DDM-Sicherheitsprofile

Sofern der ***Initialstatus*** eines DDMs nicht automatisch auf PUBLIC gesetzt ist (siehe oben), müssen Sie für jedes DDM, das verwendet werden soll, ein Sicherheitsprofil definieren.

Neben dem **internen** und **externen** Status eines DDMs können Sie in einem DDM-Sicherheitsprofil auch einige andere Optionen festlegen:

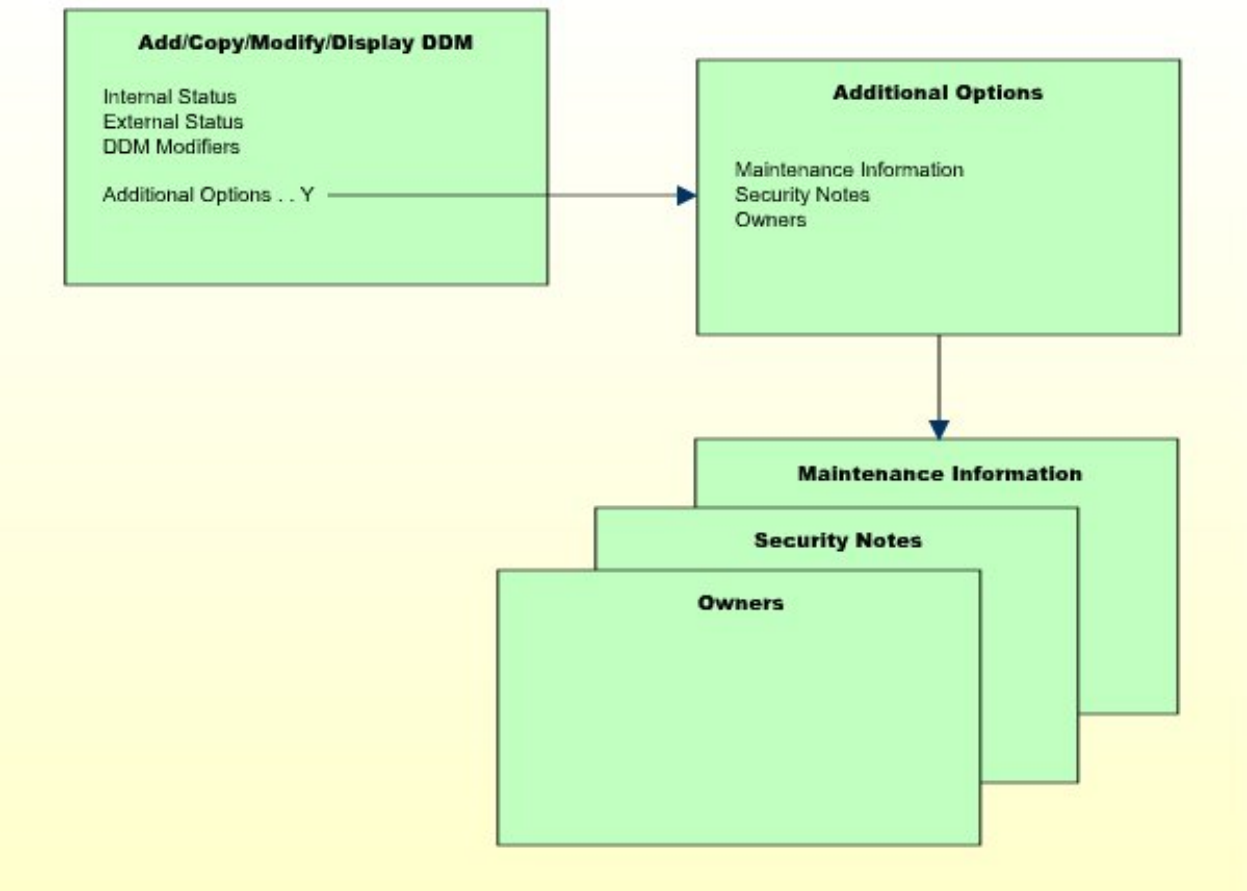
- Sie können die Verwaltung des DDMs selbst auf bestimmte Benutzer (DDM-Änderer) beschränken.
- Sie können die Verwaltung des DDM-Sicherheitsprofils auf bestimmte Benutzer (Eigentümer) beschränken.
- Sie können Vermerke zum Sicherheitsprofil eingeben.

Diese Optionen werden im Folgenden erläutert.

Folgende Themen werden behandelt:

- Bestandteile eines DDM-Sicherheitsprofils

Bestandteile eines DDM-Sicherheitsprofils



In diesem Abschnitt werden folgende Themen behandelt:

- Optionen eines DDM-Sicherheitsprofils
- Zusätzliche Optionen eines DDM-Sicherheitsprofils

Optionen eines DDM-Sicherheitsprofils

Feld	Erläuterung
DDM Name (nur Anzeige)	Der Name, unter dem das DDM generiert wurde.
DBID / FNR (nur Anzeige)	Die Datenbankkennung und Dateinummer der Datenbankdatei, auf die das DDM verweist.
Internal Status / External Status	Erläuterungen siehe oben unter *Status eines DDMs*. Mögliche Werte:

Feld	Erläuterung
	■ PUBL = PUBLIC ■ ACCE = ACCESS ■ PRIV = PRIVATE Wenn Sie ein DDM-Sicherheitsprofil anlegen, wird der interne und externe Status standardmäßig auf PUBL gesetzt.
DDM Modifiers	DDM-Änderer. Sie können bis zu acht Kennungen von Benutzern eingeben. Nur diese Benutzer sind dann berechtigt, das DDM in Predict (oder mit den DDM-Services von Natural) zu verwalten. Wenn Sie keine DDM-Änderer angeben, können die Eigentümer des Sicherheitsprofils (siehe *Zusätzliche Optionen - Additional Options* unten) das DDM verwalten. Wenn weder DDM-Änderer noch Eigentümer angegeben werden, ist die Verwaltung des DDMs nicht eingeschränkt. Neben der Kennung jedes DDM-Änderers können Sie optional eine Zahl von 1 bis 3 angeben. Diese Zahl legt fest, wie viele der anderen angegebenen DDM-Änderer für die Verwaltungserlaubnis gegenzeichnen müssen (die Gegenzeichnungslogik, die für die DDM-Verwaltungserlaubnis gilt, ist analog zu der von Eigentümern und Miteigentümern, siehe Kapitel *Gegenzeichnungen*).

Zusätzliche Optionen eines DDM-Sicherheitsprofils

Wenn Sie das Feld **Additional Options** im Basis-Bildschirm des DDM-Sicherheitsprofils mit Y markieren, wird ein Fenster angezeigt, in dem Sie die folgenden Optionen auswählen können:

- **Maintenance Information** - Verwaltungsinformationen
- **Security Notes** - Sicherheitsvermerke
- **Owners** - Eigentümer

Die Optionen, bei denen schon etwas angegeben oder definiert wurde, sind mit einem Pluszeichen (+) gekennzeichnet.

Sie können ein oder mehrere Elemente aus dem Fenster auswählen, indem Sie sie mit einem beliebigen Zeichen markieren. Für jedes ausgewählte Element wird ein weiteres Fenster angezeigt:

Zusätzliche Optionen - Additional Options	
Maintenance Information (nur Anzeige)	Verwaltungsinformationen. Folgende Informationen werden angezeigt: ■ Das Datum und die Uhrzeit, wann das Sicherheitsprofil angelegt wurde, die Kennung des Administrators, der es angelegt hat, und (falls zutreffend) die Kennungen der Miteigentümer, die für die Erstellung gegengezeichnet haben. ■ Das Datum und die Uhrzeit der letzten Änderung des Sicherheitsprofils, die Kennung des Administrators, der die letzte Änderung vorgenommen hat, und (falls zutreffend) die Kennungen der Miteigentümer, die die Änderung gegengezeichnet haben.
Security Notes	Sicherheitsvermerke. Hier können Sie Anmerkungen zum Sicherheitsprofil eingeben.
Owners	Eigentümer Sie können bis zu acht Kennungen von Administratoren eingeben. Nur die hier angegebenen Administratoren dürfen dieses DDM-Sicherheitsprofil verwalten oder Bibliotheken damit verlinken. Wenn kein Eigentümer angegeben wird, kann jeder Benutzer vom Typ Administrator das Sicherheitsprofil verwalten und verlinken. Zu jedem Eigentümer kann optional im Feld hinter der Kennung die Anzahl der Miteigentümer angegeben werden, deren Gegenzeichnung für die Verwaltungs-/Verlinkungserlaubnis erforderlich ist. Eine Erläuterung der Begriffe Eigentümer und Miteigentümer finden Sie im Kapitel *Gegenzeichnungen*.

DDM-Sicherheitsprofile anlegen und verwalten

Anmerkung: Wenn der Natural-Profilparameter `FDDM` gesetzt ist, können DDM-Sicherheitsprofile nur für DDMs angelegt und verwaltet werden, die in der Bibliothek `SYSTEM` enthalten sind.

Um DDM-Sicherheitsprofile anzulegen oder zu verwalten:

1 Markieren Sie in der **Library Maintenance**-Auswahlliste eine Bibliothek mit dem Code `MD` (oder, im Falle einer privaten Bibliothek, wenn private Bibliotheken im Private Mode verwendet werden, markieren Sie den Benutzer mit der gleichen Kennung in der **User Maintenance**-Auswahlliste mit dem Code `MD`).

2 Es wird ein Fenster angezeigt, in dem Sie einen Startwert für die Liste der DDMs eingeben können (wie im Kapitel *Grundlagen der Benutzung* beschrieben).

3 Anschließend wird eine Liste der in der Bibliothek enthaltenen DDMs angezeigt.

Zu jedem DDM werden der DDM-Name, die Kennung der Bibliothek sowie der interne und externe Status angezeigt.

Wenn für ein DDM ein Sicherheitsprofil existiert, wird dies in Spalte **P** angezeigt:

X	Sowohl das DDM-Sicherheitsprofil als auch das entsprechende DDM existieren.
N	Das DDM-Sicherheitsprofil existiert, aber kein entsprechendes DDM.
leer	Weder das DDM-Sicherheitsprofil noch das entsprechende DDM existieren.

In der Liste kann geblättert werden, siehe *Grundlagen der Benutzung*.

Externer Status als Auswahlkriterium

Wenn Sie nur DDMs mit einem bestimmten Status auflisten möchten, können Sie im Feld **External Status** oberhalb der Liste eines der folgenden Auswahlkriterien angeben:

PUBL	Alle DDMs mit dem Status PUBLIC.
ACCE	Alle DDMs mit dem Status ACCESS.
PRIV	Alle DDMs mit dem Status PRIVATE.
DEFI	Definiert, d. h. alle DDMs mit dem Status PRIV, ACCE und PUBL (*).
UNDF	Nicht definiert, d. h. alle DDMs, deren Status nicht PRIV, ACCE oder PUBL (*).ist.
DDM	Alle definierten und nicht definierten DDMs (*).
NDDM	DDM-Sicherheitsprofile, für die keine entsprechenden DDMs existieren (*).

Dies ist kein echter DDM-Status, sondern dient nur zu Auswahlzwecken.

Der Standardstatus für die Auswahl ist DDM, d. h. *alle* DDMs werden aufgelistet.

Funktion auswählen

Aus der DDM-Liste rufen Sie alle Funktionen zum Anlegen und Verwalten eines DDM-Sicherheitsprofils auf. Die folgenden Funktionen stehen zur Verfügung (mögliche Codeabkürzungen sind unterstrichen):

Code	Funktion
AD	**Add DDM Profile** - DDM-Sicherheitsprofil anlegen
CO	**Copy DDM Profile** - DDM-Sicherheitsprofil kopieren
MO	**Modify DDM Profile** - DDM-Sicherheitsprofil ändern
DE	**Delete DDM Profile** - DDM-Sicherheitsprofil löschen
DI	**Display DDM Profile** - DDM-Sicherheitsprofil anzeigen

Code	Funktion
CU	**Copy Profile/Link to All Special Links** - Profil kopieren/Verlinken mit allen Special-Links

Um eine bestimmte Funktion für ein DDM aufzurufen, müssen Sie das DDM mit dem entsprechenden Funktionscode in Spalte **Co** markieren.

Sie können mehrere DDMs gleichzeitig für verschiedene Funktionen auswählen, d.h. Sie können mehrere DDMs auf dem Bildschirm mit einem Funktionscode markieren. Für jedes markierte DDM wird der entsprechende Verarbeitungsbildschirm angezeigt, und Sie können für ein DDM nach dem anderen die ausgewählten Funktionen ausführen.

DDM-Sicherheitsprofil anlegen - Add DDM Profile

Mit dieser Funktion können Sie ein DDM in Natural Security definieren, d.h. ein neues DDM-Sicherheitsprofil anlegen.

Dazu:

1 Geben Sie in der DDM-Auswahlliste im Feld **Ext. Status** das Auswahlkriterium `UNDF` (nicht definiert) ein.

Es werden nur die DDMs in der Bibliothek aufgelistet, die noch nicht in Natural Security definiert wurden.

In der Liste kann geblättert werden, siehe *Grundlagen der Benutzung*.

2 Markieren Sie in der Liste das DDM, für das Sie ein Sicherheitsprofil erstellen möchten, mit dem Funktionscode `AD`.

Der Bildschirm **Add DDM** wird angezeigt.

3 Die einzelnen Bestandteile, die Sie auf diesem Bildschirm definieren können, sowie alle zusätzlichen Fenster, die Teil eines DDM-Sicherheitsprofils sein können, sind unter *Bestandteile eines DDM-Sicherheitsprofils* beschrieben.

Wenn Sie ein DDM anlegen, werden die im Sicherheitsprofil der Bibliothek, in der das DDM enthalten ist, angegebenen Eigentümer automatisch in das DDM-Sicherheitsprofil übernommen.

DDM-Sicherheitsprofil kopieren - Copy DDM Profile

Mit dieser Funktion können Sie ein DDM in Natural Security definieren, indem Sie ein Sicherheitsprofil anlegen, das mit einem bereits vorhandenen DDM-Sicherheitsprofil in derselben Bibliothek identisch ist.

- Was wird kopiert?
- Wie wird kopiert?
- Mit Links kopieren - Copying With Links

Was wird kopiert?

Alle Bestandteile des bestehenden DDM-Sicherheitsprofils werden in das neue DDM-Sicherheitsprofil kopiert - *jedoch nicht*:

- die Dateinummer und die Kennung der Datenbank,
- die Eigentümer (die Eigentümer werden aus Ihrem eigenen Benutzersicherheitsprofil in das neue DDM-Sicherheitsprofil kopiert).

Ob Links kopiert werden, hängt davon ab, ob Sie das Kopieren mit oder ohne Links wählen (siehe unten beim Feld **With Links = Y/N**).

Wie wird kopiert?

1. Markieren Sie in der DDM-Auswahlliste das DDM, dessen Sicherheitsprofil Sie duplizieren möchten, mit dem Funktionscode `CO`.
2. Es wird ein Fenster angezeigt, in dem Sie folgende Angaben machen können:

Feld	Erläuterung
To DDM	Nach DDM. Geben Sie den Namen des „neuen“ DDM ein.
With links	Mit Links. Geben Sie `Y` oder `N` ein. Mit dieser Option können Sie zusätzlich zum DDM-Sicherheitsprofil auch dessen Links kopieren; siehe ***Mit Links kopieren*** weiter unten.

3. Das neue DDM-Sicherheitsprofil wird angezeigt. Seine Bestandteile, die Sie definieren oder ändern können, sind unter ***Bestandteile eines DDM-Sicherheitsprofils*** beschrieben.

Mit Links kopieren - Copying With Links

Wenn Sie **With Links = N** wählen, werden alle Verlinkungen von Bibliotheken mit dem bestehenden DDM nicht für das neue DDM übernommen.

Wenn Sie **With Links = Y** wählen, werden alle Verlinkungen von Bibliotheken zum bestehenden DDM für das neue DDM kopiert, und Sie haben die Möglichkeit, die Links aufzuheben, die Sie nicht für das neue DDM übernehmen möchten. Die Vorgehensweise ist wie folgt:

1. Nachdem Sie Änderungen am kopierten DDM-Sicherheitsprofil vorgenommen und den Bildschirm **Copy DDM** durch Drücken von PF3 verlassen haben, wird eine Liste der Bibliotheken angezeigt: Sie enthält alle Bibliotheken, die mit dem bestehenden DDM verlinkt sind.
2. In der Liste können Sie einzelne Bibliotheken mit CL (Cancel) markieren, um Verknüpfungen aufzuheben, die Sie nicht für das neue DDM übernehmen möchten. Alle Bibliotheken, die Sie *nicht* markieren, werden automatisch mit dem neuen DDM auf dieselbe Weise verlinkt (Read- oder Update-Link) wie das bestehende DDM.

DDM-Sicherheitsprofil ändern - Modify DDM Profile

Mit dieser Funktion können Sie ein bestehendes DDM-Sicherheitsprofil ändern.

Dazu:

1 Markieren Sie in der DDM-Auswahlliste das DDM, dessen Sicherheitsprofil Sie ändern möchten, mit dem Funktionscode MO.

2 Das DDM-Sicherheitsprofil wird angezeigt. Seine Bestandteile, die Sie definieren oder ändern können, sind unter *Bestandteile eines DDM-Sicherheitsprofils* beschrieben.

DDM-Sicherheitsprofil löschen - Delete DDM Profile

Mit dieser Funktion können Sie ein bestehendes DDM-Sicherheitsprofil löschen.

Dazu:

1 Markieren Sie in der **DDM Maintenance**-Auswahlliste das DDM, das Sie löschen möchten, mit dem Funktionscode DE.

2 Es wird ein Fenster angezeigt.

- Wenn Sie sich gegen das Löschen des DDM-Sicherheitsprofils entscheiden, können Sie das Fenster verlassen, indem Sie ENTER drücken, ohne etwas eingegeben zu haben.

- Um das DDM-Sicherheitsprofil zu löschen, müssen Sie den Namen des DDMs in das Fenster eingeben, um den Löschvorgang zu bestätigen.

Wenn Sie ein DDM-Sicherheitsprofil löschen, werden auch alle bestehenden Links zu diesem Profil gelöscht.

Wenn Sie ein DDM-Sicherheitsprofil löschen, wird das DDM selbst nicht gelöscht. Der DDM-Name verbleibt in der DDM-Auswahlliste, wobei der interne Status entweder auf `UNDF` (nicht definiert) oder `PUBL` (öffentlich) gesetzt wird, je nach der Option **Set Status of DDMs** (diese Option wird im Kapitel *Bibliotheken verwalten* beschrieben).



Anmerkung: Wenn ein DDM selbst gelöscht wird (in Predict oder mit den DDM Services oder dem Dienstprogramm `SYSMAIN` von Natural), wird das zugehörige DDM-Sicherheitsprofil nicht gelöscht. Um die DDM-Sicherheitsprofile ohne DDMs in einer Bibliothek aufzulisten, müssen Sie NDDM als Auswahlkriterium für die Liste der DDM-Sicherheitsprofile eingeben.

Wenn Sie mehr als ein DDM mit `DE` markieren, erscheint ein Fenster, in dem Sie gefragt werden, ob Sie die Löschung jedes DDM-Sicherheitsprofils durch Eingabe des DDM-Namens bestätigen wollen, oder ob alle zum Löschen ausgewählten DDM-Sicherheitsprofile ohne diese individuelle Bestätigung gelöscht werden sollen. Achten Sie darauf, dass Sie nicht versehentlich ein DDM-Sicherheitsprofil löschen.

DDM-Sicherheitsprofil anzeigen - Display DDM Profile

Mit dieser Funktion können Sie sich ein bestehendes DDM-Sicherheitsprofil anzeigen lassen.

Dazu:

1 Markieren Sie in der DDM-Auswahlliste mit dem Funktionscode `DI` das DDM, dessen Sicherheitsprofil Sie anzeigen möchten.

2 Das DDM-Sicherheitsprofil wird angezeigt. Seine Bestandteile sind unter ***Bestandteile eines DDM-Sicherheitsprofils*** beschrieben.

Profil kopieren/Verlinken mit allen Special-Links - Copy Profile/Link to All Special Links

Diese Funktion führt Folgendes aus:

- Sie kopiert ein vorhandenes DDM-Sicherheitsprofil aus dieser Bibliothek in die Sicherheitsprofile aller vorhandenen Special-Links zur Bibliothek. Dadurch wird sichergestellt, dass für dieses DDM dasselbe DDM-Sicherheitsprofil innerhalb des Bibliothekssicherheitsprofils und aller seiner Special-Link-Profile vorhanden ist.
- Sie kopiert einen bestehenden Link zwischen einem DDM und einer personengeschützten Bibliothek, so dass zwischen dem DDM und allen Benutzern, die einen Special-Link zu dieser Bibliothek haben, gleichzeitig die gleiche Art von Link (Read-Link oder Update-Link) hergestellt wird.

Dazu:

1. Markieren Sie in der DDM-Auswahlliste das DDM, dessen Link/Profil Sie kopieren möchten, mit dem Funktionscode `CU`.

   Es wird eine Meldung angezeigt, dass es kopiert wurde.

Bibliothek mit einem geschützten DDM verlinken

Wenn der Natural-Profilparameter `FDDM` nicht gesetzt ist, können Sie eine Bibliothek wie folgt mit geschützten DDMs in einer Steplib verlinken:

1. Rufen Sie die DDM-Auswahlliste dieser Bibliothek auf (wie unter *DDM-Sicherheitsprofile anlegen und verwalten* beschrieben).
2. Geben Sie in das Feld **Library** oberhalb der Liste einen Stern (*) ein. Es wird ein Fenster angezeigt, in dem alle für die Bibliothek definierten Steplibs aufgelistet sind.
3. Markieren Sie die Steplib, die das DDM oder die DDMs enthält, mit denen Sie die Bibliothek verlinken möchten. Es wird eine Liste aller DDMs in der ausgewählten Steplib mit dem externen Status `ACCESS` und `PRIVATE` angezeigt.

   In der Liste kann geblättert werden, siehe *Grundlagen der Benutzung*.
4. Markieren Sie in der Spalte **Co** der Liste ein oder mehrere DDMs mit einem der unten aufgeführten Funktionscodes.

Wenn der Natural-Profilparameter `FDDM` gesetzt ist, kann eine Bibliothek nur mit geschützten DDMs verlinkt werden, die in der Steplib `SYSTEM` enthalten sind. Dies geschieht wie folgt:

1. Rufen Sie die DDM-Auswahlliste dieser Bibliothek auf (wie unter *DDM-Sicherheitsprofile anlegen und verwalten* beschrieben).
2. Es wird eine Liste aller DDMs in der Steplib `SYSTEM` mit dem externen Status `ACCESS` und `PRIVATE` angezeigt.

   In der Liste kann geblättert werden, siehe Kapitel *Grundlagen der Benutzung* beschrieben.
3. Markieren Sie in der Spalte **Co** der Liste ein oder mehrere DDMs mit einem der folgenden Funktionscodes:

Code	Funktion
`RE`	Read-Link - Die so verlinkte Bibliothek darf das DDM nur lesen, aber nicht ändern.
`UP`	Update-Link - Die so verlinkte Bibliothek darf das DDM lesen und ändern.
`CL`	Cancel - Eine bestehende Verlinkung wird aufgehoben.
`CU`	Copy - Eine bestehende Verlinkung zwischen einem DDM und einer personengeschützten Bibliothek wird kopiert, so dass die gleiche Art von Verlinkung (Read- oder Update-Link) gleichzeitig zwischen dem DDM und allen Benutzern hergestellt wird, die einen Special-Link zu dieser Bibliothek haben.

Eine Verlinkung zu einem PRIVATE DDM kann als Read-Link (`RE`) oder Update-Link (`UP`) angegeben werden. Eine Verbindung zu einem ACCESS-DDM kann nur als Update-Link (`UP`) angegeben werden, da zum Lesen eines ACCESS-DDM kein Link erforderlich ist.

14 Dienstprogramme (Utilities) schützen

- Allgemeine Überlegungen zum Schutz von Dienstprogrammen (Utilities) 262
- Welche Dienstprogramme (Utilities) können geschützt werden? 263
- Dienstprogrammprofile - Utility Profiles 263
- Standardprofile definieren 275
- Individuelle Profile definieren - Utility Maintenance 277
- Bestandteile von Dienstprogrammprofilen 286

Dieses Kapitel beschreibt, wie Sie mit Natural Security die Verwendung von Natural-Dienstprogrammen (Utilities) steuern können.

Folgende Themen werden behandelt:

Allgemeine Überlegungen zum Schutz von Dienstprogrammen (Utilities)

Der in diesem Kapitel beschriebene Schutz von Dienstprogrammen (Utilities) durch Natural Security ist funktionsorientiert, d. h., er basiert auf dem Konzept, dass Sie einzelne Funktionen eines Dienstprogramms zulassen oder verbieten können. Sie kontrollieren die Verwendung eines Dienstprogramms, indem Sie für dieses Dienstprogramm Dienstprogramm-Sicherheitsprofile festlegen (auch als Dienstprogrammprofile bezeichnet, engl. Utility Profile), in denen Sie seine Funktionen zulassen oder verbieten können. Die Dienstprogramme, die auf diese Weise geschützt werden können, sind unten aufgeführt.

Um ein Natural-Dienstprogramm aufzurufen, geben Sie den Namen des Dienstprogramms in der Regel als Systemkommando ein (um z. B. das Dienstprogramm `SYSERR` aufzurufen, geben Sie das Systemkommando `SYSERR` ein). Wenn ein Dienstprogramm auf diese Weise aufgerufen wird, gilt eines der für dieses Dienstprogramm definierten Dienstprogrammprofile, das die Verwendung des Dienstprogramms steuert und so für einen einheitlichen Schutz des Dienstprogramms sorgt.

Der Aufruf eines Dienstprogramms führt nicht zu einem Wechsel der Bibliothek, in der Sie sich gerade befinden; das heißt, wenn Sie das Dienstprogramm beenden, befinden Sie sich immer noch in derselben Bibliothek, aus der Sie das Dienstprogramm aufgerufen haben. Siehe auch den Abschnitt *Utility-Aktivierung* in der *Debugger und Dienstprogramme (Utilities)*-Dokumentation.

Um die Verwendung eines Dienstprogramms zu steuern, müssen Sie kein Bibliothekssicherheitsprofil für die Bibliothek definieren, die das Dienstprogramm enthält. Ein Dienstprogrammprofil für ein Dienstprogramm ist nur dann relevant, wenn das Dienstprogramm Zugriff auf Programme in anderen Bibliotheken benötigt (z. B. User Exits, die in Steplibs enthalten sind).

Wenn für eine Bibliothek, die ein Dienstprogramm enthält, ein Dienstprogrammprofil definiert ist und Sie sich bei einer Dienstprogrammbibliothek anmelden, gelten dieselben Anmelderegeln wie für eine Anmeldung bei einer anderen Bibliothek (wie im Kapitel ***Anmeldung*** beschrieben). In der Dienstprogrammbibliothek kann das Dienstprogramm entweder durch Eingabe des Dienstprogrammnamens als Systemkommando (wie in jeder anderen Bibliothek) oder durch die Ausführung der Starttransaktion `MENU` (falls im Bibliothekssicherheitsprofil des Dienstprogramms definiert) aufgerufen werden. Im letzteren Fall wird jedoch ein `LOGOFF`-Kommando ausgeführt, wenn Sie das Dienstprogramm verlassen.

Die Dienstprogramme `SYSERR` und `SYSMAIN` verarbeiten den Inhalt von Bibliotheken. Wenn die Verwendung dieser Dienstprogramme nicht durch Dienstprogrammprofile gesteuert wird, gilt die Option **Utilities** im Bibliothekssicherheitsprofil der bearbeiteten Bibliothek.

Welche Dienstprogramme (Utilities) können geschützt werden?

Die Verwendung der folgenden Natural-Dienstprogramme kann mit Dienstprogrammprofilen gesteuert werden:

- **PROFILER**
- **SYSBPM**
- **SYSCP - Codepage-Verwaltung**
- **SYSDB2 - Tools für DB2**
- **SYSDDM**
- **SYSERR**
- **SYSMAIN**
- **SYSOBJH - Object Handler**
- **SYSPARM**
- **SYSPCI**
- **SYSRPC**
- **ZIIP**

Dienstprogrammprofile - Utility Profiles

Dieser Abschnitt behandelt die folgenden Themen:

- Dienstprogrammprofiltypen
- Standard-Dienstprogrammprofil
- Benutzerspezifische Dienstprogrammprofile
- Bibliotheksspezifische Dienstprogrammprofile
- Benutzerbibliotheksspezifische Dienstprogrammprofile
- Welches Dienstprogramm-Profil wird angewendet?
- Wann tritt ein Dienstprogrammprofil in Kraft?
- Verfügbare Systemkommandos

- Wo werden Profile definiert?

Dienstprogrammprofiltypen

Ein Dienstprogrammprofil besteht im Wesentlichen aus einer Liste der Funktionen des Dienstprogramms, die jeweils mit einem `A` = Allow/Erlauben bzw. `D` = Disallow/Nicht erlauben gekennzeichnet werden können.

Zu jedem Dienstprogramm, das unter ***Welche Dienstprogramme (Utilities) können geschützt werden?*** aufgeführt sind, können Sie Folgendes definieren:

- ein Standardprofil,
- benutzerspezifische Profile,
- bibliotheksspezifische Profile,
- benutzerbibliotheksspezifische Profile.

Jedes Dienstprogramm wird individuell behandelt, d.h. Dienstprogrammprofile gelten nur für das Dienstprogramm, für das sie definiert sind, und nicht für andere Dienstprogramme.

Anmerkung: Wenn die Verwendung eines Dienstprogramms durch ein Dienstprogrammprofil geschützt ist, gelten automatisch die Natural-Profilparametereinstellungen `MADIO=0` und `MAXCL=0`.

Standard-Dienstprogrammprofil

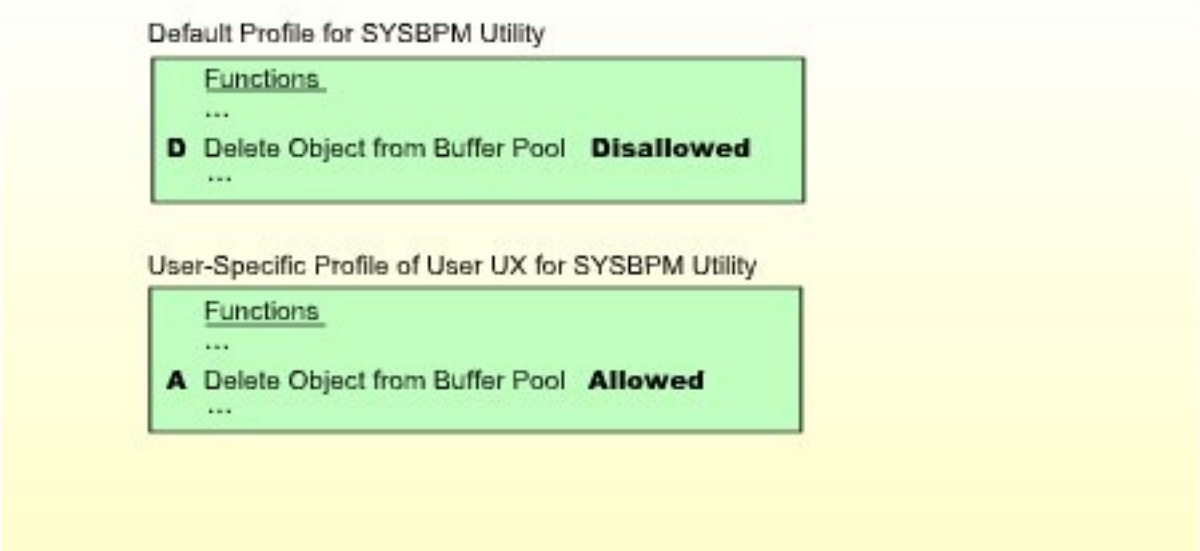
Das *Standardprofil* (Default Profile) eines Dienstprogramms gilt für alle Benutzer (außer denen, für die benutzerspezifische Profile definiert sind). Es legt fest, welche Funktionen des Dienstprogramms die Benutzer nutzen dürfen und welche nicht.

Benutzerspezifische Dienstprogrammprofile

Wenn ein einzelner Benutzer andere Funktionen nutzen (oder nicht nutzen) soll als die anderen Benutzer, können Sie ein *benutzerspezifisches Dienstprogrammprofil* (User-specific Profile) definieren.

Ein solches Profil gilt nur für diesen Benutzer, hat Vorrang vor dem Standardprofil und legt fest, welche Funktionen des Dienstprogramms dieser Benutzer nutzen darf und welche nicht.

Beispiel:



In diesem Beispiel ist die SYSBPM-Funktion **Delete Object from Buffer Pool** (Objekt aus dem Pufferpool löschen) für alle Benutzer nicht erlaubt - außer für den Benutzer UX, für den sie erlaubt ist. Dies bedeutet, dass UX der einzige Benutzer ist, der Objekte aus dem Buffer-Pool löschen darf.

Benutzerspezifische Dienstprogrammprofile können für Benutzer der Typen Group, Administrator und Person definiert werden.

Ein benutzerspezifisches Dienstprogrammprofil kann nur definiert werden, wenn ein Standardprofil (oder eine Vorlage) für dieses Dienstprogramm definiert wurde. (Vorlagen werden weiter unten unter *Standardprofile definieren* beschrieben).

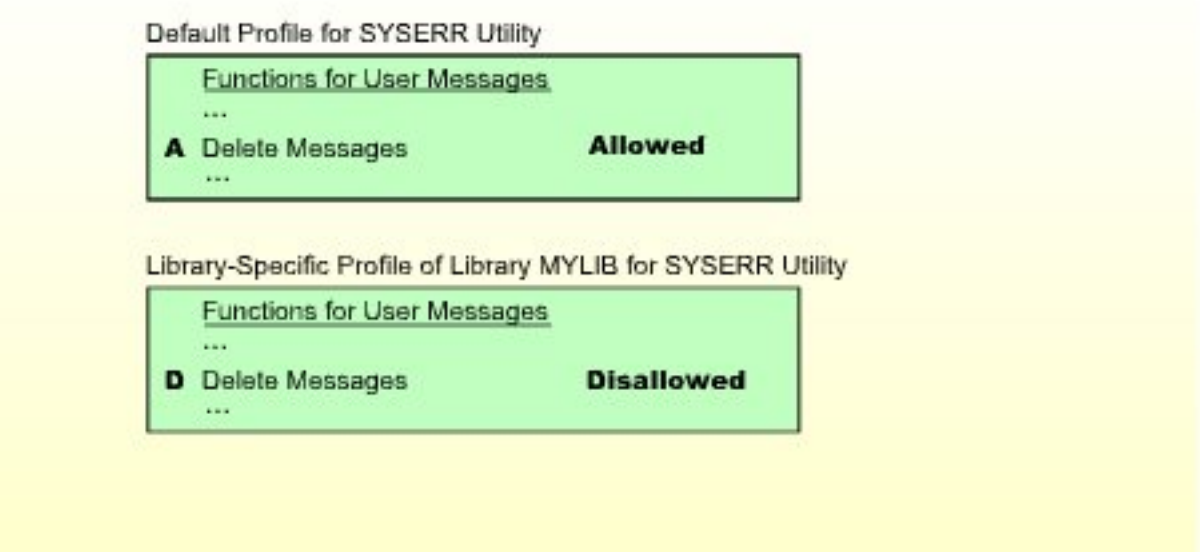
Bibliotheksspezifische Dienstprogrammprofile

Einige Dienstprogramme wirken sich auf einzelne Natural-Bibliotheken aus (z.B. kann die SYSERR Utility verwendet werden, um Fehlermeldungen zu verwalten, die zu einer bestimmten Bibliothek gehören). In der Regel gilt das Standardprofil des Dienstprogramms für alle betroffenen Bibliotheken.

Sollen jedoch einige Funktionen des Dienstprogramms nur für eine bestimmte Bibliothek erlaubt bzw. nicht erlaubt werden, können Sie ein *bibliotheksspezifisches Dienstprogrammprofil* definieren.

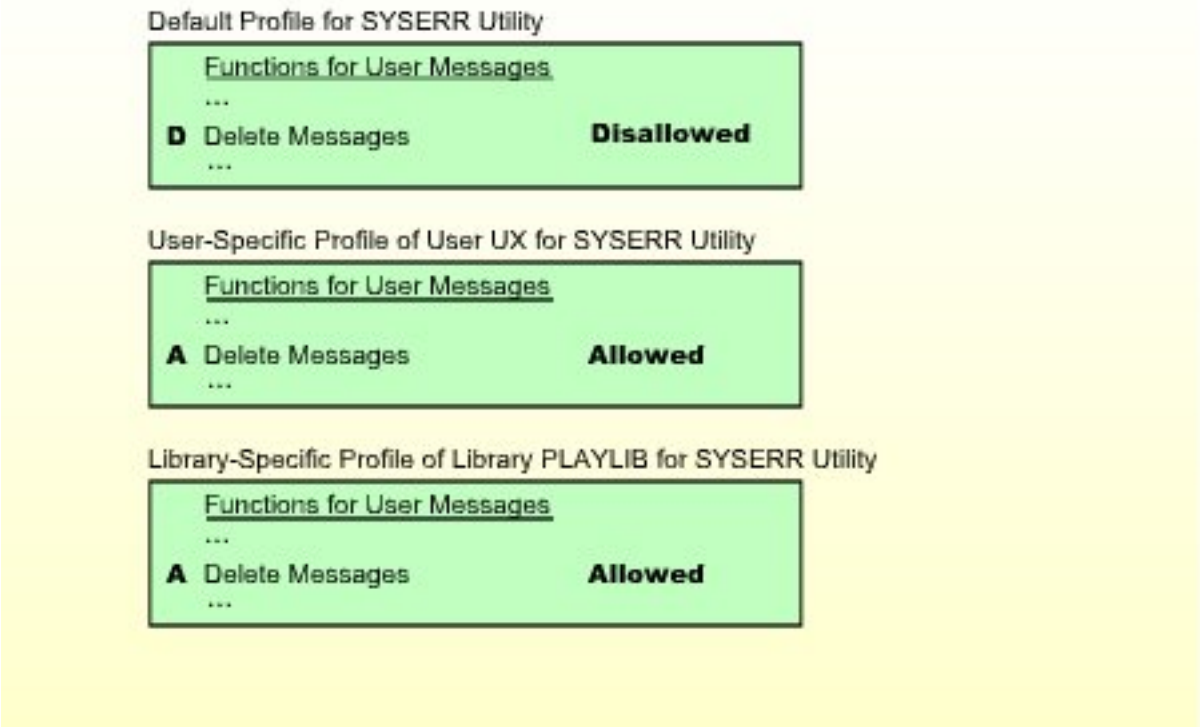
Ein solches Profil gilt nur für diese Bibliothek, setzt das Standardprofil sowie alle benutzerspezifischen Profile für dieses Dienstprogramm außer Kraft und bestimmt, welche Funktionen des Dienstprogramms auf diese Bibliothek angewendet werden dürfen und welche nicht.

Beispiel 1:



In diesem Beispiel ist die SYSERR-Funktion **Delete Messages** (Meldungen löschen) für alle Bibliotheken erlaubt - außer für die Bibliothek `MYLIB`, für die sie nicht erlaubt ist. Das bedeutet, dass alle Benutzer Benutzerfehlermeldungen aus allen Bibliotheken löschen können, außer aus der Bibliothek `MYLIB`. Niemand kann Meldungen aus `MYLIB` löschen. (Wenn benutzerspezifische Profile für `SYSERR` definiert wären, würden sie für alle anderen Bibliotheken gelten, aber nicht für die Bibliothek `MYLIB`).

Beispiel 2:



In diesem Beispiel ist die SYSERR-Funktion **Delete Messages** (Meldungen löschen) für alle Bibliotheken nicht erlaubt - außer für die Bibliothek PLAYLIB, für die sie erlaubt ist. Für den Benutzer UX ist die Funktion **Delete Messages** für alle Bibliotheken erlaubt. Das bedeutet, dass alle Benutzer Fehlermeldungen aus der Bibliothek PLAYLIB löschen können. Kein Benutzer - außer dem Benutzer UX - kann jedoch Meldungen aus einer anderen Bibliothek löschen. Benutzer UX ist der einzige Benutzer, der Meldungen aus allen Bibliotheken (einschließlich PLAYLIB) löschen darf. Beachten Sie, dass die Berechtigung von Benutzer UX zum Löschen von Meldungen aus der PLAYLIB vom bibliotheksspezifischen Profil abhängt, nicht vom benutzerspezifischen Profil.

Bibliotheksspezifische Dienstprogrammprofile können für die folgenden Dienstprogramme definiert werden: SYSBPM, SYSDDM, SYSERR, SYSMAIN, SYSOBJH.

Ein bibliotheksspezifisches Dienstprogrammprofil kann nur definiert werden, wenn ein Standardprofil für dieses Dienstprogramm definiert wurde.

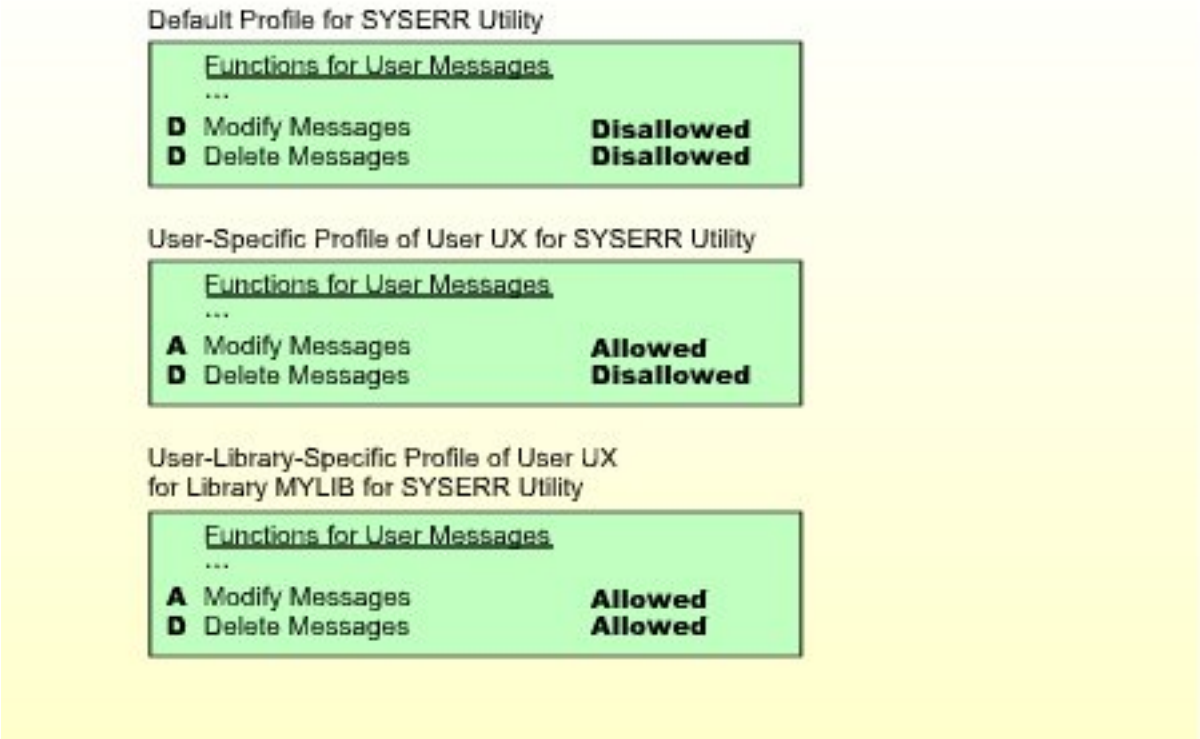
Benutzerbibliotheksspezifische Dienstprogrammprofile

Wie oben beschrieben, betreffen einige Dienstprogramme einzelne Natural-Bibliotheken. Es gibt zwei Arten von Situationen, in denen eventuell ein *benutzerbibliotheksspezifisches Dienstprogrammprofil* definiert werden muss:

- Ein *benutzerspezifisches* Dienstprogrammprofil legt fest, welche Funktionen eines Dienstprogramms ein bestimmter Benutzer verwenden darf, unabhängig von den Bibliotheken, die von den Funktionen betroffen sind (vorausgesetzt, für dieses Dienstprogramm sind keine *bibliotheksspezifischen* Profile definiert). Soll dieser Benutzer jedoch für eine bestimmte Bibliothek, die von den Funktionen des Dienstprogrammprofils betroffen ist, andere Funktionsnutzungsrechte haben, können Sie diese in einem *benutzerbibliotheksspezifischen* Dienstprogrammprofil festlegen.
- Ein *bibliotheksspezifisches* Dienstprogrammprofil legt fest, welche Funktionen eines Dienstprogramms verwendet werden dürfen, wenn es auf eine bestimmte Bibliothek angewendet wird. Für diese Bibliothek gilt es für alle Benutzer (unabhängig von etwaigen benutzerspezifischen Profilen). Soll jedoch ein bestimmter Benutzer andere Funktionsnutzungsrechte für diese Bibliothek haben, können Sie diese in einem *benutzerbibliotheksspezifischen* Dienstprogrammprofil festlegen.

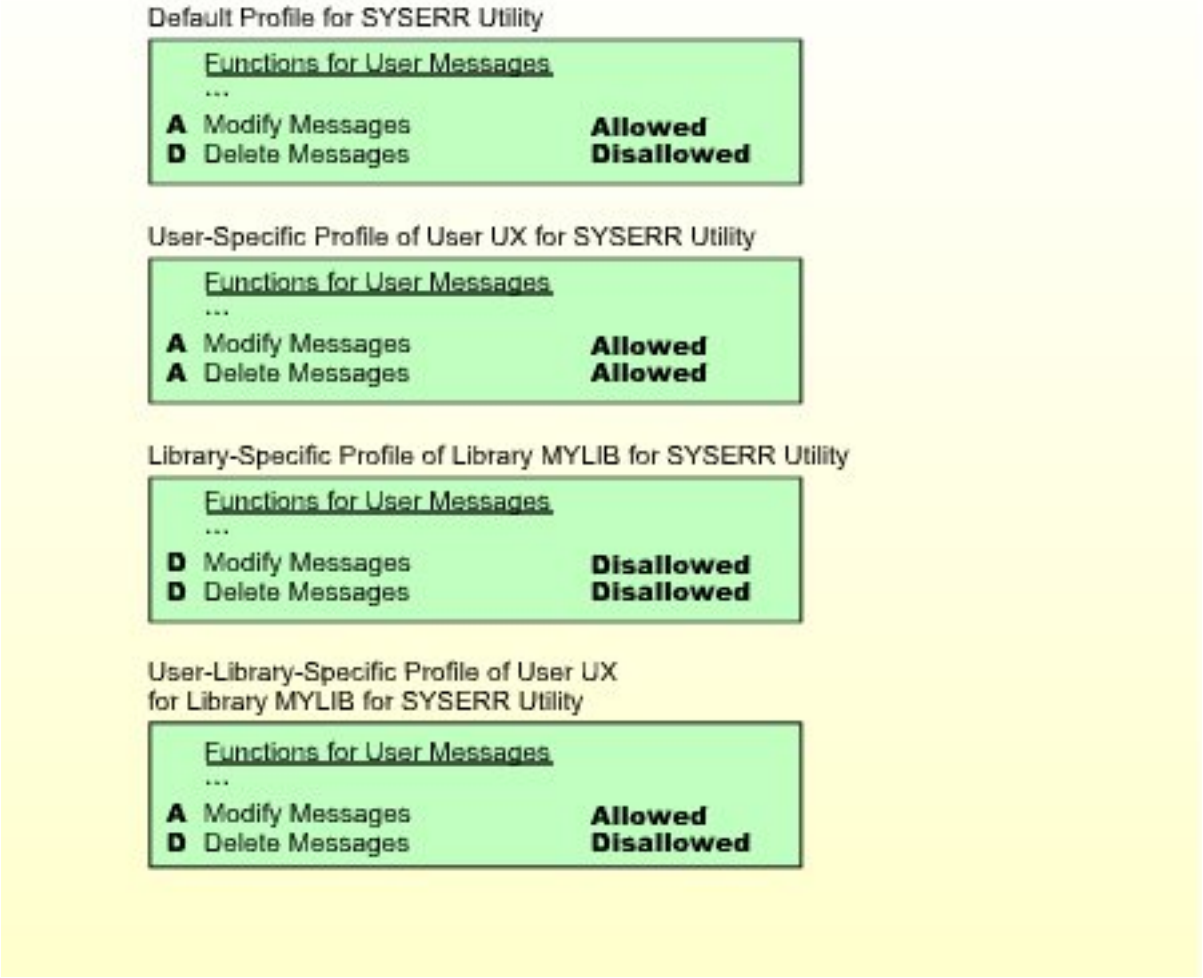
Ein *benutzerbibliotheksspezifisches* Profil gilt nur für einen Benutzer und eine Bibliothek. Es setzt das bibliotheksspezifische Dienstprogrammprofil dieser Bibliothek sowie das benutzerspezifische Profil dieses Benutzers außer Kraft und legt fest, welche Funktionen des Dienstprogramms der Benutzer für diese Bibliothek nutzen darf.

Beispiel 1:



In diesem Beispiel ist die SYSERR-Funktion **Delete Messages** (Meldungen löschen) für alle Benutzer (aufgrund des Standardprofils) nicht erlaubt. Die SYSERR-Funktion **Modify Messages** (Meldungen ändern) ist ebenfalls für alle Benutzer nicht erlaubt (aufgrund des *Standardprofils*) - außer für den Benutzer UX, für den sie erlaubt ist (aufgrund seines *benutzerspezifischen* Profils). Auch für den Benutzer UX sind beide Funktionen für die Bibliothek MYLIB erlaubt (aufgrund des *benutzerbibliotheksspezifischen* Profils). Das bedeutet, dass kein Benutzer Fehlermeldungen aus irgendeiner Bibliothek ändern oder löschen kann. Die einzige Ausnahme ist der Benutzer UX: Er darf Meldungen aus jeder beliebigen Bibliothek ändern. Außerdem darf er Meldungen aus der Bibliothek MYLIB löschen (aber nicht aus einer anderen Bibliothek). Beachten Sie, dass die Berechtigung des Benutzers UX, Nachrichten aus MYLIB zu ändern, vom *benutzerbibliotheksspezifischen* Profil des Benutzers abhängt, nicht vom *benutzerspezifischen* Profil.

Beispiel 2:



In diesem Beispiel ergibt sich die folgende Einteilung:

- Fehlermeldungen der Bibliothek `MYLIB` dürfen nur vom Benutzer UX geändert werden.
- Fehlermeldungen einer beliebigen anderen Bibliothek können von jedem Benutzer geändert werden.
- Fehlermeldungen der Bibliothek `MYLIB` können von keinem Benutzer gelöscht werden.
- Fehlermeldungen einer beliebigen anderen Bibliothek dürfen nur vom Benutzer UX, aber nicht von einem anderen Benutzer gelöscht werden.

Benutzerbibliotheksspezifische Dienstprogrammprofile können für die folgenden Dienstprogramme definiert werden: `SYSBPM`, `SYSDDM`, `SYSERR`, `SYSMAIN`, `SYSOBJH`.

Ein benutzerbibliotheksspezifisches Dienstprogrammprofil kann nur für einen Benutzer definiert werden, für den ein benutzerspezifisches Dienstprogrammprofil definiert wurde.

Welches Dienstprogramm-Profil wird angewendet?

Wenn ein Benutzer versucht, eine Dienstprogrammfunktion zu verwenden, sucht Natural Security nach dem entsprechenden Dienstprogrammprofil, um festzustellen, ob der Benutzer die Funktion ausführen darf.

Wie unten gezeigt, können Sie die Suchreihenfolge mit den Sitzungsoptionen **Privileged Groups** und ***GROUP Only** beeinflussen, die im Standardprofil eines Dienstprogramms festgelegt werden können.

Wenn ***GROUP Only** auf `N` gesetzt ist, sucht Natural Security nach den folgenden Dienstprogrammprofilen in der folgenden Reihenfolge:

1. das *benutzerbibliotheksspezifische* Benutzersicherheitsprofil
   a. des *Benutzers* für die betroffene Bibliothek (nur wenn der Benutzer vom Typ `A` oder `P` ist),
   b. einer *privilegierten Gruppe* für die betroffene Bibliothek (nur wenn **Privileged Groups** auf `Y` gesetzt ist,
   c. der *aktuellen Gruppe*, in der der Benutzer für die betroffene Bibliothek enthalten ist,
   d. einer *anderen Gruppe*, in der der Benutzer für die betroffene Bibliothek enthalten ist,
2. das *bibliotheksspezifische* Profil der betroffenen Bibliothek,
3. das *benutzerspezifische* Profil
   a. des *Benutzers* (nur wenn der Benutzer vom Typ `A` oder `P` ist),
   b. einer *privilegierten Gruppe* (nur wenn **Privileged Groups** auf `Y` gesetzt ist,
   c. der *aktuellen Gruppe*, in der der Benutzer enthalten ist,
   d. einer *anderen Gruppe*, in der der Benutzer enthalten ist,
4. das *Standardprofil* des Dienstprogramms.

Wenn ***GROUP Only** auf `Y` gesetzt ist, sucht Natural Security nach den folgenden Dienstprogrammprofilen in der folgenden Reihenfolge:

1. das *benutzerbibliotheksspezifische* Benutzersicherheitsprofil
   a. des *Benutzers* für die betroffene Bibliothek (nur wenn der Benutzer vom Typ `A` oder `P` ist),
   b. der *aktuellen Gruppe*, in der der Benutzer für die betroffene Bibliothek enthalten ist,
2. das *bibliotheksspezifische* Profil der betroffenen Bibliothek,
3. das *benutzerspezifische* Profil
   a. des *Benutzers* (nur wenn der Benutzer vom Typ `A` oder `P` ist),

   b. der *aktuellen Gruppe*, in der der Benutzer enthalten ist,

4. das *Standardprofil* des Dienstprogramms.

Für die Suche werden der Benutzer und die aktuelle Gruppe durch die aktuellen Werte der Natural-Systemvariablen `*USER` bzw. `*GROUP` bestimmt.

Privilegierte Gruppen sind die Gruppen, die im Sicherheitsprofil des Benutzers als **„Privileged Groups“** angegeben sind. Ihre Kennungen werden in der Reihenfolge verarbeitet, in der sie im Benutzersicherheitsprofil angegeben sind. Die Kennungen der anderen Gruppen werden in alphabetischer Reihenfolge verarbeitet.

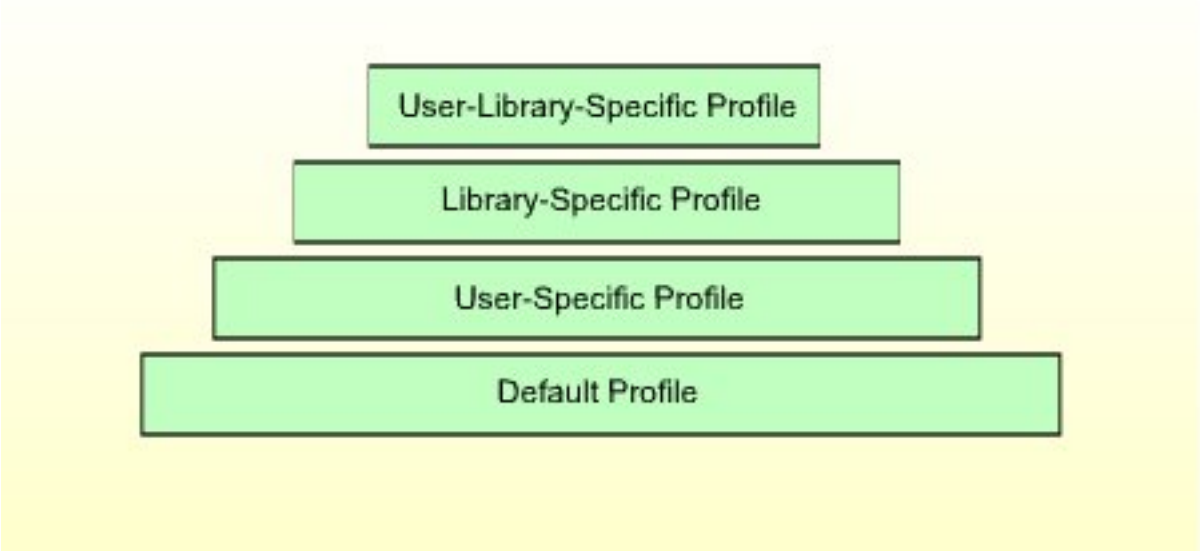
Das erste Profil, das bei dieser Suche gefunden wird, bestimmt, ob der Benutzer die Funktion ausführen darf.

Wenn keines der oben genannten Profile existiert und die Dienstprogrammfunktion den Inhalt einer Bibliothek betrifft, gilt die Option **Utilities** im Bibliothekssicherheitsprofil.

Informationen über das aktuell gültige Dienstprogrammprofil erhält der Benutzer mit dem Natural- Systemkommando `PROFILE` (siehe auch das ***PROFILE-Kommando*** im Kapitel *Bibliotheken schützen*).

Die folgende Abbildung zeigt die Hierarchie der Dienstprogrammprofile.

Hierarchie bei Dienstprogrammprofilen (Utility Profiles)



Beispiel:

Nehmen wir folgende Situation an: Benutzer UX (Benutzertyp `A`), der in der Gruppe GX enthalten ist, möchte Programmierobjekte mit dem Dienstprogramm `SYSMAIN` von Bibliothek `LIB1` nach Bibliothek `LIB2` kopieren.

Zunächst prüft Natural Security, ob der Benutzer Programmierobjekte mit `SYSMAIN` aus Bibliothek `LIB1` kopieren darf, d.h. ob die Kopierfunktion für „Programming Objects“ erlaubt ist:

1. Natural Security prüft das *benutzerbibliotheksspezifische* Profil des Benutzers UX und die Bibliothek `LIB1` für `SYSMAIN`.
2. Wenn kein solches Profil vorhanden ist, wird das *benutzerbibliotheksspezifische* Profil des Benutzers GX und der Bibliothek `LIB1` für `SYSMAIN` geprüft.
3. Wenn kein solches Profil vorhanden ist, wird das *bibliotheksspezifische* Profil der Bibliothek `LIB1` für `SYSMAIN` geprüft.
4. Wenn kein solches Profil vorhanden ist, wird das *benutzerspezifische* Profil des Benutzers UX für `SYSMAIN` geprüft.
5. Wenn kein solches Profil vorhanden ist, wird das benutzerspezifische Profil des Benutzers GX für `SYSMAIN` geprüft.
6. Wenn kein solches Profil vorhanden ist, wird das *Standardprofil* (Default Profile) von `SYSMAIN` geprüft.

Dann prüft Natural Security, ob der Benutzer Programmierobjekte mit `SYSMAIN` *in die Bibliothek LIB2* kopieren darf, d.h. ob die Kopierfunktion für „Programming Objects“ erlaubt ist:

1. Natural Security prüft das *benutzerbibliotheksspezifische* Profil des Benutzers UX und der Bibliothek `LIB2` für `SYSMAIN`.
2. Wenn kein solches Profil vorhanden ist, wird das *benutzerbibliotheksspezifische* Profil des Benutzers GX und der Bibliothek `LIB2` für `SYSMAIN` geprüft.
3. Wenn kein solches Profil vorhanden ist, wird das *bibliotheksspezifische* Profil der Bibliothek `LIB2` für `SYSMAIN` geprüft.
4. Wenn kein solches Profil vorhanden ist, wird das *benutzerspezifische* Profil des Benutzers UX für `SYSMAIN` geprüft.
5. Wenn kein solches Profil vorhanden ist, wird das *benutzerspezifische* Profil des Benutzers GX für `SYSMAIN` geprüft.
6. Wenn kein solches Profil vorhanden ist, wird das *Standardprofil* (Default Profile) von `SYSMAIN` geprüft.

Wann tritt ein Dienstprogrammprofil in Kraft?

Da sich die verschiedenen Natural- Dienstprogramme und ihre Funktionen stark voneinander unterscheiden, ist der Zeitpunkt, zu dem Natural Security prüft, ob ein Benutzer eine angeforderte Dienstprogrammfunktion verwenden darf, von Dienstprogramm zu Dienstprogramm und von Funktion zu Funktion sehr unterschiedlich.

Verfügbare Systemkommandos

Wenn ein Benutzer ein Dienstprogramm unter der Kontrolle eines Dienstprogrammprofils verwendet, sind die einzigen Natural- Systemkommandos, die dem Benutzer innerhalb des Dienstprogramms zur Verfügung stehen:

`FIN`, `LOGON`, `MAIL` und `PROFILE`.

Alle anderen Systemkommandos können nicht verwendet werden. Damit soll verhindert werden, dass der von den Dienstprogrammprofilen eingerichtete Schutz durch „Schlupflöcher“ beeinträchtigt wird.

Wo werden Profile definiert?

Um Standardprofile zu definieren, müssen Sie den Bereich **Administrator Services** von Natural Security benutzen (siehe ***Standardprofile definieren***).

Um *alle anderen Dienstprogrammprofile* zu definieren, müssen Sie den Bereich **Utility Maintenance** (Dienstprogrammverwaltung) von Natural Security benutzen (wie unter ***Individuelle Profile definieren - Utility Maintenance*** beschrieben).

Standardprofile definieren

Wählen Sie im Hauptmenü (**Main Menu**) den Eintrag **Administrator Services**.

Wenn Sie **berechtigt** sind, auf die **Administrator Services** zuzugreifen, wird das Menü **Administrator Services Menu 1** angezeigt.

Drücken Sie PF8.

Wählen Sie im **Administrator Services Menu 2** die Option **Utility Defaults/Templates**.

Der Bildschirm **Define Utility Defaults/Templates** (Dienstprogrammstandardeinstellungen/Vorlagen definieren) wird angezeigt, in dem alle Dienstprogramme aufgelistet sind, für die Profile definiert werden können.

Der Status eines Dienstprogramms (wie im Feld **Message** angezeigt) kann einer der folgenden sein:

Status	Bedeutung
Nothing defined	Nichts definiert. Es ist kein Profil für das Dienstprogramm definiert. Wenn sich eine Dienstprogrammfunktion auf den Inhalt einer Bibliothek auswirkt, wird ihre Verwendung durch die Option **Utilities** im Bibliothekssicherheitsprofil gesteuert.
Default defined	Standard definiert. Ein Standardprofil wurde für das Dienstprogramm definiert. Dieses Standardprofil gilt für alle Benutzer, für die kein individuelles benutzerspezifisches Profil definiert ist. Die Option **Utilities** in Bibliothekssicherheitsprofilen wird bei diesem Dienstprogramm ignoriert.
Template defined	Vorlage definiert. Für das Dienstprogramm wurde ein Profil definiert. Dieses Profil kann jedoch nur als Vorlage für die Definition individueller benutzerspezifischer Dienstprogrammprofile verwendet werden. Wenn sich eine Dienstprogrammfunktion auf den Inhalt einer Bibliothek auswirkt, wird ihre Verwendung durch die Option **Utilities** im Bibliothekssicherheitsprofil gesteuert - außer für die Benutzer, für die ein benutzerspezifisches Dienstprogrammprofil definiert ist.

Ob ein Standardprofil ein reales Profil oder nur eine Vorlage ist, wird durch das Feld **Applies as Default Profile** (siehe unten) innerhalb des Profils bestimmt.

Vorsicht: Um die Anwendbarkeit von Dienstprogrammprofilen und der Option **Utilities** in Bibliothekssicherheitsprofilen nicht zu verwechseln, sollten Sie immer ein Standardprofil (nicht nur eine Vorlage) für ein Dienstprogramm definieren, wenn Sie beabsichtigen, benutzerspezifische Profile für dieses Dienstprogramm zu definieren.

Auf dem Bildschirm **Define Utility Defaults/Templates** können Sie ein Dienstprogramm mit einem der folgenden Funktionscodes markieren:

Code	Funktion
AD	Standardprofil oder eine Vorlage für das Dienstprogramm definieren.
MO	Bestehendes Standardprofil oder -vorlage des Dienstprogramms ändern.
DE	Bestehendes Standardprofil oder -vorlage des Dienstprogramms löschen.
DI	Bestehendes Standardprofil oder -vorlage des Dienstprogramms anzeigen.

Wenn Sie ein Dienstprogramm mit dem Code DE markieren, wird ein Fenster angezeigt, in dem Sie das Löschen durch Eingabe des Dienstprogrammnamens bestätigen müssen. Wenn Sie das Standardprofil oder die Vorlage eines Dienstprogramms löschen, werden auch alle anderen Profile für dieses Dienstprogramm - d. h. benutzerspezifische, bibliotheksspezifische und benutzerbibliotheksspezifische Dienstprogrammprofile - gelöscht.

Wenn Sie ein Dienstprogramm mit dem Code AD, MO oder DI markieren, wird sein Standardprofil bzw. seine Standardvorlage angezeigt.

Das Standardprofil bzw. die Standardvorlage für jedes Dienstprogramm bietet mehrere Optionen, die den Funktionen des betreffenden Dienstprogramms entsprechen. Die Optionen für jedes Dienstprogramm werden unter *Bestandteile von Dienstprogrammprofilen* weiter unten beschrieben.

Sie können jede Option *erlauben* oder *nicht erlauben*, indem Sie sie mit A (Allow) bzw. D (Disallow) markieren. Zu Beginn sind alle Optionen nicht erlaubt.

Mit PF16 und PF17 können Sie alle Optionen in einem Dienstprogrammprofil gleichzeitig auf A bzw. D setzen.

Anmerkung: Natural Security führt Konsistenzprüfungen für die Kombinationen von erlaubten und nicht erlaubten Optionen durch - nicht mögliche Kombinationen von A und D werden automatisch abgelehnt.

Darüber hinaus enthält jedes Profil das Feld **Applies as Default Profile** (Gilt als Standardprofil), das festlegt, ob das Profil ein „reales“ Standardprofil oder nur eine Vorlage ist:

Applies as Default Profile

Wert	Bedeutung
Y	**Default Profile** - Standardprofil. Das Profil gilt für alle Benutzer, für die kein individuelles Dienstprogrammprofil definiert ist.
N	**Template** - Vorlage. Das Profil gilt für keinen Benutzer. Es kann nur als Vorlage für die Definition von individuellen benutzerspezifischen Dienstprogrammprofilen verwendet werden.

Sobald dieses Feld auf `Y` gesetzt ist und benutzerspezifische oder bibliotheksspezifische Profile für dieses Dienstprogramm definiert wurden, kann es nicht mehr auf `N` zurückgesetzt werden. Auf diese Weise wird ein durchgehend einheitlicher Schutz der Dienstprogramme gewährleistet.

Individuelle Profile definieren - Utility Maintenance

Mit der Dienstprogrammverwaltung (**Utility Maintenance**) in Natural Security können Sie alle Funktionen im Zusammenhang mit der Verwaltung von individuellen Dienstprogramm-(Utility-)Profilen ausführen: benutzerspezifische Profile, bibliotheksspezifische Profile und benutzerbibliotheksspezifische Profile.

Die Bestandteile eines individuellen Profils entsprechen denen des entsprechenden Standardprofils. Sie sind weiter unten unter ***Bestandteile von Dienstprogrammprofilen*** beschrieben.

Anmerkung: Für das Anlegen und Verwalten von individuellen Dienstprogrammprofilen gilt die Eigentümerlogik.

In diesem Abschnitt werden die folgenden Themen im Zusammenhang mit dem Anlegen und Verwalten von Dienstprogrammprofilen behandelt:

- Dienstprogrammverwaltung (Utility Maintenance) aufrufen
- Funktionen der Dienstprogrammverwaltung
- Benutzerspezifisches Dienstprogrammprofil anlegen
- Benutzerspezifisches Dienstprogrammprofil ändern/anzeigen
- Benutzerspezifisches Dienstprogrammprofil löschen
- Bibliotheksspezifisches Dienstprogrammprofil anlegen
- Bibliotheksspezifisches Dienstprogrammprofil ändern/anzeigen
- Bibliotheksspezifisches Dienstprogrammprofil löschen
- Benutzerbibliotheksspezifisches Dienstprogrammprofil anlegen
- Benutzerbibliotheksspezifisches Dienstprogrammprofil ändern oder anzeigen
- Benutzerbibliotheksspezifisches Dienstprogrammprofil löschen

Dienstprogrammverwaltung (Utility Maintenance) aufrufen

Um die Utility Maintenance aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) die Option **Maintenance**.

Es wird ein Fenster angezeigt.

2 Markieren Sie im Fenster den Objekttyp **Utility** mit einem Zeichen oder mit dem Cursor.

Die **Utility Maintenance**-Auswahlliste wird angezeigt.

Sie zeigt alle Dienstprogramme (Utilities) an, für die entweder ein Standardprofil oder eine Vorlage definiert wurde. Zu jedem Dienstprogramm werden die folgenden Informationen angezeigt:

Feld	Erläuterung
Default	Standard. Zeigt an, ob ein Standardprofil für dieses Dienstprogramm definiert wurde (`YES/NO`). `NO` bedeutet, dass nur eine Vorlage definiert wurde.
User	Benutzer. Zeigt an, ob benutzerspezifische Profile für dieses Dienstprogramm vorhanden sind (`YES/NO`).
Library	Bibliothek. Zeigt an, ob bibliotheksspezifische Profile für dieses Dienstprogramm vorhanden sind (`YES/NO`).
User-Lib.	Zeigt an, ob benutzerbibliotheksspezifische Profile für dieses Dienstprogramm vorhanden sind (`YES/NO`).

Funktionen der Dienstprogrammverwaltung

Aus der **Utility Maintenance**-Auswahlliste können Sie alle Funktionen zum Anlegen, Ändern, Löschen und Anzeigen von einzelnen Dienstprogrammprofilen aufrufen.

Folgende Funktionen stehen zur Verfügung:

Code	Funktion
DD	Standardprofil oder Vorlage anzeigen. Diese Funktion zeigt das für ein Dienstprogramm definierte Standardprofil (bzw. die Vorlage) an.
Funktionen für *benutzerspezifische* Dienstprogrammprofile:	
DU	Benutzerspezifische Profile anzeigen. Diese Funktion zeigt eine Liste der vorhandenen benutzerspezifischen Profile für ein Dienstprogramm an. Aus der Liste können Sie die Profile auswählen, die angezeigt werden sollen.
AU	Benutzerspezifische Profile anlegen oder verwalten. Mit dieser Funktion wird eine Liste von Benutzern (vom Typ `A`, `P` und `G`) angezeigt. Aus der Liste können Sie die Benutzer auswählen, für die Sie benutzerspezifische Profile für ein Dienstprogramm definieren möchten.
MU	Benutzerspezifische Profile verwalten. Diese Funktion zeigt eine Liste der vorhandenen benutzerspezifischen Profile für ein Dienstprogramm an. Aus der Liste können Sie die zu verwaltenden Profile auswählen.
Funktionen für *bibliotheksspezifische* Dienstprogrammprofile:	

Code	Funktion
DL	Bibliotheksspezifische Profile anzeigen. Diese Funktion zeigt eine Liste der vorhandenen bibliotheksspezifischen Profile für ein Dienstprogramm an. Aus der Liste können Sie die Profile auswählen, die angezeigt werden sollen.
AL	Bibliotheksspezifische Profile anlegen oder verwalten. Mit dieser Funktion wird eine Liste von Bibliotheken angezeigt. Aus der Liste können Sie die Bibliotheken auswählen, für die Sie bibliotheksspezifische Dienstprogrammprofile definieren möchten.
ML	Bibliotheksspezifische Profile verwalten. Diese Funktion zeigt eine Liste der vorhandenen bibliotheksspezifischen Profile für ein Dienstprogramm an. Aus der Liste können Sie die Profile auswählen, die verwaltet werden sollen.
Funktionen für *benutzerbibliotheksspezifische* Dienstprogrammprofile:	
DX	Benutzerbibliotheksspezifische Profile anzeigen. Diese Funktion zeigt eine Liste der vorhandenen benutzerbibliotheksspezifischen Profile eines bestimmten Benutzers für ein Dienstprogramm an. Aus der Liste können Sie die Profile auswählen, die angezeigt werden sollen.
AX	Benutzerbibliotheksspezifische Profile anlegen oder verwalten. Diese Funktion zeigt eine Liste von Bibliotheken an. Aus der Liste können Sie die Bibliotheken auswählen, für die Sie benutzerbibliotheksspezifische Dienstprogrammprofile für einen bestimmten Benutzer definieren möchten.
MX	Benutzerbibliotheksspezifische Profile verwalten. Diese Funktion zeigt eine Liste der vorhandenen benutzerbibliotheksspezifischen Profile eines bestimmten Benutzers für ein Dienstprogramm an. Aus der Liste können Sie die zu verwaltenden Profile auswählen.

"Add oder Maintain" oder "Maintain"

Es gibt folgende Unterschiede bei den oben aufgelisteten Funktionen:

- **Funktionen zum Anlegen oder Verwalten**
  Die „Add oder Maintain"-Funktionen mit den Codes `AU`, `AL` und `AX` aufgerufen werden können, zeigen Listen aller Benutzer/Bibliotheken an, sowohl derjenigen, für die Dienstprogrammprofile existieren, als auch derjenigen, für die keine Dienstprogrammprofile definiert wurden.

  Sie ermöglichen das Anlegen neuer Dienstprogrammprofile sowie das Ändern, Löschen und Anzeigen vorhandener Dienstprogrammprofile.

- **Funktionen zum Verwalten**
  Die „Maintain“-Funktionen (Codes `MU`, `ML`, `MX`) zeigen nur die Listen der Benutzer/Bibliotheken an, für die Dienstprogrammprofile vorhanden sind.

  Sie ermöglichen es, bestehende Dienstprogrammprofile zu ändern, zu löschen und anzuzeigen.

Sie können direkt von „Anlegen oder Verwalten“ auf „Verwalten“ umschalten, indem Sie die angezeigte Liste von einer Liste aller Benutzer/Bibliotheken auf eine Liste derjenigen mit vorhandenen Profilen reduzieren: Markieren Sie in der Listenüberschrift das Auswahlkriterium `U` (benutzerspezifisches Profil vorhanden), `L` (bibliotheksspezifisches Profil vorhanden) bzw. `U-L` (benutzerbibliotheksspezifisches Profil vorhanden) mit `X`.

Wenn Sie jedoch schon vorher wissen, dass Sie nur bestehende Profile verwalten, aber keine neuen anlegen wollen, empfiehlt es sich (zwecks besserer Performance), direkt die Codes `MU`, `ML` bzw. `MX` zu verwenden.

Startwerte - Start Values

Jede der aufgeführten Funktionen zeigt eine Liste von Bestandteilen (Benutzer, Bibliotheken, Profile) an. Wenn Sie eine Funktion aufrufen, wird ein Fenster angezeigt, in dem Sie einen Startwert für die Liste der anzuzeigenden Bestandteile eingeben können.

Bei Funktionen, die sich auf *benutzerbibliotheksspezifische* Profile beziehen, muss im Startwertfenster auch die Kennung des Benutzers angegeben werden, dessen benutzerbibliotheksspezifische Profile aufgelistet werden sollen.

Unterfunktionen - Subfunctions

Wenn Sie eine der aufgeführten Funktionen aufrufen, erhalten Sie eine Liste von Bestandteilen (Benutzer, Bibliotheken oder Dienstprogrammprofile).

Markieren Sie in dieser Liste einen oder mehrere Bestandteile mit einem Code, um eine Subfunktion aufzurufen, die mit dem Bestandteil ausgeführt werden soll.

Die verfügbaren Unterfunktionen (Anlegen, Ändern usw.) unterscheiden sich je nach der aufgerufenen Funktion.

Um eine Liste der verfügbaren Unterfunktionen zu erhalten, können Sie ein Fragezeichen (?) in das Feld Co eingeben.

Angezeigte Informationen

Add/Maintain/Display User-Specific Utility Profiles

(Benutzerspezifische Dienstprogrammprofile anlegen/verwalten/anzeigen)

In der Auswahlliste der Benutzer, die mit den Funktionscodes AU, DU und MU angezeigt werden, werden für jeden Benutzer die folgenden Informationen angezeigt:

Type	Zeigt den Benutzertyp an (A, P oder G).
U	Ein X zeigt an, dass der Benutzer ein benutzerspezifisches Profil für dieses Dienstprogramm hat.
U-L	in X zeigt an, dass der Benutzer ein oder mehrere benutzerbibliotheksspezifische Profile für dieses Dienstprogramm hat.

Add/Maintain/Display Library-Specific Utility Profiles

(Bibliotheksspezifische Dienstprogrammprofile anlegen/verwalten/anzeigen)

In der Auswahlliste der Bibliotheken, die mit den Funktionscodes AL, DL und ML angezeigt werden, werden für jede Bibliothek die folgenden Informationen angezeigt:

Prot.	Zeigt die Einstellungen „people-protected“ (personengeschützt) und „terminal-protected“ (terminalgeschützt) an, die im Sicherheitsprofil der Bibliothek definiert sind.
Link	(leer)
L	Ein X zeigt an, dass die Bibliothek ein bibliothekspezifisches Profil für dieses Dienstprogramm hat.
U	Ein X zeigt an, dass die Bibliothek ein oder mehrere bibliotheksspezifische Profile für dieses Dienstprogramm hat.

Add/Maintain/Display User-Library-Specific Utility Profiles

(Benutzerbibliothekspezifische Dienstprogrammprofile anlegen/verwalten/anzeigen)

In der Auswahlliste der Bibliotheken, die mit den Funktionscodes AX, DX und MX angezeigt werden, werden für jede Bibliothek die folgenden Informationen angezeigt:

Prot.	Zeigt die im Sicherheitsprofil der Bibliothek definierten Einstellungen „people-protected“ (personengeschützt) und „terminal-protected“ (terminalgeschützt) an.
Link	Zeigt an, ob der Benutzer mit der Bibliothek verlinkt ist (LK = normaler Link, SL = spezieller Link).
U-L	Ein X zeigt an, dass der Benutzer ein benutzerbibliotheksspezifisches Profil für diese Bibliothek für dieses Dienstprogramm hat.
L	Ein X zeigt an, dass die Bibliothek ein bibliotheksspezifisches Profil für dieses Dienstprogramm hat.

Benutzerspezifisches Dienstprogrammprofil anlegen

Ein benutzerspezifisches Dienstprogrammprofil kann nur für ein Dienstprogramm definiert werden, für das entweder ein *Standardprofil* oder eine *Vorlage* existiert.

Um ein benutzerspezifisches Dienstprogrammprofil anzulegen:

1 Markieren Sie in der **Utility Maintenance**-Auswahlliste das gewünschte Dienstprogramm mit `AU`.

Es erscheint ein Fenster, in dem Sie einen Startwert für die anzuzeigende Liste der Benutzer eingeben können. Anschließend wird eine Liste der Benutzer (vom Typ `A`, `P` und `G`) angezeigt.

2 Markieren Sie in dieser Liste den gewünschten Benutzer mit `AD`.

Es wird das benutzerspezifische Profil für das Dienstprogramm zum Definieren angezeigt.

Die Optionen, die Sie innerhalb des Profils erlauben oder nicht erlauben können, sind dieselben wie im entsprechenden Standardprofil oder in der Vorlage (siehe *Bestandteile von Dienstprogrammprofilen* unten).

Die anfangs „erlaubten/nicht erlaubten“ Einstellungen im benutzerspezifischen Profil werden aus dem Standardprofil oder der Vorlage übernommen.

Benutzerspezifisches Dienstprogrammprofil ändern/anzeigen

Um ein benutzerspezifisches Dienstprogrammprofil zu ändern oder anzuzeigen:

1 Markieren Sie in der **Utility Maintenance**-Auswahlliste das gewünschte Dienstprogramm mit `MU` bzw. `DU`.

Es wird ein Fenster angezeigt, in dem Sie einen Startwert für die Liste der anzuzeigenden benutzerspezifischen Profile eingeben können.

Anschließend wird eine Liste der vorhandenen benutzerspezifischen Profile für das ausgewählte Dienstprogramm angezeigt.

2 Markieren Sie in dieser Liste das gewünschte Profil mit `MO` (Ändern) bzw. `DU` (Anzeigen).

Das Dienstprogrammprofil wird zur Änderung/Anzeige angezeigt.

Die Optionen, die Sie innerhalb des Dienstprogrammprofils erlauben oder nicht erlauben können, sind dieselben wie im entsprechenden Standardprofil oder in der Vorlage (siehe *Bestandteile von Dienstprogrammprofilen* unten).

Benutzerspezifisches Dienstprogrammprofil löschen

Um ein benutzerspezifisches Dienstprogrammprofil zu löschen:

1 Markieren Sie in der **Utility Maintenance**-Auswahlliste das gewünschte Dienstprogramm mit `MU`.

Es wird ein Fenster angezeigt, in dem Sie einen Startwert für die Liste der anzuzeigenden benutzerspezifischen Profile eingeben können.

2 Markieren Sie in dieser Liste das gewünschte Profil mit `DE`.

3 Es wird ein Fenster angezeigt, in dem Sie den Löschvorgang bestätigen müssen.

Wenn Sie ein benutzerspezifisches Dienstprogrammprofil löschen, werden auch alle *benutzerbibliotheksspezifischen* Dienstprogrammprofile für diesen Benutzer für dieses Dienstprogramm gelöscht.

Bibliotheksspezifisches Dienstprogrammprofil anlegen

Ein bibliotheksspezifisches Dienstprogrammprofil kann nur für ein Dienstprogramm definiert werden, für das ein Standardprofil (nicht nur eine Vorlage) definiert wurde.

Um ein bibliotheksspezifisches Dienstprogrammprofil anzulegen:

1 Markieren Sie in der **Utility Maintenance**-Auswahlliste das gewünschte Dienstprogramm mit `AL`.

Ein Fenster wird angezeigt, in dem Sie einen Startwert für die Liste der anzuzeigenden Bibliotheken eingeben können. Anschließend wird eine Liste von Bibliotheken angezeigt

2 Markieren Sie in dieser Liste die gewünschte Bibliothek mit `AD`.

Es wird das benutzerspezifische Profil für das Dienstprogramm zum Definieren angezeigt.

Die Optionen, die Sie innerhalb des Dienstprogrammprofils erlauben oder nicht erlauben können, sind dieselben wie im entsprechenden Standardprofil (siehe ***Bestandteile von Dienstprogrammprofilen*** unten).

Die anfangs „erlaubten/nicht erlaubten“-Einstellungen im bibliotheksspezifischen Profil werden aus dem Standardprofil übernommen.

Bibliotheksspezifisches Dienstprogrammprofil ändern/anzeigen

Um ein bibliotheksspezifisches Dienstprogrammprofil zu ändern oder anzuzeigen:

1 Markieren Sie das gewünschte Dienstprogramm in der **Utility Maintenance**-Auswahlliste mit `ML` bzw. `DL`.

Es wird ein Fenster angezeigt, in dem Sie einen Startwert für die Liste der anzuzeigenden bibliotheksspezifischen Profile eingeben können.

Anschließend wird eine Liste der vorhandenen bibliotheksspezifischen Profile für das ausgewählte Dienstprogramm angezeigt.

2 Markieren Sie in dieser Liste das gewünschte Profil mit `MO` (Ändern) bzw. `DL` (Anzeigen).

Das Profil wird zum Ändern/Anzeigen angezeigt.

Die Optionen in dem Profil sind dieselben wie in dem entsprechenden Standardprofil (siehe *Bestandteile von Dienstprogrammprofilen* unten).

Bibliotheksspezifisches Dienstprogrammprofil löschen

Um ein bibliotheksspezifisches Dienstprogrammprofil zu löschen:

1 Markieren Sie das gewünschte Dienstprogramm in der **Utility Maintenance**-Auswahlliste mit `ML`.

Es wird ein Fenster angezeigt, in dem Sie einen Startwert für die Liste der anzuzeigenden bibliotheksspezifischen Profile eingeben können.

Anschließend wird eine Liste der vorhandenen bibliotheksspezifischen Profile für das ausgewählte Dienstprogramm angezeigt.

2 Markieren Sie in dieser Liste das gewünschte Profil mit `DE`.

3 Es wird ein Fenster angezeigt, in dem Sie das Löschen bestätigen müssen.

Benutzerbibliotheksspezifisches Dienstprogrammprofil anlegen

Ein benutzerbibliotheksspezifisches Dienstprogrammprofil kann nur für einen Benutzer definiert werden, für den ein *benutzerspezifisches Profil* für dieses Dienstprogramm existiert.

Um ein benutzerbibliotheksspezifisches Dienstprogrammprofil anzulegen:

1 Markieren Sie das gewünschte Dienstprogramm in der **Utility Maintenance**-Auswahlliste mit `AX`.

Es erscheint ein Fenster, in dem Sie die Kennung des Benutzers eingeben müssen, für den ein benutzerbibliotheksspezifisches Profil definiert werden soll. Außerdem können Sie einen Startwert für die Liste der anzuzeigenden Bibliotheken eingeben.

Anschließend wird eine Liste der Bibliotheken angezeigt.

2 Markieren Sie in dieser Liste die gewünschte Bibliothek mit `AD`.

Das benutzerbibliotheksspezifische Profil für den angegebenen Benutzer für diese Bibliothek wird angezeigt und kann jetzt von Ihnen definiert werden.

Die Optionen, die Sie innerhalb des Profils erlauben oder nicht erlauben können, sind dieselben wie im entsprechenden Standardprofil (siehe *Bestandteile von Dienstprogrammprofilen* unten).

Die anfangs „erlaubten/nicht erlaubten“ Einstellungen im benutzerbibliotheksspezifischen Profil werden aus dem entsprechenden bibliotheksspezifischen Profil übernommen. Wenn kein solches Profil existiert, werden sie aus dem entsprechenden benutzerspezifischen Profil übernommen.

Benutzerbibliotheksspezifisches Dienstprogrammprofil ändern oder anzeigen

Um ein benutzerbibliotheksspezifisches Dienstprogrammprofil zu ändern oder anzuzeigen:

1 Markieren Sie das gewünschte Dienstprogramm in der **Utility Maintenance**-Auswahlliste mit `MX` bzw. `DX`.

Es erscheint ein Fenster, in dem Sie die Kennung des Benutzers eingeben müssen, dessen benutzerbibliotheksspezifische(s) Profil(e) aufgelistet werden soll(en). Außerdem können Sie einen Startwert für die Liste der anzuzeigenden Profile eingeben.

Anschließend wird eine Liste der vorhandenen benutzerbibliotheksspezifischen Profile des angegebenen Benutzers für das ausgewählte Dienstprogramm angezeigt.

2 Markieren Sie in dieser Liste das gewünschte Profil mit `MO` (Ändern) bzw. `DX` (Anzeigen).

Das Profil wird zum Ändern bzw. Anzeigen angezeigt.

Die Optionen in dem Profil sind dieselben wie im entsprechenden Standardprofil (siehe *Bestandteile von Dienstprogrammprofilen* unten).

Benutzerbibliotheksspezifisches Dienstprogrammprofil löschen

Um ein benutzerbibliotheksspezifisches Dienstprogrammprofil zu löschen:

1 Markieren Sie das gewünschte Dienstprogramm in der **Utility Maintenance**-Auswahlliste mit `MX`.

Es erscheint ein Fenster, in dem Sie die Kennung des Benutzers eingeben müssen, dessen benutzerbibliotheksspezifische(s) Profil(e) aufgelistet werden soll(en). Außerdem können Sie einen Startwert für die Liste der anzuzeigenden Profile eingeben.

Anschließend wird eine Liste der vorhandenen benutzerbibliotheksspezifischen Profile des angegebenen Benutzers für das ausgewählte Dienstprogramm angezeigt.

2 Markieren Sie in dieser Liste das gewünschte Profil mit `DE`.

3 Es wird ein Fenster angezeigt, in dem Sie das Löschen bestätigen müssen.

Bestandteile von Dienstprogrammprofilen

Ein Dienstprogrammprofil bietet mehrere Optionen, die den Funktionen des betreffenden Dienstprogramms entsprechen. Diese Optionen sind in allen Profilen, die sich auf dieses Dienstprogramm beziehen, gleich: Standardprofil, benutzerspezifische, bibliotheksspezifische und benutzerbibliotheksspezifische Profile.

Die einzelnen Optionen werden im Folgenden für jedes Dienstprogramm beschrieben:

- PROFILER-Dienstprogramm
- SYSBPM-Dienstprogrammprofile
- SYSCP-Dienstprogrammprofile
- SYSDB2-Dienstprogrammprofile
- SYSDDM-Dienstprogrammprofile
- SYSERR-Dienstprogrammprofile
- SYSMAIN-Dienstprogrammprofile
- SYSOBJH-Dienstprogrammprofile (Object Handler)
- Dienstprogrammprofile für SYSPARM Utility
- Dienstprogrammprofile für SYSPCI Utility
- Dienstprogrammprofile für SYSRPC Utility
- Dienstprogrammprofile für ZIIP-Systemkommando

- Zusätzliche Optionen in Standardsicherheitsprofilen für Dienstprogramme

PROFILER-Dienstprogramm

Die Profile für das Dienstprogramm `PROFILER` bieten mehrere Optionen. Jede Option entspricht der gleichnamigen `PROFILER`-Funktion. Durch Erlauben/Nicht-Erlauben einer Option bestimmen Sie, ob der Benutzer die entsprechende Funktion verwenden darf.

SYSBPM-Dienstprogrammprofile

Das Dienstprogramm `SYSBPM` ist nur bei Natural auf Großrechnern verfügbar.

Die Profile für das Dienstprogramm `SYSBPM` bieten mehrere Optionen. Jede Option entspricht der gleichnamigen `SYSBPM`-Funktion bzw. dem gleichnamigen `SYSBPM`-Kommando. Durch Erlauben/Nicht-Erlauben einer Option bestimmen Sie, ob der Benutzer die entsprechende Funktion/das entsprechende Kommando verwenden darf.

SYSCP-Dienstprogrammprofile

Die Profile für das Dienstprogramm `SYSCP` (Natural Code Page Administration Utility) bieten mehrere Optionen. Jede Option entspricht der gleichnamigen Funktion der Natural-Codepage-Verwaltung. Durch Erlauben/Nicht-Erlauben einer Option bestimmen Sie, ob der Benutzer die entsprechende Funktion verwenden darf.

SYSDB2-Dienstprogrammprofile

Das Dienstprogramm `SYSDB2` (Natural Tools for Db2) ist nur bei Natural auf Großrechnern verfügbar.

Die Profile für das Dienstprogramm `SYSDB2` bieten mehrere Optionen. Jede Option entspricht der gleichnamigen Funktion bzw. dem gleichnamigen Kommando von Natural Tools for DB2. Durch das Erlauben/Nicht-Erlauben einer Option bestimmen Sie, ob der Benutzer die entsprechende Funktion/das entsprechende Kommando verwenden darf.

SYSDDM-Dienstprogrammprofile

Das Dienstprogramm `SYSDDM` ist nur bei Natural auf Großrechnern und Linux verfügbar (unter Linux heißt es „DDM Services“).

Die Profile für das Dienstprogramm `SYSDDM` bieten mehrere Optionen. Jede Option entspricht der gleichnamigen `SYSDDM`-Funktion. Durch das Erlauben/Nicht-Erlauben einer Option bestimmen Sie, ob der Benutzer die entsprechende Funktion verwenden darf.

SYSERR-Dienstprogrammprofile

Die Profile für das Dienstprogramm SYSERR bieten die folgenden Optionen:

Option	Erläuterung
Add New Messages	Sie können festlegen, ob der Benutzer die gleichnamigen SYSERR-Funktionen verwenden darf.
Delete Messages	
Display Messages	
Modify Messages	
Print Messages	
Scan in Messages	
Select Messages from a List	
Translate Messages into Another Language	

Sie können diese Optionen separat erlauben/nicht erlauben für:

- Benutzermeldungen (PF7),
- Natural-Systemmeldungen (PF8).

Darüber hinaus können Sie nach erneutem Drücken von PF8 die Verwendung der folgenden SYSERR-Direktkommandos erlauben oder nicht erlauben:

Kommando	Erläuterung
EXPORT	Mögliche Werte für jedes Kommando: ■ A = Das Kommando ist für alle Benutzer erlaubt. ■ R = Das Kommando ist eingeschränkt: Es ist nur für Natural Security-Administratoren erlaubt. ■ D = Das Kommando ist für alle Benutzer nicht erlaubt.
IMPORT	
LAYOUT	
NEXT	
RESTART	
SAMPLE	
SHIFT	
TRACE	
USER	

SYSMAIN-Dienstprogrammprofile

Da das Dienstprogramm SYSMAIN nicht auf allen Plattformen identisch ist, sind einige SYSMAIN-Optionen/Funktionen möglicherweise auf einigen Plattformen nicht verfügbar.

Da das Dienstprogramm SYSMAIN kann auf zwei Arten aufgerufen werden:

- mit dem Natural-Systemkommando SYSMAIN,
- über die Anwendungsprogrammierschnittstelle MAINUSER.

Standardmäßig gelten die Dienstprogrammprofile, die für das Dienstprogramm SYSMAIN definiert wurden, für beide Aufrufarten. Es ist jedoch möglich, einen separaten Satz von Dienstprogrammprofilen zu definieren, die die Verwendung von SYSMAIN-Funktionen steuern, wenn diese über MAINUSER aufgerufen werden. Einzelheiten dazu finden Sie bei der **MAINUSER API** im Abschnitt *Zusätzliche Optionen* weiter unten.

Die Profile für das Dienstprogramm SYSMAIN bieten die folgenden Optionen:

Option	Erläuterung
Programming Objects	Diese allgemeine Einstellung in der ersten Spalte des Bildschirms legt fest, ob der Benutzer das Dienstprogramm SYSMAIN überhaupt für diesen Objekttyp verwenden darf. Ist diese Einstellung auf D (Disallowed/nicht erlaubt) gesetzt, müssen alle untergeordneten Funktionsspezifikationen für diesen Objekttyp ebenfalls auf D gesetzt sein.
Debug Environments	
User Messages	
DDMs	
Natural Messages	
Profiles	
Rules	
Resources	
Predict Sets (on mainframes only)	

Darüber hinaus können Sie die folgenden Funktionen für jeden Objekttyp einzeln erlauben/nicht erlauben:

Option	Legt fest, ob der Benutzer die SYSMAIN-Funktion für diesen Objekttyp verwenden darf:
Co	COPY
De	DELETE
Fi	FIND
Im	IMPORT
Li	LIST
Mo	MOVE
Ren	RENAME
Rep	REPLACE

Option	Legt fest, ob der Benutzer die SYSMAIN-Funktion für diesen Objekttyp verwenden darf:
FNAT	SET FNAT
FSEC	SET FSEC (*)
FDIC	SET FDIC (*)

(*) Diese Optionen können im Standardprofil und in benutzerspezifischen Profilen gestzt werden, nicht aber in bibliotheks- oder benutzerbibliotheksspezifischen Profilen.

SYSOBJH-Dienstprogrammprofile (Object Handler)

Die Profile für das Dienstprogramm `SYSOBJH` (Natural Object Handler) bieten die folgenden Optionen:

Option	Erläuterung
Unload	Legt fest, ob der Benutzer die gleichnamigen Object Handler-Funktionen verwenden darf.
UnDeLi	
Load	
Delete	
Scan	

Darüber hinaus können Sie die folgenden Funktionen für jeden Objekttyp einzeln erlauben/nicht erlauben:

Option	Legt fest, ob die Funktion angewendet werden darf auf:
Nat	Natural-Programmierobjekte.
Err	Fehlermeldungen.
CPr	Kommandoprozessoren.
NRe	Natural-bezogene Objekte.
Ext	Externe Objekte.
FDT	Adabas FDTs.
MfD	Großrechner-DDMs.
MfR	Großrechner-bezogene Objekte.
App	Anwendungen.

Weitere funktionsbezogene Optionen, die erlaubt/nicht erlaubt werden können::

Option	Legt fest, ob die Funktion angewendet werden darf auf:
Del (*)	Diese Option legt fest, ob der Object Handler-Parameter DELETEALLOWED für die Funktion angegeben werden darf.
Par (*)	Diese Option legt fest, ob Object Handler-Parameter für die Funktion angegeben werden dürfen.
Rep	Diese Option legt fest, ob der Object Handler-Parameter REPLACE für die Funktion angegeben werden darf.

(*) Diese Optionen können nur in benutzerspezifischen Profilen gesetzt werden. Ihre Einstellungen in den benutzerspezifischen Profilen gelten auch für die bibliotheksspezifischen und benutzerbibliotheksspezifischen Profile.

Anmerkung: In bibliotheksspezifischen und benutzerbibliotheksspezifischen Profilen können Optionen, die nicht bibliotheksbezogene Objekttypen betreffen, die sind, weder erlaubt noch nicht erlaubt werden.

Außerdem bieten die Profile für SYSOBJH die folgenden allgemeinen Optionen:

Option	Erläuterung
Admin	Legt fest, ob der Benutzer den Abschnitt **Admin** des Object Handlers verwenden darf.
FSEC	Legt fest, ob der Benutzer die gleichnamigen Object Handler-Parameter angeben darf.
FDIC	
Transfer only	■ Y = Es darf nur das Transferformat verwendet werden (verarbeitet nur Quellcodes). ■ N = Transfer und interne Formate können verwendet werden (verarbeitet Quellcodes und katalogisierte Objekte).

In den Profilen für SYSOBJH können Sie auch die folgenden Direktkommandos des Object Handlers zulassen oder verbieten:

Kommando	Erläuterung
Navigationskommandos:	
GO	Sie können festlegen, ob der Benutzer die gleichnamigen Direktkommandos des Object Handlers verwenden darf.
- GO HOME	
- GO UNLOAD	
- GO LOAD	
- GO SCAN	
- GO RESTART	
- GO ADMIN	
- GO VIEW	
- GO FIND	
Konfigurationskommandos:	

Kommando	Erläuterung
SET	Sie können festlegen, ob der Benutzer die gleichnamigen Direktkommandos des Object Handlers verwenden darf.
- SET TRACE ON	
- SET TRACE WORKFILE	
- SET TRACEFILE	
- SET FREE ON/OFF	
- SET EXECUTIONMSG ON/OFF	
- SET ADVANCEDCMD ON/OFF	
Anzeigekommandos:	
SHOW	Sie können festlegen, ob der Benutzer die gleichnamigen Direktkommandos des Object Handlers verwenden darf.
- SHOW LAST RESULT	
- SHOW LAST MESSAGE	
- SHOW PROFILE	
- SHOW REPORT	
- SHOW STATUS	
- SHOW TRACE	
Sonstige Kommandos:	
CHANGE WORKPLAN LIBRARY	Sie können festlegen, ob der Benutzer die gleichnamigen Direktkommandos des Object Handlers verwenden darf.
CLEAR	
INIT	
READ PROFILE (*)	
SETTINGS	

(*) Die Verwendung dieses Kommandos hängt auch von der Benutzersicherheitsprofiloption **Profile Maintenance** ab (beschrieben im Kapitel *Benutzer verwalten*).

Dienstprogrammprofile für SYSPARM Utility

Das Dienstprogramm `SYSPARM` ist nur bei Natural for z/OS verfügbar.

Die Profile für das Dienstprogramm `SYSPARM` bieten mehrere Optionen. Jede Option entspricht der `SYSPARM`-Funktion mit demselben Namen. Durch das Erlauben/Nicht-Erlauben einer Option bestimmen Sie, ob der Benutzer die entsprechende Funktion verwenden darf.

Dienstprogrammprofile für SYSPCI Utility

Das Dienstprogramm SYSPCI ist nur bei Natural für Linux und Windows verfügbar.

Die Profile für das Dienstprogramm SYSPCI bieten mehrere Optionen. Jede Option entspricht der SYSPCI-Funktion mit demselben Namen. Durch das Erlauben/Nicht-Erlauben einer Option bestimmen Sie, ob der Benutzer die entsprechende Funktion verwenden darf.

Dienstprogrammprofile für SYSRPC Utility

Die Profile für das Dienstprogramm SYSRPC bieten mehrere Optionen. Jede Option entspricht der SYSRPC-Funktion mit demselben Namen. Durch das Erlauben/Nicht-Erlauben einer Option bestimmen Sie, ob der Benutzer die entsprechende Funktion verwenden darf.

Dienstprogrammprofile für ZIIP-Systemkommando

ZIIP ist zwar ein Natural System Kommando, aber aufgrund seiner Komplexität wird es von Natural Security jedoch wie ein Dienstprogramm behandelt. ZIIP ist nur bei Natural for z/OS verfügbar.

Die Dienstprogrammprofile für ZIIP bieten mehrere Optionen. Jede Option entspricht der gleichnamigen ZIIP-Funktion. Durch Erlauben/Nicht-Erlauben einer Option legen Sie fest, ob der Benutzer die entsprechende Funktion verwenden darf.

Zusätzliche Optionen in Standardsicherheitsprofilen für Dienstprogramme

Die folgenden zusätzlichen Optionen sind im Teil **Additional Options** der Standardsicherheitsprofile aller Dienstprogramme enthalten. Sie können nur in den Standardprofilen eingestellt werden, nicht aber in einzelnen benutzerspezifischen, bibliotheksspezifischen oder benutzerbibliotheksspezifischen Profilen. Bei jedem Dienstprogramm gelten die Einstellungen der zusätzlichen Optionen für alle Dienstprogrammprofile, die sich auf das jeweilige Dienstprogramm beziehen.

Wenn Sie auf dem Basis-Bildschirm eines Standardprofils für ein Dienstprogramm PF4 drücken, wird ein Fenster angezeigt, in dem Sie die folgenden Optionen auswählen können:

- Maintenance Information (Verwaltungsinformationen)
- Security Notes (Sicherheitsvermerke)
- Owners (Eigentümer)
- Session Options (Sitzungsoptionen)

Die Optionen, bei denen schon etwas angegeben oder definiert wurde, sind mit einem Pluszeichen (+) gekennzeichnet.

Sie können ein oder mehrere Elemente aus dem Fenster auswählen, indem Sie sie mit einem beliebigen Zeichen markieren. Für jedes ausgewählte Element wird ein weiteres Fenster angezeigt.

Additional Option	Erläuterung
Maintenance Information (nur Anzeige)	Verwaltungsinformationen. In diesem Fenster werden die folgenden Informationen angezeigt: ■ Das Datum und die Uhrzeit, zu der das Sicherheitsprofil erstellt wurde, die Kennung des Administrators, der es angelegt hat, und (falls zutreffend) die Kennungen der Miteigentümer, die für das Anlegen gegengezeichnet haben. ■ Das Datum und die Uhrzeit der letzten Änderung des Sicherheitsprofils, die Kennung des Administrators, der die letzte Änderung vorgenommen hat, und (falls zutreffend) die Kennungen der Miteigentümer, die für die Änderung gegengezeichnet haben.
Security Notes	Sicherheitsvermerke. Hier können Sie Anmerkungen zum Sicherheitsprofil eingeben.
Owners	Eigentümer. In diesem Fenster können Sie bis zu acht Kennungen von Administratoren eingeben. Nur die hier angegebenen Administratoren sind berechtigt, dieses Dienstprogrammprofil zu verwalten. Wird kein Eigentümer angegeben, kann jeder Benutzer des Typs Administrator das Sicherheitsprofil verwalten. Bei jedem Eigentümer kann optional die Anzahl der Miteigentümer, deren Gegenzeichnung für die Verwaltungsberechtigung erforderlich ist, in dem Feld hinter der Kennung angegeben werden. Informationen zu Eigentümern und Miteigentümern finden Sie im Kapitel *Gegenzeichnungen*.
Session Options	Sitzungsoptionen, siehe unten.

Sitzungsoptionen - Session Options

Wenn Sie **Session Options** im Fenster **Additional Options** mit einem beliebigen Zeichen markieren, wird das Fenster **Session Options** angezeigt, in dem Sie die folgenden Optionen einstellen können:

Option	Erläuterung
Access Recorded	Zugriff aufgezeichnet. Diese Option legt fest, ob der Zugriff der Benutzer auf das Dienstprogramm aufgezeichnet werden soll oder nicht. ■ `Y` = Jedes Mal, wenn ein Benutzer das Dienstprogramm aufruft, wird von Natural Security ein Datensatz geschrieben. Sie können die Verwendung des Dienstprogramms durch Einsicht in diese Zugriffsaufzeichnungen überprüfen (weitere Informationen finden Sie unter *Anmeldesätze - Logon Records* im Kapitel *Administrator Services*). ■ `N` = Der Zugriff auf das Dienstprogramm wird nicht aufgezeichnet.
Privileged Groups	Mit dieser Option können Sie die Reihenfolge beeinflussen, in der Natural Security nach dem anzuwendenden Dienstprogrammprofil sucht. Sie bestimmt, ob Dienstprogrammprofile, die für Gruppen definiert sind, die in einem Benutzersicherheitsprofil als Privilegierte Gruppen (**Privileged Groups**) angegeben sind, Teil der Suchreihenfolge sind oder nicht. Siehe Abschnitt *Welches Dienstprogramm-Profil wird angewendet?* .

Option	Erläuterung
	■ Y = Benutzerbibliotheksspezifische und benutzerspezifische Profile von privilegierten Gruppen sind Teil der Suchreihenfolge. ■ N = Privilegierte Gruppen haben keinen Einfluss auf die Suchreihenfolge. Wenn die Option ***GROUP Only** (siehe unten) auf Y gesetzt ist, muss diese Option auf N gesetzt werden.
*GROUP Only	Mit dieser Option können Sie die Reihenfolge beeinflussen, in der Natural Security nach dem passenden Dienstprogrammprofil sucht, das angewendet werden soll: ■ Y = Benutzerbibliotheksspezifische und benutzerspezifische Profile der aktuellen Gruppe (wie durch den Wert der Natural-Systemvariablen *GROUP bestimmt) sind Teil der Suchreihenfolge, die aller anderen Gruppen, in denen der Benutzer enthalten ist, jedoch nicht. ■ N = Benutzerbibliotheksspezifische und benutzerspezifische Profile aller Gruppen, in denen der Benutzer enthalten ist, sind Teil der Suchreihenfolge. Weitere Informationen finden Sie im Abschnitt *Welches Dienstprogramm-Profil wird angewendet?* . Wenn die Option **Privileged Groups** (siehe oben) auf Y gesetzt ist, muss diese Option auf N gesetzt werden.
MAINUSER API	Diese Option ist nur für das Dienstprogramm SYSMAIN verfügbar. Sie steuert die Verwendung von SYSMAIN-Funktionen, die über die Anwendungsprogrammierschnittstelle (API) MAINUSER aufgerufen werden. Wenn Sie diese Option auf Y setzen, wird ein separater Eintrag mit dem Namen MAINUSER auf dem Bildschirm **Define Utility Defaults/Templates** erstellt. Damit können Sie einen separaten Satz von Dienstprogrammprofilen erstellen, um die Verwendung von SYSMAIN-Funktionen beim Aufruf über die MAINUSER-API zu erlauben/nicht zu erlauben. Diese Profile sind unabhängig von den „normalen“ Dienstprogrammprofilen, die die Verwendung von SYSMAIN-Funktionen steuern, wenn sie über das Kommando SYSMAIN aufgerufen werden. Die Komponenten der MAINUSER-Dienstprogrammprofile sind die gleichen wie die der **SYSMAIN-Dienstprogrammprofile**.
Utilities option	Diese Option ist nur für die Dienstprogramme SYSMAIN und SYSOBJH (Object Handler) verfügbar. Sie kann verwendet werden, um die Option **Utilities** in Bibliothekssicherheitsprofilen auf diese Dienstprogramme anzuwenden. ■ Y = Die Option **Utilities** in einem Bibliothekssicherheitsprofil legt fest, wer SYSMAIN/SYSOBJH verwenden darf, um den Inhalt der Bibliothek zu bearbeiten. ■ O = Gleich wie Y. Wenn die Option **Utilities** in einem Bibliothekssicherheitsprofil auf O gesetzt ist und ein Eigentümer eine Gegenzeichnung anfordert, wird die Aufforderung zur Gegenzeichnung unterdrückt. Stattdessen wird die Bibliothek von der Verarbeitung durch SYSMAIN/SYSOBJH ausgeschlossen.

Option	Erläuterung
	■ N = Die Option **Utilities** in Bibliothekssicherheitsprofilen hat keine Wirkung bei SYSOBJH. Sie hat keine Wirkung bei SYSMAIN, wenn kein Dienstprogrammprofil für SYSMAIN definiert ist.
Xref option	Diese Option ist nur für die Dienstprogramme SYSMAIN auf Großrechnern und SYSOBJH verfügbar. Sie legt fest, wie Predict-Cross-Referenzdaten, die sich auf die mit diesen Dienstprogrammen verarbeiteten Objekte beziehen, behandelt werden. ■ * = Es gilt die Option **Cross-reference** in den Bibliothekssicherheitsprofilen (dies ist die Standardeinstellung). ■ N = Es gilt die Xref-Option, die im Dienstprogramm selbst eingestellt ist. ■ Ein Objekt und seine Cross-Referenzdaten können nur verarbeitet werden, wenn für dieses Objekt Cross-Referenzdaten vorhanden sind. ■ D = Ein Objekt kann nur verarbeitet werden, wenn es in Predict dokumentiert ist. Eventuell vorhandene Cross-Referenzdaten werden ebenfalls verarbeitet. ■ F = Ein Objekt und seine Cross-Referenzdaten können nur bearbeitet werden, wenn das Objekt in Predict dokumentiert ist und wenn Cross-Referenzdaten dazu existieren. ■ S = Ein Objekt kann unabhängig davon bearbeitet werden, ob es Cross-Referenzdaten hat oder nicht. Eventuell vorhandene Cross-Referenzdaten werden ebenfalls bearbeitet.
Enable Unrestricted Use of Libraries	Uneingeschränkte Nutzung von Bibliotheken aktivieren: Diese Option ist nur für das Dienstprogramm SYSMAIN verfügbar. Sie kann verwendet werden, um Benutzern vom Typ Administrator die uneingeschränkte Nutzung von Bibliotheken mit SYSMAIN zu ermöglichen. ■ N = Administratoren haben keine speziellen Rechte für die Verwendung von Bibliotheken mit SYSMAIN. ■ Y = Administratoren dürfen SYSMAIN-Funktionen bei allen in Natural Security definierten Bibliotheken anwenden - unabhängig von etwaigen Zugriffsbeschränkungen, die für diese Bibliotheken bestehen. Damit ein Administrator dies tun kann, muss die Option **Process All Libraries** (siehe unten) in seinem benutzerspezifischen SYSMAIN-Dienstprogrammprofil auf A gesetzt sein.
Nur für benutzerspezifische SYSMAIN-Dienstprogrammprofile:	
Process All Libraries	Alle Bibliotheken verarbeiten: Diese Option kann nur in benutzerspezifischen SYSMAIN-Dienstprogrammprofilen von Benutzern des Typs Administrator gesetzt werden, und auch nur dann, wenn im SYSMAIN-Standardprofil die Option **Enable Unrestricted Use of Libraries** (siehe oben) auf Y gesetzt ist. ■ N = Der Benutzer darf SYSMAIN-Funktionen zur Bearbeitung des Inhalts von Bibliotheken nur im Rahmen der geltenden Zugriffsbeschränkungen verwenden. ■ A = Der Benutzer darf mit SYSMAIN-Funktionen den Inhalt *aller* in Natural Security definierten Bibliotheken bearbeiten - *unabhängig* von den Zugriffsbeschränkungen, die für diese Bibliotheken möglicherweise bestehen.

15 Natural Development Server-Umgebung und -Anwendungen schützen

- Natural Development Server-Umgebung schützen 298
- Natural Development Server-Anwendungen schützen 305

In diesem Kapitel werden die folgenden Themen behandelt:

Natural Development Server-Umgebung schützen

In diesem Abschnitt wird beschrieben, wie Sie die Natural Development Server-Umgebung mit Natural Security schützen und wie sich die Sicherheitsdefinitionen in der FSEC-Systemdatei, die der Serverumgebung zugeordnet ist, auf Aktionen auf dem Server auswirken.

Folgende Themen werden behandelt:

- Client- und Server-Aktionen
- Map Environment und Bibliotheksauswahl
- Schützbare Funktionen in der gemappten Umgebung

Client- und Server-Aktionen

Generell ist zu unterscheiden zwischen:

- Natural-Aktionen, die in der Server-Umgebung verarbeitet werden,
- Natural-Aktionen, die nur in der Client-Umgebung verarbeitet werden.

Wenn ein Natural Development Server unter der Kontrolle von Natural Security läuft, können nur Aktionen auf dem Server durch Natural Security geschützt werden. Die von Natural Security festgelegten Nutzungsbedingungen, die für eine Benutzersitzung auf dem *Server* gelten, werden *nicht* auf eine *Client*-Sitzung übertragen.

Beachten Sie auch, dass einige Aktionen, die auf einem Natural Development Server-Client (gemappte Umgebung) ausgeführt werden, einen Aufruf des Natural Development Server-Servers erzeugen, während andere nicht dazu führen. Nur wenn eine Client-Aktion eine Aktion auf dem Natural Development Server auslöst, unterliegt die daraus resultierende Server-Aktion der Kontrolle von Natural Security.

Map Environment und Bibliotheksauswahl

Die Funktion **Map Environment** wird durch die Natural Security-Einstellungen gesteuert, die für die FNAT-Systemdatei gelten, auf der diese Funktion ausgeführt wird. Wenn die Funktion ausgeführt wird, führt Natural Security eine Anmeldung gemäß den Regeln durch, die unter ***Vorgehensweise bei der Anmeldung*** beschrieben sind. Die Anmeldung erfolgt bei der Standardbibliothek des Benutzers. Daher müssen die Sicherheitseinstellungen so gewählt werden, dass sich der Benutzer bei seiner Standardbibliothek anmelden kann.

Anmerkung: Sobald die Umgebung gemappt wurde, ist eine Anmeldung mit einer anderen Benutzerkennung innerhalb der zugeordneten Umgebung nicht mehr möglich.

Nachdem die Umgebung gemappt wurde, werden in der Baumansicht (Tree View) der gemappten Umgebung alle nicht leeren Bibliotheken der Systemdatei (FUSER/FNAT) aufgelistet, die der gemappten Umgebung zugeordnet sind und auf die der Benutzer Zugriff hat. Bibliotheken, in deren Sicherheitsprofilen eine andere FUSER-Datei oder FDIC-Datei angegeben ist (unter **Library File**), werden nicht aufgelistet.

Wenn der Benutzer eine dieser Bibliotheken in der Baumansicht auswählt, wird eine Anmeldung bei dieser Bibliothek durchgeführt - nach den Regeln, die unter ***Vorgehensweise bei der Anmeldung*** beschrieben sind. So kann es z.B. sein, dass eine Startup-Transaktion ausgeführt wird. Wenn die Ausführung von Startup-Transaktionen nicht erwünscht ist, kann sie durch Setzen der Option **NDV Startup Inactive** unterdrückt werden (siehe ***Voreingestellte Werte für Bibliothekssicherheitsprofile - Library Preset Values*** im Kapitel *Administrator Services*).

Der Benutzer kann eine Bibliothek nur in der Baumansicht auswählen. Eine andere Bibliotheksauswahl (z. B. über das Systemkommando `LOGON *`) ist nicht möglich.

Innerhalb einer Bibliothek in der gemappten Umgebung können einige Funktionen durch Natural Security geschützt werden, andere können nicht geschützt werden. Welche Funktionen dies sind, wird im Folgenden beschrieben.

Schützbare Funktionen in der gemappten Umgebung

Die Verwendung der folgenden Funktionen in einer Bibliothek innerhalb der gemappten Umgebung kann folgendermaßen geschützt werden:

- Baumansicht-Aktionen - Tree-View Actions
- Übertragungsoperationen
- Kommandozeilenaktionen
- Systemkommandos
- Kommandos LIST DDM und EDIT DDM
- Funktionen in der Menüleiste

Baumansicht-Aktionen - Tree-View Actions

Anmerkung: Mehrere der unten aufgeführten Aktionen in der Baumansicht (Tree View) werden von SYSMAIN-Dienstprogrammprofilen gesteuert. Wenn jedoch keine Dienstprogrammprofile für SYSMAIN definiert sind, werden diese Aktionen durch die Option **Utilities** im Bibliothekssicherheitsprofil der bearbeiteten Bibliothek gesteuert.

Position in Baumansicht	Aktion	Gesteuert durch
System-file node Systemdateiknoten	List library Bibliothek auflisten	Die Aktion als solche ist immer erlaubt und kann nicht unterbunden werden. Was aufgelistet wird, finden Sie unter *Map Environment und Bibliotheksauswahl* oben.
	Find object Objekt suchen	*Client-Aktion, die nicht vom Server validiert wird.*
Library node Bibliotheksknoten	Open source Quellcodeobjekt öffnen	Kommandoeinschränkungen (Kommando `LIST`) im Bibliothekssicherheitsprofil*.
	New source Neues Quellcodeobjekt	Kommandoeinschränkungen (Kommando `EDIT`) und Editiereinschränkungen im Bibliothekssicherheitsprofil*.
	Catall Objekt katalogisieren	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
	Find object Quellcodeobjekt durchsuchen	Kommandoeinschränkungen (Kommando `SCAN`) im Bibliothekssicherheitsprofil*.
	Rename ** Umbenennen	Die Aktion als solche ist immer erlaubt und kann nicht unterbunden werden. Es muss jedoch ein Bibliothekssicherheitsprofil für die Bibliothek mit dem neuen Namen existieren (es sei denn, die allgemeine Option **Transition Period Logon** ist auf `Y` gesetzt). Damit der Bibliotheksinhalt übertragen werden kann, muss außerdem die Option **Mo** (Move) für das Verschieben von Bibliothek (**from library**) und nach Bibliothek (**to library**) für alle Objekttypen im SYSMAIN-Dienstprogrammprofil erlaubt sein.
	Delete ** Löschen	Option **De** (Delete) für den Objekttyp im SYSMAIN-Dienstprogrammprofil.
	Cut Ausschneiden	Option **Co** (Copy) **from library** für Objekttyp in SYSMAIN-Dienstprogrammprofil.
	Copy Kopieren	Option **Mo** (Move/Verschieben) von Bibliothek (**from library**) für den Objekttyp im SYSMAIN-Dienstprogrammprofil.
	Drag Ziehen	Option **Co** (Copy/Kopieren) oder **Mo** (Move/Verschieben) von Bibliothek (**from library**) für den Objekttyp im SYSMAIN-Dienstprogrammprofil.

Position in Baumansicht	Aktion	Gesteuert durch
	Paste / Drop Einfügen / Ablegen	Option **Co** (Copy/Kopieren) oder **Mo** (Move/Verschieben) von Bibliothek (**from library**) für den Objekttyp im SYSMAIN-Dienstprogrammprofil.
Group node Gruppenknoten	Open Öffnen	Kommandoeinschränkungen (`LIST`-Kommando) im Bibliothekssicherheitsprofil*.
	New Neu	Bearbeitungseinschränkungen im Bibliothekssicherheitsprofil*.
	Catall Katalogisieren (kompilieren) und speichern	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
	Find Suchen	Kommandoeinschränkungen (Kommando `SCAN`) im Bibliothekssicherheitsprofil*.
	Delete Löschen	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
	Cut Ausschneiden	Option **Mo** (Move) **from library** für Objekttyp in SYSMAIN-Dienstprogrammprofil.
	Copy Kopieren	Option **Co** (Copy) **from library** für den Objekttyp im SYSMAIN-Dienstprogrammprofil.
	Drag Ziehen	Option **Co** (Kopieren) oder **Mo** (Verschieben) **from library** für Objekttyp in SYSMAIN-Dienstprogrammprofil.
	Paste / Drop Einfügen / Ablegen	Option **Co** (Copy) oder **Mo** (Move) **to library** für den Objekttyp im SYSMAIN-Dienstprogrammprofil.
Object node Objektknoten	Open Öffnen	Bearbeitungseinschränkungen im Bibliothekssicherheitsprofil*.
	List Auflisten	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
	Catalog Katalogisieren (kompilieren)	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
	Stow In Quellcode- und Objektform speichern	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.

Position in Baumansicht	Aktion	Gesteuert durch
	Execute Ausführen	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
	Debug Debuggen (Diagnose, Fehlerbehebung)	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
	Find Suchen	Kommandoeinschränkungen (Kommando SCAN) im Bibliothekssicherheitsprofil*.
	Rename Umbenennen	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
	Delete Löschen	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
	Cut Ausschneiden	Option **Mo** (Move) **from library** für Objekttyp in SYSMAIN-Dienstprogrammprofil.
	Copy Kopieren	Option **Co** (Copy) **from library** für Objekttyp in SYSMAIN-Dienstprogrammprofil.
	Drag Ziehen	Option **Co** (Copy) oder **Mo** (Move) **from library** für Objekttyp in SYSMAIN-Dienstprogrammprofil.
	Paste / Drop Einfügen / Ablegen	Option **Co** (Copy) oder **Mo** (Move) **to library** für Objekttyp in SYSMAIN-Dienstprogrammprofil.

* oder Special-Link-Sicherheitsprofil

** Diese Aktionen können im Kontextmenü des Bibliotheksknotens durch die Option **Disable Rename and Delete of Library Node** (beschrieben im Kapitel *Administrator Services*) nicht unverfügbar gemacht werden.

Position in Baumansicht	Aktion	Gesteuert durch
DDM node DDM-Knoten	Open Öffnen	Option **List** im SYSDDM-Dienstprogrammprofil. (*)
	New Neu	Option **Gen** im SYSDDM-Dienstprogrammprofil. (*)
	Cut	Option **Mo** (Move) **from library** für DDM im SYSMAIN-Dienstprogrammprofil.

Position in Baumansicht	Aktion	Gesteuert durch
	Ausschneiden	
	Copy Kopieren	Option **Co** (Copy) **from library** für DDM im SYSMAIN-Dienstprogrammprofil.
	Paste Einfügen	Option **Co** (Copy) oder **Mo** (Move) **to library** für DDM im SYSMAIN-Dienstprogrammprofil.
Object node Objektknoten	Open Öffnen	Option **Edit** im SYSDDM Utility-Profil. (*)
	Stow In Quellcode- und Objektform speichern	Option **Cat** im SYSDDM Utility-Profil. (*)
	Cat Katalogisieren (Kompilieren)	Option **Cat** im SYSDDM-Dienstprogrammprofil. (*)

(*) Wenn kein SYSDDM-*Dienstprogrammprofil* definiert ist, gelten die Kommandoeinschränkungen (**Command Restrictions**) im SYSDDM-*Bibliothekssicherheitsprofil*.

Übertragungsoperationen

Übertragungsoperationen, z. B. Verschieben (Move), Kopieren (Copy), und Löschoperationen für alle unterstützten Natural-Objekte werden von den SYSMAIN-Dienstprogrammprofilen gesteuert. Wenn jedoch keine Dienstprogrammprofile für SYSMAIN definiert sind, werden sie von der Option **Utilities** im Bibliothekssicherheitsprofil der bearbeiteten Bibliothek gesteuert). Ausnahme: Die Übertragung von DDMs wird durch die SYSDDM-Dienstprogrammprofile gesteuert.

Die folgenden Aktionen werden durch die folgenden SYSMAIN-Dienstprogrammprofil-Optionen gesteuert und vom Server validiert (außer wie angegeben):

Aktion	Option im SYSMAIN-Dienstprogrammprofil	Entsprechender Eintrag im Kontextmenü
List	Li	-
Find	*Client-Aktion, die nicht vom Server validiert wird.*	-
Copy	Co	Copy
Move	Mo	Cut und Paste
Delete	De	Delete
Rename	Ren	-
Import	*Client-Aktion, die nicht vom Server validiert wird.*	-

Diese Optionen können für jeden Objekttyp einzeln erlaubt/nicht erlaubt werden.

Kommandozeilenaktionen

Anmerkung: Einige der unten aufgeführten Kommandozeilenaktionen werden von SYSMAIN-Dienstprogrammprofilen gesteuert. Wenn jedoch keine Dienstprogrammprofile für SYSMAIN definiert sind, werden diese Aktionen durch die Option **Utilities** im Bibliothekssicherheitsprofil der bearbeiteten Bibliothek gesteuert.

Die folgenden Aktionen werden, wenn sie in die Kommandozeile von Natural Studio eingegeben werden, von den folgenden Natural Security-Einstellungen gesteuert und vom Server validiert (außer wie angegeben):

Aktion	Gesteuert durch
Edit object	Bearbeitungseinschränkungen im Bibliothekssicherheitsprofil*.
List object	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
Scratch	Option **De** (Delete) für Objekttyp im SYSMAIN-Dienstprogrammprofil.
Uncat	Option **De** (Delete) für Objekttyp im SYSMAIN-Dienstprogrammprofil.
Purge	Option **De** (Delete) für Objekttyp im SYSMAIN-Dienstprogrammprofil.
Save	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
Cat	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
Stow	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
Compopt	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
Scan	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
Unlock	Session-Option **Unlock Objects** im Benutzersicherheitsprofil.

* oder Special-Link-Sicherheitsprofil

Systemkommandos

Nur Natural- Systemkommandos, die auf dem Server verarbeitet werden, können durch Natural Security geschützt werden. Ihre Verwendung wird durch die Kommandoeinschränkungen im Bibliothekssicherheitsprofil (oder Special-Link-Sicherheitsprofil) gesteuert. Dazu gehören die folgenden Systemkommandos:

```
AIV, CATALL, CATALOG, CHECK, CLEAR, COMPOPT, EXECUTE, GLOBALS, HELP, LIST, MAIL,
PROFILE, READ, REGISTER, RETURN, RUN, SAVE, SCAN, SETUP, STOW, TEST, UNREGISTER,
UPDATE, XREF.
```

Kommandos LIST DDM und EDIT DDM

Wenn DDMs in einer Systemdatei gespeichert sind, die mit dem Natural-Profilparameter `FDIC` oder `FDDM` angegeben wurde, gilt Folgendes:

In Natural Studio ist der Kommando `EDIT DDM` auch innerhalb einer vom Benutzer angelegten Bibliothek verfügbar. Das bedeutet, dass es nicht notwendig ist, den DDM-Knoten in der Baumansicht zu erweitern, um ein bestimmtes DDM bearbeiten zu können. Die Verwendung der Kommandos `LIST DDM` und `EDIT DDM` in einer Serverumgebung kann jedoch nur über das Sicherheitsprofil des Natural-Dienstprogramms SYSDDM eingeschränkt werden.

Funktionen in der Menüleiste

Die Benutzung der Funktion **Development Tools > Error Messages**, die über die Menüleiste aufgerufen wird, wird durch die Profile des SYSERR-Dienstprogramms gesteuert.

Die Benutzung der Funktion **Development Tools > Object Handler**, die über die Menüleiste aufgerufen wird, wird durch die Profile des SYSERR-Dienstprogramms gesteuert.

Natural Development Server-Anwendungen schützen

In diesem Abschnitt wird beschrieben, wie Sie den Zugriff auf Basisanwendungen (Base Applications) und Verbundanwendungen (Compound Applications) mit Natural Security kontrollieren können.

Folgende Themen werden behandelt:

- Anwendungen schützen
- Bestandteile eines Anwendungsprofils
- Anwendungsverwaltung aufrufen
- Anwendung zur Bearbeitung auswählen
- Neues Anwendungsprofil anlegen
- Anwendungsprofil kopieren
- Anwendungsprofil ändern
- Anwendungsprofil umbenennen
- Anwendungsprofil löschen
- Anwendungsprofil anzeigen

- Benutzer mit Anwendungen verlinken

Anwendungen schützen

Dieser Abschnitt behandelt folgende Themen:

- Was sind Anwendungen?
- Voraussetzungen
- Generelles Konzept
- Namenskonventionen
- Hierarchien bei Anwendungsprofilen
- Informationen für Predict-Benutzer
- Anwendungssicherheit definieren und aktivieren

Was sind Anwendungen?

Anwendungen sind *Basisanwendungen* (Base Applications) und *Verbundanwendungen* (Compound Applications), die im Anwendungsarbeitsbereich (im Folgenden „Application Workspace“) von Natural Studio erstellt und gepflegt und in Verbindung mit dem Natural Development Server verwendet werden.

Informationen zu Basisanwendungen und Verbundanwendungen finden Sie in der *Natural Development Server*-Dokumentation.

Sofern nicht anders angegeben, umfasst der Begriff „Anwendung“ in der Natural Security-Dokumentation sowohl Basisanwendungen als auch Verbundanwendungen.

Voraussetzungen

Für den Schutz von Anwendungen in der Development Server-Datei müssen die folgenden Voraussetzungen erfüllt sein:

- Der Natural Development Server muss an Ihrem Standort installiert sein (wie bei der Installation in der *Natural Development Server*-Dokumentation beschrieben).
- Es muss eine Development Server-Datei definiert sein. Diese Definition ist Teil des Natural Development Server-Installationsvorgangs.
- Die verwendete FSEC-Systemdatei muss die Anwendungsprofile `* Base Application *` und `* Compound Application *` enthalten. Diese beiden Profile werden sowohl bei der Installation von Natural Security als auch bei der Installation von Natural Development Server automatisch erstellt und in der FSEC-Datei gespeichert.
- Die aktuelle Natural Security-Sitzung muss eine Development Server-Datei verwenden.

Generelles Konzept

Der Schutz von Anwendungen ist nur in Verbindung mit dem Natural Development Server relevant. Wenn Sie den Natural Development Server nicht verwenden, brauchen Sie sich um den Anwendungsschutz in Natural Security nicht zu kümmern.

Wenn Sie den Natural Development Server einsetzen, sollten Sie Natural Security verwenden, um den Zugriff auf Anwendungen in der Development Server-Datei zu kontrollieren.

Indem Sie eine Anwendung schützen, steuern Sie den Zugriff der Benutzer auf die Anwendung, d. h. Sie bestimmen, ob Benutzer die Anwendung im Application Workspace von Natural Studio lesen, anlegen, ändern oder löschen dürfen. Diese Zugriffsrechte werden in einem Anwendungssicherheitsprofil definiert.

Der Anwendungsschutz in Natural Security wirkt sich nur auf den Zugriff auf die Anwendung als solche aus. Er hat keine Auswirkungen auf den Zugriff auf die in den Bibliotheken enthaltenen Natural-Programmierobjekte, die Teil der Anwendung sein können.

Namenskonventionen

Die Anwendungskennungen (Application IDs) in Natural Security müssen den Namenskonventionen für Anwendungen entsprechen, die im Natural Development Server definiert sind. Natural Security prüft diese Übereinstimmung.

Hierarchien bei Anwendungsprofilen

Die Installationsverfahren für Natural Security und für den Natural Development Server erstellen automatisch zwei Anwendungssicherheitsprofile mit den Anwendungskennungen `* Base Application *` und `* Compound Application *`. Dies sind die grundlegenden Sicherheitsprofile, die für alle Basisanwendungen bzw. Verbundanwendungen gelten, für die keine individuellen Sicherheitsprofile definiert sind. Die Zugriffseinstellungen in den beiden Basisprofilen sind standardmäßig alle auf `N` voreingestellt. Sie können sie Ihren Anforderungen entsprechend ändern.

Die Namenskonventionen für den Natural Development Server ermöglichen es Ihnen, bei Anwendungsprofilen eine Hierarchie einzurichten: Wenn Sie ein Anwendungssicherheitsprofil für eine Anwendung erstellen, deren Kennung (ID) eine bestimmte Zeichenkette ist, gilt das Profil für alle Anwendungen, deren Kennung mit dieser Zeichenkette beginnt. Sie müssen also nicht für jede einzelne Anwendung ein Profil definieren.

Wenn Sie beispielsweise ein Sicherheitsprofil für eine Basisanwendung mit der Kennung `A` definieren, gilt das für alle Basisanwendungen, deren Kennung mit „A“ beginnt (wie APPLX, AA01, ABC, ADE usw.). Ein Profil mit der Kennung `ABC` würde wiederum z.B. für ABCA, ABCXYZ usw. gelten.

Stern als Standardzugriff

Eine solche Profilhierarchie kann verwendet werden, um die einzelnen **Standardzugriffsmethoden** (siehe unten), die innerhalb der Anwendungsprofile zu definieren sind, auf verschiedenen Ebenen zu erlauben/nicht zu erlauben. Wird ein Standardzugriff in einem Anwendungsprofil auf Stern (*) gesetzt, gilt für diese Zugriffsmethode die Einstellung im Profil auf der nächsthöheren Ebene.

Als Beispiel sei von den folgenden Basis-Anwendungsprofilen mit den folgenden Einstellungen ausgegangen:

Kennung (ID)	Einstellungen im Profil			
* Base Application *	Read=Y	Add=Y	Modify=Y	Delete=N
A	Read=*	Add=N	Modify=*	Delete=Y
ABC	Read=*	Add=*	Modify=N	Delete=*
ABCXYZ	Read=*	Add=N	Modify=*	Delete=N

Es gelten die folgenden Einstellungen:

Kennung (ID)	Applicable Settings	Erläuterung
ABCXYZ	Read ist erlaubt.	Die Read-Einstellung wird bestimmt durch "* Base Application *".
	Add ist nicht erlaubt.	Die Add-Einstellung wird bestimmt durch "ABCXYZ" itself.
	Modify ist nicht erlaubt.	Die Modify-Einstellung wird auf der nächsthöheren Ebene durch "ABC" bestimmt.
	Delete ist nicht erlaubt.	Die Delete-Einstellung wird bestimmt durch "ABCXYZ" selbst.
ABC	Read ist erlaubt.	Die Read-Einstellung wird bestimmt durch "* Base Application *".
	Add ist nicht erlaubt.	Die Add-Einstellung wird auf der nächsthöheren Ebene durch "A" bestimmt.
	Modify ist nicht erlaubt.	Die Modify-Einstellung wird bestimmt durch "ABC" selbst.
	Delete ist erlaubt.	Die Delete-Einstellung wird auf der nächsthöheren Ebene durch "A" bestimmt.
ADE	Read ist erlaubt.	Da für diese Anwendung kein Sicherheitsprofil definiert ist, werden ihre Einstellungen von der Anwendung bestimmt, die auf der nächsthöheren Ebene definiert ist, d. h. von "A".
	Add ist nicht erlaubt.	
	Modify ist erlaubt.	
	Delete ist erlaubt.	
A	Read ist erlaubt.	Die Read-Einstellung wird bestimmt durch "* Base Application *".
	Add ist nicht erlaubt.	Die Add-Einstellung wird bestimmt durch "A" selbst.
	Modify ist erlaubt.	Die Modify-Einstellung wird bestimmt durch "* Base Application *".
	Delete ist erlaubt.	Die Delete-Einstellung wird bestimmt durch "A" selbst.

Informationen für Predict-Benutzer

Die oben beschriebene Hierarchie entspricht der Hierarchie, die Sie für Predict-Dokumentationsobjekte einrichten können. Basis- und Verbundanwendungen entsprechen den Predict-Dokumentationsobjekten des Typs `System`, Untertypen `-B` bzw. `-O` (wie in der Predict-Dokumentation beschrieben).

Basis- und Verbundanwendungen erscheinen auch als Predict-Dokumentationsobjekte vom Typ `SY-B` und `SY-O` im Natural Security-Subsystem für **externe Objekte**. Es ist daher möglich, Anwendungsprofile entweder im Subsystem für die Verwaltung externer Objekte oder im Subsystem für die Verwaltung von Anwendungen zu verwalten. Es wird jedoch dringend empfohlen, nur das Anwendungssubsystem - und nicht das Subsystem für externe Objekte - für die Pflege von Anwendungsprofilen zu verwenden.

Anwendungssicherheit definieren und aktivieren

Innerhalb von Natural Security wird der Anwendungsschutz in zwei Schritten durchgeführt:

- die Definition der erforderlichen Sicherheitsprofile und Verlinkungen,
- die Aktivierung dieser Profile und Verlinkungen.

Sicherheitsprofile und Links definieren

Um den Zugriff auf eine Anwendung zu kontrollieren, müssen Sie die folgenden Sicherheitsprofile und Links definieren:

- Sie müssen ein Sicherheitsprofil für die *Bibliothek SYSDIC* erstellen (falls nicht bereits definiert). Im Sicherheitsprofil der Bibliothek SYSDIC muss die Option **People-protected** auf `Y` gesetzt werden.
- Erstellen Sie ein *Sicherheitsprofil für die Anwendung*, und legen Sie darin die Zugriffsrechte fest, die für die meisten Benutzer gelten sollen.
- Erstellen Sie ein *Gruppensicherheitsprofil* für alle Benutzer, die Zugang zu den Anwendungen haben sollen, und fügen Sie alle diese Benutzer der Gruppe hinzu.
- *Verlinken* Sie die Gruppe *mit der Bibliothek SYSDIC*. Ohne diesen Link ist der Zugriff auf die Anwendungen nicht möglich. Die Kennung (ID) dieses Links wird auch vom Natural Development Server als Sitzungsprofilkennung verwendet.
- Wenn einige Benutzer eingeschränkte oder erweiterte Zugriffsrechte haben sollen, erstellen Sie für jede Gruppe von Benutzern, die dieselben Zugriffsrechte haben sollen, ein weiteres Gruppensicherheitsprofil und fügen die Benutzer entsprechend zu den Gruppen hinzu.
- Anschließend *verlinken* Sie diese anderen Gruppen *mit der Anwendung* und legen ihre Zugriffsrechte im Link-Profil fest.
- Außerdem müssen Sie jede dieser Gruppen *mit der Bibliothek SYSDIC verlinken*.

Sicherheitsprofile und Links aktivieren

Um die Anwendungsprofile (und die zugehörigen Link-Profile) und die damit verbundenen Schutzmechanismen zu aktivieren, müssen Sie die Option **Activate Security for Development Server File** auf `Y` setzen (**Administrator Services Menu > General Options**). Solange diese Option auf `N` gesetzt ist, sind die Anwendungen in der Development Server-Datei nicht vor unberechtigtem Zugriff geschützt. Es wird empfohlen, dass Sie zunächst alle benötigten Anwendungsprofile, Gruppenprofile und Links anlegen, bevor Sie diese Option auf `Y` setzen.

Bestandteile eines Anwendungsprofils

Bestandteile eines Basisanwendungsprofils

Der folgende Bildschirmtyp ist der Profilbildschirm-Grundtyp, der angezeigt wird, wenn Sie eine der Funktionen Add (Anlegen), Copy (Kopieren), Modify (Ändern) oder Read/Display (Anzeigen) für ein Basis-Anwendungsprofil aufrufen:

```
14:15:03                    *** NATURAL SECURITY ***                2021-12-31
                           -Modify Base Application -

                                              Modified .. 2021-12-15 by SAG

Base Application ... XYZ-BASE


------ Default Access -------                            Library  DBID  FNR  NSC
Y R Read                                                 LIBA       123   10  N
* A Add                                                  LIBB       123   11  P
Y M Modify                                               LIBC       345   33  P
N D Delete




Additional Options ... N


Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help  PrevM Exit  AddOp MaLib Flip                                  Canc
```

Die einzelnen Bestandteile, die Sie als Teil eines Basisanwendungssicherheitsprofils definieren können, werden im Folgenden erläutert.

<table>
<tr><th>Feld</th><th>Erläuterung</th></tr>
<tr><td>Default Access</td><td>Standardzugriff. In dieser Spalte können Sie Zugriffsmethoden für das Anwendungsobjekt auf dem Natural Development Server erlauben oder nicht erlauben. Die möglichen Zugriffsmethoden sind:
<table>
<tr><td>R</td><td>Read: Lesen der Anwendung.</td></tr>
<tr><td>A</td><td>Add: Anlegen der Anwendung.</td></tr>
<tr><td>M</td><td>Modify: Ändern der Anwendung.</td></tr>
<tr><td>D</td><td>Delete: Löschen der Anwendung.</td></tr>
<tr><td colspan="2">Für jede Zugriffsmethode können Sie einen der folgenden Werte angeben:</td></tr>
<tr><td>Y</td><td>Die Zugriffsmethode ist erlaubt.</td></tr>
<tr><td>N</td><td>Die Zugriffsmethode ist nicht erlaubt.</td></tr>
<tr><td>*</td><td>Die Einstellung im Anwendungssicherheitsprofil auf der nächsthöheren Ebene in der Hierarchie (siehe Hierarchien von Anwendungsprofilen oben) bestimmt, ob die Zugriffsmethode erlaubt ist oder nicht erlaubt ist..</td></tr>
</table>
Wenn Sie den Lesezugriff (Read) auf N setzen, wird der Zugriff bei Add, Modify und Delete automatisch auf N gesetzt.

Wenn Sie den Zugriff auf Add, Modify oder Delete auf Y setzen, wird der Read-Zugriff automatisch auf Y gesetzt.

Wenn Sie den Read-Zugriff auf * setzen, können Sie den Zugriff auf Add, Modify und Delete nur auf N oder * setzen, aber nicht auf Y.

Die im Anwendungsprofil erlaubten/ nicht erlaubten Zugriffsmethoden gelten für alle Benutzer, für die kein spezieller Zugriff über einen Link definiert ist (Informationen zu Links finden Sie unter Benutzer mit Anwendungen verlinken weiter unten).</td></tr>
<tr><td>Library (nur Anzeige)</td><td>Bibliothek. Die Kennungen (IDs) der Bibliotheken, die mit der Anwendung auf dem Natural Development Server verknüpft sind.

Es werden bis zu 10 Bibliotheken auf einmal angezeigt. Wenn es mehr sind, können Sie mit PF7 und PF8 in der Liste der Bibliotheken blättern.

Wenn Sie PF5 drücken, können Sie die Bibliotheksverwaltung für die angezeigten Bibliotheken aufrufen. (Wenn Sie die Bibliotheksverwaltung von hier aus aufrufen, umfasst sie nur die Funktionen, die für die Verwaltung der mit der Anwendung verknüpften Bibliotheken relevant sind, und Sie können nur diese Bibliotheken verwalten).</td></tr>
<tr><td>DBID / FNR (nur Anzeige)</td><td>Zu jeder Bibliothek werden die Datenbankkennung und die Dateinummer der zugehörigen FUSER-Systemdatei angezeigt.</td></tr>
<tr><td>NSC (nur Anzeige)</td><td>Zu jeder Bibliothek werden Informationen über ihre Natural Security-Definition angezeigt:
<table>
<tr><td>leer</td><td>Die Bibliothek ist nicht in Natural Security definiert.</td></tr>
<tr><td>N</td><td>Die Bibliothek ist als nicht geschützt definiert (d. h. weder personen- noch terminalgeschützt).</td></tr>
</table></td></tr>
</table>

Feld	Erläuterung	
	P	Die Bibliothek ist als personengeschützt oder terminalgeschützt oder beides definiert.
	U	Die Bibliothek ist die private Bibliothek eines Benutzers.
	?	Die Bibliothek ist in Natural Security definiert, aber die FUSER DBID/FNR-Angaben im Bibliothekssicherheitsprofil stimmen nicht mit den im Anwendungssicherheitsprofil definierten überein.

Bestandteile eines Verbundanwendungsprofils

Bei dem folgenden Bildschirm handelt es sich um den Basis-Profilbildschirm, der angezeigt wird, wenn Sie eine der Funktionen Add (Anlegen), Copy (Kopieren), Modify (Ändern) oder Display (Anzeigen) für ein Verbundanwendungssicherheitsprofil aufrufen:

```
14:16:05                    *** NATURAL SECURITY ***                 2021-12-31
                        - Modify Compound Application -

                                              Modified .. 2021-09-15 by SAG

Compound Application ... XYZ-COMP


------ Default Access -------              Base Application                NSC
Y R Read                                   ABCB0012-BASE-APPL               X
* A Add                                    ABCB0015-BASE-APPL
Y M Modify                                 ABCB0019A01                      X
N D Delete









Additional Options ... N


Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help  PrevM Exit  AddOp MaBAp Flip                                  Canc
```

Die einzelnen Bestandteile, die Sie als Teil eines Verbundanwendungssicherheitsprofils definieren können, werden im Folgenden erläutert.

<table>
<tr><th>Feld</th><th>Erläuterung</th></tr>
<tr><td>Default Access</td><td>In dieser Spalte können Sie Zugriffsmethoden für das Anwendungsobjekt auf dem Natural Development Server erlauben oder nicht erlauben. Die möglichen Zugriffsmethoden sind:
<table>
<tr><td>R</td><td>Read: Lesen/Anzeigen der Anwendung.</td></tr>
<tr><td>A</td><td>Add: Anlegen der Anwendung.</td></tr>
<tr><td>M</td><td>Modify: Ändern der Anwendung.</td></tr>
<tr><td>D</td><td>Delete: Löschen der Anwendung.</td></tr>
<tr><td colspan="2">Bei jeder Zugriffsmethode können Sie einen der folgenden Werte angeben:</td></tr>
<tr><td>Y</td><td>Die Zugriffsmethode ist erlaubt.</td></tr>
<tr><td>N</td><td>Die Zugriffsmethode ist nicht erlaubt.</td></tr>
<tr><td>*</td><td>Die Einstellung im Anwendungssicherheitsprofil auf der nächsthöheren Ebene in der Hierarchie (siehe Hierarchien von Anwendungsprofilen oben) bestimmt, ob die Zugriffsmethode erlaubt ist oder nicht erlaubt ist.</td></tr>
</table>
Wenn Sie den Read-Zugriff auf N setzen, wird der Add-, Modify- und Delete-Zugriff automatisch auf N gesetzt.

Wenn Sie den Add-, Modify- oder Delete-Zugriff auf Y setzen, wird auch der Read-Zugriff automatisch auf Y gesetzt.

Wenn Sie den Read-Zugriff auf * setzen, können Sie den Add-, Modify- und Delete-Zugriff nur auf N oder * setzen, nicht aber auf Y.

Die im Anwendungsprofil erlaubten/nicht erlaubten Zugriffsmethoden gelten für alle Benutzer, für die kein spezieller Zugriff über einen Link definiert ist (Informationen zu Links finden Sie unter Benutzer mit Anwendungen verlinken weiter unten).</td></tr>
<tr><td>Base Application (nur Anzeige)</td><td>Basisanwendung. Die Kennungen der Basisanwendungen, die in der Verbundanwendung enthalten sind.

Es werden jeweils bis zu 10 Basisanwendungen angezeigt. Wenn es mehr sind, können Sie mit PF7 und PF8 in der Liste der Basisanwendungen blättern.

Wenn Sie PF5 drücken, können Sie die Anwendungsverwaltung (Application Maintenance) für diese Basisanwendungen aufrufen.</td></tr>
<tr><td>NSC (nur Anzeige)</td><td>
<table>
<tr><td>X</td><td>Die Basisanwendung ist in Natural Security definiert.</td></tr>
<tr><td>leer</td><td>Die Basisanwendung ist nicht in Natural Security definiert.</td></tr>
</table>
</td></tr>
</table>

Zusätzliche Optionen (Anwendungen) - Additional Options (Applications)

Wenn Sie das Feld **Additional Options** auf dem Basis-Bildschirm für das Sicherheitsprofil mit `Y` markieren, wird ein Fenster angezeigt, in dem Sie die folgenden Optionen auswählen können:

- Maintenance Information - Verwaltungsinformationen
- Security Notes - Sicherheitsvermerke
- Owners - Eigentümer

Die Optionen, für die schon etwas angegeben oder definiert wurde, sind mit einem Pluszeichen (+) gekennzeichnet.

Sie können ein oder mehrere Elemente aus dem Fenster auswählen, indem Sie sie mit einem beliebigen Zeichen markieren. Für jedes ausgewählte Element wird ein weiteres Fenster angezeigt:

Zusätzliche Option	Erläuterung
Maintenance Information (nur Anzeige)	Verwaltungsinformationen. Die folgenden Informationen werden angezeigt: ■ Das Datum und die Uhrzeit, zu der das Sicherheitsprofil erstellt wurde, die Kennung des Administrators, der es erstellt hat, und (falls zutreffend) die Kennungen der Miteigentümer, die für die Erstellung gegengezeichnet haben. ■ Das Datum und die Uhrzeit der letzten Änderung des Sicherheitsprofils, die Kennung des Administrators, der die letzte Änderung vorgenommen hat, und (falls zutreffend) die Kennungen der Miteigentümer, die die Änderung gegengezeichnet haben.
Security Notes	Sicherheitsvermerke. Hier können Sie Anmerkungen zum Sicherheitsprofil eingeben.
Owners	Eigentümer. Sie können bis zu acht Kennungen von Administratoren eingeben. Nur die hier angegebenen Administratoren sind berechtigt, das Sicherheitsprofil zu verwalten. Wenn kein Eigentümer angegeben wird, kann jeder Benutzer vom Typ Administrator das Sicherheitsprofil verwalten. Bei jedem Eigentümer kann optional die Anzahl der Miteigentümer, deren Gegenzeichnung für die Verwaltungsgenehmigung erforderlich ist, in dem Feld hinter der Kennung angegeben werden. Eine Erläuterung zu Eigentümern und Miteigentümern finden Sie im Kapitel *Gegenzeichnungen*.

Anwendungsverwaltung aufrufen

Die Anwendungsverwaltung kann nur aufgerufen werden, wenn die oben beschriebenen **Voraussetzungen** erfüllt sind.

Um die Anwendungsverwaltung aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) den Eintrag **Maintenance**.

Es wird ein Fenster angezeigt.

2 Markieren Sie in dem Fenster den Objekttyp **Application** mit einem Zeichen oder mit dem Cursor.

Die Auswahlliste **Application Maintenance** wird angezeigt.

3 In dieser Auswahlliste können Sie alle Funktionen der Anwendungsverwaltung wie unten beschrieben aufrufen.

Anwendung zur Bearbeitung auswählen

Wenn Sie die Funktion **Application Maintenance** aufrufen, wird eine Liste mit allen Anwendungsprofilen angezeigt, die in Natural Security definiert wurden.

Wenn Sie keine Liste aller vorhandenen Anwendungsprofile wünschen, sondern nur bestimmte Anwendungen aufgelistet haben möchten, können Sie die Optionen **Start Value** (Startwert) und **Type/Status** verwenden, siehe *Grundlagen der Benutzung*.

Wählen Sie im Hauptmenü (**Main Menu**) die Option **Maintenance**. Es wird ein Fenster angezeigt.

Markieren Sie in dem Fenster den Objekttyp **Application** mit einem Zeichen oder mit dem Cursor (und geben Sie, falls gewünscht, einen Startwert und/oder einen Anwendungstyp ein). Die Auswahlliste **Application Maintenance** wird angezeigt:

```
14:49:01                    *** NATURAL SECURITY ***                 2021-12-31
                          - Application Maintenance -

 Co Application                          Type Status Access  Message
 __ _____________________________________ ____  ____ ________ ________________________
 __ * Base Application *                 Base  NApp RAM
 __ A                                    Base  Defi * *D
 __ ABC                                  Base  Defi ** *
 __ ABCB0014-BASE-APPL                   Base  Defi RAMD
 __ ABCB0015-BASE-APPL                   Base  NApp RA
 __ ABCB0016-BASE-APPL                   Base  Defi RAMD
 __ ABCB0017-BASE-APPL                   Base  NApp RAM
 __ ABCXYZ                               Base  Defi * *
 __ ABCXYZ1                              Base  Defi RA
 __ ABCXYZ2                              Base  Defi R***
 __ * Compound Application *             Comp  NApp R
 __ COMP                                 Comp  Defi RAMD
 __ COMP-APPLIC                          Comp  Defi R**
 __ COMP-APPLIC-DEP                      Comp  Defi RAM*


Command ===>
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
Help        Exit              Flip  -     +                       Canc
```

Zu jeder Anwendung werden die Anwendungskennung, der Typ (`Base` oder `Comp`(ound)), der Status und die Standardzugriffsdefinition angezeigt.

In der Liste kann geblättert werden, siehe Kapitel *Grundlagen der Benutzung*.

Status als Auswahlkriterium

Wenn Sie nur bestimmte Anwendungen auflisten möchten, können Sie im Feld **Status** oberhalb der Liste eines der folgenden Auswahlkriterien angeben (mögliche Abkürzungen sind unterstrichen):

leer	Alle Anwendungssicherheitsprofile - unabhängig davon, ob eine entsprechende Anwendung existiert oder nicht.
ALL	Alle Anwendungen - unabhängig davon, ob ein entsprechendes Sicherheitsprofil definiert wurde oder nicht.
DEFI	Definiert, d.h. Anwendungen, für die Sicherheitsprofile definiert wurden.
UNDF	Nicht definiert, d. h. Anwendungen, für die keine Sicherheitsprofile definiert wurden.
NAPP	Keine Anwendung, d. h. Anwendungssicherheitsprofile, für die keine entsprechenden Anwendungen existieren.

Der Standardwert ist *leer*, d.h. alle Anwendungssicherheitsprofile werden aufgelistet.

Funktion auswählen

Die folgenden Funktionen zur Anwendungsverwaltung stehen zur Verfügung (mögliche Code-Abkürzungen sind unterstrichen):

Code	Funktion
AD	**Anwendung anlegen**
CO	**Anwendung kopieren**
MO	**Anwendung ändern**
RE	**Anwendung umbenennen**
DE	**Anwendung löschen**
DI	**Anwendung anzeigen**
LU	**Benutzer mit Anwendung verlinken**

Um eine Funktion für eine Anwendung aufzurufen, müssen Sie die Anwendung mit dem entsprechenden Funktionscode in Spalte **Co** markieren.

Sie können verschiedene Objekte für verschiedene Funktionen gleichzeitig auswählen, d.h. Sie können mehrere Anwendungen auf dem Bildschirm mit einem Funktionscode markieren. Für jede markierte Anwendung wird dann der entsprechende Bearbeitungsbildschirm angezeigt. Sie können dann für eine Anwendung nach der anderen die ausgewählten Funktionen ausführen.

Neues Anwendungsprofil anlegen

Um eine Anwendung in Natural Security zu definieren, müssen Sie ein Sicherheitsprofil für sie anlegen.

Sie können Sicherheitsprofile für Anwendungen anlegen, die bereits in der Development-Server-Datei vorhanden sind. Es ist aber auch möglich, Sicherheitsprofile für Anwendungen zu erstellen, die noch nicht in der Development-Server-Datei vorhanden sind, d.h. bevor die entsprechenden Anwendungen selbst in der Development-Server-Datei definiert sind.

Um ein Profil für eine existierende Anwendung anzulegen:

1 Geben Sie in der Auswahlliste **Application Maintenance** im Feld **Status** den Wert UNDF (d.h., nicht definiert) ein.

Es werden nur die Anwendungen aufgelistet, die noch nicht in Natural Security definiert worden sind.

In der Liste kann geblättert werden, siehe *Grundlagen der Benutzung*.

Die angezeigten Anwendungskennungen sind diejenigen, unter denen die Anwendungen in der Development-Server-Datei definiert sind.

2 Markieren Sie in der Liste die Anwendung, für die Sie ein Sicherheitsprofil anlegen möchten, mit dem Funktionscode `AD`.

3 Der Bildschirm **Add Application** wird angezeigt.

Die Bestandteile, die Sie definieren können, und alle zusätzlichen Fenster, die Teil eines Anwendungssicherheitsprofils sein können, sind unter ***Bestandteile eines Anwendungsprofils*** beschrieben.

Um ein Profil für eine nicht existierende Anwendung anzulegen:

1 Geben Sie in der Kommandozeile der Auswahlliste **Application Maintenance** das Kommando `ADD` ein.

2 Es wird ein Fenster angezeigt, in dem Sie eine Kennung (ID) für die Anwendung eingeben müssen. Diese Kennung muss mit den Namenskonventionen für Anwendungen übereinstimmen, die im Natural Development Server definiert sind. Natural Security prüft, ob die Kennung mit diesen Namenskonventionen übereinstimmt.

Je nachdem, von wo aus Sie das Fenster aufgerufen haben, müssen Sie eventuell auch den gewünschten Anwendungstyp (Base oder Compound) angeben.

3 Nachdem Sie eine gültige Kennung (ID) eingegeben (und den Anwendungstyp angegeben) haben, wird das Fenster **Add Application** angezeigt.

Die Bestandteile, die Sie auf diesem Bildschirm definieren können, und alle zusätzlichen Fenster, die Teil eines Anwendungssicherheitsprofils sein können, werden unter ***Bestandteile eines Anwendungsprofils*** beschrieben.

Wenn Sie ein neues Anwendungsprofil hinzufügen, werden die in Ihrem eigenen Benutzersicherheitsprofil angegebenen Eigentümer automatisch in das Anwendungssicherheitsprofil kopiert.

Anwendungsprofil kopieren

Mit der Funktion **Copy Application** können Sie eine neue Anwendung in Natural Security definieren, indem Sie ein Sicherheitsprofil erstellen, das mit einem bereits vorhandenen Anwendungssicherheitsprofil identisch ist.

Alle Bestandteile des bestehenden Sicherheitsprofils werden in das neue Sicherheitsprofil kopiert - *mit Ausnahme der Eigentümer* (diese werden aus Ihrem eigenen Benutzersicherheitsprofil in das neue Anwendungsicherheitsprofil kopiert).

Links von Benutzern zur bestehenden Anwendung werden *nicht* kopiert.

Um ein Anwendungsprofil zu kopieren:

1 Markieren Sie in der **Maintenance**-Auswahlliste die Anwendung, deren Sicherheitsprofil Sie duplizieren möchten, mit dem Funktionscode `CO`.

2 Es wird ein Fenster angezeigt, in dem Sie die Kennung der neuen Anwendung eingeben müssen. Die Kennung muss den Namenskonventionen des Natural Development Server entsprechen.

3 Nachdem Sie eine gültige Kennung eingegeben haben, wird das neue Sicherheitsprofil angezeigt.

Seine Bestandteile, die Sie definieren oder ändern können, sind unter *Bestandteile eines Anwendungsprofils* beschrieben.

Anwendungsprofil ändern

Mit der Funktion **Modify Application** können Sie ein bestehendes Anwendungssicherheitsprofil ändern.

Dazu:

1 Markieren Sie in der Auswahlliste **Application Maintenance** die Anwendung, deren Sicherheitsprofil Sie ändern möchten, mit dem Funktionscode `MO`.

2 Es wird das Sicherheitsprofil der ausgewählten Anwendung angezeigt.

Seine Bestandteile, die Sie definieren oder ändern können, sind unter *Bestandteile eines Anwendungsprofils* beschrieben.

Anwendungsprofil umbenennen

Mit der Funktion **Rename Application** können Sie die Anwendungskennung (ID) eines bestehenden Anwendungssicherheitsprofils ändern.

Dazu:

1 Markieren Sie in der Auswahlliste **Application Maintenance** die Anwendung, deren Kennung (ID) Sie ändern möchten, mit dem Funktionscode `RE`.

2 Es wird ein Fenster angezeigt, in dem Sie eine neue Kennung (ID) für das Anwendungsprofil eingeben können. Die Kennung muss den Namenskonventionen des Natural Development Server entsprechen.

Wenn Sie ein Anwendungssicherheitsprofil umbenennen, wird die Anwendung selbst nicht umbenannt.

Anwendungsprofil löschen

Mit der Funktion **Delete Application** können Sie ein bestehendes Anwendungssicherheitsprofil löschen.

Dazu:

1 Markieren Sie in der Auswahlliste **Application Maintenance** die Anwendung, deren Sicherheitsprofil Sie löschen möchten, mit dem Funktionscode `DE`.

2 Das Fenster **Delete Application** wird angezeigt.

- Wenn Sie sich gegen das Löschen des Anwendungssicherheitsprofils entscheiden, können Sie das Fenster verlassen, indem Sie ENTER drücken, ohne etwas eingegeben zu haben.
- Um das Anwendungssicherheitsprofil zu löschen, müssen Sie die Kennung (ID) der Anwendung in das Fenster eingeben, um den Löschvorgang zu bestätigen.

Wenn Sie ein Anwendungsprofil löschen, werden auch alle bestehenden Links zu diesem Anwendungsprofil gelöscht.

Wenn Sie ein Anwendungssicherheitsprofil löschen, wird die Anwendung selbst nicht gelöscht. Die Anwendungskennung (ID) verbleibt in der Auswahlliste **Application Maintenance** und der Status wird auf `UNDF` (nicht definiert) gesetzt.

Wenn Sie mehr als eine Anwendung mit `DE` markieren, wird ein Fenster angezeigt, in dem Sie gefragt werden, ob Sie die Löschung jedes einzelnen Anwendungssicherheitsprofils durch Eingabe der Anwendungskennung (ID) bestätigen möchten, oder ob alle zum Löschen ausgewählten Anwendungsprofile ohne Einzelbestätigung gelöscht werden sollen. Achten Sie darauf, dass Sie nicht versehentlich eine Anwendung löschen.

Anmerkung: Wenn eine Anwendung im Natural Development Server gelöscht wird, wird das zugehörige Natural Security-Anwendungsprofil nicht gelöscht, sondern sein Status wird auf `NAPP` (No Application/keine Anwendung) gesetzt.

Anwendungsprofil anzeigen

Mit der Funktion **Display Application** können Sie ein bestehendes Anwendungssicherheitsprofil anzeigen.

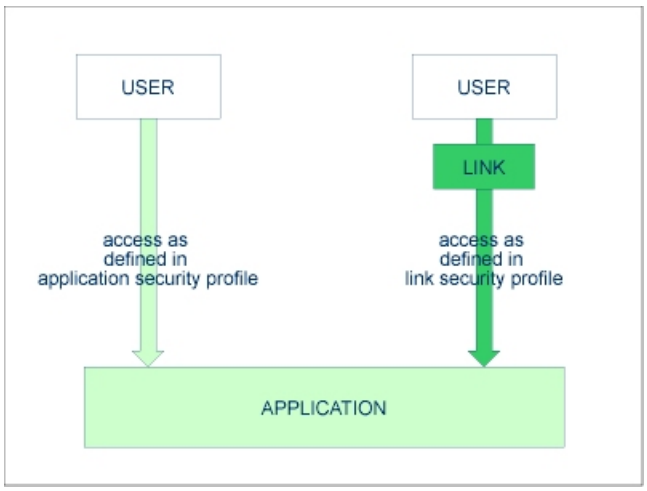
Dazu:

- Markieren Sie in der Auswahlliste **Application Maintenance** die Anwendung, deren Sicherheitsprofil Sie anzeigen möchten, mit dem Funktionscode `DI`.

Es wird das Sicherheitsprofil der ausgewählten Anwendung angezeigt. Seine Bestandteile sind unter *Bestandteile eines Anwendungsprofils* erläutert.

Benutzer mit Anwendungen verlinken

Die im Sicherheitsprofil einer Anwendung erlaubten/nicht erlaubten Zugriffsmethoden gelten für alle Benutzer, die nicht mit dieser Anwendung verlinkt sind. Wenn Sie einem einzelnen Benutzer mehr oder weniger Zugriffsmethoden erlauben wollen, können Sie den Benutzer mit der Anwendung verlinken und im Sicherheitsprofil des Links festlegen, welche Zugriffsmethoden für diesen bestimmten Benutzer verfügbar sein sollen. Das bedeutet, dass Sie durch die Verwendung von Links für verschiedene Benutzer unterschiedliche Zugriffsrechte auf dieselbe Anwendung festlegen können.



Nur Benutzer der Typen Administrator, Person und Gruppe (Group) können mit einer Anwendung verlinkt werden. Ein Administrator oder eine Person kann entweder direkt oder über eine Gruppe mit einer Anwendung verlinkt werden. Benutzer der Typen Mitglied (Member) und Terminal können nur über eine Gruppe mit einer Anwendung verlinkt werden, d.h. sie müssen einer Gruppe zugewiesen werden und die Gruppe muss mit der Anwendung verlinkt werden.

Um Verlinkungen zwischen Benutzern und Anwendungen herzustellen und zu verwalten, stehen zwei Funktionen zur Verfügung:

- Die Funktion **User Maintenance**, mit der Sie *einen Benutzer mit einer oder mehreren Anwendungen verlinken* können.
- Die Funktion **Application Maintenance**, mit der Sie *einen oder mehrere Benutzer mit einer Anwendung verlinken* können.

Die Funktionen werden im Folgenden beschrieben.

Einzelnen Benutzer mit Anwendungen verlinken

Um einen Benutzer mit einer oder mehreren Anwendungen zu verlinken:

1 Markieren Sie in der Auswahlliste **User Maintenance** den Benutzer, den Sie verlinken möchten mit dem Funktionscode `LA`.

2 Es erscheint ein Fenster, in dem Sie den Typ der Anwendungen (`Base`, `Compound` oder beide) auswählen können, mit denen Sie den Benutzer verlinken möchten.

Darüber hinaus bietet das Fenster die folgenden Optionen:

- **Start value - Startwert**
  Sie können einen Startwert (siehe *Grundlagen der Benutzung*) für die Auflistung der anzuzeigenden Anwendungen eingeben.
- **Selection criterion - Auswahlkriterium**
  Sie können eines der folgenden Auswahlkriterien angeben:

  `N` None/Kein Startwert. Alle Anwendungen werden aufgelistet.

  `L` Linked. Nur Anwendungen, mit denen der Benutzer bereits verlinkt ist, werden aufgelistet.

  `U` Unlinked: Nur Anwendungen, mit denen der Benutzer noch nicht verlinkt ist, werden aufgelistet.

3 Anschließend wird die Auswahlliste **Link User To Applications** angezeigt, die die Liste der Anwendungen zeigt.

In der Liste kann geblättert werden, siehe *Grundlagen der Benutzung*.

Markieren Sie in der Liste die Anwendungen, mit denen Sie den Benutzer verlinken möchten.

In der Spalte **Co** können Sie jede Anwendung mit einem der folgenden Funktionscodes markieren (mögliche Code-Abkürzungen sind unterstrichen):

Code	Funktion
`LK`	Link. Der Benutzer kann die Anwendung mit einem speziellen Sicherheitsprofil verwenden, das für den Link zu definieren ist. Das Linkprofil hat Vorrang vor dem Anwendungsprofil. Siehe *Link-Sicherheitsprofil anlegen und ändern (Anwendungen)* weiter unten.
`CL`	Cancel. Ein bestehender Link wird abgebrochen.
`DI`	Display Application. Das Sicherheitsprofil der Anwendung wird angezeigt.
`DL`	Display Link. Das Link-Sicherheitsprofil wird angezeigt.

Sie können eine oder mehrere Anwendungen auf dem Bildschirm mit einem Funktionscode markieren.

4 Für jedes markierte Objekt werden die ausgewählten Funktionen nacheinander ausgeführt. Wenn die Verarbeitung abgeschlossen ist, wird eine Meldung angezeigt, in der die aktuelle Verlinkungssituation zwischen dem Benutzer und der jeweiligen Anwendung beschrieben wird.

Mehrere Benutzer mit einer Anwendung verlinken

Um einen oder mehrere Benutzer mit einer Anwendung zu verlinken:

1 Markieren Sie in der Auswahlliste **Application Maintenance** die Anwendung, mit der Sie Benutzer verlinken möchten, mit dem Code `LU`.

2 Es erscheint ein Fenster mit den folgenden Optionen:

- **Start value - Startwert**
  Sie können einen Startwert (siehe *Grundlagen der Benutzung*) für die Auflistung der anzuzeigenden Anwendungen eingeben.
- **Selection criterion - Auswahlkriterium**
  Sie können eines der folgenden Auswahlkriterien angeben:

  `N` None/Kein Startwert. Alle Benutzer werden aufgelistet.

  `L` Linked. Nur Benutzer, die mit der Anwendung bereits verlinkt sind, werden aufgelistet.

  `U` Unlinked: Nur Benutzer, die noch nicht mit der Anwendung verlinkt sind, werden aufgelistet.

3 Anschließend wird die Auswahlliste **Link Users To Application** (Benutzer mit Anwendung verlinken) angezeigt, die die Liste der Benutzer zeigt. Sie enthält alle Benutzer der Typen Gruppe (Group), Administrator und Person.

In der Liste kann geblättert werden, siehe *Grundlagen der Benutzung*.

Markieren Sie in der Liste die Benutzer, die mit der Anwendung verlinkt werden sollen.

In der Spalte **Co** können Sie jeden einzelnen Benutzer mit einem der folgenden Funktionscodes markieren (mögliche Code-Abkürzungen sind unterstrichen):

Code	Funktion
`LK`	Link. Der Benutzer kann die Anwendung mit einem speziellen Sicherheitsprofil verwenden, das für den Link zu definieren ist. Das Linkprofil hat Vorrang vor dem Anwendungsprofil. Siehe *Link-Sicherheitsprofil anlegen und ändern (Anwendungen)* weiter unten.
`CL`	Cancel. Ein bestehender Link wird abgebrochen.
`DI`	Display User. Das Benutzersicherheitsprofil wird angezeigt.
`DL`	Display Link. Das Link-Sicherheitsprofil wird angezeigt.

Sie können einen oder mehrere Benutzer auf dem Bildschirm mit einem Funktionscode markieren.

4 Für jeden markierten Benutzer werden die ausgewählten Funktionen nacheinander ausgeführt. Wenn die Verarbeitung abgeschlossen ist, wird eine Meldung angezeigt, die besagt, dass die Verlinkung zwischen dem jeweiligen Benutzer und der Anwendung nun wirksam ist.

Link-Sicherheitsprofil anlegen und ändern (Anwendungen)

Um ein Link-Sicherheitsprofil anzulegen oder zu ändern

1 Markieren Sie in der Auswahlliste **Link User To Applications** (einzelnen Benutzer mit Anwendungen verlinken) einen Benutzer mit `LK`.

Oder:

Markieren Sie in der Auswahlliste **Link Users To Application** (mehrere Benutzer mit Anwendung verlinken) einen Benutzer mit `LK`.

2 Es wird ein Fenster angezeigt, in dem Sie das Sicherheitsprofil für diesen Link festlegen können.

Die Standardeinstellungen, die im Link-Sicherheitsprofil erscheinen, werden aus dem Sicherheitsprofil der Anwendung übernommen.

Die Bestandteile eines Link-Sicherheitsprofils entsprechen denen eines Anwendungs-Sicherheitsprofils (siehe *Bestandteile eines Anwendungsprofils*). Darüber hinaus können Sie Aktivierungsdaten festlegen. Diese entsprechen den Aktivierungsdaten in einem Benutzersicherheitsprofil (siehe *Bestandteile eines Benutzersicherheitsprofils*).

Anstatt die Zugriffsmethoden im Link-Sicherheitsprofil zu erlauben/nicht zu erlauben, können Sie auch die entsprechenden Buchstaben (`R`, `A`, `M`, `D`) an den entsprechenden Stellen in der Spalte **Access** (Zugriff) der Auswahlliste **Link User To Applications** oder **Link Users To Application** eingeben/löschen.

16 Natural-Entwicklungsumgebung in Eclipse schützen

- Natural Server-Ansicht schützen 326
- Navigator-Ansicht schützen 330

In diesem Kapitel wird beschrieben, wie Sie die Benutzung der Natural-Server-Ansicht und der Eclipse-Navigator-Ansicht, die von Natural in einer Eclipse-Umgebung in Verbindung mit NaturalONE verwendet werden, steuern.

Folgende Themen werden behandelt:

Um die Optionen der Natural Server-Ansicht und der Eclipse-Navigator-Ansicht sowie die für eine bestimmte Bibliothek und einen bestimmten Benutzer erlaubten bzw. nicht erlaubten Aktionen anzuzeigen, können Sie die Anwendungsprogrammierschnittstelle `NSCONE` verwenden.

Natural Server-Ansicht schützen

In diesem Abschnitt wird beschrieben, wie Sie einen in Eclipse verwendeten Natural Server mit Natural Security schützen können und wie sich die Sicherheitsdefinitionen in der FSEC-Systemdatei, die der Serverumgebung zugeordnet ist, auf Aktionen auf dem Server auswirken.

Folgende Themen werden behandelt:

- Map Environment und Bibliotheksauswahl
- Schützbare Funktionen in der gemappten Umgebung

Map Environment und Bibliotheksauswahl

Die Funktion **Map Environment** wird durch die Natural Security-Einstellungen gesteuert, die für die FNAT-Systemdatei gelten, in der diese Funktion ausgeführt wird. Wenn die Funktion ausgeführt wird, führt Natural Security eine Anmeldung gemäß den Regeln durch, die im Kapitel *Vorgehensweise bei der Anmeldung* beschrieben sind. Die Anmeldung erfolgt bei der Standardbibliothek des Benutzers, daher müssen die Sicherheitseinstellungen so sein, dass der Benutzer sich bei seiner Standardbibliothek anmelden kann.

Bei der Anmeldung in der gemappten Umgebung ist es möglich, 32-stellige Benutzernamen als Kennungen (IDs) für die Anmeldung zu verwenden. Dies setzt voraus, dass im LDAP-Sicherheitsprofil des verwendeten Servers die **Option Support user names as IDs** gesetzt ist. Siehe dazu den Abschnitt *Authentifizierungsoptionen (LDAP)*. Der Benutzername muss im Benutzersicherheitsprofil in Natural Security als **User Name** definiert sein. Dabei ist zu beachten, dass bei Benutzerkennungen in NaturalONE zwischen Groß- und Kleinschreibung unterschieden wird.

Anmerkung: Nach dem Mapping der Umgebung ist eine Anmeldung mit einer anderen Benutzerkennung innerhalb der gemappten Umgebung nicht mehr möglich.

Nach dem Mapping der Umgebung enthält die Server-Ansicht in der gemappten Umgebung eine Auflistung aller nicht leeren Bibliotheken in der der gemappten Umgebung zugeordneten FUSER-Systemdatei, auf die der Benutzer zugreifen kann. Bibliotheken, in deren Sicherheitsprofilen eine andere FUSER-Datei oder FDIC-Datei angegeben ist (unter **Library File**), werden nicht aufgeführt.

Wenn der Benutzer eine dieser Bibliotheken in der Server-Ansicht auswählt, wird eine Anmeldung bei dieser Bibliothek durchgeführt - nach den Regeln, die im Abschnitt *Vorgehensweise bei der Anmeldung* beschrieben sind. So kann es z.B. sein, dass eine Startup-Transaktion ausgeführt wird. Der Benutzer kann eine Bibliothek nur in der Baumansicht auswählen. Eine andere Bibliotheksauswahl (z.B. über das Systemkommando `LOGON *`) ist nicht möglich.

Innerhalb einer Bibliothek in der gemappten Umgebung können einige Funktionen durch Natural Security geschützt werden, andere können nicht geschützt werden. Welche Funktionen dies sind, wird im Folgenden beschrieben.

Die von der Natural Server-Ansicht verwendeten Natural Security-Daten werden im Cache gespeichert und erst aktualisiert, wenn der Natural Server erneut gemappt wird.

Anmerkung: Wenn eine Startup-Transaktion für eine Bibliothek in der Natural Server-Ansicht definiert ist, muss sie die Bedingungen erfüllen, die unter *Startup Transactions* im Abschnitt *Using an Existing Natural Development Server Environment* in der *NaturalONE-Installationsdokumentation* beschrieben sind.

Schützbare Funktionen in der gemappten Umgebung

Die Nutzung der folgenden Funktionen in einer Bibliothek innerhalb der gemappten Umgebung kann wie folgt geschützt werden:

- Aktionen in der Server-Ansicht

Nicht erlaubte Aktionen werden in den Kontextmenüs der Natural Server-Ansicht deaktiviert.

Aktionen in der Server-Ansicht

Anmerkung: Einige der unten aufgeführten Aktionen der Server-Ansicht werden von `SYSMAIN`-Dienstprogrammprofilen gesteuert. Wenn jedoch keine Dienstprogrammprofile für `SYSMAIN` definiert sind, werden diese Aktionen durch die Option **Utilities** im Bibliothekssicherheitsprofil der bearbeiteten Bibliothek gesteuert.

Position in der Server-Ansicht Aktion	Aktion	Gesteuert durch
Systemdateiknoten	Unlock	Session-Option **Unlock Objects** im Benutzersicherheitsprofil.
Bibliotheksknoten	Open	Kommandoeinschränkungen (`LIST`- oder `EDIT`-Kommando) im Bibliothekssicherheitsprofil*.
	Add to New Project / Add to Existing Project	Option **Co** (Copy) **from library** für Objekttyp im `SYSMAIN`-Dienstprogrammprofil.
	Rename (**)	Die Aktion als solche ist immer erlaubt und kann nicht untersagt werden. Es muss jedoch ein Bibliothekssicherheitsprofil für die Bibliothek mit dem neuen

Position in der Server-Ansicht Aktion	Aktion	Gesteuert durch
		Namen existieren (es sei denn, die allgemeine Option **Transition Period Logon** ist auf `Y` gesetzt). Damit der Bibliotheksinhalt übertragen werden kann, muss außerdem die Option **Mo** (Move) **from library** und **to library** für alle Objekttypen im `SYSMAIN`-Dienstprogrammprofil erlaubt sein.
	Delete (**)	Option **De** (Delete) für den Objekttyp im `SYSMAIN`-Dienstprogrammprofil.
	Copy	Option **Co** (Copy) **from library** für den Objekttyp im `SYSMAIN`-Dienstprogrammprofil.
	Paste	Option **Co** (Copy) oder **Mo** (Move) **from library** für Objekttyp in `SYSMAIN`-Dienstprogrammprofil.
Programmierobjekte		
Gruppenknoten für Programmierobjekte ts	Open / Add to New Project / Add to Existing Project	Kommandoeinschränkungen ((Kommando `LIST` oder `READ`) im Bibliothekssicherheitsprofil*.
	Delete	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
	Copy	Option **Co** (Copy) **from library** für Objekttyp in `SYSMAIN`-Dienstprogrammprofil.
	Paste	Option **Co** (Copy) oder **Mo** (Move) **from library** für Objekttyp im `SYSMAIN`-Dienstprogrammprofil.
Objektknoten für Programmierobjekte	Open / Add to New Project / Add to Existing Project	Editiereinschränkungen im Bibliothekssicherheitsprofil*.
	Catalog	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
	Stow	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
	Execute	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
	Rename	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
	Delete	Kommandoeinschränkungen im Bibliothekssicherheitsprofil*.
	Copy	Option **Co** (Copy) **from library** für Objekttyp in `SYSMAIN`-Dienstprogrammprofil.
	Paste	Option **Co** (Copy) oder **Mo** (Move) **from library** für Objekttyp im `SYSMAIN`-Dienstprogrammprofil.
	Edit	Option **Co** (Copy) **from library** für Objekttyp in `SYSMAIN`-Dienstprogrammprofil.
	List	Option **Co** (Copy) **from library** für Objekttyp in `SYSMAIN`-Dienstprogrammprofil.
DDMs		
Gruppenknoten für DDMs	Add to New Project / Add to Existing Project	Option **Edit** in **SYSDDM**-Dienstprogrammprofil (***) und Option **Co** (Copy) **from environment** für DDM in `SYSMAIN`-Dienstprogrammprofil.

Position in der Server-Ansicht Aktion	Aktion	Gesteuert durch
	Copy	Option **Co** (Copy) **from environment** für DDM in SYSMAIN-Dienstprogrammprofil.
	Delete	Option **Delete** im SYSDDM-Dienstprogrammprofil. (***)
	Move	Option **Mo** (Move) **from environment** für DDM in SYSMAIN-Dienstprogrammprofil.
	Open	Option **List** im SYSDDM-Dienstprogrammprofil. (***)
	Paste	Option **Co** (Copy) **to environment** für DDM in SYSMAIN-Dienstprogrammprofil.
Objektknoten für DDMs	Add to New Project / Add to Existing Project	Option **Edit** in SYSDDM-Dienstprogrammprofil (***) und Option **Co** (Copy) **from environment** für DDM in SYSMAIN-Dienstprogrammprofil.
	Catalog	Option **Cat** im SYSDDM-Dienstprogrammprofil. (***)
	Copy	Option **Co** (Copy) **from environment** für DDM im SYSMAIN-Dienstprogrammprofil.
	Delete	Option **Delete** im SYSDDM-Dienstprogrammprofil. (***)
	Edit	Option **Edit** im SYSDDM-Dienstprogrammprofil (***) *und* Option **Co** (Copy) **from environment** für DDM im **SYSMAIN**-Dienstprogrammprofil.
	Move	Option **Mo** (Move) **from environment** für DDM im SYSMAIN-Dienstprogrammprofil.
	Paste	Option **Co** (Copy) **to environment** für DDM in **SYSMAIN**-Dienstprogrammprofil.
	Stow	Option **Cat** in SYSDDM-Dienstprogrammprofil. (***)

* oder Special-Link-Sicherheitsprofil

** Diese Aktionen können im Kontextmenü des Bibliotheksknotens durch die Option **Disable Rename and Delete of Library Node** (siehe Kapitel *Administrator Services*) unverfügbar gemacht werden.

*** Wenn kein SYSDDM-Dienstprogrammprofil definiert ist, gelten die Kommandoeinschränkungen im SYSDDM-Bibliothekssicherheitsprofil.

Navigator-Ansicht schützen

Anmerkung: Verwechseln Sie nicht den Begriff *private-mode library*, wie er in diesem Abschnitt verwendet wird, mit dem Begriff *private library*, wie er im Abschnitt *Benutzer verwalten* verwendet wird. Sie beziehen sich auf unterschiedliche Funktionen, die nicht miteinander zusammenhängen.

Für Natural-Projekte unterstützt NaturalONE zwei Entwicklungsmodi: **Shared Mode** und **Private Mode**. Sie werden in NaturalONE gesetzt und sind im Abschnitt *Different Modes for Developing Natural Applications* der *NaturalONE Introduction*-Dokumentation beschrieben. Für diese Modi können in Natural Security sogenannte **Development Mode**-Optionen gesetzt werden. Sie legen fest, wie Natural Security die Verwendung von Natural-Server-Aktionen steuert, die durch die Eclipse-Navigator-Ansichten-Aktionen ausgelöst werden. Sie haben zwei Möglichkeiten:

- Schutz ohne Development Mode-Optionen
- Schutz mit Development Mode-Optionen

Die Form des Schutzes wird durch die **Development Mode**-Option bestimmt, die im Abschnitt *Voreingestellte Werte für Bibliothekssicherheitsprofile - Library Preset Values* in den Administrator Services eingestellt wird.

Schutz ohne Development Mode-Optionen

Wenn der Bibliotheksvoreinstellungswert **Development Mode** auf Stern (*) gesetzt ist, kann die Verwendung der folgenden Serveraktionen, die durch die Aktionen in der Eclipse-Navigator-Ansicht ausgelöst werden, durch die folgenden Natural Security-Definitionen geschützt werden:

Position in der Navigator-Ansicht	Aktion	Gesteuert durch	Im Private Mode auch gesteuert durch
Projektknoten	Upload	Kommando `SAVE` in Kommandoeingeschränkungen (Command Restrictions) in Bibliotheks- (oder Special-Link-)Sicherheitsprofil.	Option **Co** (Kopieren) **from library** für Objekttyp in `SYSMAIN`-Dienstprogrammprofil.
	Update	Kommando `STOW` in Kommandoeingeschränkungen (Command Restrictions) in Bibliotheks- (oder Special-Link-)Sicherheitsprofil.	
	Build Project		
	Rebuild Project		

Nicht erlaubte Aktionen werden in den Kontextmenüs der Navigator-Ansicht nicht deaktiviert. Die entsprechenden Natural Security-Einschränkungen werden erst ausgewertet, wenn der Benutzer versucht, eine Aktion durchzuführen.

Wenn der Development Mode in NaturalONE auf Private Mode eingestellt ist, gelten die Sicherheitsdefinitionen für die ursprüngliche Bibliothek auch für alle ihre Bibliotheken im Private Mode.

Schutz mit Development Mode-Optionen

Wenn der Bibliotheksvoreinstellungswert **Development Mode** auf Y gesetzt ist, können die Server-Aktionen, die durch die Aktionen in der Eclipse-Navigator-Ansicht ausgelöst werden, in Natural Security durch Development Mode-Optionen geschützt werden - unter Berücksichtigung des in NaturalONE eingestellten Development Mode. Dies wird in diesem Abschnitt beschrieben.

- Generelle Development Mode-Optionen
- User Development Mode-Optionen
- Optionen für den Entwicklungsmodus der Bibliothek
- Beispiele für Development Mode-Einstellungen

Generell haben für einzelne Bibliotheken gemachte Angaben Vorrang vor Angaben, die für einzelne Benutzer gemacht wurden.

Generelle Development Mode-Optionen

Wenn Sie den Bibliotheksvoreinstellungswert **Development Mode** auf Y setzen und dann PF5 auf dem Bildschirm **Preset Library Values** drücken, wird der Bildschirm **General Development Mode Options** angezeigt. Auf diesem Bildschirm können Sie die folgenden Optionen einstellen:

Feld	Erläuterung	
Development mode	Diese Option legt fest, welcher Entwicklungsmodus für das Natural-Projekt in NaturalONE eingestellt werden kann:	
	M	Mixed mode: Für das Projekt sind sowohl der Shared Mode als auch der Private Mode erlaubt. Dies ist die Standardeinstellung und die Option, die die größte Flexibilität bietet.
	S	Für das Projekt ist nur der Shared Mode erlaubt.
	P	Für das Projekt ist nur der Private Mode erlaubt.
	Diese Option gilt nicht für Natural-Projekte, die zum Zeitpunkt der Festlegung bereits in NaturalONE vorhanden sind, sondern nur für neue Natural-Projekte, die danach angelegt werden. Wenn diese Option auf M gesetzt ist, können Sie für einzelne Benutzer und Bibliotheken in deren Sicherheitsprofilen einen bestimmten Entwicklungsmodus zulassen. Wenn diese Option auf S oder P gesetzt ist, gilt dies für alle Benutzer und Bibliotheken innerhalb des Projekts und kann für einzelne Benutzer oder Bibliotheken nicht geändert werden.	
Prefix for private mode	Diese Option legt fest, welches Präfix für die Bibliothekskennungen der in Natural Security definierten Private-Mode-Bibliotheken verwendet wird:	
	Undefined	Es wird das in den **Natural Preferences** von NaturalONE definierte Präfix verwendet.
	<Project>	Die ersten 6 Zeichen des Projektnamens (wie in NaturalONE definiert) werden als Präfix verwendet.

Feld	Erläuterung	
	<Library ID>	Die ersten 6 Zeichen der Bibliothekskennung werden als Präfix verwendet.
	<User ID>	Die ersten 6 Zeichen der Benutzerkennung werden als Präfix verwendet.
	<string>	Eine angegebene Zeichenfolge von bis zu 6 Zeichen wird als Präfix verwendet. Sie können diese Zeichenfolge in einem Feld angeben, das angezeigt wird, wenn Sie diese Option auswählen. Die Zeichenfolge muss den Regeln für Bibliothekskennungen entsprechen (siehe *Neue Bibliothek anlegen*).
Aktionen in der Navigator-Ansicht		
Die folgenden beiden Optionen gelten nur, wenn für das Natural-Projekt in NaturalONE der Private Mode eingestellt ist:		
Upload	Diese Option steuert die Verwendung der Aktion **Upload** im Projekt:	
	*	Die Aktion **Update** ist nur erlaubt, wenn die Option **Co** (Copy) **from library** für den Objekttyp im Dienstprogramm `SYSMAIN` erlaubt ist und wenn das Kommando `SAVE` in den Kommandoeinschränkungen (Command Restrictions) des Bibliothekssicherheitsprofils (oder des Special-Link-Profils) erlaubt ist.
	Y	Die Aktion **Upload** ist erlaubt.
Update/Build/Rebuild	Diese Option steuert die Verwendung der Aktionen **Update**, **Build** und **Rebuild** im Projekt:	
	*	Die Aktionen **Update**, **Build Project** und **Rebuild** Project sind nur erlaubt, wenn die Option **Co** (Copy) **from library** für den Objekttyp im `SYSMAIN`-Dienstprogrammprofil erlaubt ist und wenn die Kommandos `CHECK`, `CATALOG` und `STOW` in den Kommandoeinschränkungen (Command Restrictions) des Bibliotheks- (oder Special-Link-)Sicherheitsprofils erlaubt sind.
	Y	Die Aktionen **Update**, **Build Project** und **Rebuild Project** sind erlaubt.
Optionen in der Server-Ansicht		
Die folgenden drei Optionen gelten generell und können nicht für einzelne Benutzer oder Bibliotheken geändert werden:		
General profile active	Diese Option bestimmt die Anwendbarkeit der folgenden allgemeinen Development Mode-Optionen: **Development mode**, **Prefix for private mode**, **Upload** und **Update/Build/Rebuild**:	
	Y	Wenn eine Development Mode-Option nicht in einem Benutzer- oder Bibliothekssicherheitsprofil definiert ist, gilt die entsprechende allgemeine Development Mode-Option für den Benutzer/die Bibliothek.

Feld	Erläuterung	
	N	Es gelten nur die in den Benutzersicherheitsprofilen und Bibliothekssicherheitsprofilen definierten Development Mode-Optionen.
ETID	Diese Option bestimmt, welche ETIDs verwendet werden, wenn die Natural-Server-Sitzung mit `ETID=OFF` gestartet wird.	
	N	Es gelten nur die in den Benutzersicherheitsprofilen und Bibliothekssicherheitsprofilen definierten Optionen für den Entwicklungsmodus.
	F	ETIDs werden von Natural Security generiert. Dies entspricht dem Benutzervoreinstellungswert **ETID**, wenn er auf `F` gesetzt ist.
Private-mode library	Diese Option legt fest, ob Sicherheitsprofile für Private-Mode-Bibliotheken automatisch von Natural Security erstellt werden.	
	N	Sicherheitsprofile für Private-Mode-Bibliotheken werden nicht automatisch erstellt.
	Y	Sicherheitsprofile für Private-Mode-Bibliotheken werden automatisch erstellt.
	F	Wie bei `Y`. Darüber hinaus wird jede Private-Mode-Bibliothek automatisch mit allen Dateien/DDMs verlinkt, mit denen die Originalbibliothek verlinkt ist. Dies gilt für Links, die für die Originalbibliothek zum Zeitpunkt des Anlegens ihrer Private-Mode-Bibliotheken bestehen. Wenn später Links für die Originalbibliothek angelegt/geändert/entfernt werden, können Sie die Bibliotheksverwaltungsfunktion `LF` benutzen, um die Linksituation für die Private-Mode-Bibliotheken manuell anzupassen.
	Weitere Einzelheiten zu Private-Mode-Bibliotheken finden Sie weiter unten.	
Natural Server-Aktionen		
SYSLSO command	Diese Option steuert die Verwendung des `SYSLSO`-Kommandos, das die Reihenfolge der Bibliothekssuche für Private-Mode-Bibliotheken bestimmt.	
	A	Das `SYSLSO`-Kommando kann sowohl online als auch im Batch-Modus ausgeführt werden (dies ist die Standardeinstellung).
	B	Das `SYSLSO`-Kommando kann nur im Batch-Modus ausgeführt werden.
	O	Das `SYSLSO`-Kommando kann nur online ausgeführt werden.
	N	Die Verwendung des `SYSLSO`-Kommandos ist nicht erlaubt.

Feld	Erläuterung	
	*	Die Verwendung des SYSLSO- Kommandos wird durch die entsprechende Option in den Benutzer- und Bibliothekssicherheitsprofilen gesteuert.
	Informationen zum SYSLSO-Kommando finden Sie in der *NaturalONE*-Dokumentation.	
Commands priv-mode lib.	Diese Option steuert die Verwendung von Natural-Systemkommandos für Private-Mode-Bibliotheken.	
	*	Die Verwendung von Systemkommandos wird durch die Einstellungen in Benutzersicherheitsprofilen und Bibliothekssicherheitsprofilen gesteuert (dies ist die Standardeinstellung).
	A	Alle Systemkommandos sind in Private-Mode-Bibliotheken immer erlaubt, unabhängig von den Kommandoeinschränkungen, die im entsprechenden Bibliotheks- oder Special-Link-Profil eingestellt sind.

Private-Mode-Bibliotheken

Sicherheitsprofile für Private-Mode-Bibliotheken erscheinen in der **Library Maintenance**-Auswahlliste. Sie sind mit PM in der Spalte **Prot.** gekennzeichnet.

Das Sicherheitsprofil einer Bibliothek im Private-Mode kann nicht geändert werden. Abgesehen von der Bibliothekskennung und dem Bibliotheksnamen sind die Bestandteile der Bibliothek identisch mit denen der Originalbibliothek.

Die einzigen für Private-Mode-Bibliotheken verfügbaren Bibliotheksverwaltungsfunktionen sind: DI (Display), DE (Delete) und LF (Link library to files/Bibliothek mit Dateien verlinken). Mit letzterem können Sie eine bestehende Verlinkung nicht ändern, sondern nur anzeigen (Display) oder aufheben (Cancel).

Eine Anmeldung mit der Bibliothekskennung einer Private-Mode-Bibliothek ist nicht möglich.

Wenn ein Benutzer eine Private-Mode-Bibliothek in der Navigator-Ansicht löscht, wird das entsprechende Sicherheitsprofil, das von Natural Security erstellt wurde, automatisch ebenfalls gelöscht.

Wenn Sie den Link einer Originalbibliothek zu einer Datei ändern, werden die bestehenden Links aller Private-Mode-Bibliotheken zu dieser Datei automatisch entsprechend geändert.

LSO-Container-Bibliotheken

LSO-Container-Bibliotheken (LSO = Library Search Order) werden unter *Using Private-mode Libraries in Batch* im Abschnitt *Working in a Team* der *NaturalONE in a Nutshell*-Dokumentation beschrieben.

Wenn LSO-Container-Bibliotheken in NaturalONE generiert werden, erstellt Natural Security automatisch Sicherheitsprofile für sie.

Sicherheitsprofile für LSO-Container-Bibliotheken erscheinen in der **Library Maintenance**-Auswahlliste. Sie sind in der Spalte **Prot.** mit `PO` gekennzeichnet.

Das Sicherheitsprofil einer LSO-Container-Bibliothek kann nicht geändert werden. Abgesehen von der Bibliothekskennung und dem Bibliotheksnamen sind ihre Bestandteile identisch mit denen der Originalbibliothek.

Die einzigen für LSO-Container-Bibliotheken verfügbaren Bibliotheksverwaltungsfunktionen sind: `DI` (Display) und `DE` (Delete).

Eine Anmeldung mit der Bibliothekskennung einer LSO-Container-Bibliothek ist nicht möglich.

User Development Mode-Optionen

Wenn der Bibliotheksvoreinstellungswert **Development Mode** auf `Y` gesetzt ist, wird der Abschnitt **Additional Options** der Benutzersicherheitsprofile um die **User Development Mode Options** erweitert. Hier können Sie die folgenden Optionen für diesen Benutzer einstellen:

Feld	Erläuterung	
Development mode	Diese Option kann nur gesetzt werden, wenn die *allgemeine* Entwicklungsmodusoption **Development mode** auf `M` gesetzt ist. Und sie gilt nur für Bibliotheken, in denen die Option **Development mode** auf `M` gesetzt ist. Für diese Bibliotheken bestimmt sie, welcher Entwicklungsmodus für diesen Benutzer gilt:	
	M	Mixed mode: Für diesen Benutzer sind sowohl der Shared Mode als auch der Private Mode erlaubt.
	S	Nur der Shared Mode ist für diesen Benutzer erlaubt.
	P	Nur der Private Mode ist für diesen Benutzer erlaubt.
Prefix for private mode	Wie bei den **General Development Mode Options**, jedoch nur für diesen Benutzer.	
Aktionen in der Navigator-Ansicht	Diese beiden Optionen gelten nur, wenn der Private Mode aktiv ist:	
Upload	Wie bei den **General Development Mode Options**, jedoch nur für diesen Benutzer.	
Update/Build/Rebuild	Wie bei den **General Development Mode Options**, jedoch nur für diesen Benutzer.	
Natural Server-Aktionen		
SYSLSO command	Wenn die *General* Development Mode Option **SYSLSO command** auf einen anderen Wert als * gesetzt ist, gilt dieser Wert auch für diesen Benutzer und kann hier nicht überschrieben werden. Wenn sie auf * gesetzt ist, können Sie hier einen Wert angeben:	

Feld	Erläuterung	
	A	Das SYSLSO-Kommando kann von diesem Benutzer sowohl online als auch im Batch-Modus ausgeführt werden (dies ist die Standardeinstellung).
	B	Das SYSLSO-Kommando kann von diesem Benutzer nur im Batch-Modus ausgeführt werden.
	O	Das SYSLSO-Kommando kann von diesem Benutzer nur online ausgeführt werden.
	N	Die Verwendung des SYSLSO-Kommandos ist für diesen Benutzer nicht erlaubt.
Commands priv-mode lib.	Wenn die *General* Development Mode Option **SYSLSO command** auf A gesetzt ist, gilt dieser Wert auch für diesen Benutzer und kann hier nicht überschrieben werden. Wenn sie auf * gesetzt ist, können Sie hier einen Wert angeben:	
	Y	In den von dieser Bibliothek abgeleiteten Private-Mode-Bibliotheken sind für diesen Benutzer alle Systemkommandos erlaubt.
	*	Es gelten die Kommandoeinschränkungen (Command Restrictions) des Bibliothekssicherheitsprofils oder des Special-Link-Profils.

Optionen für den Entwicklungsmodus der Bibliothek

Wenn der Voreinstellungswert Development Mode für die Bibliothek auf Y gesetzt ist,

Wenn der Bibliotheksvoreinstellungswert **Development Mode** auf Y gesetzt ist, wird der Abschnitt **Restrictions** (Einschränkungen) der Bibliothekssicherheitsprofile um die **Library Development Mode Options** erweitert. Hier können Sie die folgenden Optionen für diese Bibliothek einstellen:

Feld	Erläuterung	
Development mode	Diese Option kann nur gesetzt werden, wenn die *allgemeine* Entwicklungsmodusoption **Development mode** auf M gesetzt ist (siehe oben). In diesem Fall bestimmt diese Option, welcher Entwicklungsmodus für diese Bibliothek in NaturalONE eingestellt werden kann:	
	M	Mixed mode: Sowohl der Shared Mode als auch der Private Mode sind für diese Bibliothek erlaubt.
	S	Nur der Shared Mode ist für diese Bibliothek erlaubt.
	P	Nur der Private Mode ist für diese Bibliothek erlaubt.
Prefix for private mode	Wie bei den **General Development Mode Options**, jedoch nur für Private-Mode-Bibliotheken, die von dieser Bibliothek abgeleitet sind.	
Aktionen in der Navigator-Ansicht	Diese beiden Optionen gelten nur, wenn der Private Mode aktiv ist:	

Feld	Erläuterung	
Upload	Wie bei den **General Development Mode Options**, jedoch nur für Private-Mode-Bibliotheken, die von dieser Bibliothek abgeleitet sind.	
Update/Build/Rebuild	Wie bei den **General Development Mode Options**, jedoch nur für Private-Mode-Bibliotheken, die von dieser Bibliothek abgeleitet sind.	
Natural Server Actions		
SYSLSO command	Wenn die *General* Development Mode Option **SYSLSO command** auf einen anderen Wert als * gesetzt ist, gilt dieser Wert auch für diese Bibliothek und kann hier nicht überschrieben werden. Wenn sie auf * gesetzt ist, können Sie hier einen Wert angeben:	
	A	Das SYSLSO-Kommando kann in dieser Bibliothek sowohl online als auch im Batch-Modus ausgeführt werden (dies ist die Standardeinstellung).
	B	Das SYSLSO-Kommando kann in dieser Bibliothek nur im Batch-Modus ausgeführt werden.
	O	Das SYSLSO-Kommando kann in dieser Bibliothek nur online ausgeführt werden.
	N	Die Verwendung des SYSLSO-Kommandos ist in dieser Bibliothek nicht erlaubt.
Commands priv-mode lib.	Wenn die *General* Development Mode Option**Commands priv-mode lib.** auf A gesetzt ist, gilt dieser Wert auch für diese Bibliothek und kann hier nicht überschrieben werden. Wenn sie auf * gesetzt ist, können Sie hier einen Wert angeben:	
	Y	Alle Systemkommandos sind erlaubt bei Private-Mode-Bibliotheken, die von dieser Bibliothek abgeleitet sind.
	*	Es gelten die Kommandoeinschränkungen des Bibliothekssicherheitsprofils oder des Special-Link-Sicherheitsprofils.

Beispiele für Development Mode-Einstellungen

Die folgende Tabelle zeigt einige Beispiele für die Auswirkungen verschiedener Kombinationen von Development Mode Option-Optionen:

Wenn die folgenden Angaben gemacht werden ...			... gilt für die betreffende Bibliothek Folgendes:
General Development Mode Options	**User Development Mode Options**	**Library Development Mode Options**	

`Development mode: M`
 	
`Prefix: Undefined`
	`Development mode: M`
	
	`Prefix: Undefined`
		`Development mode: M`
		
		`Prefix: Undefined`
			Der Entwicklungsmodus wird durch die Einstellungen in NaturalONE bestimmt.
			
			Handelt es sich um den Private Mode, wird das in NaturalONE definierte Präfix verwendet.

`Development mode: M`
 	
`Prefix: Undefined`
	`Development mode: M`
	
	`Prefix: <string>`
		`Development mode: M`
		
		`Prefix: Undefined`
			Der Entwicklungsmodus wird durch die Einstellungen in NaturalONE bestimmt.
			
			Handelt es sich um den Private Mode, wird das in NaturalONE definierte Präfix verwendet.

`Development mode: M`
 	
`Prefix: Undefined`
	`Development mode: M`
	
	`Prefix: Undefined`
		`Development mode: M`
		
		`Prefix: <User ID>`
			Der Entwicklungsmodus muss in NaturalONE auf Private Mode eingestellt werden.
			
			Die Benutzerkennung wird als Präfix für die von der Bibliothek abgeleiteten Bibliotheken im Private Mode verwendet.

`Development mode: M`
 	
`Prefix: Undefined`
	`Development mode: P`
	
	`Prefix: <string>`
		Optionen nicht gesetzt.	Der Entwicklungsmodus muss in NaturalONE auf Private Mode gesetzt werden.
			
			Die angegebene Zeichenkette wird als Präfix für die von der Bibliothek abgeleiteten Private-Mode-Bibliotheken verwendet.

17 Natural RPC Server und Services schützen

- RPC Service Requests (Dienstanforderungen) 340
- RPC Server-Einstellungen in Natural 340
- RPC Server-Einstellungen in Natural Security 342
- Gültigkeitsprüfung einer RPC-Dienstanforderung 342
- Sicherheitsprofile für Natural RPC-Server 347
- Bestandteile eines RPC-Serverprofils 348
- RPC Serverprofile anlegen und verwalten 352
- Dienste erlauben/nicht erlauben 357
- Weitere RPC-bezogene Funktionen 360

In diesem Kapitel werden die verschiedenen Aspekte des Natural Remote Procedure Call-Schutzes beschrieben.

Folgende Themen werden behandelt:

Allgemeine Informationen zu Natural Remote Procedure Calls finden Sie in der *Natural RPC*-Dokumentation.

RPC Service Requests (Dienstanforderungen)

In einer Client/Server-Umgebung können Sie Natural Security einsetzen, um die Verwendung von Natural Remote Procedure Calls zu schützen. Sie können sowohl Natural RPC Server als auch die Art und Weise schützen, wie von Clients ausgehende Natural RPC Service Requests (Dienstanforderungen, Anfragen) behandelt werden.

Ein RPC Service Request ist die Anforderung eines Clients an einen Natural RPC Server, ein Natural-Subprogramm aufzurufen, das sich in einer Bibliothek auf dem Server befindet.

Wenn ein Remote `CALLNAT` ausgeführt wird und die Natural RPC Logon Option auf dem Client gesetzt ist, werden die folgenden Daten zur Validierung an den Natural RPC Server übergeben:

- der Name des aufzurufenden Subprogramms;
- die Kennung (ID) der Bibliothek auf dem Server, die das aufzurufende Subprogramm enthält;
- die Natural RPC-Benutzerkennung (User ID) und das Passwort (d. h. die Natural-Benutzerkennung und das Passwort, die mit dem Natural RPC Service Request übermittelt wurden);
- die EntireX-Benutzerkennung (User ID). Die Gültigkeitsprüfung hängt von der Anmeldeoption ab; siehe unten.

Siehe auch *Natural RPC mit Natural Security verwenden* in der *Natural RPC*-Dokumentation.

RPC Server-Einstellungen in Natural

Wenn der Natural RPC Server durch Natural Security geschützt werden soll, sollten Sie die Einstellungen der folgenden Natural-Profilparameter überprüfen:

Profilparameter	Erläuterung
RPC	Die Einstellungen für eine Natural-Sitzung, die als Natural RPC Server gestartet wird, werden durch den Natural-Profilparameter RPC bestimmt. Für einen Server, der durch Natural Security geschützt werden soll, sind zwei Schlüsselwort-Subparameter des Profilparameters RPC von besonderer Bedeutung: SRVNAME und LOGONRQ. SRVNAME gibt den Namen des Servers an. Dies ist der Name, der als Kennung (ID) für ein entsprechendes Sicherheitsprofil verwendet werden muss. LOGONRQ bestimmt, ob der Server nur gesicherte Dienstanforderungen oder sowohl öffentliche (public) als auch gesicherte (secured) Dienstanforderungen akzeptieren soll: ■ **Public Request** Dies ist ein Service Request, dessen Natural RPC-Benutzerkennung und Passwort nicht auf Gültigkeit geprüft werden. Stattdessen wird für den Service Request die Benutzerkennung verwendet, die zum Starten der Server-Sitzung verwendet wurde (wie sie in der Natural-Systemvariablen *USER enthalten ist). ■ **Secured Request** Dies ist ein Service Request, bei dem Natural RPC-Benutzerkennung und -Passwort auf Gültigkeit geprüft werden. Damit ein Server durch Natural Security geschützt wird und nur Secured Requests akzeptiert werden, müssen Sie den Schlüsselwort-Subparameter LOGONRQ auf ON setzen.
FSEC	Mit dem Profilparameter FSEC können Sie die FSEC-Systemdatei festlegen, die mit dem Natural RPC Server verknüpft werden soll.
ETID	Wenn Sie die Server-Sitzung starten und mit dem Profilparameter ETID (Adabas-Benutzerkennung) einen konkreten Wert angeben, wird bei allen Service Requests an den Server dieselbe angegebene ETID verwendet. Wenn Sie die Server-Sitzung mit dem Profilparameter ETID=' ' (leer) starten, kann von Natural Security keine ETID geliefert werden. Wenn Sie die Server-Sitzung mit dem Profilparameter ETID=OFF starten, werden die ETIDs, die von den Service Requests verwendet werden, durch die Einstellung der Option **ETID** im Sicherheitsprofil des RPC-Servers bestimmt (siehe ***Bestandteile eines RPC-Serverprofils*** unten). Indem Sie diese Option auf S (oder F) setzen, können Sie eine ETID-Behandlung mit entsprechender Datenbank-Open-/Close-Verarbeitung sicherstellen, die es Ihnen ermöglicht, die Datenbanktransaktionen jedes Service Request eindeutig zu identifizieren. Wenn Sie einen Server mit Replikaten starten, muss der Parameter ETID auf OFF oder ' ' (leer) gesetzt werden.
AUTO	Der Profilparameter AUTO (automatische Anmeldung) wird nur beim Start der Server-Sitzung ausgewertet. Bei nachfolgenden Service Requests an den laufenden Server wird der Profilparameter AUTO ignoriert. Wenn Sie die Server-Sitzung mit AUTO=OFF starten, sollten Sie mit dem Profilparameter STACK=(LOGON *library-ID* ,...) eine Bibliothek zuweisen.

RPC Server-Einstellungen in Natural Security

Die Festlegung der Zugriffsrechte auf die angeforderte Bibliothek auf dem Server erfolgt generell durch die der Natural RPC Server-Sitzung zugewiesenen Natural Security-Benutzersicherheitsprofile und -Bibliothekssicherheitsprofile in der FSEC-Systemdatei.

Speziell für den Schutz von Natural RPC-Servern bietet Natural Security die folgenden Optionen:

- Im Sicherheitsprofil einer Bibliothek können Sie verschiedene Optionen setzen, die beim Zugriff auf die Bibliothek mittels eines Natural RPC Service Request gelten. Diese Optionen sind unter ***Natural RPC-Einschränkungen*** im Kapitel *Bibliotheken verwalten* beschrieben.
- Sie können Sicherheitsprofile für Natural RPC-Server definieren, wie unten im Abschnitt ***Sicherheitsprofile für Natural RPC-Server*** beschrieben.
- Im Abschnitt ***Voreingestellte Werte für Bibliothekssicherheitsprofile - Library Preset Values*** im Kapitel *Administrator Services* können Sie verschiedene Natural RPC-Server-Sitzungsoptionen festlegen, die die Anmeldung bei Bibliotheken über Natural RPC Service Requests steuern.

Gültigkeitsprüfung einer RPC-Dienstanforderung

Dieser Abschnitt behandelt die folgenden Themen:

- Unterstützte RPC Server-Situationen
- Vom Client zu übermittelnde Sicherheitsdaten
- Impersonation
- Gültigkeitsprüfung im Natural RPC-Server
- Anmeldemodus - Logon Mode-Option
- Zusammenfassung der Prüfungen auf der Grundlage von Einstellungen in Sicherheitsprofilen

Unterstützte RPC Server-Situationen

Die folgenden Situationen werden von Natural Security unterstützt:

- Nur Natural RPC Server, die durch Natural Security geschützt sind: Die Natural RPC- Benutzerkennung wird auf Gültigkeit geprüft.
- Natural RPC Server, der durch Natural Security und EntireX Security geschützt ist: Die Natural RPC-Benutzerkennung und die EntireX-Benutzerkennung werden auf Gültigkeit geprüft.

Vom Client zu übermittelnde Sicherheitsdaten

- Natural Clients
- Nicht-Natural-Clients

Natural Clients

Die Sicherheitsdaten werden vom Natural Client geliefert, wenn die Natural RPC Logon-Option gesetzt ist. In diesem Fall gilt das Folgende:

- Die Natural RPC-Benutzerkennung und das Passwort, die für den Natural RPC Service Request verwendet werden sollen, müssen über die Natural-Anwendungsprogrammierschnittstelle `USR1071N` (enthalten in der Bibliothek `SYSEXT`) angegeben werden. Um sicherzustellen, dass diese Benutzerkennung und das Passwort bei Bedarf verfügbar sind, sollte die Ausführung von USR1071N eine der ersten Aufgaben sein, die eine Anwendung auf dem Client ausführt. Wenn `USR1071N` nicht ausgeführt wird und der Client unter Natural Security läuft, werden stattdessen die Benutzerkennung und das Passwort aus der Natural Security-Anmeldung auf dem Client verwendet.

  Wenn die Option **Impersonation** im Sicherheitsprofil des RPC Servers auf `A` gesetzt ist und der Server mit `ETID=OFF` gestartet wurde, wird die Benutzerkennung auf dem Client über die Natural-Anwendungsprogrammierschnittstelle `USR4371N` (enthalten in der Bibliothek `SYSEXT`) angegeben. Außerdem kann `USR4371N` dazu verwendet werden, die ETID für den Service Request festzulegen.
- Die EntireX-Benutzerkennung wird über die Natural-Anwendungsprogrammierschnittstelle `USR2071N` bereitgestellt.
- Die Bibliothekskennung, die für den Service Request verwendet werden soll, muss über die Natural-Anwendungsprogrammierschnittstelle `USR4008N` (enthalten in der Bibliothek `SYSEXT`) angegeben werden. Wird `USR4008N` nicht ausgeführt, wird stattdessen die Kennung der Client-Bibliothek verwendet, in der das `CALLNAT`-Statement ausgeführt wurde.

Anmerkung: Wenn die Natural RPC-Passwörter, die für einen Service Request verwendet werden, Sonderzeichen enthalten können, müssen Sie sicherstellen, dass die Natural-Zeichenumsetzungstabellen `NTTABA1` und `NTTABA2` auf dem Natural RPC Server entsprechend angepasst wurden.

Nicht-Natural-Clients

Die Remote Procedure Call-Dokumentation für den Client enthält Informationen, wie die erforderlichen Sicherheitsdaten mit einem RPC Service Request von einem Nicht-Natural-Client zu übermitteln sind an einen

- Natural RPC Server, der durch Natural Security geschützt ist;
- Natural RPC Server, der durch Natural Security und EntireX Security geschützt ist.

Impersonation

Für die Benutzerauthentifizierung auf dem Natural RPC Server sind zwei Modi möglich:

- Gültigkeitsprüfung mit Impersonation,
- Gültigkeitsprüfung ohne Impersonation.

Impersonation setzt voraus, dass der Zugriff auf das Betriebssystem, auf dem ein Natural RPC Server läuft, durch ein SAF-konformes externes Security-System kontrolliert wird. Die Benutzerauthentifizierung (Überprüfung der Natural RPC-Benutzerkennung und - optional - des Passworts) wird von diesem externen Security-System durchgeführt. Impersonation bedeutet, dass nach erfolgreicher Authentifizierung und Feststellung der Identität des Benutzers alle nachfolgenden Berechtigungsprüfungen auf der Grundlage dieser Identität durchgeführt werden. Dazu gehören auch Berechtigungsprüfungen für den Zugriff auf externe Ressourcen (z. B. Datenbanken oder Arbeitsdateien).

Impersonation ist nur möglich, wenn der Natural RPC Server unter z/OS im Batch-Modus oder unter CICS läuft. Impersonation kann verwendet werden, wenn ein SAF-konformes externes Security-System verwendet wird und die Benutzerauthentifizierung von diesem externen Security-System durchgeführt werden soll.

Impersonation wird durch die Einstellung Impersonation im Sicherheitsprofil des Natural RPC Servers aktiviert (siehe *Bestandteile eines RPC-Serverprofils* unten).

Gültigkeitsprüfung im Natural RPC-Server

Gültigkeitsprüfung ohne Impersonation

Wenn die Impersonation für den Natural RPC-Server nicht aktiv ist, wird Natural Security eine Anmeldung bei der angefragten Bibliothek durchführen, wobei die Natural RPC-Benutzerkennung verwendet wird. Die Anmeldung erfolgt gemäß den Natural Security-Anmelderegeln und den Sicherheitseinstellungen, die in der dem Server zugeordneten FSEC-Systemdatei definiert sind.

Eine Prüfung, die während der Anmeldung durchgeführt wird, basiert auf der Auswertung der Option **Natural RPC Restrictions > Logon Option** im Sicherheitsprofil der angeforderten Bibliothek.

Diese Option legt fest, ob nur die Natural RPC-Benutzerkennung oder sowohl die Benutzerkennung als auch das Passwort durch das Natural Security-Anmeldeverfahren überprüft werden sollen:

- Wenn die **Logon Option** auf `N` oder `E` gesetzt ist, werden sowohl die Benutzerkennung als auch das Passwort überprüft.
- Wenn die **Logon Option** auf `A` oder S gesetzt ist, wird nur die Benutzerkennung (User ID) überprüft - unter der Annahme, dass das Passwort bereits überprüft wurde (ähnlich wie beim Natural-Profilparameter `AUTO=ON`).
- Wenn die Anmeldeoption auf `E` oder `S` gesetzt ist, prüft Natural Security zusätzlich, ob die Natural RPC-Benutzerkennung mit der EntireX-Benutzerkennung identisch ist. Sind beide Kennungen nicht identisch, wird der Service Request abgelehnt.

Nach einer erfolgreichen Anmeldung wird das angeforderte Subprogramm ausgeführt.

Wenn die Verarbeitung des Service Request einen Zugriff auf eine externe Ressource (z.B. eine Datenbank oder eine Arbeitsdatei) beinhaltet, wird die externe Benutzerkennung, die zum Starten des Natural RPC Servers verwendet wurde, zur Überprüfung der Berechtigung für einen solchen Zugriff verwendet.

Gültigkeitsprüfung mit Impersonation

Impersonation (Impersionierung) kann verwendet werden, wenn die Benutzerauthentifizierung durch ein SAF-konformes externes Sicherheitssystem durchgeführt wird.

Wenn Impersonation für den Natural RPC Server aktiv ist, übergibt das Natural Server Frontend die Natural RPC-Benutzerkennung und das Passwort (oder nur die Benutzerkennung) zur Überprüfung an das externe Sicherheitssystem.

Nach erfolgreicher Benutzerauthentifizierung durch das externe Sicherheitssystem führt Natural Security eine Anmeldung bei der angeforderten Bibliothek durch. Für diese Anmeldung verwendet Natural Security die Natural RPC-Benutzerkennung, führt aber keine Passwortprüfung für diesen Benutzer durch. Die Anmeldung erfolgt gemäß den Natural Security-Anmelderegeln und den Sicherheitseinstellungen, die in der dem Server zugeordneten FSEC-Systemdatei definiert sind.

Eine Prüfung, die während der Anmeldung durchgeführt wird, basiert auf der Auswertung der Natural RPC Restrictions > **Logon**-Option im Sicherheitsprofil der angeforderten Bibliothek: Wenn die Anmeldeoption auf `E` oder `S` gesetzt ist, prüft Natural Security, ob die Natural RPC-Benutzerkennung mit der EntireX-Benutzerkennung identisch ist. Wenn die beiden Kennungen nicht identisch sind, wird der RPC Service Request abgelehnt.

Nach erfolgreicher Anmeldung wird das angeforderte Subprogramm ausgeführt.

Beinhaltet die Bearbeitung des Service Request einen Zugriff auf eine externe Ressource (z. B. eine Datenbank oder eine Arbeitsdatei), wird die Natural RPC-Benutzerkennung verwendet, um die Berechtigung für einen solchen Zugriff zu prüfen.

Anmeldemodus - Logon Mode-Option

Wenn Sie einen Natural RPC Server verwenden, der Dienste bereitstellt, die von Subprogrammen ausgeführt werden, die in einer einzigen Bibliothek enthalten sind, können Sie die Option **Logon Mode** im Sicherheitsprofil des Natural RPC Servers verwenden, um die Performance zu verbessern. Dadurch wird die Anzahl der Datenbankzugriffe auf die Natural Security-Systemdatei FSEC reduziert.

Die Bibliothek auf dem Server wird zu Beginn der Server-Sitzung festgelegt und bleibt bis zum Ende der Server-Sitzung unverändert. Service Requests für eine andere Bibliothek werden zurückgewiesen. Ist die Bibliothek ungeschützt (**People protected** = `N`), wird die Berechtigung des Benutzers zum Zugriff auf die Bibliothek nicht geprüft. Ist die Bibliothek geschützt (**People protected** = `Y`), wird die Berechtigung des Benutzers zum Zugriff auf die Bibliothek geprüft. Nach erfolgreicher Prüfung werden die Bedingungen des Benutzers für die Benutzung der Bibliothek durch das Bibliothekssicherheitsprofil festgelegt. Auch wenn eine spezielle Verlinkung zwischen dem Benutzer und der Bibliothek besteht, werden die Einstellungen im speziellen Link-Profil ignoriert.

Anmerkung: Wenn **Logon Mode** auf `S` gesetzt wird, um die Performance zu verbessern, ist zu bedenken, dass auch andere Einstellungen von Natural Security die Performance beeinflussen, insbesondere die Option **Logon recorded** in Benutzer- und Bibliothekssicherheitsprofilen. Darüber hinaus kann die Leistung der ETID-getriggerten Behandlung von Datenbanktransaktionen nicht optimiert werden.

Zusammenfassung der Prüfungen auf der Grundlage von Einstellungen in Sicherheitsprofilen

Dieser Abschnitt fasst die Prüfungen zusammen, die von Natural Security abhängig von den Einstellungen in den Sicherheitsprofilen durchgeführt werden, wenn ein Service Request an einen Natural RPC Server gestellt wird. Die folgenden Schritte werden durchgeführt:

1. Die Benutzerauthentifizierung wird durchgeführt (siehe Abschnitt *Gültigkeitsprüfung auf dem Server* oben).
2. RPC Server Profile > die Option **Logon Mode** wird zu Beginn der Natural RPC Server-Sitzung ausgewertet (siehe Abschnitt *Anmeldemodus - Logon Mode-Option* oben).
3. Library Profile > General Options > die Option **People-protected** (Personengeschützt) wird ausgewertet.
4. Library Profile > Natural RPC Restrictions > die Option **Logon Option** wird ausgewertet (siehe Abschnitt *Gültigkeitsprüfung auf dem Server* weiter oben): Je nach Einstellung wird geprüft, ob die Natural RPC-Benutzerkennung mit der EntireX-Benutzerkennung identisch ist.
5. RPC Server Profile > die Option **Service Protection** wird beim Start der Natural RPC Server-Sitzung ausgewertet.

Sicherheitsprofile für Natural RPC-Server

Standard-Profil

Bei der Installation von Natural Security wird automatisch ein Standard-Sicherheitsprofil (Default Security Profile) mit der Serverkennung * erstellt. Dieses Profil gilt für alle Natural RPC Server, für die keine individuellen Sicherheitsprofile definiert sind. Sie können die Einstellungen in diesem Standardprofil an Ihre Anforderungen anpassen.



Anmerkung: Sollte in Ihrer FSEC-Systemdatei kein Standard-RPC-Serverprofil * vorhanden sein (dies kann der Fall sein, weil die Datei bei der Installation nicht vorhanden war), dann müssen Sie das Programm `NSCRPCAC` in der Bibliothek `SYSSEC` ausführen. Dieses Programm erstellt das Standard-Serverprofil.

Stern-Notation bei Serverkennungen

Wenn Sie nicht für jeden einzelnen Server ein Sicherheitsprofil definieren wollen, können Sie Stern-Notation für die Serverkennung verwenden: Wenn Sie ein Serversicherheitsprofil erstellen und als Serverkennung eine Zeichenkette gefolgt von einem Stern (*) wählen, gilt das Profil für alle Server, deren Kennung mit dieser Zeichenkette beginnt. Für einen einzelnen Server innerhalb eines solchen Bereichs können Sie dennoch ein individuelles Sicherheitsprofil definieren.

Wenn Sie beispielsweise ein Serversicherheitsprofil mit der Kennung `A*` definieren, gilt es für alle Server, deren Kennung mit `A` beginnt (z.B. `ARPC1`, `AA01`, `ABC`, `ADE` usw.). Ein Profil mit der Kennung `ABC*` würde dann beispielsweise für `ABCA`, `ABCXYZ` usw. gelten.

Bestandteile und Funktionen von Serverprofilen

Im Folgenden werden die **Bestandteile** von Serversicherheitsprofilen und die **Funktionen** beschrieben, mit denen sie angelegt und verwaltet werden.

Bei einigen Natural Security-Funktionen wird der Code `RP` verwendet, um den Objekttyp *Natural RPC Server* zu repräsentieren.

Bestandteile eines RPC-Serverprofils

Der folgende Bildschirmtyp ist der primäre Profilbildschirm, der angezeigt wird, wenn Sie eine der Funktionen **Add**, **Copy**, **Modify** oder **Display** für das Sicherheitsprofil eines Natural RPC Servers aufrufen:

```
11:55:00                    *** NATURAL SECURITY ***                2021-12 31
                            - Modify NatRPC Server -

                                                Modified .. 2021-12-31 by SAG

NatRPC Server ... RPCS01
Description ..... _____________________________________


--------------- Options -------------
Impersonation ............ (N,Y,A): Y
Lock User ................ (N,X,*): X
ETID ................. (N,*,S,F,C): S
Logon Mode .................. (N,S): S
Domain separator .................: _
Service protection ......... (R,*): *



Additional Options ... N


Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help  PrevM Exit  AddOp       Flip                                 Canc
```

Die einzelnen Elemente, die Sie als Teil des Sicherheitsprofils eines Natural RPC Servers definieren können, werden im Folgenden erläutert.

Feld	Erläuterung	
Impersonation	Impersonierung ist nur relevant, wenn ein SAF-konformes externes Sicherheitssystem zur Benutzerauthentifizierung verwendet wird. Impersonierung ist oben unter *Gültigkeitsprüfung einer RPC-Dienstanforderung (Service Request)* beschrieben. Mit dieser Option wird die Impersonierung für den Server aktiviert:	
	N	Impersonierung ist nicht aktiv.
	Y	Impersonierung ist aktiv - mit Gültigkeitsprüfung der Benutzerkennung und des Passworts.

Feld	Erläuterung	
	A	Impersonierung ist aktiv - mit Gültigkeitsprüfung der Benutzerkennung, aber nicht des Passworts.
	Impersonierung ist nur möglich, wenn der Server unter z/OS im Batch-Modus oder unter CICS läuft. Ist dies nicht der Fall, wird die Einstellung dieser Option ignoriert.	
Lock User	Benutzer sperren. Diese Option gilt nur für Bibliotheken, in deren Sicherheitsprofil die Option **Lock User** (im Abschnitt ***Natural RPC-Einschränkungen*** des Bibliothekssicherheitsprofils) auf „*“ gesetzt ist. Für diese Bibliotheken steuert sie die Sperrung von Benutzern, wenn diese versuchen, über Natural RPC-Dienstanforderungen auf diese Bibliotheken auf dem Server zuzugreifen:	
	N	Die Funktion **Lock User** ist nicht aktiv.
	X	Die Funktion **Lock User** ist für Zugriffsversuche auf Bibliotheken auf dem Server mittels Natural RPC Service Calls aktiv. Sobald ein Benutzer die maximale Anzahl von Anmeldeversuchen erreicht hat, ohne das korrekte Passwort einzugeben, wird er gesperrt, d.h. die Benutzerkennung wird „ungültig“ gemacht. Natural Security merkt sich erfolglose Anmeldeversuche über mehrere Sitzungen hinweg: Die Fehlerzähler für die Client-Benutzerkennungen, die erfolglos ausprobiert wurden, werden für Zugriffsversuche in nachfolgenden Sitzungen gespeichert, so dass sich die Anzahl der nachfolgenden Versuche um diese Kennungen verringert. Der Fehlerzähler für eine Benutzerkennung wird erst nach einer erfolgreichen Anmeldung zurückgesetzt.
	*	Der Wert der Option **Lock user** in ***Voreingestellte Werte für Bibliothekssicherheitsprofile - Library Preset Values*** unter *Administrator Services* bestimmt, ob die Funktion **Lock User** für Zugriffsversuche auf Libraries über Natural RPC-Dienstanforderungen aktiv ist oder nicht.
	Weitere Informationen zur Funktion **Lock User** finden Sie auch unter der Option **Lock User** im Abschnitt *General Options* im Kapitel *Administrator Services*.	
ETID	Diese Option gilt nur für Secured Service Requests, die von Natural Clients an den Natural RPC Server übergeben werden. Sie legt fest, welche ETIDs für diese Clients während der Server-Sitzung verwendet werden sollen:	
	N	Die Standard-ETID, die im Benutzersicherheitsprofil des Natural Client definiert ist, bestimmt die zu verwendende ETID.
	S	Für jede Dienstanforderung, die auf den Natural RPC Server unter der Kontrolle von Natural Security zugreift, wird eine zeitstempelbezogene ETID generiert. Die ETID wird beim Zugriff auf den Server generiert und bleibt so lange gültig, bis die Dienstanforderung verarbeitet wurde. Anmeldungen beim Server werden aufgezeichnet.

Feld	Erläuterung	
		Informationen zu zeitstempelbezogenen ETIDs finden Sie auch unter **ETID** im Abschnitt *Voreingestellte Werte für Benutzer - User Preset Values* im Kapitel *Administrator Services*.
	F	Wie S, jedoch werden Anmeldungen beim Natural RPC Server nicht aufgezeichnet.
	C	Die ETID wird vom Client geliefert, wobei als ETID der von der Anwendungsprogrammierschnittstelle USR1071N gelieferte Passwortwert verwendet wird (siehe auch *Vom Client zu liefernde Sicherheitsdaten*). ETID=C ist nur möglich, wenn das Feld **Impersonation** auf A gesetzt ist.
	*	Die Einstellung der Option **ETID** im Abschnitt *Voreingestellte Werte für Benutzer - User Preset Values*, die für das Sicherheitsprofil des Benutzers gilt, bestimmt die zu verwendende ETID.
	Wenn diese Option auf einen anderen Wert als N gesetzt ist, wird empfohlen, die RPC Server-Sitzung mit dem Natural-Profilparameter ETID=OFF zu starten. Bei Public Service Requests hat diese Option keine Auswirkung. Bei diesen wird die ETID des Natural RPC Servers verwendet, die beim Start der Server-Sitzung festgelegt wurde.	
Logon Mode	Anmeldemodus. Diese Option kann verwendet werden, wenn nur auf eine Bibliothek auf dem Natural RPC Server zugegriffen wird:	
	N	Es gilt kein spezieller Anmeldemodus.
	S	Es gilt der statische Modus: Die Bibliothek auf dem Natural RPC Server wird zu Beginn der Server-Sitzung festgelegt. Sie bleibt bis zum Ende der Server-Sitzung unverändert. Der Server verarbeitet Service Requests nur für diese eine Bibliothek. Jeder Service Request mit einer anderen Bibliothekskennung wird zurückgewiesen. Wenn diese Option gesetzt ist, werden die Nutzungsbedingungen der Bibliothek durch das Bibliothekssicherheitsprofil bestimmt. Selbst wenn ein spezieller Link zwischen dem Benutzer und der Bibliothek besteht, wird das Profil des speziellen Links ignoriert.
	Wenn der Natural RPC Server Dienste anbietet, die von Subprogrammen ausgeführt werden, die in einer einzigen Bibliothek enthalten sind, können Sie diese Option verwenden, um die Performance zu verbessern. Siehe auch *Gültigkeitsprüfung einer RPC-Dienstanforderung (Service Request)* oben.	
Domain Separator	Dieses Feld ist nur relevant, wenn ■ Ihr externes Sicherheitssystem ein sogenanntes Domänentrennzeichen verwendet, um den Domänennamen von der Benutzerkennung zu trennen, und	

Feld	Erläuterung	
	■ die **Logon Option** im Sicherheitsprofil der angeforderten Bibliothek auf E oder S gesetzt ist, d.h. es wird geprüft, ob die Natural RPC-Benutzerkennung mit der EntireX-Benutzerkennung identisch ist. Um sicherzustellen, dass diese Prüfung korrekt durchgeführt wird, müssen Sie das Domänenzeichen in diesem Feld angeben: Die Prüfung wird dann auf die ersten 8 Zeichen nach dem Domänen-Trennzeichen angewendet.	
Service Protection	Mit dieser Option kann der Zugriff auf den Natural RPC Server eingeschränkt werden:	
	*	Der Zugriff ist nicht eingeschränkt: Alle Benutzer können auf den Server zugreifen.
	R	Der Zugriff ist eingeschränkt: Nur Benutzer, die mit dem Serverprofil verlinkt sind, dürfen auf den Server zugreifen. Außerdem können Sie den Zugriff auf den Server auf bestimmte Dienste (Subprogramme) beschränken. Weitere Informationen finden Sie unter ***Dienste erlauben/nicht erlauben***.
	Bevor Sie dieses Feld von R auf * zurücksetzen können, müssen Sie die Liste der erlaubten Dienste löschen, die Sie eventuell über ***Dienste erlauben/nicht erlauben*** festgelegt haben.	

Zusätzliche Optionen (Natural RPC Server) - Additional Options

Wenn Sie entweder das Feld **Additional Options** mit Y markieren oder PF4 drücken, wird ein Fenster angezeigt, in dem Sie die folgenden Optionen auswählen können:

- Maintenance Information - Verwaltungsinformationen
- Security Notes - Sicherheitsvermerke
- Owners - Eigentümer

Optionen, bei denen bereits etwas angegeben oder definiert wurde, sind mit einem Pluszeichen (+) gekennzeichnet.

Sie können ein oder mehrere Elemente aus dem Fenster auswählen, indem Sie sie mit einem beliebigen Zeichen markieren. Für jedes ausgewählte Element wird ein weiteres Fenster angezeigt:

Zusätzliche Option	Erläuterung
Maintenance Information (nur Anzeige)	Verwaltungsinformationen. In diesem Fenster werden die folgenden Informationen angezeigt: ■ das Datum und die Uhrzeit, wann das Sicherheitsprofil erstellt wurde, die Kennung des Administrators, der es angelegt hat, und (falls zutreffend) die Kennungen der Miteigentümer, die beim Anlegen gegengezeichnet haben; ■ das Datum und die Uhrzeit der letzten Änderung des Sicherheitsprofils, die Kennung des Administrators, der die letzte Änderung vorgenommen hat, und (falls

Zusätzliche Option	Erläuterung
	zutreffend) die Kennungen der Miteigentümer, die bei der Änderung gegengezeichnet haben.
Security Notes	Sicherheitsvermerke. Hier können Sie Anmerkungen zum Sicherheitsprofil eingeben.
Owners	Eigentümer. In diesem Fenster können Sie bis zu acht Kennungen von Administratoren eingeben. Nur die hier angegebenen Administratoren sind berechtigt, dieses Serversicherheitsprofil zu verwalten. Wird kein Eigentümer angegeben, kann jeder Benutzer des Typs Administrator das Sicherheitsprofil verwalten. Zu jedem Eigentümer kann optional im Feld nach der Kennung die Anzahl der Miteigentümer angegeben werden, deren Gegenzeichnung für die Verwaltungsberechtigung erforderlich ist. Informationen zu Eigentümern und Miteigentümern finden Sie im Kapitel *Gegenzeichnungen*.

RPC Serverprofile anlegen und verwalten

Dieser Abschnitt beschreibt die Funktionen zum Anlegen und Verwalten von Sicherheitsprofilen für Natural RPC Server.

Folgende Themen werden behandelt:

- Verwaltung von Natural RPC-Servern aufrufen
- Neues Serverprofil anlegen
- Vorhandene Serverprofile zur Bearbeitung auswählen
- Serverprofil kopieren
- Serverprofil ändern
- Serverprofil umbenennen
- Serverprofil löschen
- Serverprofil anzeigen

Verwaltung von Natural RPC-Servern aufrufen

Um die Verwaltung von Natural RPC-Servern aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) die Option **Maintenance**.

Es wird ein Fenster angezeigt.

2 Markieren Sie im Fenster den Objekttyp **Natural RPC Server** mit einem Zeichen oder mit dem Cursor.

Die Auswahlliste **Natural RPC Server Maintenance** wird angezeigt.

3 In dieser Auswahlliste können Sie alle Funktionen der Natural RPC Server-Verwaltung wie unten beschrieben aufrufen.

Neues Serverprofil anlegen

Um einen Natural RPC-Server in Natural Security zu definieren, müssen Sie ein Sicherheitsprofil für ihn anlegen.

Dazu:

1 Geben Sie in der Kommandozeile der Auswahlliste **Natural RPC Server Maintenance** das Kommando `ADD` ein.

2 Es wird ein Fenster angezeigt, in dem Sie eine Kennung (ID) für den Server eingeben müssen.

Diese Kennung entspricht dem Servernamen, wie er mit dem Natural-Profilparameter RPC angegeben wurde (siehe *RPC-Server-Einstellungen in Natural* oben), und muss den Namenskonventionen für Natural RPC Server entsprechen. Die Serverkennung kann auch mit Stern-Notation angegeben werden, siehe oben unter *Sicherheitsprofile für Natural RPC-Server*.

3 Nachdem Sie eine gültige Kennung eingegeben haben, wird der Bildschirm **Add Natural RPC Server** angezeigt.

Die Bestandteile, die Sie auf diesem Bildschirm definieren können, sowie alle zusätzlichen Fenster, die Teil eines Serversicherheitsprofils sein können, werden unter *Bestandteile eines RPC-Serverprofils* beschrieben.

Wenn Sie ein neues Serverprofil hinzufügen, werden die in Ihrem eigenen Benutzersicherheitsprofil angegebenen Eigentümer automatisch in das Serversicherheitsprofil kopiert.

Vorhandene Serverprofile zur Bearbeitung auswählen

Wenn Sie die Option **Natural RPC Server Maintenance** aufrufen, wird eine Liste aller Natural RPC-Serverprofile angezeigt, die in Natural Security definiert wurden.

Wenn Sie nicht alle vorhandenen Profile, sondern nur bestimmte Server auflisten möchten, können Sie die Option **Start Value** (Startwert) verwenden, siehe Kapitel *Grundlagen der Benutzung*.

Wählen Sie im Hauptmenü (**Main Menu**) die Option **Maintenance**. Es wird ein Fenster angezeigt.

Markieren Sie in dem Fenster den Objekttyp **Natural RPC Server** mit einem Zeichen oder mit dem Cursor (und geben Sie, falls gewünscht, einen Startwert ein). Die Auswahlliste **Natural RPC Server Maintenance** wird angezeigt:

```
14:34:42                    *** NATURAL SECURITY ***                 2021-12-31
                          - NatRPC Server Maintenance -              FSEC (47,11)

Co NatRPC Server                        Description           P Message
__ _____________________________________ _____________________ _ _____________________
__ A_NATRPC_SERVER_PAYROLL              Department Duckville  R
__ ADE_RPC                              Arch. Department Ge.. R
__ BEST_SERVER                          Third party logistics R
__ DOBANCO_SRV1                         Credit transfer Ban.. R
__ EMPLOYEES_SRV1                       Headquarter Server P1 *
__ ESSENHEIM_SRV1                       Location Essenheim    R
__ NATURAL_RPC_SERVER_NAME_32_BYTES     Test SRVNAME          *
__ RPC_TIME                             8 * 7 Support         R
__ RPC_TIME_LONG_LIFE                   24 * 7 Support        *
__ RPC_TIME_LONG_LIFE_B                 24 * 7 Support Backup *
__ TEST_SRV0                            QA env. 1             *
__ TEST_SRV1                            QA env. 2             R
__ TEST_SRV2                            QA env. 3             *
__ UHE_SRV                              Developer Test env.   *
__ WWESRV                                                     *
Command ===>
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help        Exit              Flip  -     +                       Canc
```

Bei jedem Server wird die Serverkennung angezeigt.

In der Liste kann geblättert werden, siehe *Grundlagen der Benutzung*.

Funktion auswählen

Für Natural RPC Serverprofile stehen die folgenden Verwaltungsfunktionen zur Verfügung (mögliche Code-Abkürzungen sind unterstrichen):

Code	Funktion
CO	**Copy**: Serverprofil kopieren
MO	**Modify**: Serverprofil ändern
RE	**Rename**: Serverprofil umbenennen
DE	**Delete**: Serverprofil löschen
DI	**Display**: Serverprofil anzeigen
LU	**Link Users**: Benutzer mit Serverprofil verlinken

Um eine Funktion für ein Serverprofil aufzurufen, müssen Sie den Server in der Spalte **Co** mit dem entsprechenden Funktionscode markieren.

Sie können verschiedene Serverprofile für verschiedene Funktionen gleichzeitig auswählen, d.h. Sie können mehrere Server auf dem Bildschirm mit einem Funktionscode markieren. Für jeden

markierten Server wird dann der entsprechende Bearbeitungsbildschirm angezeigt. Sie können dann die ausgewählten Funktionen für ein Serverprofil eine nach der anderen ausführen.

Serverprofil kopieren

Mit der Funktion **Copy Server Profile** können Sie einen neuen Natural RPC Server in Natural Security definieren, indem Sie ein Sicherheitsprofil erstellen, das mit einem bereits vorhandenen Natural RPC Serversicherheitsprofil identisch ist.

Alle Bestandteile des bestehenden Sicherheitsprofils werden in das neue Sicherheitsprofil kopiert - mit *Ausnahme* der Eigentümer (diese werden aus Ihrem eigenen Benutzersicherheitsprofil in das neue Serversicherheitsprofil kopiert).

Links von Benutzern zum bestehenden Server werden *nicht* kopiert.

Um ein Serverprofil zu kopieren:

1. Markieren Sie in der Auswahlliste **Natural RPC Server Maintenance** den Server, dessen Sicherheitsprofil Sie duplizieren möchten, mit dem Funktionscode `CO`.
2. Es wird ein Fenster angezeigt, in dem Sie die Kennung (ID) des neuen Servers eingeben müssen.

   Die Kennung entspricht dem Servernamen, wie er mit dem Natural-Profilparameter `RPC` angegeben wurde (siehe ***RPC-Server-Einstellungen in Natural*** oben), und muss den Namenskonventionen für Natural RPC Server entsprechen. Die Serverkennung kann auch mit Stern-Notation angegeben werden, siehe ***Sicherheitsprofile für Natural RPC-Server***.
3. Nachdem Sie eine gültige Kennung eingegeben haben, wird das neue Sicherheitsprofil angezeigt.

   Seine Bestandteile, die Sie definieren oder ändern können, sind unter ***Bestandteile eines RPC-Serverprofils*** beschrieben.

Serverprofil ändern

Mit der Funktion **Modify Server Profile** können Sie ein bestehendes Sicherheitsprofil eines Natural RPC Servers ändern.

Dazu:

1. Markieren Sie in der Auswahlliste **Natural RPC Server Maintenance** den Server, dessen Sicherheitsprofil Sie ändern möchten, mit dem Funktionscode `MO`.
2. Das Sicherheitsprofil des ausgewählten Servers wird angezeigt.

   Seine Bestandteile, die Sie definieren oder ändern können, sind unter ***Bestandteile eines RPC-Serverprofils*** beschrieben.

Serverprofil umbenennen

Mit der Funktion **Rename Server Profile** können Sie die Serverkennung (ID) eines bestehenden Natural RPC Serversicherheitsprofils ändern.

Dazu:

1 Markieren Sie in der Auswahlliste **Natural RPC Server Maintenance** den Server, dessen Kennung Sie ändern möchten, mit dem Funktionscode `RE`.

2 Es wird ein Fenster angezeigt, in dem Sie eine neue Kennung für das Serverprofil eingeben können.

Die Kennung entspricht dem Servernamen, wie er mit dem Natural-Profilparameter `RPC` angegeben wurde (siehe *RPC Server-Einstellungen in Natural* oben), und muss den Namenskonventionen für Natural RPC Server entsprechen. Die Serverkennung kann auch mit Stern-Notation angegeben werden, siehe oben unter *Sicherheitsprofile für Natural RPC-Server*.

Serverprofil löschen

Mit der Funktion **Delete Server Profile** können Sie ein bestehendes Natural RPC-Serversicherheitsprofil löschen.

Dazu:

1 Markieren Sie in der Auswahlliste **Natural RPC Server Maintenance** den Server, dessen Profil Sie löschen möchten, mit dem Funktionscode `DE`.

2 Das Fenster **Delete Server Profile** wird angezeigt.

- Wenn Sie sich gegen das Löschen des Serversicherheitsprofils entscheiden, können Sie das Fenster verlassen, indem Sie ENTER drücken, ohne etwas eingegeben zu haben.
- Um das Serversicherheitsprofil zu löschen, müssen Sie die Serverkennung in das Fenster eingeben, um die Löschung zu bestätigen.

Wenn Sie mehr als ein Serverprofil mit `DE` markieren, wird ein Fenster angezeigt, in dem Sie gefragt werden, ob Sie die Löschung jedes einzelnen Serversicherheitsprofils mit der Eingabe der Serverkennung bestätigen wollen, oder ob alle zum Löschen ausgewählten Serverprofile ohne diese Einzelbestätigung gelöscht werden sollen. Achten Sie darauf, dass Sie nicht versehentlich ein Serverprofil löschen.

Serverprofil anzeigen

Mit der Funktion **Display Server Profile** können Sie ein bestehendes Natural RPC Serversicherheitsprofil anzeigen.

Dazu:

- Markieren Sie in der Auswahlliste **Natural RPC Server Maintenance** den Server, dessen Sicherheitsprofil Sie anzeigen möchten, mit dem Funktionscode `DI`.

  Das Sicherheitsprofil des ausgewählten Servers wird angezeigt.

  Seine Bestandteile sind unter *Bestandteile eines RPC-Serverprofils* beschrieben.

Dienste erlauben/nicht erlauben

Wenn der Zugriff auf einen Natural RPC Server durch die Option **Service Protection** im Serverprofil eingeschränkt ist (siehe *Bestandteile eines RPC-Serverprofils*), können Sie mit den unten beschriebenen Funktionen Benutzern den Zugriff auf Dienste (Subprogramme) auf dem Server erlauben/nicht erlauben.

Sie können:

- Dienste erlauben/nicht erlauben durch Option RPC Server Maintenance oder User Maintenance
- Erlauben/nicht erlauben via Library Maintenance

Dienste erlauben/nicht erlauben durch Option RPC Server Maintenance oder User Maintenance

Um einen Dienst zu erlauben/nicht zu erlauben:

1 Markieren Sie in der Auswahlliste **Natural RPC Server Maintenance** den gewünschten Server mit dem Funktionscode `LU`. Dies ist nur für Server möglich, in deren Sicherheitsprofil die Option **Service Protection** auf `R` gesetzt ist (erkennbar an der Spalte **P** in der Auswahlliste).

  Es erscheint ein Fenster, in dem Sie angeben können, ob die Liste der anzuzeigenden Benutzer alle Benutzer (`U`), nur verlinkte Benutzer (`L`) oder nur nicht-verlinkte Benutzer (`N`) enthalten soll.

  Anschließend wird die Liste der Benutzer angezeigt.

  Oder:

  Markieren Sie in der Auswahlliste **User Maintenance** den gewünschten Benutzer (Benutzertyp `A`, `P` oder `G`) mit dem Funktionscode `LR`.

Es wird eine Liste aller Server angezeigt, bei denen die Option **Service Protection** auf R gesetzt ist.

2 In den Listen kann geblättert werden, siehe Kapitel *Grundlagen der Benutzung*.

3 Markieren Sie in der Spalte **Co** jeden Benutzer bzw. Server mit einem der folgenden Funktionscodes:

Code	Funktion
*A	**Allow Access** Zugriff erlauben. Der Benutzer darf auf den Server zugreifen. Der Zugriff ist nicht auf bestimmte Subprogramme beschränkt (abgesehen von nicht erlaubten Modulen; siehe unten).
RA	**Restrict Access** Zugriff einschränken. Der Benutzer kann nur über explizit erlaubte Dienste (Subprogramme) auf den Server zugreifen. Die Verwendung bestimmter Subprogramme in einer Bibliothek kann generell über den Abschnitt **Disallow/Allow Modules** eines Bibliotheks- oder Special-Link-Profils eingeschränkt werden. Diese Einschränkungen gelten innerhalb und außerhalb eines RPC Server-Kontextes. Das heißt, wenn ein Subprogramm in der Bibliothek oder im speziellen Linkprofil nicht erlaubt ist, kann es auch nicht in einem RPC Server-Kontext erlaubt werden. Sie können jedoch den Zugriff auf Subprogramme in einem RPC Server-Kontext weiter einschränken. Der Zugriff auf den Server ist dann nur über die explizit erlaubten Subprogramme möglich: Wenn Sie einen Benutzer mit dem Funktionscode RA markieren, wird ein Fenster angezeigt, in dem Sie ein Subprogramm erlauben können, indem Sie dessen Subprogramm- und Bibliothekskennung angeben. Wenn bereits erlaubte Subprogramme vorhanden sind, wird eine Liste mit diesen Subprogrammen angezeigt: ■ Um weitere Subprogramme zu erlauben, müssen Sie PF5 drücken. Es erscheint ein Fenster, in dem Sie die gewünschte Subprogramm- und Bibliothekskennung angeben können (für eine Auswahlliste von Bibliothekskennungen können Sie einen Stern (*) eingeben). ■ Um ein Subprogramm nicht zu erlauben, müssen Sie es in der Liste mit DE markieren.
DA	**Disallow Access** Der Benutzer kann nicht auf den Server zugreifen.

Erlauben/nicht erlauben via Library Maintenance

Um einen Dienst zu erlauben/nicht zu erlauben:

1 Markieren Sie in der Auswahlliste **Library Maintenance** die gewünschte Bibliothek mit dem Funktionscode RA.

2 Es wird ein Fenster angezeigt, in dem Sie Folgendes angeben können:

- U, um eine Liste aller Benutzer (Benutzertypen A, P und G) zu erhalten, die die Bibliothek benutzen dürfen (wenn die Bibliothek personengeschützt ist (**People protected** = Y), enthält die Liste nur Benutzer, die mit ihr verlinkt sind); oder
- R, um eine Liste aller RPC Server zu erhalten, in deren Sicherheitsprofil die Option **Service Protection** auf R gesetzt ist.

In den Listen kann geblättert werden, siehe Kapitel *Grundlagen der Benutzung*.

Wenn Sie U gewählt haben, gehen Sie wie folgt vor:

1 Markieren Sie in der Liste der Benutzer einen Benutzer mit RA.

2 Es wird eine Liste aller Server angezeigt, in deren Sicherheitsprofil die Option **Service Protection** auf R gesetzt ist.

Markieren Sie einen Server mit dem Funktionscode RA.

3 Eine Liste aller Dienste (Subprogramme) in der Bibliothek, auf die der Benutzer zugreifen darf, wird angezeigt.

- Um weitere Dienste zu erlauben, müssen Sie PF5 drücken. Es wird ein Fenster angezeigt, in dem Sie das gewünschte Subprogramm angeben können.
- Um einen Dienst nicht zu erlauben, müssen Sie ihn in der Liste mit DE markieren.

Wenn Sie R gewählt haben, gehen Sie wie folgt vor:

1 Markieren Sie in der Liste der Benutzer einen Benutzer mit RA.

2 Es wird eine Liste aller Benutzer (Benutzertypen A, P und G) und der Dienste (Subprogramme) in der Bibliothek angezeigt, auf die sie zugreifen dürfen.

- Um weitere Dienste zu erlauben, müssen Sie PF5 drücken. Es erscheint ein Fenster, in dem Sie die gewünschte Benutzerkennung(ID) und das Subprogramm angeben müssen (für eine Auswahlliste mit Benutzerkennungen können Sie einen Stern (*) eingeben).
- Um einen Dienst nicht zu erlauben, müssen Sie ihn in der Liste mit DE markieren.

Weitere RPC-bezogene Funktionen

User Exit LOGONEX4

Der Natural Security User Exit `LOGONEX4` wird vom Natural Security RPC-Logon-Programm nach einer erfolgreichen Anmeldung eines Natural RPC Clients bei einem Natural RPC Server aufgerufen. Weitere Informationen siehe ***RPC-relevanter User Exit*** im Kapitel *User Exits*.

Passwortänderung via RPC Service Request - User Exit USR2074N

Mit dem Natural User Exit USR2074N, der in der Bibliothek `SYSEXT` enthalten ist, können Sie das Benutzerpasswort über einen Natural RPC Service Request (Dienstanforderung) ändern.

18 Externe Objekte schützen

- Externe Objekttypen - Types of External Objects 362
- Kennungen für externe Objekte 363
- Bestandteile eines Sicherheitsprofils für ein externes Objekt 364
- Sicherheitsprofile für externe Objekte anlegen und verwalten 367
- Benutzer mit externen Objekten verlinken 371

In diesem Kapitel werden die folgenden Themen behandelt:

Externe Objekttypen - Types of External Objects

Mit Natural Security können Sie die Benutzung verschiedener Objekttypen steuern, die verwendet werden von:

- Predict-Objekte
- Andere Objekte

Der in der Natural-Security-Dokumentation verwendete Begriff externe Objekte (External Objects) umfasst alle im Folgenden aufgeführten Objekttypen.

Predict-Objekte

Im Folgenden sind die Predict-Objekttypen aufgeführt (sie sind in der Predict-Dokumentation unter *Natural Security External Object Types for Predict* beschrieben):

Externe Objekttypen für Predict		Code *
Dokumentationsobjekte	*PRD-Docu-Object	PO
Externe Objekte	*PRD-Ext-Object	PE
Funktionen	*PRD-Function	PF
3GL-Bibliotheken	*PRD-3GL-Library	PL

* Die zweistelligen Codes sind die entsprechenden Objekttyp-Codes, die von einigen Natural Security-Funktionen verwendet werden.

Vorsicht: Für Dokumentationsobjekte der Typen Base Application (Basisanwendung) und Compound Application (Verbundanwendung) (SY-B und SY-O) wird dringend empfohlen, anstelle des Natural Security-Subsystems für externe Objekte das Application Maintenance Subsystem zu verwenden. Siehe Kapitel *Natural Development Server-Anwendungen schützen*.

Andere Objekte

Die folgenden Objekttypen werden von verschiedenen anderen Produkten verwendet (sie werden in der entsprechenden Produktdokumentation beschrieben):

Objekt	Code *
Batch-Jobs	JB
Datasets	DS
Nodes	ND
Operations	OP
Printers	PR
Volume Serials	VS
VTAM Applications	VT

* Die zweistelligen Codes sind die entsprechenden Objekttyp-Codes, die von einigen Natural Security-Funktionen verwendet werden.

Kennungen für externe Objekte

Kennungen (IDs) werden von Natural Security verwendet, um externe Objekte und ihre Sicherheitsprofile zu identifizieren. Die Kennung eines externen Objekts muss unter allen Kennungen von Objekten desselben Typs, die in Natural Security definiert sind, eindeutig sein.

Die Länge der Kennungen und andere Namenskonventionen, die für externe Objekte gelten können, unterscheiden sich von Objekttyp zu Objekttyp. Informationen hierzu finden Sie in der jeweiligen Produktdokumentation.

Stern-Notation

Für die Kennung (ID) eines externen Objekts können Sie Stern-Notation verwenden: Wenn Sie ein Sicherheitsprofil für ein externes Objekt anlegen und als Kennung eine Zeichenkette gefolgt von einem Stern (*) wählen, gilt das Sicherheitsprofil für alle Objekte dieses Typs, deren Kennungen mit dieser Zeichenkette beginnen. Für einzelne Objekte (oder Bereiche von Objekten) innerhalb eines solchen Bereichs können Sie weiterhin individuelle Sicherheitsprofile definieren.

Sie können beispielsweise ein Sicherheitsprofil für einen Batch-Job mit der Kennung „ADAX“ erstellen, das für den Batch-Job ADAX gilt. Darüber hinaus können Sie ein Sicherheitsprofil für einen Batch-Job mit der Kennung „ADA*“ anlegen, das für alle anderen Batch-Jobs gilt, deren Kennungen mit „ADA“ beginnen. Sie können ferner ein Sicherheitsprofil für einen Batch-Job mit der Kennung „A*“ erstellen, das für alle anderen Batch-Jobs gilt, deren Kennungen mit „A“ beginnen, und Sie können auch ein Sicherheitsprofil für einen Batch-Job mit der Kennung „*“

erstellen, das für alle anderen Batch-Jobs gilt, für die keine individuellen Sicherheitsprofile definiert sind.

Bestandteile eines Sicherheitsprofils für ein externes Objekt

Bei dem folgenden Bildschirm handelt es sich um den Basis-Bildschirm für ein Sicherheitsprofil für ein externes Objekt, der angezeigt wird, wenn Sie eine der Funktionen Add (Anlegen), Copy (Kopieren), Modify (Ändern), Display (Anzeigen) für das Sicherheitsprofil eines externen Objekts aufrufen:

```
11:31:46                    *** NATURAL SECURITY ***                2021-12-31
                                 - Modify Dataset -

                                                    Modified .. 2021-12-12 by SAG

  Dataset ........... XYZ.SYS.SOURCE


  ------ Default Access -------
  N I Info
  N R Read
  N A Alter
  N D Delete









  Additional Options ... N


  Enter-PF13--PF14--PF15--PF16--PF17--PF18--PF19--PF20--PF21--PF22--PF23--PF24---
        Refr        Menu
```

Dieser Bildschirm ist je nach Objekttyp geringfügig unterschiedlich.

Die einzelnen Bestandteile, die Sie als Teil des Sicherheitsprofils eines externen Objekts definieren können, werden im folgenden erläutert.

Default Access - Standardzugriff

In dieser Spalte können Sie allgemeine Zugriffsmethoden für das externe Objekt zulassen oder nicht zulassen. Die möglichen Zugriffsmethoden unterscheiden sich, wie unten dargestellt, von Objekttyp zu Objekttyp:

Zugriff auf Predict-Dokumentationsobjekte, externe Objekte und 3GL-Bibliotheken:	
R	Read: Lesen
A	Add: Anlegen
M	Modify: Ändern
D	Delete: Löschen
Zugriff auf Predict-Funktionen:	
E	Execute: Ausführen
Zugriff auf Batch-Jobs:	
I	Display: Anzeigen
S	Submit: Starten
A	Alter: Ändern
D	Delete: Löschen
Zugriff auf Datasets:	
I	Info: Informationen anzeigen
R	Read: Lesen
A	Alter: Ändern
D	Delete: Löschen
Zugang zu Knoten, Druckern, VTAM-Anwendungen:	
U	Use: Benutzen
Zugriff auf Operationen:	
P	Passiv
A	Aktiv
Zugriff auf Volume Serials:	
I	Info: Informationen anzeigen
C	Allocate: Zuordnen
A	Alter: Ändern
D	Delete: Löschen

Die einzelnen Zugriffsmethoden sind die gleichen wie in der entsprechenden Produktdokumentation beschrieben.

Kreuzen Sie mit `Y` die Zugriffsmethoden an, die erlaubt werden sollen, mit `N` die Zugriffsmethoden, die nicht erlaubt werden sollen.

Die hier erlaubten/ nicht erlaubten Zugriffsmethoden gelten für alle Benutzer, für die kein spezieller Zugriff über einen Link definiert ist (Informationen zu Links siehe unten unter *Benutzer mit externen Objekten verlinken*).

Zusätzliche Optionen (externe Objekte) - Additional Options (External Objects)

Wenn Sie das Feld **Additional Options** auf dem Basis-Bildschirm für das Sicherheitsprofil mit `Y` markieren, wird ein Fenster angezeigt, in dem Sie die folgenden Optionen auswählen können:

- Maintenance Information - Verwaltungsinformationen
- Security Notes - Sicherheitsvermerke
- Owners - Eigentümer

Die Optionen, bei denen bereits etwas angegeben oder definiert wurde, sind mit einem Pluszeichen (+) gekennzeichnet.

Sie können ein oder mehrere Elemente aus dem Fenster auswählen, indem Sie sie mit einem beliebigen Zeichen markieren. Für jedes ausgewählte Element wird ein weiteres Fenster angezeigt:

Zusätzliche Option	Erläuterung
Maintenance Information (nur Anzeige)	Verwaltungsinformationen. Die folgenden Informationen werden angezeigt: ■ das Datum und die Uhrzeit, wann das Sicherheitsprofil erstellt wurde, die Kennung des Administrators, der es angelegt hat, und (falls zutreffend) die Kennungen der Miteigentümer, die beim Anlegen gegengezeichnet haben; ■ das Datum und die Uhrzeit der letzten Änderung des Sicherheitsprofils, die Kennung des Administrators, der die letzte Änderung vorgenommen hat, und (falls zutreffend) die Kennungen der Miteigentümer, die bei der Änderung gegengezeichnet haben.
Security Notes	Sicherheitsvermerke. Hier können Sie Anmerkungen zum Sicherheitsprofil eingeben.
Owners	Eigentümer. In diesem Fenster können Sie bis zu acht Kennungen von Administratoren eingeben. Nur die hier angegebenen Administratoren sind berechtigt, dieses Serversicherheitsprofil zu verwalten. Wird kein Eigentümer angegeben, kann jeder Benutzer des Typs „Administrator“ das Sicherheitsprofil verwalten. Zu jedem Eigentümer kann optional im Feld nach der Kennung die Anzahl der Miteigentümer angegeben werden, deren Gegenzeichnung für die Verwaltungsberechtigung erforderlich ist. Informationen zu Eigentümern und Miteigentümern finden Sie im Kapitel *Gegenzeichnungen*.

Sicherheitsprofile für externe Objekte anlegen und verwalten

In diesem Abschnitt werden die Funktionen beschrieben, mit denen Sie Sicherheitsprofile für externe Objekte anlegen und verwalten können.

Folgende Themen werden behandelt:

- Verwaltung externer Objekte aufrufen
- Neues externes Objekt anlegen
- Vorhandene externe Objekte zur Bearbeitung auswählen
- Externes Objekt kopieren
- Externes Objekt ändern
- Externes Objekt umbenennen
- Externes Objekt löschen
- Externes Objekt anzeigen

Verwaltung externer Objekte aufrufen

Um die Verwaltung externer Objekte aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) die Option **Maintenance**.

Es wird ein Fenster angezeigt.

2 Markieren Sie in dem Fenster einen externen Objekttyp mit einem Zeichen oder mit dem Cursor.

Die Auswahlliste **Maintenance** für den gewählten Objekttyp wird angezeigt.

3 Von dieser Auswahlliste aus können Sie alle Verwaltungsfunktionen wie unten beschrieben aufrufen.

Neues externes Objekt anlegen

Die Funktion **Add External Object** wird verwendet, um externe Objekte in Natural Security zu definieren, d.h. um Sicherheitsprofile für sie anzulegen.

Um ein neues externes Objekt anzulegen:

1 Geben Sie in der Kommandozeile der **Maintenance**-Auswahlliste das Kommando `ADD` ein.

Es wird ein Fenster angezeigt.

2 In diesem Fenster können Sie eine **Kennung (ID)** für das Objekt eingeben.

Das Fenster **Add** wird für den angegebenen Objekttyp angezeigt.

3 Auf diesem Bildschirm können Sie ein Sicherheitsprofil für das externe Objekt definieren.

Die einzelnen Bestandteile, die Sie auf diesem Bildschirm definieren können, sowie alle zusätzlichen Fenster, die Teil des Sicherheitsprofils eines externen Objekts sein können, werden unter *Bestandteile eines Sicherheitsprofils für ein externes Objekt* beschrieben.

Wenn Sie ein neues externes Objekt anlegen, werden die in Ihrem eigenen Benutzersicherheitsprofil angegebenen Eigentümer automatisch in das Sicherheitsprofil des externen Objekts übernommen.

Vorhandene externe Objekte zur Bearbeitung auswählen

Wenn Sie die Verwaltung für ein externes Objekt aufrufen, wird eine Liste aller externen Objekte dieses Typs angezeigt, für die ein Sicherheitsprofil existiert.

Wenn Sie keine Liste aller vorhandenen externen Objekte wünschen, sondern nur bestimmte externe Objekte aufgelistet haben möchten, können Sie die Option **Start Value** verwenden, siehe Kapitel *Grundlagen der Benutzung*.

Wählen Sie im Hauptmenü (**Main Menu**) die Option **Maintenance**. Es wird ein Fenster angezeigt.

Markieren Sie in dem Fenster einen externen Objekttyp mit einem Zeichen oder mit dem Cursor (und geben Sie, falls gewünscht, einen Startwert ein). Die Auswahlliste für den markierten Objekttyp wird angezeigt, zum Beispiel:

```
13:11:23                *** NATURAL SECURITY ***                2021-12-31
                        - Dataset Maintenance -

 Co Dataset                                                  Message
 __ _____________________________________________________ _____________________
 __ XYZ.S
 __ XYZ.SYS









 Command ===>
 Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
       Help        Exit             Flip  -     +                      Canc
```

In der Liste kann geblättert werden, siehe Kapitel *Grundlagen der Benutzung*.

Die folgenden Verwaltungsfunktionen stehen für externe Objekte zur Verfügung (mögliche Codekürzel sind unterstrichen):

Code	Funktion
CO	**Copy**: Kopieren
MO	**Modify**: Ändern
RE	**Rename**: Umbenennen
DE	**Delete**: Löschen
DI	**Display**: Anzeigen
LU	**Link user**: Benutzer verlinken

Die einzelnen Funktionen werden im Folgenden beschrieben.

Um eine bestimmte Funktion für ein externes Objekt aufzurufen, müssen Sie das Objekt in der Spalte **Co** mit dem entsprechenden Funktionscode markieren.

Sie können mehrere Objekte gleichzeitig für verschiedene Funktionen markieren, d.h. Sie können mehrere Objekte auf dem Bildschirm mit einem Funktionscode kennzeichnen. Für jedes markierte Objekt wird dann der entsprechende Bearbeitungsbildschirm angezeigt. Sie können dann nacheinander für ein Objekt die ausgewählten Funktionen ausführen.

Externes Objekt kopieren

Die Funktion **Copy** wird verwendet, um ein neues externes Objekt in Natural Security zu definieren, indem ein Sicherheitsprofil erstellt wird, das mit dem Sicherheitsprofil eines bereits vorhandenen externen Objekts identisch ist.

Alle Bestandteile des bestehenden Sicherheitsprofils werden in das neue Sicherheitsprofil kopiert - mit *Ausnahme* der Eigentümer (diese werden aus dem Sicherheitsprofil Ihres eigenen Benutzers in das neue Sicherheitsprofil kopiert).

Links, die zu dem bestehenden externen Objekt bestehen, werden *nicht* kopiert.

Um ein externes Objekt zu kopieren:

1. Markieren Sie in der **Maintenance**-Auswahlliste das externe Objekt, dessen Sicherheitsprofil Sie duplizieren möchten, mit dem Funktionscode `CO`.
2. Es wird ein Fenster angezeigt, in dem Sie die Kennung des neuen externen Objekts eingeben müssen.
3. Der Bildschirm **Copy** *`object`* wird angezeigt, auf dem das neue Sicherheitsprofil zu sehen ist.

Seine Bestandteile, die Sie definieren oder ändern können, sind unter *Bestandteile des Sicherheitsprofils eines externen Objekts* beschrieben.

Externes Objekt ändern

Die Funktion **Modify** wird verwendet, um das Sicherheitsprofil eines bestehenden externen Objekts zu ändern.

Dazu:

1 Markieren Sie in der **MaintenanceMaintenance**-Auswahlliste das externe Objekt, dessen Sicherheitsprofil Sie ändern möchten, mit dem Funktionscode `MO`.

2 Der Bildschirm Modify object wird angezeigt. Er zeigt das Sicherheitsprofil an.

Seine Bestandteile, die Sie definieren oder ändern können, sind unter *Bestandteile des Sicherheitsprofils eines externen Objekts* beschrieben.

Externes Objekt umbenennen

Mit der Funktion **Rename** können Sie die Kennung (ID) eines bestehenden Sicherheitsprofils eines externen Objekts ändern.

Dazu:

1 Markieren Sie in der **Maintenance**-Auswahlliste das externe Objekt, dessen Kennung Sie ändern möchten, mit dem Funktionscode `RE`.

2 Es wird ein Fenster angezeigt, in dem Sie eine neue Kennung für das externe Objekt eingeben können.

Externes Objekt löschen

Die Funktion **Delete** wird verwendet, um ein bestehendes Sicherheitsprofil eines externen Objekts zu löschen.

Dazu:

1 Markieren Sie in der **Maintenance**-Auswahlliste das externe Objekt, das Sie löschen möchten, mit dem Funktionscode `DE`.

Das Fenster **Delete** wird angezeigt.

2 ■ Wenn Sie sich gegen das Löschen des Sicherheitsprofils des externen Objekts entscheiden, können Sie das Fenster verlassen, indem Sie ENTER drücken, ohne etwas eingegeben zu haben.

- Um das Sicherheitsprofil des externen Objekts zu löschen, müssen Sie dessen Kennung (ID) in das Fenster eingeben, um das Löschen zu bestätigen.

Wenn Sie ein externes Objekt löschen, werden auch alle bestehenden Links zu diesem externen Objekt gelöscht.

Wenn Sie mehr als ein externes Objekt mit `DE` markieren, wird ein Fenster angezeigt, in dem Sie gefragt werden, ob Sie die Löschung des Sicherheitsprofils jedes einzelnen externen Objekts mit der Eingabe der Kennung des Objekts bestätigen möchten, oder ob alle zum Löschen ausgewählten externen Objekte ohne diese Einzelbestätigung gelöscht werden sollen. Achten Sie darauf, nicht versehentlich ein externes Objekt zu löschen.

Externes Objekt anzeigen

Die Funktion **Display** wird verwendet, um das Sicherheitsprofil eines bestehenden externen Objekts anzuzeigen.

Dazu:

- Markieren Sie in der **Maintenance**-Auswahlliste das externe Objekt, dessen Sicherheitsprofil Sie anzeigen möchten, mit dem Funktionscode `DI`.

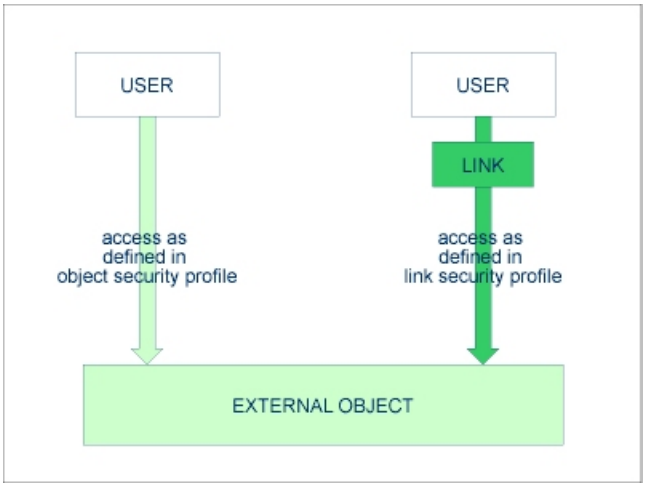
  Der Bildschirm **Display** *`object`* wird angezeigt.

  Er zeigt das Sicherheitsprofil an. Seine Bestandteile sind unter ***Bestandteile des Sicherheitsprofils eines externen Objekts*** beschrieben.

Benutzer mit externen Objekten verlinken

Die im Sicherheitsprofil eines externen Objekts erlaubten/nicht erlaubten Zugriffsmethoden gelten für alle Benutzer, die nicht mit dem externen Objekt verlinkt sind.

Wenn Sie einem einzelnen Benutzer mehr oder weniger Zugriffsmethoden erlauben wollen, können Sie den Benutzer mit dem externen Objekt *verlinken* und im Sicherheitsprofil des Links festlegen, welche Zugriffsmethoden für diesen bestimmten Benutzer verfügbar sein sollen. Das bedeutet, dass Sie durch die Verwendung von Links für verschiedene Benutzer unterschiedliche Zugriffsrechte auf dasselbe externe Objekt definieren können.



Nur Benutzer der Typen Administrator, Person und Group (Gruppe) können mit einem externen Objekt verlinkt werden. Administratoren und Personen können entweder direkt oder über eine Gruppe mit einem externen Objekt verlinkt werden. Benutzer vom Typ Mitglied und Terminal können nur über eine Gruppe mit einem externen Objekt verlinkt werden, d.h. sie müssen einer Gruppe zugeordnet werden und die Gruppe muss mit dem externen Objekt verlinkt werden.

Um Verknüpfungen zwischen Benutzern und externen Objekten herzustellen und zu verwalten, stehen zwei Funktionen zur Verfügung:

- eine Benutzerverwaltungsfunktion (**User Maintenance**), um *einen Benutzer* mit *einem oder mehreren externen Objekten* zu *verlinken*,
- eine Funktion zur Verwaltung externer Objekte (**External Object Maintenance**), um *einen oder mehrere Benutzer mit einem externen Objekt* zu verlinken.

Die beiden Funktionen werden im Folgenden beschrieben.

Einzelnen Benutzer mit externen Objekten verlinken

Um einen einzelnen Benutzer mit einem oder mehreren externen Objekten zu verlinken:

1 Markieren Sie in der **User Maintenance**-Auswahlliste den Benutzer, den Sie verlinken möchten, mit dem Funktionscode `LO`.

2 Es erscheint ein Fenster, in dem Sie mit dem Cursor oder mit einem Zeichen den Typ des externen Objekts markieren, mit dem Sie den Benutzer verlinken möchten.

Außerdem bietet das Fenster die folgenden Optionen:

- **Start value**
  Sie können einen Startwert für die Liste der anzuzeigenden Objekte eingeben, siehe Kapitel *Grundlagen der Benutzung*.
- **Selection criterion**
  `N` = None/kein Selektionskriterium: Es werden alle Objekte aufgelistet.

  `L` = Linked: Es werden nur Objekte aufgelistet, mit denen der Benutzer bereits verlinkt ist (normale und spezielle Links, einschließlich vorübergehend gesperrter).

  `U` = Unlinked: Es werden nur Objekte aufgelistet, mit denen der Benutzer noch nicht verlinkt ist.

3 Anschließend wird die Auswahlliste **Link User to** *objects* angezeigt, die die Liste der Objekte enthält. Zum Beispiel:

```
16:04:48                  *** NATURAL SECURITY ***                2021-12-31
                           - Link User to Dataset -                          ↩
                                                                             ↩
 User ID .... AD          User Name .... ARTHUR DENT                       ↩
                                                  Access                     ↩
 Co Dataset                                       IRAD     Message           ↩
__ ____________________________________________ ________ ____________________
__ XYZ.S                                         I_______                   ↩
__ XYZ.SYS                                       I_A_____                   ↩
                                                                             ↩
                                                                             ↩
                                                                             ↩
                                                                             ↩
                                                                             ↩
                                                                             ↩
                                                                             ↩
                                                                             ↩
                                                                             ↩
                                                                             ↩
                                                                             ↩
                                                                             ↩
                                                                             ↩
                                                                             ↩
 Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
       Help        Exit             Flip  -     +                      Canc ↩
 Command ===> ____________________________________________________________________
```

In der Liste kann geblättert werden, siehe *Grundlagen der Benutzung*.

Markieren Sie in der Liste die externen Objekte, mit denen Sie den Benutzer verlinken möchten. In der Spalte **Co** können Sie jedes Objekt mit einem der folgenden Funktionscodes markieren (mögliche Code-Abkürzungen sind unterstrichen):

Code	Funktion
LK	Link: Der Benutzer kann das externe Objekt mit einem speziellen Sicherheitsprofil verwenden, das für den Link zu definieren ist. Das Linkprofil hat Vorrang vor dem Profil des externen Objekts (siehe *Link-Sicherheitsprofil anlegen und ändern (externe Objekte)* unten).
CL	Cancel: Ein bestehender Link wird aufgehoben.
DI	Display Object: Das Sicherheitsprofil des Objekts wird angezeigt.
DL	Display Link: Das Sicherheitsprofil des Links wird angezeigt.

Sie können ein oder mehrere Objekte mit einem Funktionscode markieren.

4 Für jedes markierte Objekt werden dann die ausgewählten Funktionen nacheinander ausgeführt. Wenn die Verarbeitung abgeschlossen ist, wird eine Meldung angezeigt, dass der Link zwischen dem Benutzer und dem jeweiligen Objekt nun in Funktion ist.

Mehrere Benutzer mit einem externen Objekt verlinken

Um einen oder mehrere Benutzer mit einem externen Objekt zu verlinken:

1 Markieren Sie in der **Maintenance**-Auswahlliste eines externen Objekts das Objekt, mit dem Sie Benutzer verlinken möchten, mit dem Funktionscode LU.

2 Es wird ein Fenster angezeigt, das folgende Optionen zur Auswahl anbietet:

- **Start value**
  Sie können einen Startwert für die Liste der anzuzeigenden Benutzer eingeben, siehe Kapitel *Grundlagen der Benutzung*.
- **Selection criterion**
  N = None/kein Selektionskriterium: Es werden alle Benutzer aufgelistet.

  L = Linked: Es werden nur Benutzer aufgelistet, mit denen das Objekt bereits verlinkt ist (normale und spezielle Links, einschließlich vorübergehend gesperrter).

  U = Unlinked: Es werden nur Benutzer aufgelistet, mit denen das Objekt noch nicht verlinkt ist.

3 Anschließend wird die Auswahlliste **Link Users to** *object* angezeigt. Zum Beispiel:

```
13:21:12                  *** NATURAL SECURITY ***                2021-12-31
                           - Link Users to Dataset -                        ↩
                                                                            ↩
 Dataset ........... ABC.S                                                  ↩
 Default Access .... I                                                      ↩
                                                 Access                     ↩
 Co User ID  User Name                          T IRAD     Message          ↩
__ ________ ____________________________________ _ ________ ________________
 __ AD       ARTHUR DENT                        A I_A_____                  ↩
 __ ADMIN1   BUNGALOW BILL                      A I_AD____                  ↩
 __ ADMIN2   MARIA ALVAREZ                      P I_______                  ↩
 __ ADMIN3   SARA SANDOVAL                      A I_______                  ↩
 __ ADMIN4   ALOYSIUS PENDERGAST                A IRA_____                  ↩
 __ ADMIN5   JACK SPARROW                       A __AD____                  ↩
 __ ADSON    BRIAN OF NAZARETH                  A I_______                  ↩
 __ AGROUP   CUALQIER GRUPO                     G I__D____                  ↩
 __ HC       HAGBARD CELINE                     P I_______                  ↩
 __ KG       KARL GLOGAUER                      P IR______                  ↩
 __ MW       MIA WALLACE                        A I_______                  ↩
 __ NH       NATHANIEL HAWKEYE                  A ___D____                  ↩
                                                                            ↩
 Command ===> ____________________________________________________________
 Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
       Help        Exit             Flip  -     +                      Canc
```

Die Liste enthält alle Benutzer der Typen (**T**) **G**ruppe (Group), **A**dministrator und **P**ersion.

In der Liste kann geblättert werden, siehe *Grundlagen der Benutzung*.

In der Liste können Sie Benutzer markieren, die Sie mit dem externen Objekt verlinkt haben wollen.

Markieren Sie dazu in der Spalte **Co** jeden betreffenden Benutzer mit einem der folgenden Funktionscodes (mögliche Code-Abkürzungen sind unterstrichen):

Code	Funktion
LK	Link: Der Benutzer kann das externe Objekt mit einem speziellen Sicherheitsprofil verwenden, das für den Link zu definieren ist. Das Linkprofil hat Vorrang vor dem Profil des externen Objekts (siehe *Link-Sicherheitsprofil anlegen und ändern (externe Objekte)* unten).
CL	Cancel: Ein bestehender Link wird aufgehoben.
DI	Display User: Das Sicherheitsprofil des Benutzers wird angezeigt.
DL	Display Link: Das Sicherheitsprofil des Links wird angezeigt.

Sie können ein oder mehrere Objekte mit einem Funktionscode markieren. Für jeden markierten Benutzer werden dann die ausgewählten Funktionen nacheinander ausgeführt. Wenn die Verarbeitung abgeschlossen ist, wird eine Meldung angezeigt, die die zwischen dem Benutzer und dem jeweiligen Objekt nun bestehende Link-Situation bestätigt.

Link-Sicherheitsprofil anlegen und ändern (externe Objekte)

Um ein Link-Sicherheitsprofil anzulegen oder zu ändern:

1 Markieren Sie auf dem Bildschirm **Link User to** *objects* ein externes Objekt mit LK.

Oder:

Markieren Sie auf dem Bildschirm **Link Users to** *object* einen Benutzer mit LK.

2 Es wird ein Bildschirm angezeigt, auf dem Sie das Sicherheitsprofil für diesen Link definieren können.

Die Standardeinstellungen, die im Link-Sicherheitsprofil erscheinen, werden aus dem Sicherheitsprofil des externen Objekts übernommen.

Die Bestandteile eines Link-Sicherheitsprofils entsprechen denen eines Sicherheitsprofils für ein externes Objekt (siehe *Bestandteile des Sicherheitsprofils für ein externes Objekt*). Darüber hinaus können Sie Aktivierungsdaten festlegen. Diese entsprechen den **Activation Dates** in einem Benutzersicherheitsprofil (siehe *Bestandteile eines Benutzersicherheitsprofils*).

Zugriffsmethoden - Access Methods

Anstatt die Zugriffsmethoden im Link-Sicherheitsprofil zu erlauben/nicht zu erlauben, können Sie auch den entsprechenden Buchstaben an der entsprechenden Stelle in der Spalte **Access** der Auswahlliste **Link User to** *objects* oder **Link Users to** *object* eingeben/löschen.

19 Mailboxen

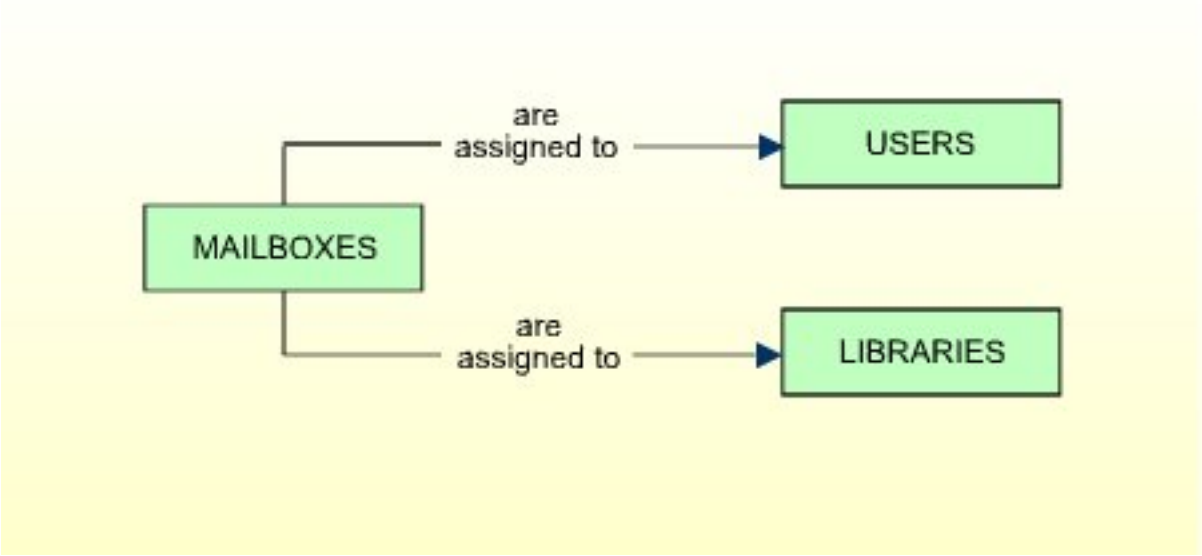
- Was ist eine Mailbox? 380
- Nachricht senden 380
- Nachricht empfangen 381
- Mailbox-Kennung - Mailbox ID 382
- Bestandteile eines Mailbox-Sicherheitsprofils 382
- Mailbox-Sicherheitsprofile anlegen und verwalten 385

In diesem Kapitel werden die folgenden Themen behandelt:

Was ist eine Mailbox?

Eine Mailbox ist ein Informationsbildschirm, der dazu verwendet werden kann, Nachrichten an Natural-Benutzer zu senden. Sie lässt sich am besten als Schwarzes Brett beschreiben.

Mailboxen können Benutzern und/oder Bibliotheken zugewiesen werden.



Wenn sich ein Benutzer bei einer Bibliothek anmeldet, werden ihm die seinem Sicherheitsprofil zugeordneten Mailboxen sowie die Mailboxen, die dem Sicherheitsprofil der Bibliothek zugeordnet sind, angezeigt.

Um eine Mailbox anzulegen, müssen Sie sie in Natural Security definieren, d. h. ein Sicherheitsprofil für sie erstellen.

Nachricht senden

Jeder, der in einem Mailbox-Sicherheitsprofil als Mailer (Versender) angegeben ist, darf die Mailbox benutzen. Wenn eine Gruppe als Mailer angegeben ist, kann jeder in der Gruppe enthaltene Benutzer die Mailbox verwenden. Ist kein Mailer angegeben, kann jeder Benutzer die Mailbox verwenden.

Ein Mailer kann eine Mailbox mit dem Natural-Systemkommando `MAIL` aufrufen (vorausgesetzt, der Mailer ist an einer Bibliothek angemeldet, für die der Kommandomodus erlaubt ist).

Beispiele:

`MAIL FUGAZI`	Dieses Kommando ruft den Nachrichtenbildschirm der Maibox `FUGAZI` auf.
`MAIL ?`	Dieses Kommando zeigt eine Liste aller Mailboxen an, die der Mailer benutzen darf. Der Mailer kann dann eine Mailbox aus der Liste auswählen.

Sobald die gewünschte Mailbox aufgerufen ist, kann der Mailer eine Nachricht eingeben, Text zu einer bestehenden Nachricht hinzufügen oder aus ihr löschen oder das Gültig-von/Bis-Datum (**Valid from/to**) ändern.

Die Mailer haben nur Zugriff auf den Nachrichtenbildschirm einer Mailbox, nicht auf das Sicherheitsprofil der Mailbox. Eigentümer können ebenfalls Nachrichten versenden, da sie über das Sicherheitsprofil Zugriff auf den Nachrichtenbildschirm einer Mailbox haben. Das Natural-Systemkommando `MAIL` kann jedoch nur von Mailern verwendet werden.

Nachricht empfangen

Sobald eine Mailbox definiert ist, kann sie Benutzern und Bibliotheken zugewiesen werden, indem die Mailbox-Kennung (Mailbox ID) im Fenster **Mailboxes** (unter **Additional Options**) der betreffenden Benutzer- und Bibliothekssicherheitsprofile eingegeben wird.

Für die Zuweisung von Mailboxen gilt die Eigentümerlogik, d. h. wenn im Mailboxprofil Eigentümer angegeben sind (siehe *Bestandteile eines Mailboxprofils* unten), können nur diese Eigentümer die Mailbox einem Benutzer oder einer Bibliothek zuweisen.

Die Mailboxen werden einem Benutzer sofort nach jeder erfolgreichen Anmeldung bei einer Bibliothek angezeigt. Folgende Mailboxen werden dem Benutzer in der folgenden Reihenfolge angezeigt:

1. alle Mailboxen, die dem Benutzer zugewiesenen sind,
2. alle Mailboxen, die der Bibliothek zugewiesen sind,
3. alle Mailboxen, die der Gruppe zugeordnet sind, über die der Benutzer angemeldet ist (wenn die Bibliothek personengeschützt ist und der Benutzer über eine Gruppe verlinkt ist),
4. alle Mailboxen, die dem Terminal des Benutzers zugewiesen sind, und alle Mailboxen, die der Gruppe zugewiesen sind, über die das Terminal verlinkt ist (wenn die Bibliothek terminalgeschützt ist (**Terminal-protected** auf `A` gesetzt)).

Müsste eine Mailbox einem Benutzer mehrfach angezeigt werden (z. B. wenn dieselbe Mailbox sowohl dem eigenen Sicherheitsprofil als auch dem der Gruppe, über die der Benutzer verlinkt ist, zugewiesen ist), wird sie nur einmal angezeigt. Eine wiederholte Anzeige wird unterdrückt.

Die Anzeige von Mailboxen kann vom Benutzer nicht unterdrückt werden.

Eine Mailbox wird nicht angezeigt,

- wenn sie leer ist, d. h. wenn sie nur Leerzeichen enthält,
- wenn das Gültig ab-Datum (**Valid from**) noch nicht erreicht oder das Gültig bis-Datum (**Valid to**) überschritten ist.

Mailbox-Kennung - Mailbox ID

Mailbox-Kennungen werden von Natural Security verwendet, um Mailboxen und ihre Sicherheitsprofile zu identifizieren.

Eine Mailbox-Kennung kann bis zu 8 Zeichen lang sein, muss mit einem alphabetischen Zeichen beginnen und muss unter allen in Natural Security definierten Mailbox-Kennungen eindeutig sein.

Bevor Sie mit der Definition von Mailboxen beginnen, ist es ratsam, ein logisches System von Mailbox-Kennungen zu entwerfen. Dies erleichtert Ihnen die Identifizierung von Mailboxen bei der Verwaltung von Natural Security.

Mailbox für die Erstanmeldung (Initial Logon)

Die Mailbox-Kennung `1INITIAL` dient einem besonderen Zweck: Wenn Sie eine Mailbox mit dieser Mailbox-Kennung definieren, wird sie jedem Benutzer nach einer erfolgreichen Erstanmeldung bei Natural angezeigt.

Die Mailbox `1INITIAL` muss keinem Benutzer und keiner Bibliothek zugewiesen werden.

Bestandteile eines Mailbox-Sicherheitsprofils

Der folgende Bildschirm zeigt ein Beispiel für ein Mailbox-Sicherheitsprofil:

```
13:00:00                  *** NATURAL SECURITY ***                  2021-12-31
                             - Modify Mailbox -

 Mailbox ID: MAIL2112                            Created: 2002-09-14 by: SAG
 Mailb.Name: MAILBOX YYZ_____________________  Modified: 2021-10-12 by: SAG
 Last mailed on .. 2021-06-11 at: 12:00:58 by: IW
 Valid from ...... 1999-12-31 to  2699-12-31

 ------------- Mailbox Security Notes -------------  Mailers-    -- Owners --
 ____________________________________________________  AD_______    _________   _
 ____________________________________________________  HW_______    _________   _
 ____________________________________________________  IW_______    _________   _
 ____________________________________________________  _________    _________   _
 ____________________________________________________  _________    _________   _
 ____________________________________________________  _________    _________   _
 ____________________________________________________  _________    _________   _
 ____________________________________________________  _________    _________   _
 ____________________________________________________  _________
 ____________________________________________________  _________
 ------------------------------------------------------ ----------   -------------


 Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
       Help  PrevM Exit  AddOp       Flip                              Canc
```

Die einzelnen Bestandteile eines Mailbox-Sicherheitsprofils werden im Folgenden erläutert.

Die folgenden Informationen werden von Natural Security eingegeben:

Feld	Erläuterung
Mailbox ID	Mailbox-Kennung. Die Kennung (ID), mit der Sie die Mailbox in Natural Security definiert haben.
Created/by	Erstellt/von. Das Datum, an dem das Sicherheitsprofil angelegt wurde, und die Kennung des Administrators, der das Sicherheitsprofil angelegt hat.
Modified/by	Geändert/von. Das Datum, an dem das Sicherheitsprofil zuletzt geändert wurde, und die Kennung (ID) des Administrators, der die letzte Änderung vorgenommen hat.
Last mailed on/at/by	Zuletzt gesendet am/bei/von. Das Datum, die Uhrzeit und die Benutzerkennung der letzten Änderung des Mailbox-Nachrichtenbildschirms und/oder die Gültig von/bis-Daten (**Valid from/to**).
Valid from/to	Gültig von/bis. Der Zeitraum, in dem die Mailbox den Benutzern angezeigt wird, wenn sie sich anmelden. Diese Zeiträume können auf dem Mailbox-Nachrichtenbildschirm festgelegt werden, aber nicht auf dem Sicherheitsprofilbildschirm.

Sie können die folgenden Bestandteile als Teil eines Mailbox-Sicherheitsprofils angeben:

Feld	Erläuterung
Mailbox Name	Mailbox-Name. In diesem Feld können Sie einen Namen für die Mailbox angeben, der bis zu 32 Zeichen lang sein darf.
Mailbox Security Notes	Mailbox-Sicherheitsvermerke. In diesen Zeilen können Sie Anmerkungen zum Sicherheitsprofil eingeben.
Mailers	Versender. Sie können bis zu 10 Kennungen (IDs) von Benutzern (eines beliebigen Benutzertyps) eingeben, die die Mailbox verwenden dürfen, um Nachrichten zu versenden, d. h. den Inhalt des Mailbox-Nachrichtenbildschirms zu ändern. Wird kein Eigentümer angegeben, kann jeder Benutzer vom Typ Administrator dies tun.
Owners	Eigentümer. Sie können bis zu 8 Kennungen von Administratoren eingeben. Nur die hier angegebenen Administratoren sind berechtigt, das Sicherheitsprofil der Mailbox zu verwalten und die Mailbox Benutzern/Bibliotheken zuzuweisen. Wird kein Eigentümer angegeben, kann jeder Benutzer vom Typ Administrator dies tun. Für jeden Eigentümer kann optional im Feld nach der Kennung die Anzahl der Miteigentümer angegeben werden, deren Gegenzeichnung für die Verwaltungs-/Zuweisungserlaubnis erforderlich ist. Eine Erläuterung zu Eigentümern und Miteigentümern finden Sie im Kapitel *Gegenzeichnungen*.

Wenn Sie auf dem Bildschirm **Add Mailbox** PF4 drücken, wird der Nachrichtenbildschirm der Mailbox angezeigt:

```
13:00:27              *** Mailbox Message Screen ***               2021-12-31

         Mailbox ID ... MAIL2112      Valid from 2021-05-24 to 2699-12-31
         Last mailed on 2021-06-11 at 12:00:58 by IW
         +------------------------------------------------------------+
         I THERE IS UNREST IN THE FOREST                              I
         I THERE IS TROUBLE WITH THE TREES                            I
         I FOR THE MAPLES WANT MORE SUNLIGHT                          I
         I AND THE OAKS IGNORE THEIR PLEAS                            I
         I                                                            I
         I                                                            I
         I                                                            I
         I                                                            I
         I                                                            I
         I                                                            I
         I                                                            I
         I                                                            I
         I                                                            I
         I                                                            I
         I                                                            I
         +------------------------------------------------------------+
```

Valid from/to	Gültig von/bis. Diese Angaben können gemacht werden, wenn eine Nachricht nur für einen bestimmten Zeitraum relevant ist und die Mailbox daher nur innerhalb dieses Zeitraums den Benutzern bei der Anmeldung angezeigt werden soll. Wird ein von-Datum angegeben, wird die Mailbox erst ab diesem Tag angezeigt. Wird ein bis-Datum angegeben, wird die Mailbox nach diesem Tag nicht mehr angezeigt. Jeder Versender (Mailer) oder Eigentümer (Owner) kann diese Angaben machen. Das Format, in dem die Angaben gemacht werden müssen, hängt von der Einstellung des Natural-Profilparameters `DTFORM` ab.

Mailbox-Sicherheitsprofile anlegen und verwalten

In diesem Abschnitt werden die Funktionen zum Anlegen (Add) und Verwalten (Maintain) von Mailbox-Sicherheitsprofilen beschrieben. Die folgenden Themen werden behandelt:

- Mailbox-Verwaltung aufrufen
- Neue Mailbox anlegen
- Vorhandene Mailboxen zur Bearbeitung auswählen
- Mailbox kopieren
- Mailbox ändern
- Mailbox umbenennen

- Mailbox löschen
- Mailbox anzeigen

Mailbox-Verwaltung aufrufen

Um die Mailbox-Verwaltung aufzurufen:

1 Wählen Sie im Hauptmenü (**Main Menu**) den Menüpunkt **Maintenance**.

2 Es wird ein Fenster angezeigt, in dem Sie den Objekttyp **Mailbox** mit einem Zeichen oder mit dem Cursor markieren können.

3 Die **Mailbox Maintenance**-Auswahlliste wird angezeigt.

Von dieser Auswahlliste aus können Sie alle Funktionen der Mailbox-Verwaltung wie im Folgenden beschrieben aufrufen.

Neue Mailbox anlegen

Die Funktion **Add Mailbox** wird verwendet, um eine neue Mailbox in Natural Security zu definieren, d.h. ein Mailbox-Sicherheitsprofil anzulegen.

Um ein neues Mailbox-Sicherheitsprofil anzulegen:

1 Geben Sie das Kommando `ADD` in die Kommandozeile der **Mailbox Maintenance**-Auswahlliste ein.

2 Es wird ein Fenster angezeigt, in dem Sie eine Mailbox-Kennung (**Mailbox ID**) eingeben können.

3 Der Bildschirm **Add Mailbox** wird angezeigt. Auf diesem Bildschirm können Sie ein Sicherheitsprofil für die Mailbox definieren. Die Bestandteile, die Sie definieren oder angeben können, werden unter *Bestandteile eines Mailbox-Sicherheitsprofils* erläutert.

Wenn Sie eine neue Mailbox anlegen, werden die in Ihrem eigenen Benutzer-Sicherheitsprofil angegebenen Eigentümer automatisch in das Sicherheitsprofil der Mailbox kopiert.

Vorhandene Mailboxen zur Bearbeitung auswählen

Wenn Sie die Option **Mailbox Maintenance** aufrufen, wird eine Liste aller Mailboxen angezeigt, die in Natural Security definiert wurden.

Wenn Sie nicht alle, sondern nur bestimmte Mailboxen auflisten möchten, können Sie die Option **Start Value** verwenden, siehe Kapitel *Grundlagen der Benutzung*.

Wählen Sie im Hauptmenü (**Main Menu**) die Option **Maintenance**. Es wird ein Fenster angezeigt.

Markieren Sie in dem Fenster den Objekttyp **Mailbox** mit einem Zeichen oder mit dem Cursor (und geben Sie, falls gewünscht, einen Startwert ein).

Die **Mailbox Maintenance**-Auswahlliste wird angezeigt:

```
11:35:19                  *** NATURAL SECURITY ***                2021-12-31
                            - Mailbox Maintenance -

 Co Mailbox ID Mailbox Name                      Message
 __ __________ ____________________________ ____________________
 __ MAILAZ     MAILAZ
 __ MAILB      MAILBOX B
 __ MAILF      MAIL-FINANCE
 __ MAILLP     PLEASE MR POSTMAN
 __ MAILLP1    CHAIN MAIL
 __ MAILLP2
 __ MAILSAG    MAILBOX FOR SAG
 __ MAILTM
 __ MAIL1
 __ MAIL10     NEWS AT 10
 __ MAIL11
 __ MAIL12
 __ MAIL13
 __ MAIL14
 __ MAIL2112   MAILBOX YYZ

 Command ===>
 Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
       Help        Exit              Flip  -     +                      Canc
```

Zu jeder Mailbox werden ihre Mailbox-Kennung (Mailbox ID) und ihr Name angezeigt.

In der Liste kann geblättert werden, siehe *Grundlagen der Benutzung*.

Die folgenden Mailbox-Verwaltungsfunktionen stehen zur Verfügung (mögliche Code-Abkürzungen sind unterstrichen):

Code	Funktion
CO	**Copy**: Mailbox kopieren
MO	**Modify**: Mailbox ändern
RE	**Rename**: Mailbox umbenennen
DE	**Delete**: Mailbox löschen
DI	**Display**: Mailbox anzeigen

Um eine bestimmte Funktion für eine Mailbox aufzurufen, müssen Sie die Mailbox in der Spalte **Co** mit dem entsprechenden Funktionscode markieren.

Sie können mehrere Mailboxen gleichzeitig mit verschiedenen Funktionen markieren, d.h. Sie können mehrere Mailboxen auf dem Bildschirm mit einem Funktionscode markieren. Für jede markierte Mailbox wird der entsprechende Verarbeitungsbildschirm angezeigt. Sie können dann für eine Mailbox nach der anderen die ausgewählten Funktionen ausführen.

Mailbox kopieren

Die Funktion **Copy Mailbox** wird verwendet, um eine neue Mailbox in Natural Security zu definieren. Dazu wird ein Sicherheitsprofil angelegt, das mit einem bestehenden Mailbox-Sicherheitsprofil identisch ist.

Alle Bestandteile des bestehenden Sicherheitsprofils werden in das neue Mailbox-Sicherheitsprofil kopiert - mit *Ausnahme* der Eigentümer (diese werden aus Ihrem eigenen Benutzersicherheitsprofil in das neue Mailbox-Sicherheitsprofil kopiert).

Um eine Mailbox zu kopieren:

1. Markieren Sie in der **Mailbox Maintenance**-Auswahlliste die Mailbox, deren Sicherheitsprofil Sie duplizieren möchten, mit dem Funktionscode `CO`.
2. Es wird ein Fenster angezeigt, in dem Sie die Mailbox-Kennung (Mailbox ID) und den Namen der neuen Mailbox eingeben können.
3. Es erscheint das Fenster **Copy Mailbox**, in dem das neue Sicherheitsprofil angezeigt wird.

   Seine Bestandteile, die Sie definieren oder ändern können, werden unter ***Bestandteile eines Mailbox-Sicherheitsprofils*** erläutert.

Mailbox ändern

Die Funktion **Modify Mailbox** wird verwendet, um ein bestehendes Mailbox-Sicherheitsprofil zu ändern.

Dazu:

1. Markieren Sie in der **Mailbox Maintenance**-Auswahlliste die Mailbox, deren Sicherheitsprofil Sie ändern möchten, mit dem Funktionscode `MO`.
2. Der Bildschirm **Modify Mailbox** wird angezeigt. Er zeigt das Mailbox-Sicherheitsprofil an.

   Die Bestandteile, die Sie ändern können, werden unter ***Bestandteile eines Mailbox-Sicherheitsprofils*** erläutert.

Mailbox umbenennen

Die Funktion **Rename Mailbox** wird verwendet, um die Mailbox-Kennung (Mailbox ID) eines bestehenden Mailbox-Sicherheitsprofils zu ändern.

Dazu:

1 Markieren Sie in der **Mailbox Maintenance**-Auswahlliste die Mailbox, deren Sicherheitsprofil Sie ändern möchten, mit dem Funktionscode `RE`.

2 Es wird ein Fenster angezeigt, in dem Sie eine neue Kennung für die Mailbox eingeben (und optional den Namen ändern) können.

Mailbox löschen

Mit der Funktion **Delete Mailbox** können Sie eine bestehende Mailbox löschen.

Dazu:

1 Markieren Sie in der **Mailbox Maintenance**-Auswahlliste die Mailbox, deren Sicherheitsprofil Sie löschen möchten, mit dem Funktionscode `DE`.

2 Das Fenster **Delete Mailbox** wird angezeigt.

- Wenn Sie die Mailbox nicht löschen wollen, können Sie das Fenster mit ENTER verlassen, ohne etwas einzutippen.
- Um die Mailbox zu löschen, müssen Sie die Mailbox-Kennung (Mailbox ID) in das Fenster eingeben, um den Löschvorgang zu bestätigen.

Wenn Sie eine Mailbox löschen, wird die Mailbox-Kennung (Mailbox ID) gleichzeitig aus den Sicherheitsprofilen der Benutzer und Bibliotheken entfernt, denen die Mailbox zugewiesen wurde.

Wenn Sie mehrere Mailboxen mit `DE` markieren, wird ein Fenster angezeigt, in dem Sie gefragt werden, ob Sie die Löschung jeder einzelnen Mailbox durch Eingabe der Mailbox-Kennung (Mailbox ID) bestätigen möchten, oder ob alle zum Löschen markierten Mailboxen ohne Einzelbestätigung gelöscht werden sollen. Achten Sie darauf, dass Sie nicht versehentlich eine Mailbox löschen.

Mailbox anzeigen

Die Funktion **Display Mailbox** wird verwendet, um ein bestehendes Mailbox-Sicherheitsprofil anzuzeigen.

Dazu:

1 Markieren Sie in der **Mailbox Maintenance**-Auswahlliste die Mailbox, deren Sicherheitsprofil Sie anzeigen möchten, mit dem Funktionscode `DI`.

2 Sie gelangen auf den Bildschirm **Display Mailbox**, der das Sicherheitsprofil der markierten Mailbox anzeigt.

Seine Bestandteile werden unter *Bestandteile eines Mailbox-Sicherheitsprofils* erläutert.

3 Um den Nachrichtenbildschirm der Mailbox anzuzeigen, müssen Sie auf dem Bildschirm **Display Mailbox** PF4 drücken.

20 Retrieval-Funktionen (Retrieval Subsystem)

- Verwendungszweck der Retrieval-Funktionen 392
- Retrieval-Funktionen aufrufen 392
- Cross-Referenz Benutzer 393
- Cross-Referenz Bibliothek 393
- Cross-Referenz Datei 394
- Cross-Referenz Dienstprogramm (Utility) 394
- Cross-Referenz Anwendung 395
- Cross-Referenz Externes Objekt 395
- Cross-Reference Mailbox 396
- Retrieval-Funktionen in Batch Mode - Program RETRIEVE 396

In diesem Kapitel werden die folgenden Themen behandelt:

Verwendungszweck der Retrieval-Funktionen

Mit dem Retrieval-Subsystem von Natural Security können Sie Informationen über die in Natural Security definierten Objekte und über die bestehenden Beziehungen zwischen diesen Objekten auffinden. Die Retrieval-Funktionen ermöglichen es Ihnen, die vorhandenen Sicherheitsprofildefinitionen und ihre Auswirkungen zu überprüfen.

Mit dem Retrieval-Subsystem können Sie keine Natural-Security-Verwaltung durchführen. Sie können nur Dinge ansehen.

Retrieval-Funktionen aufrufen

Um Retrieval-Funktionen aufzurufen:

1 Markieren Sie im Hauptmenü (**Main Menu**) die Option **Retrieval**.

2 Es wird ein Fenster angezeigt, in dem Sie einen Objekttyp mit einem Zeichen oder mit dem Cursor markieren können (und, wenn Sie möchten, die Optionen **Start Value** und **Type/Status** verwenden können, wie im Kapitel *Grundlagen der Benutzung* beschrieben).

Die Auswahlliste für den markierten Objekttyp wird angezeigt.

In der Liste kann geblättert werden, wie im Kapitel *Grundlagen der Benutzung* beschrieben.

3 Von der Liste aus können Sie die folgenden Retrieval-Funktionen aufrufen (mögliche Code-Abkürzungen sind unterstrichen):

Code	Funktion	Erläuterung
DI	Display	Diese Anzeigefunktionen sind dieselben, die in den entsprechenden Kapiteln für jeden Objekttyp beschrieben sind.
XR	Cross-Reference	Diese Funktionen werden im Folgenden für jeden Objekttyp beschrieben.

Um eine bestimmte Funktion für ein Objekt aufzurufen, müssen Sie das Objekt mit dem entsprechenden Funktionscode in der Spalte **Co** in der Auswahlliste markieren.

Sie können mehrere Objekte gleichzeitig für verschiedene Funktionen markieren, d.h. Sie können mehrere Objekte auf dem Bildschirm mit einem Funktionscode kennzeichnen. Für jedes markierte Objekt wird dann der entsprechende Verarbeitungsbildschirm angezeigt. Sie können dann für ein Objekt nach dem anderen die ausgewählten Funktionen ausführen.

Cross-Referenz Benutzer

Mit der Funktion **Cross-Reference User** können Sie Informationen über einen Benutzer abrufen.

Dazu:

1 Markieren Sie in der **User Retrieval**-Auswahlliste den betreffenden Benutzer mit dem Funktionscode `XR`.

2 Es wird ein Fenster angezeigt, in dem Sie durch Markieren mit einem beliebigen Zeichen einen oder mehrere der folgenden Objekte auswählen können:

Objekt	Angezeigte Informationen
Applications	Eine Liste aller Basis- und Verbundanwendungen (Base und Compound Applications), mit denen der Benutzer verlinkt ist.
Libraries	Eine Liste aller Bibliotheken, die dem Benutzer zur Verfügung stehen.
Linked Libraries	Eine Liste aller Bibliotheken, mit denen der Benutzer verlinkt ist (direkt oder über eine Gruppe).
DDMs / Files	Eine Liste aller DDMs, mit denen die private Bibliothek des Benutzers verlinkt ist.
Groups / Members	Eine Liste aller Gruppen, denen der Benutzer angehört. Wenn der Benutzer eine Gruppe ist, eine Liste aller Benutzer, die in dieser Gruppe enthalten sind.
Owned Objects	Eine Liste aller Sicherheitsprofile, deren Eigentümer der Benutzer ist.
DDM Modifier	Eine Liste aller DDM/Datei-Sicherheitsprofile, in denen der Benutzer als DDM-Änderer angegeben ist.
External Objects	Eine Liste aller externen Objekte, mit denen der Benutzer verlinkt ist.
Command Processors	Die Funktionssicherheitsangaben für jeden Kommandoprozessor, für den Funktionssicherheit für den Benutzer definiert ist.
Utilities	Eine Liste aller benutzerspezifischen und benutzerbibliotheksspezifischen Dienstprogrammprofile, die für den Benutzer definiert sind.

Cross-Referenz Bibliothek

Mit der Funktion **Cross-Reference Library** können Sie Informationen über eine Bibliothek abrufen.

Dazu:

1 Markieren Sie in der **Library Retrieval**-Auswahlliste die betreffende Bibliothek mit dem Funktionscode `XR`.

2 Es wird ein Fenster angezeigt, in dem Sie durch Markieren mit einem beliebigen Zeichen einen oder mehrere der folgenden Objekte auswählen können:

Objekt	Angezeigte Informationen
DDMs / Files	Eine Liste aller Benutzer, die mit der Bibliothek verlinkt sind.
Users	Eine Liste aller Benutzer, die mit der Bibliothek verlinkt sind.
Command Processors	Die Funktionssicherheitsangaben zu jedem Kommandoprozessor in der Bibliothek, für den Funktionssicherheit definiert ist.
Utilities	Eine Liste aller bibliotheksspezifischen und benutzerbibliotheksspezifischen Dienstprogrammprofile, die für die Bibliothek definiert sind.

Cross-Referenz Datei

Die Funktion **Cross-Reference File** ist nur auf Großrechnern verfügbar. Sie können damit feststellen, welche Bibliotheken mit einer Datei verlinkt sind.

Dazu:

1 Markieren Sie in der **File Retrieval**-Auswahlliste die betreffende Datei mit dem Funktionscode `XR`.

2 Es wird ein Fenster angezeigt, in dem Sie durch Markieren mit einem beliebigen Zeichen einen oder beide der folgenden Objekte auswählen können:

Objekt	Angezeigte Informationen
Libraries	Eine Liste aller Bibliotheken, die mit der Datei verlinkt sind.
Private Libraries	Eine Liste aller Benutzer, deren private Bibliotheken mit der Datei verlinkt sind.

Cross-Referenz Dienstprogramm (Utility)

Mit der Funktion **Cross-Reference Utility** können Sie feststellen, welche Dienstprogrammprofile zu einem Dienstprogramm existieren.

Dazu:

1 Markieren Sie in der **Utility Retrieval**-Auswahlliste das betreffende Dienstprogramm mit dem Funktionscode `XR`.

2 Es wird ein Fenster angezeigt, in dem Sie durch Markieren mit einem beliebigen Zeichen einen oder mehrere der folgenden Objekte auswählen können:

Objekt	Angezeigte Informationen
Library-Specific Profiles	Bibliotheksspezifische Profile. Eine Liste aller für dieses Dienstprogramm definierten bibliotheksspezifischen Profile (sowie das Standardprofil des Dienstprogramms).
User-Specific and User-Library-Specific Profiles	Benutzerspezifische und benutzerbibliotheksspezifische Profile. Eine Liste aller benutzerspezifischen Profile und benutzerbibliotheksspezifischen Profile, die für dieses Dienstprogramm definiert wurden.
All Profiles	Eine Liste aller benutzerspezifischen Profile, bibliotheksspezifischen Profile und benutzerbibliotheksspezifischen Profile sowie des für dieses Dienstprogramm definierten Standardprofils.

Cross-Referenz Anwendung

Mit der Funktion **Cross-Reference Application** können Sie feststellen, welche Benutzer mit einer Anwendung verlinkt sind.

Dazu:

- Markieren Sie in der **Application Retrieval**-Auswahlliste die betreffende Anwendung mit dem Funktionscode `XR`.

  Es wird eine Liste aller Benutzer angezeigt, die mit der Anwendung verlinkt sind.

Cross-Referenz Externes Objekt

Mit der Funktion **Cross-Reference External Object** können Sie feststellen, welche Benutzer mit einem externen Objekt verlinkt sind.

Dazu:

- Markieren Sie in der **Retrieval**-Auswahlliste für einen externen Objekttyp das betreffende Objekt mit dem Funktionscode `XR`.

  Es wird eine Liste aller Benutzer angezeigt, die mit dem externen Objekt verlinkt sind.

Cross-Reference Mailbox

Mit der Funktion **Cross-Reference Mailbox** können Sie feststellen, welchen Benutzern und Bibliotheken eine Mailbox zugewiesen ist.

Dazu:

1 Markieren Sie in der **Mailbox Retrieval**-Auswahlliste die betreffende Mailbox mit dem Funktionscode `XR`.

2 Es wird ein Fenster angezeigt, in dem Sie durch Markieren mit einem beliebigen Zeichen eines oder beide der folgenden Objekte auswählen können:

Objekt	Angezeigte Informationen
Libraries	Eine Liste aller Bibliotheken, denen die Mailbox zugewiesen ist.
Users	Eine Liste aller Benutzer, denen die Mailbox zugewiesen ist.

Retrieval-Funktionen in Batch Mode - Program RETRIEVE

Sie können alle Retrieval-Informationen für alle Objekte eines bestimmten Objekttyps auf einmal abrufen. Zu diesem Zweck steht Ihnen in der Bibliothek `SYSSEC` das Programm `RETRIEVE` zur Verfügung. Dieses Programm führt die Funktionen **Display** und **Cross-Reference** für alle Objekte eines bestimmten Objekttyps aus, d.h. es zeigt Anzeige- und Cross-Referenz-Informationen für alle ausgewählten Objekte an.

Die folgenden Informationen können abgerufen werden:

- Ausgabe 1: eine Liste aller ausgewählten Objekte, mit grundlegenden Informationen zu jedem Objekt.
- Ausgabe 2: Anzeige der Sicherheitsprofile der ausgewählten Objekte.
- Ausgabe 3: Cross-Referenz-Informationen zu den ausgewählten Objekten.
- Ausgabe 4: Anzeige der Sicherheitsprofile von speziellen Links zwischen Benutzern und Bibliotheken.

Mit Eingabeparametern können Sie die Funktionen auf einen bestimmten Bereich von Objekten einschränken und die Reihenfolge der Ausgabe bestimmen. Die Eingabeparameter für das Programm `RETRIEVE` sind:

Parameter	Erläuterung	
1. Parameter	**Objekttyp**: US (Users) für Benutzer LI (Libraries) für Bibliotheken FI (Files) für Dateien (nur auf Großrechnern) MA für Mailboxen, oder der entsprechende Code für einen externen Objekttyp.	
2. Parameter	■ **User type** Benutzertyp (für Objekttyp US): A = Administrator, P = Person, M = Member, G = Group, T = Terminal, B = Batch User. ■ **File status** File Status (für den Objekttyp FI): PUBL = Public, ACCE = Access, PRIV = Private.	
3. Parameter	**Start value** Startwert: Ein Objektname (optional mit Stern), um nur Informationen über einen bestimmten Bereich von Objekten zu erhalten.	
4. und 5. Parameters	**Date from/to** Datum von/bis: Ein Datumsbereich, um nur Informationen über Objekte zu erhalten, die innerhalb eines bestimmten Zeitraums erstellt/zuletzt geändert wurden.	
6. Parameter	**Function** Legt fest, welche Informationen ausgegeben werden und die Ausgabereihenfolge:	
	S	Ausgabe 1.
	A	Ausgabe 1, dann Ausgabe 2 & 3 für ein Objekt, dann Ausgabe 2 & 3 für das nächste Objekt usw.
	AE	Ausgabe 1, dann Ausgabe 2, 3 & 4 für ein Objekt, dann Ausgabe 2, 3 & 4 für das nächste Objekt usw. X Ausgabe 3.
	X	Ausgabe 3.
	XE	Ausgabe 3 & 4 für ein Objekt, dann Ausgabe 3 & 4 für das nächste Objekt usw.
	D	Ausgabe 1, dann Ausgabe 2 für jedes Objekt.
	Z	Ausgabe 1, dann Ausgabe 2 für jedes Objekt, dann Ausgabe 3 für jedes Objekt.
	ZE	Ausgabe 1, dann Ausgabe 2 für jedes Objekt, dann Ausgabe 3 für jedes Objekt, dann Ausgabe 4 für jedes Objekt.

Das Programm RETRIEVE ist in erster Linie für die Verwendung im Batch-Modus vorgesehen. Mit dem Direktkommando RETRIEVAL können Sie es aber auch online aufrufen: Es wird ein Menü angezeigt, in dem Sie die Auswahlmöglichkeiten festlegen können.

21 Gegenzeichnungen (Countersignatures)

- Eigentümer verwenden 400
- Gegenzeichnungen verwenden (Funktion Countersignature) 400
- Gruppen als Eigentümer 402
- Gruppen als Miteigentümer 403
- Benutzersicherheitsprofile von Administratoren 403
- Aufgeschobenes Gegenzeichnen 404
- Nicht erreichbare Sicherheitsprofile 406

In diesem Kapitel werden die folgenden Themen behandelt:

Eigentümer verwenden

Die Verwendung von *Eigentümern* für Sicherheitsprofile hat den Vorteil, dass die Arbeit und die Verantwortung für die Verwaltung von Natural Security auf mehrere Administratoren verteilt werden kann, anstatt in den Händen einer einzigen Person zu liegen.

Diese Aufteilung kann nach den Kriterien der Bedeutung/Sensibilität von Objekten, nach regionalen, branchenspezifischen oder abteilungsspezifischen Aspekten oder nach anderen Kriterien erfolgen, die zu Ihrer spezifischen Natural-Umgebung passen.

Die Anzahl der Administratoren sollte geringgehalten werden, und das System, mit dem Sie die Eigentümer zuweisen, sollte klar strukturiert sein.

Es ist auch möglich, eine Gruppe (Group) als Eigentümer zu bestimmen. Alle in der Gruppe enthaltenen Administratoren sind dann berechtigt, das Sicherheitsprofil zu verwalten. (Da ohnehin nur Benutzer des Typs Administrator die Natural Security-Verwaltung durchführen dürfen, sind Benutzer anderer Benutzertypen, die in dieser Gruppe enthalten sind, davon nicht betroffen).

Gegenzeichnungen verwenden (Funktion Countersignature)

Es obliegt allein den Natural Security-Administratoren, die Zugriffsrechte auf Bibliotheken für alle Benutzer zu steuern. Die Kontrolle der Administratoren dagegen kann auf gegenseitiger Basis erfolgen, indem *Gegenzeichnungen* verwendet werden.

Ein Sicherheitsprofil kann bis zu 8 Eigentümer haben. Ohne Gegenzeichnung kann jeder dieser Eigentümer das Sicherheitsprofil ungehindert ändern, löschen, verlinken oder bearbeiten.

Wenn dies nicht erwünscht ist, kann die Countersignature-Funktion verwendet werden: Neben jedem Eigentümer eines Sicherheitsprofils kann eine Zahl (1, 2 oder 3) eingegeben werden. Ein Eigentümer muss dann diese Anzahl von Gegenzeichnungen von anderen Besitzern des Sicherheitsprofils erhalten, bevor er Zugriff auf das Sicherheitsprofil erhalten kann. Auf diese Weise kann ein Eigentümer keine Änderungen ohne das Wissen und die Zustimmung der anderen Eigentümer vornehmen.

Gegenzeichnungen werden geleistet, indem die Miteigentümer ihre Benutzerpasswörter auf dem Bildschirm **Countersignatures** eingeben. Dieser Bildschirm wird automatisch angezeigt, wenn eine Funktion aufgerufen wird, die Gegenzeichnungen von Miteigentümern des betreffenden Sicherheitsprofils erfordert.

Anmerkung: Wenn die **Lock User Option** aktiv ist, kann die Eingabe eines falschen Passworts auf dem Bildschirm **Countersignatures** dazu führen, dass der Benutzer, der den Bildschirm aufgerufen hat, gesperrt wird.

Beispiel für Gegenzeichnungen:

Im Sicherheitsprofil des Benutzers IW sind die folgenden Eigentümer angegeben:

```
+---------------------------OWNERS-----------------------------+
! User ID ........... IW                                       !
!                                                              !
! AD                                                           !
! HW       + 1                                                 !
! JC       + 2                                                 !
!                                                              !
!                                                              !
!                                                              !
!                                                              !
!                                                              !
!                                                              !
!--------------------------------------------------------------+
```

Nur die drei angegebenen Administratoren dürfen das Sicherheitsprofil ändern.

Die Eigentümersituation ist die folgende:

- Eigentümer AD darf das Sicherheitsprofil ungehindert ändern, d. h. ohne eine Gegenzeichnung von einem der anderen Eigentümer einholen zu müssen.
- Eigentümer HW darf das Sicherheitsprofil nur mit Zustimmung eines der anderen Eigentümer ändern (dies muss nicht ein bestimmter Eigentümer sein, sondern kann ein beliebiger der anderen Eigentümer sein).
- Eigentümer JC darf das Sicherheitsprofil nur mit der Zustimmung von zwei, d.h. von allen anderen Eigentümern des Sicherheitsprofils, ändern.
- Alle anderen Administratoren können das Sicherheitsprofil nicht ändern, da sie nicht Eigentümer des Sicherheitsprofils sind.

Nehmen wir an, dass der Eigentümer HW das Sicherheitsprofil des Benutzers IW ändern möchte. In der Auswahlliste der Benutzerverwaltung markiert er den Benutzer IW mit dem Code `MO`. Der Bildschirm **Countersignatures** wird angezeigt:

```
13:10:14                    *** NATURAL SECURITY ***                 2021-12-31
                                - Modify User -

User ID .. IW


           Group ID  User ID     Password            Added       Modified
           --------  --------    --------            ----------  ----------
        1.           AD_______   _________        On: 1999-08-13 2021-01-18
        2.           JC_______   _________            13:08:15   13:09:10
        3.           _________   _________        By: AD         AD
        4.           _________   _________
        5.           _________   _________
        6.           _________   _________
        7.           _________   _________
        8.           _________   _________



SYSSEC5588: 1 authorized owner must enter his/her password.

Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help        Exit                                                  Canc
```

Alle anderen Eigentümer des Sicherheitsprofils werden auf dem Bildschirm aufgelistet. Einer von ihnen muss sein Passwort eingeben.

Wenn keiner der anderen Eigentümer persönlich anwesend ist, können sie miteinander kommunizieren (AD kann z. B. HW sein Passwort verraten, das HW dann auf dem Bildschirm **Countersignatures** eingeben kann. AD sollte dann unmittelbar danach sein Passwort ändern).

Sobald das richtige Passwort eines Miteigentümers (entweder AD oder JC) eingegeben wurde, wird der Bildschirm **Modify User** mit dem Sicherheitsprofil des Benutzers IW für Administrator HW aufgerufen, um die beabsichtigten Änderungen durchzuführen.

Gruppen als Eigentümer

Wenn Gruppen als Eigentümer angegeben sind, können die folgenden Fälle auftreten:

- Ein Administrator ist Eigentümer eines Sicherheitsprofils und gleichzeitig in einer Gruppe enthalten, die Eigentümer des Sicherheitsprofils ist. In diesem Fall gelten die für den Administrator selbst festgelegten Gegenzeichnungsanforderungen.
- Ein Administrator ist nicht selbst Eigentümer eines Sicherheitsprofils, ist aber in zwei oder mehr Gruppen enthalten, die Eigentümer des Sicherheitsprofils sind. In diesem Fall gelten die für die Gruppe mit den wenigsten Gegenzeichnungen festgelegten Gegenzeichnungsanforderungen.

Haben zwei oder mehr Gruppen gleich wenige Gegenzeichnungen, so ist deren alphabetische Reihenfolge entscheidend.



Anmerkung: In den oben genannten Fällen kann ein Administrator mehr als einmal Eigentümer sein. Dies bedeutet, dass er sich selbst mit einer oder mehreren der erforderlichen Gegenzeichnungen ausstatten kann.

Gruppen als Miteigentümer

Wenn eine Gruppe auf dem Bildschirm **Countersignatures** als Miteigentümer erscheint, kann jeder der in der Gruppe enthaltenen Administratoren gegenzeichnen.

Um einen Administrator aus einer Gruppe auszuwählen, müssen Sie auf dem Bildschirm **Countersignatures** ein Fragezeichen (?) in das Feld **User ID** (Benutzerkennung) neben der **Group ID** (Gruppenkennung) eingeben. Es wird eine Liste aller in der Gruppe enthaltenen Administratoren angezeigt, aus der Sie denjenigen auswählen können, dessen Gegenzeichnung Sie erhalten möchten.

Beachten Sie, dass eine Gruppe als ein Miteigentümer zählt und ein Miteigentümer nicht mehr als eine Gegenzeichnung leisten kann. Wenn beispielsweise zwei Gegenzeichnungen erforderlich sind, können diese nicht beide von Mitgliedern derselben Gruppe geleistet werden.

Ein Administrator kann jedoch mehr als einmal gegenzeichnen, wenn er mehr als einmal als Miteigentümer auf dem Bildschirm **Countersignatures** erscheint, d.h. mit seiner eigenen Berechtigung und/oder als Mitglied einer oder mehrerer Gruppen.

Benutzersicherheitsprofile von Administratoren

Wenn ein Administrator neue Sicherheitsprofile anlegen will (d.h. eine Add-Funktion (Anlegen) oder Copy-Funktion (Kopieren) verwenden will), gilt die Besitzersituation seines eigenen Sicherheitsprofils:

- Wenn dem Sicherheitsprofil des Administrators keine Eigentümer zugewiesen sind, kann er ungehindert neue Sicherheitsprofile anlegen.
- Wenn dem Sicherheitsprofil des Administrators Eigentümer zugewiesen sind, zu denen der Administrator nicht gehört, muss er die Gegenzeichnung aller Eigentümer seines Sicherheitsprofils einholen, bevor er neue Sicherheitsprofile anlegen kann.
- Wenn der Administrator einer der Eigentümer seines eigenen Sicherheitsprofils ist und eine Anzahl von Mitinhabern angegeben hat, muss der Administrator diese Anzahl von Gegenzeichnungen von anderen Eigentümern seines Sicherheitsprofils einholen, bevor er neue Sicherheitsprofile anlegen kann.

Vorsicht: Die Zuweisung von Eigentümern und Gegenzeichnungen sollte mit äußerster Sorgfalt erfolgen, da es schwierig, wenn nicht gar unmöglich sein kann, eine unerwünschte Eigentümer/Miteigentümer-Konfiguration rückgängig zu machen. Das "Experimentieren" mit dieser Funktion kann außerdem dazu führen, dass Sie sich selbst vom Zugriff auf ein Sicherheitsprofil aussperren.

Aufgeschobenes Gegenzeichnen

Das Aufschieben der Gegenzeichnung ermöglicht es Ihnen, eine Verwaltungsfunktion auszuführen und die erforderliche Gegenzeichnung zu einem späteren Zeitpunkt einzuholen.

Diese Funktionalität wird auch als zeitunabhängige Gegenzeichnung (Time-independent Countersigning, TIC) bezeichnet.

Anwendbarkeit

Das Aufschieben einer Gegenzeichnung ist möglich:

- wenn die Anzahl der Miteigentümer, deren Gegenzeichnung Sie benötigen, 1 beträgt,
- für die folgenden Verwaltungsfunktionen: Add (Anlegen), Modify (Ändern), Rename (Umbenennen) und Delete (Löschen) bei Benutzersicherheitsprofilen und Bibliothekssicherheitsprofilen.

In der folgenden Erläuterung wird zur Vereinfachung des Lesens die Aktion **Modify** (Ändern) verwendet, die Erläuterung gilt jedoch auch für die anderen genannten Funktionen.

Anmerkung: In der aktuellen Version von Natural Security ist für die oben genannten Funktionen eine verzögerte Gegenzeichnung möglich. Es ist geplant, sie in späteren Versionen für weitere Funktionen verfügbar zu machen.

Funktionsweise der aufgeschobenen Gegenzeichnung

Wenn Sie versuchen, ein Sicherheitsprofil zu ändern und der Bildschirm **Countersignatures** aufgerufen wird, aber keiner der anderen Eigentümer des Sicherheitsprofils verfügbar ist, um sein Passwort anzugeben, können Sie die Gegenzeichnung aufschieben. Das bedeutet, dass Sie mit Ihrer beabsichtigten Änderung fortfahren und die Gegenzeichnung des anderen Eigentümers später einholen können.

Dazu müssen Sie auf dem Bildschirm **Countersignatures** PF5 (Zurückstellen) drücken.

Das zu ändernde Sicherheitsprofil wird aufgerufen, und Sie können die gewünschten Änderungen daran vornehmen.

Wenn Sie die Änderung des Sicherheitsprofils abgeschlossen haben, erscheint das Sicherheitsprofil in der **Maintenance**-Auswahlliste der Objektverwaltung mit dem Hinweis, dass für die Änderung

noch eine Gegenzeichnung aussteht. Die Änderung wird erst dann aktiv, wenn die Gegenzeichnung erfolgt ist.

Bis der Miteigentümer seine Gegenzeichnung leistet oder verweigert, gibt es zwei Versionen des Sicherheitsprofils:

- die *aktive*, nicht geänderte Version,
- eine temporäre Version, die Ihre Änderungen enthält.

In der Maintenance-Auswahlliste können Sie die folgenden Funktionen für das Sicherheitsprofil ausführen:

Code	Funktion
DI	Display: Anzeigen der aktiven Version des Sicherheitsprofils.
DT	Display: Anzeigen der temporären Version des Sicherheitsprofils. Die Änderungen werden darin hervorgehoben.
MT	Modify: Ändern der vorläufigen Version des Sicherheitsprofils.
RT	Revoke: Rücknehmen der Gegenzeichnungsanforderung.

Der Miteigentümer kann die folgenden Funktionen an dem Sicherheitsprofil ausführen:

Code	Funktion
DI	Display: Anzeigen der aktiven Version des Sicherheitsprofils.
DT	Display: Anzeigen der temporären Version des Sicherheitsprofils. Die Änderungen werden darin hervorgehoben.
CT	Aufrufen des Bildschirms **Countersignatures** zur Bestätigung der Änderungen.
RT	Revoke: Rücknehmen der Gegenzeichnungsanforderung.

Solange die Gegenzeichnung nicht geleistet oder widerrufen wurde, können andere als die oben aufgeführten Verwaltungsfunktionen nicht auf das Sicherheitsprofil angewendet werden.

Wenn die Gegenzeichnung durch den Miteigentümer erfolgt, werden die Änderungen übernommen, d.h. die aktive Version des Sicherheitsprofils wird entfernt, und die temporäre Version wird zur aktiven Version.

Wird der Antrag auf Gegenzeichnung zurückgezogen - entweder von Ihnen selbst oder vom Miteigentümer - wird die vorläufige Version des Sicherheitsprofils entfernt, und nur die aktive Version bleibt bestehen. Alle Informationen über die Anforderung werden entfernt.

Anmerkung: Die Angaben zum Eigentümer/Miteigentümer in einem Sicherheitsprofil *können nicht* mittels aufgeschobener Gegenzeichnung geändert werden.

Profile mit ausstehenden Gegenzeichnungen auflisten

Um nur die Sicherheitsprofile eines bestimmten Objekttyps aufzulisten, für die Gegenzeichnungen anstehen, können Sie in der Kommandozeile der **Maintenance**-Auswahlliste das Kommando `SHOW TIC` (TIC = Time-independent Countersigning) eingeben.

Um zur normalen Auswahllistenanzeige zurückzukehren, müssen Sie das Kommando erneut eingeben.

Umbenannte und gelöschte Sicherheitsprofile

Wenn Sie die Gegenzeichnung bei einer Umbenennung eines Sicherheitsprofils zurückstellen, erscheint das Profil in der **Maintenance**-Auswahlliste des Objekts sowohl unter der alten als auch unter der neuen Kennung (ID).

Wenn Sie die Gegenzeichnung für die Löschung eines Sicherheitsprofils aufschieben, verbleibt das Profil in der **Maintenance**-Auswahlliste des Objekts, bis die Gegenzeichnung nachgereicht wird.

Nicht erreichbare Sicherheitsprofile

Wenn auf ein Sicherheitsprofil nicht mehr zugegriffen werden kann, d.h. wenn eine Eigentümer/Miteigentümer-Konfiguration eingerichtet wurde, die keinem Administrator den Zugriff auf das Sicherheitsprofil erlaubt, kann als letzter Ausweg das Natural-Systemkommando `INPL` benutzt werden, um das Sicherheitsprofil wiederherzustellen.

Dazu:

1. Geben Sie das Kommando `INPL` ein.
2. Geben Sie dann im **INPL**-Menü den Code `R` und die Ersetzungsoption `O` ein.
3. Geben Sie im nächsten Fenster den Objekttyp und die Kennung des Sicherheitsprofils ein, das wiederhergestellt werden soll.

   Dadurch werden alle Eigentümereinträge aus dem Sicherheitsprofil gelöscht.

Wenn Sie die obige **INPL**-Option im Batch-Modus verwenden, muss die Arbeitsdatei 1 die Natural Security INPL-Datei sein.

Beispiel für Batch-Modus-Input zur Security-Profile-Wiederherstellung:

```
//CMSYNIN DD *
R,O
U,AD
.
```

22 Funktionssicherheit

- Kommandoprozessoren 410
- Funktionssicherheit für einen Kommandoprozessor 410
- Schlüsselwörter erlauben/nicht erlauben 411
- Funktionssicherheit für eine Bibliothek definieren 411
- Funktionssicherheit für einen Benutzer definieren 416
- Funktionssicherheit für die Bibliothek SYSSEC 417

In diesem Kapitel werden die folgenden Themen behandelt:

Kommandoprozessoren

Kommandoprozessoren werden verwendet, um die Art und Weise zu steuern, in der Kommandos/Funktionen in einer Bibliothek ausgeführt werden. Sie werden mit dem Natural-Dienstprogramm SYSNCP erstellt. In einem Kommandoprozessor definieren Sie Kommandos - d.h. Schlüsselwörter und Schlüsselwortkombinationen - und die Aktionen, die ausgeführt werden sollen, wenn diese Kommandos von den Benutzern eingegeben werden.

Funktionssicherheit für einen Kommandoprozessor

Mit Natural Security können Sie Funktionssicherheit für jeden Kommandoprozessor in einer Bibliothek definieren: Sie können festlegen, welche der im Kommandoprozessor definierten Schlüsselwörter und Schlüsselwortkombinationen in der Bibliothek erlaubt oder nicht erlaubt sein sollen, und so die Verfügbarkeit bestimmter Funktionen innerhalb der Bibliothek einschränken. Darüber hinaus können Sie eine benutzerspezifische Funktionssicherheit definieren, d.h. Sie können für verschiedene Benutzer desselben Kommandoprozessors in einer Bibliothek unterschiedliche Funktionen verfügbar machen.

Dies geschieht über die Funktionssicherheitsoptionen (**Functional Security**) in den Sicherheitsprofilen von Bibliotheken und Benutzern, wie unten beschrieben. Die Funktionssicherheit, die für einen Kommandoprozessor in einem Bibliothekssicherheitsprofil definiert ist, gilt für alle Benutzer des Kommandoprozessors in dieser Bibliothek. Darüber hinaus können Sie in einem Benutzersicherheitsprofil für einen einzelnen Benutzer eines Kommandoprozessors in einer Bibliothek eine andere Funktionssicherheit definieren, die dann Vorrang vor den Angaben im Bibliothekssicherheitsprofil hat.

Status eines Kommandoprozessors

In Natural Security kann ein Kommandoprozessor den folgenden Status haben:

Undefined	Nicht definiert. Der Kommandoprozessor wurde mit dem Dienstprogramm `SYSNCP` erstellt, aber es ist keine Funktionssicherheit für ihn definiert.
Defined	Definiert. Der Kommandoprozessor wurde mit `SYSNCP` erstellt und Funktionssicherheit ist für ihn definiert.
Modified	Geändert. Der Kommandoprozessor wurde mit `SYSNCP` geändert, nachdem Funktionssicherheit für ihn definiert wurde. In diesem Fall müssen Sie eventuell die Funktionssicherheit für den Kommandoprozessor aktualisieren, indem Sie das Feld **Functional Security Defined** mit `UP` markieren und dann

	die Sicherheitsangaben anpassen. Um die Funktionssicherheit für alle geänderten Kommandoprozessoren in der Bibliothek zu aktualisieren, können Sie die Anwendungsprogrammierschnittstelle NSCLI (Funktionscode UC) verwenden. **Anmerkung:** Wenn ein Kommandoprozessor mit dem Dienstprogramm SYSNCP geändert wird, muss er neu katalogisiert werden, damit die Änderungen in Natural Security berücksichtigt werden können.
Unresolved	Nicht aufgelöst. Der Kommandoprozessor wurde mit SYSNCP gelöscht, aber die Funktionssicherheit ist immer noch für ihn definiert. In diesem Fall sollten Sie auch die Funktionssicherheit für den Kommandoprozessor löschen (indem Sie das Feld **Functional Security Defined** with DE markieren).

Schlüsselwörter erlauben/nicht erlauben

Standardmäßig sind alle in einem Kommandoprozessor definierten Schlüsselwörter nicht erlaubt, was bedeutet, dass keines der im Kommandoprozessor definierten Kommandos ausgeführt werden kann.

Wenn Sie nur relativ wenige Funktionen zur Verfügung stellen wollen, können Sie diese Voreinstellung unverändert lassen, so dass generell alle Schlüsselwörter nicht erlaubt sind, und Sie können dann die Verwendung einzelner Schlüsselwörter und Schlüsselwortkombinationen (Kommandos) erlauben.

Wenn Sie die meisten Funktionen verfügbar machen und nur die Verwendung relativ weniger Funktionen einschränken möchten, können Sie die Vorgabe so ändern, dass generell alle Schlüsselwörter erlaubt sind, und Sie können dann die Verwendung einzelner Schlüsselwörter und Schlüsselwortkombinationen unterbinden.

Funktionssicherheit für eine Bibliothek definieren

Wenn Sie im Fenster **Additional Options** eines Bibliothekssicherheitsprofils die Option **Functional Security** markieren (siehe *Bestandteile eines Bibliothekssicherheitsprofils*), wird das Fenster **Functional Security** angezeigt:

```
   Library ID ................... XYZLIB__
   Command Processor ............ ________

__ Functional security defined ..
__ Keyword default ..............
__ Keyword exceptions ...........
__ Command exceptions ...........
   Type of command exceptions ...
```

In diesem Fenster können Sie die Funktionssicherheit für jeden Kommandoprozessor definieren, der in dieser Bibliothek angelegt wurde.

In das Feld **Command Processor** des Fensters müssen Sie den Namen des Prozessors eingeben, den Sie für die Bibliothek definieren möchten.

Wenn Sie den Namen des gewünschten Prozessors nicht kennen, geben Sie einen Stern (*) in das Feld **Command Processor** ein: Es wird eine Liste aller in dieser Bibliothek enthaltenen Prozessoren angezeigt. Aus dieser Liste können Sie einen Prozessor auswählen, indem Sie ihn mit einem beliebigen Zeichen oder dem Cursor markieren.

Standardmäßig ist für einen Kommandoprozessor keine Funktionssicherheit definiert: Die Schlüsselwortvorgabe (**Keyword default**) ist auf „Nicht erlaubt“ gesetzt, und es sind keine Schlüsselwortausnahmen (**Keyword exceptions**) oder Kommandoausnahmen (**Command exceptions**) definiert, was bedeutet, dass keines der im Prozessor definierten Kommandos ausgeführt werden kann.

Functional Security Defined - Funktionssicherheit definiert

Das Feld **Functional Security Defined** kann die folgenden Werte annehmen:

No	Zeigt an, dass die Standardeinstellungen für **Keyword default** und **Keyword exceptions** und **Command exceptions** gelten.
Yes	Zeigt an, dass einige der Standardeinstellungen geändert wurden.
???	Zeigt an, dass der Status des Kommandoprozessors entweder „geändert“ oder „nicht aufgelöst“ ist (siehe *Status eines Kommandoprozessors* oben).

Um alle Funktionssicherheitsdefinitionen, die für den Kommandoprozessor vorgenommen wurden, zu löschen, müssen Sie dieses Feld mit `DE` markieren.

Keyword Default - Schlüsselwortvorgabe

Das Feld **Keyword Default** kann die folgenden Werte annehmen:

Disallowed	Nicht erlaubt. Standardmäßig sind alle im Prozessor angegebenen Schlüsselwörter nicht erlaubt (und Sie können einzelne Schlüsselwörter und Schlüsselwortkombinationen über Schlüsselwortausnahmen (**Keyword Exceptions**) und Kommandoausnahmen (**Command Exceptions**) erlauben).
Allowed	Erlaubt. Standardmäßig sind alle im Prozessor angegebenen Schlüsselwörter erlaubt (und Sie können einzelne Schlüsselwörter und Schlüsselwortkombinationen über Schlüsselwortausnahmen (**Keyword Exceptions**) und Kommandoausnahmen (**Command Exceptions**) auf „nicht erlaubt“ setzen).

Um den Wert von **Disallowed** in **Allowed** oder umgekehrt zu ändern, müssen Sie das Eingabefeld **Keyword Default** mit einem beliebigen Zeichen markieren.

Sie können das Feld **Keyword Default** nur dann ändern, wenn weder **Keyword Exceptions** noch **Command Exceptions** definiert sind. Sie müssen also ggf. den Status **Allowed**/**Disallowed** aller **Command Exceptions** und **Keyword Exceptions** auf ihre Standardeinstellungen zurücksetzen (wie unten erläutert), bevor Sie das Feld **Keyword Default** ändern können.

Wenn Sie das Feld **Keyword Default** mit `PU` markieren, wird der Status des Kommandoprozessors auf Public (öffentlich) gesetzt. Das bedeutet, dass Sie Schlüsselwort- und Kommandoausnahmen definieren können, diese werden jedoch nicht wirksam. Um den Kommandoprozessor so zu aktivieren, dass die Schlüsselwort-/ Kommandoausnahmen wirksam werden, müssen Sie das Feld **Keyword Default** mit `RL` (Release) markieren.

Keyword Exceptions - Schlüsselwortausnahmen

Das Feld **Keyword Exceptions** kann die folgenden Werte annehmen:

No	Nein. Zeigt an, dass die Schlüsselwortvorgaben (**Keyword Default**) für alle Schlüsselwörter gelten, d. h. alle Schlüsselwörter sind entweder erlaubt oder nicht erlaubt.
Yes	Ja. Wenn **Keyword Default** auf **Disallowed** gesetzt ist, bedeutet dies, dass einzelne Schlüsselwörter erlaubt sind. Wenn **Keyword Default** auf **Allowed** gesetzt ist, bedeutet dies, dass einzelne Schlüsselwörter nicht erlaubt sind.

Standardmäßig sind alle Schlüsselwörter entweder erlaubt oder nicht erlaubt, je nach der **Keyword Default**-Einstellung.

Um diesen Standardstatus für einzelne Schlüsselwörter zu ändern, müssen Sie das Eingabefeld **Keyword Exceptions** (Schlüsselwortausnahmen) mit einem beliebigen Zeichen (ausgenommen `DE`) markieren. Abhängig von der Einstellung in **Keyword Default** wird entweder der Bildschirm **Allow Keywords** oder der Bildschirm **Disallow Keywords** angezeigt, in denen alle Schlüsselwörter aufgelistet sind, die im Prozessor definiert worden sind:

```
14:18:03                    *** NATURAL SECURITY ***                 2021-12-31
                             - Disallow Keywords -

Library .. SYRINX      Command Processor .. PROC2112

Keyword          Type   A/D
_______________ ______  _
ACCESS           Action  A
ADD              Action  A
ADDMULTIPLE      Action  A
ADMIN            Action  A
CONVERT          Action  A
COPY             Action  D
DELETE           Action  D
DISPLAY          Action  A
DUMMY1           Action  A
DUMMY2           Action  A
DUMMY3           Action  A
DUMMY4           Action  A
EDIT             Action  A


Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help  PrevM Exit  AddOp       Flip                              Canc
```

In der Liste kann geblättert werden, siehe *Grundlagen der Benutzung*.

Markieren Sie in der Spalte **A/D** die Schlüsselwörter, die nicht erlaubt werden sollen, mit `D` (Disallow) und die, die erlaubt werden sollen, mit `A` (Allow).

Jeder Status, der sich vom **Keyword Default**-Status unterscheidet, wird hervorgehoben angezeigt.

Um den Status **Not allowed/Allowed** (nicht erlaubt/erlaubt) für alle Schlüsselwörter auf die **Keyword Default**-Einstellung zurückzusetzen, müssen Sie das Eingabefeld **Keyword Exceptions** mit `DE` (Delete) markieren. Es wird ein Fenster angezeigt, in dem Sie `Y` eingeben müssen, um die Löschung zu bestätigen.

Command Exceptions - Kommandoausnahmen

Das Feld **Keyword Exceptions** kann die folgenden Werte annehmen:

No	Zeigt an, dass alle ursprünglichen Standardeinstellungen gelten.
Yes	Zeigt an, dass einzelne Standardeinstellungen geändert wurden.

Wenn eines der Schlüsselwörter, aus denen ein Kommando besteht, nicht erlaubt ist, ist das Kommando standardmäßig nicht erlaubt. Wenn alle Schlüsselwörter, aus denen ein Kommando besteht, erlaubt sind, ist das Kommando standardmäßig erlaubt.

Um diesen Standardstatus für einzelne Kommandos zu ändern, können Sie das Eingabefeld **Command Exceptions** (Kommandoausnahmen) mit einem beliebigen Zeichen - außer `DE` - markieren. Der Bildschirm **Allow/Disallow Commands** wird angezeigt, in dem alle Kommandos aufgelistet sind, die im Prozessor definiert wurden:

```
14:19:13                    *** NATURAL SECURITY ***                 2021-12-31
                          - Allow/Disallow Commands -

Library .. SYRINX      Command Processor .. PROC2112

Action           Object           (unused)         A/D
_______________ _______________ _______________  _
ACCESS           DATASET                          A
ACCESS           JOB                              A
ACCESS           NODE                             A
ACCESS           OPERATIONS                       A
ACCESS           PRINTER                          A
ACCESS           VOLUME_SERIAL                    A
ACCESS           VTAM_APPLICATION                 A
ADD              DATASET                          A
ADD              FILE                             A
ADD              JOB                              A
ADD              LIBRARY                          A
ADD              MAILBOX                          A
ADD              NODE                             A


Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help  PrevM Exit  AddOp       Flip                              Canc
```

In der Liste kann geblättert werden, siehe Kapitel *Grundlagen der Benutzung*.

Markieren Sie in der Spalte **A/D** die Kommandos, die nicht erlaubt sein sollen, mit `D` und die, die erlaubt sein sollen, mit `A`.

Jeder Status, der vom Standardstatus abweicht, wird hervorgehoben angezeigt.

Um den Status aller Kommandos auf die Allowed/Disallowed-Standardeinstellungen zurückzusetzen, müssen Sie das Eingabefeld **Command Exceptions** mit `DE` (löschen) markieren. Es wird ein Fenster angezeigt, in dem Sie `Y` eingeben müssen, um die Löschung zu bestätigen.

Type of Command Exceptions - Kommandoausnahmearten

Wenn Kommandoausnahmen (Command Exceptions) definiert sind, kann dieses Feld die folgenden Werte annehmen:

Allowed	Zeigt an, dass ein oder mehrere der ursprünglich nicht erlaubten Kommandos erlaubt wurden.
Disallowed	Zeigt an, dass ein oder mehrere Kommandos, die ursprünglich erlaubt waren, nicht mehr erlaubt sind.
Allowed/ Disallowed	Zeigt an, dass ein oder mehrere der ursprünglich nicht erlaubten Kommandos erlaubt wurden und auch ein oder mehrere der ursprünglich erlaubten Kommandos nicht mehr erlaubt sind.

Funktionssicherheit für einen Benutzer definieren

Generell gilt die Funktionssicherheit, die für einen Kommandoprozessor in einem Bibliothekssicherheitsprofil definiert ist, für alle Benutzer des Kommandoprozessors in dieser Bibliothek. Wenn Sie für einen einzelnen Benutzer eine andere Funktionssicherheit definieren möchten, können Sie dies im Sicherheitsprofil des Benutzers tun. Die Angaben im Benutzersicherheitsprofil haben dann Vorrang vor den Angaben im Bibliothekssicherheitsprofil.

Standardmäßig gelten die Angaben zur Funktionssicherheit, wie sie für den Prozessor im Sicherheitsprofil der Bibliothek definiert sind.

Um eine dieser Angaben für einen einzelnen Benutzer zu ändern, müssen Sie die Option **Functional Security** im Fenster **Additional Options** des Sicherheitsprofils des Benutzers markieren (siehe *Bestandteile eines Benutzersicherheitsprofils*). Das Fenster **Functional Security** wird angezeigt:

```
   User ID ..................... ABC
   Library ID .................. ________
   Command Processor ........... ________

__ Functional security defined ..
__ Keyword default ..............
__ Keyword exceptions ...........
__ Command exceptions ...........
   Type of command exceptions ...
```

In diesem Fenster können Sie die benutzerspezifische Funktionssicherheit für einen Kommandoprozessor in einer Bibliothek definieren.

Geben Sie in das Feld **Library ID** des Fensters die Kennung (ID) der Bibliothek ein, in der der Prozessor enthalten ist, und geben Sie in das Feld **Command Processor** den Namen des Kommandoprozessors ein, den Sie für den Benutzer definieren möchten.

Functional Security Defined - Funktionssicherheit definiert

Das Feld **Functional Security Defined** kann die folgenden Werte enthalten:

No	Zeigt an, dass für diesen Benutzer die Funktionssicherheit gilt, wie sie für den Prozessor im Bibliothekssicherheitsprofil definiert ist.
Yes	Zeigt an, dass für diesen Benutzer eine andere Funktionssicherheit definiert wurde als die, die für den Kommandoprozessor im Bibliothekssicherheitsprofil definiert wurde.
???	Zeigt an, dass der Status des Kommandoprozessors entweder „geändert“ oder „nicht aufgelöst“ ist (siehe *Status eines Kommandoprozessors* oben).

Um die benutzerspezifischen Angaben auf die für den Kommandoprozessor im Bibliothekssicherheitsprofil definierten Angaben zurückzusetzen, müssen Sie das Eingabefeld **Functional Security Defined** mit `DE` (Delete) markieren. Es wird ein Fenster angezeigt, in dem Sie `Y` eingeben müssen, um das Löschen zu bestätigen.

Keyword Default, Keyword Exceptions, Command Exceptions, Type of Command Exceptions

(Schlüsselwortvorgabe, Schlüsselwortausnahmen, Kommandoausnahmen, Kommandoausnahmearten)

Für die Felder **Keyword Default**, **Keyword Exceptions**, **Command Exceptions** und **Type of Command Exceptions** gilt das Gleiche wie oben unter *Funktionssicherheit für eine Bibliothek definieren* beschrieben.

Funktionssicherheit für die Bibliothek SYSSEC

Der Kommandoprozessor `NSCCMD01` ist für die Natural Security-Bibliothek `SYSSEC` vorgesehen.

Natural Security verwendet immer diesen Kommandoprozessor für die Handhabung von Funktionen innerhalb von `SYSSEC`. Es ist nicht möglich, bei `SYSSEC` einen anderen Kommandoprozessor zu verwenden.

Standardmäßig ist `NSCCMD01` mit **Keyword Default** auf **Allowed** und ohne **Keyword Exceptions** oder **Command Exceptions** definiert, d.h. alle Natural Security-Funktionen sind erlaubt.

Sie können den Kommandoprozessor `NSCCMD01` selbst nicht ändern (da er nur in Objektform vorliegt). Falls gewünscht, können Sie jedoch die Verwendung von Funktionen innerhalb von `SYSSEC` steuern, indem Sie die Funktionssicherheitsaspekte von `NSCCMD01` im Bibliothekssicherheitsprofil von `SYSSEC` und in den Benutzersicherheitsprofilen der Natural Security-Administratoren ändern.

Wenn Sie beispielsweise möchten, dass ein Administrator Sicherheitsprofile nur einsehen, aber nicht ändern darf, können Sie ihm alle Aktionsschlüsselwörter außer `DISPLAY` verbieten. Oder wenn Sie möchten, dass ein Administrator nur mit Sicherheitsprofilen von Benutzern, aber nicht

mit Sicherheitsprofilen anderer Objekttypen arbeiten darf, können Sie für diesen Administrator alle Objektschlüsselwörter außer `USER` auf „nicht erlaubt“ setzen.

Die Schlüsselwörter in `NSCCDM01` entsprechen den Kommandos von Natural Security, die unter *Direktkommandos* im Kapitel *Grundlagen der Benutzung* aufgeführt sind.



Vorsicht: Setzen Sie das Schlüsselwort `Default` für den Kommandoprozessor `NSCCMD01` nicht auf `Disallowed` - es sei denn, Sie definieren unmittelbar danach Schlüsselwortausnahmen, die es Ihnen erlauben, alle benötigten Natural Security-Funktionen zu verwenden. Wenn Sie das Schlüsselwort `Default` für `NSCCMD01` auf `Disallowed` setzen und dann das Fenster **Functional Security** verlassen, sind alle Natural Security-Funktionen nicht mehr erlaubt, d.h. niemand kann Natural Security mehr verwenden. Um Natural Security wieder zugänglich zu machen, müsste man dann ein `INPL`-Kommando mit der Option `RECOVER` ausführen.

Functional Security Defined - Funktionssicherheit definiert

Für den Kommandoprozessor `NSCCMD01` kann das Feld **Functional Security Defined** auch den Wert `All` annehmen. Damit wird der Zugriff auf das Administrator Services Subsystem von Natural Security festgelegt.

Um zwischen den Werten `Yes` und `All` umzuschalten, müssen Sie das Feld mit `OW` bzw. `AL` markieren.

23 Natural Security im Batch-Modus

- Allgemeine Informationen zum Batch-Modus 420
- Anmeldung im Batch-Modus 420
- Batch-Benutzersicherheitsprofile 422
- Gegenzeichnungen im Batch-Modus 423

In diesem Kapitel werden die folgenden Themen behandelt:

Allgemeine Informationen zum Batch-Modus

Bevor Sie Natural Security im Batch-Modus verwenden, sollten Sie sich mit den allgemeinen Aspekten der Verwendung von Natural im Batch-Betrieb vertraut machen, die im Kapitel *Natural im Batch-Modus* in der Natural *Operations*-Dokumentation beschrieben sind.

Beachten Sie auch die Besonderheiten des Batch-Betriebs des zugrunde liegenden Betriebssystems.

Wenn Sie einen Job im Batch-Modus unter Natural Security verarbeiten wollen, muss die Natural-Systemvariable `*DEVICE` auf `BATCH` gesetzt werden.

Anmeldung im Batch-Modus

In diesem Abschnitt finden Sie Informationen zu folgenden Themen:

- Logon-Eingabedaten im Batch-Modus
- Passwortänderung im Batch-Modus
- Automatische Anmeldung im Batch-Modus
- Startup-Transaktion im Batch-Modus
- Mailboxen im Batch-Modus

Logon-Eingabedaten im Batch-Modus

Wenn Sie Natural Security im Batch-Modus verwenden, wird der Anmeldevorgang automatisch gestartet. Die Eingaben für das Kommando `LOGON` müssen wie folgt eingegeben werden:

Auf Großrechnern im Delimiter-Modus (`IM=D`) und auf allen anderen Plattformen:

```
%*
library-ID,user-ID,password
```

Auf Großrechnern im Forms-Modus (`IM=F`)

```
library-ID user-ID
%*
password
```

Im Forms-Modus muss die Bibliothekskennung *`library-ID`* 8 Bytes lang sein. Ist sie kürzer als 8 Zeichen, müssen die restlichen Bytes mit Leerzeichen aufgefüllt werden.

Der Eingabemodus auf Großrechnern wird mit dem Natural-Profilparameter `IM` eingestellt (siehe Natural *Parameter-Referenz*-Dokumentation).

Die Angabe von %* verhindert, dass das Passwort gedruckt wird.

Wenn das Anmeldeverfahren über dynamische Parameter initialisiert werden soll, muss das Kommando LOGON mit dem Profilparameter STACK wie folgt angegeben werden:

```
STACK=(LOGON library-ID user-ID password)
```

Wenn für das LOGON-Kommando keine Eingabedaten eingegeben werden, wird die Natural Batch-Sitzung abgebrochen.

Anmerkung: Unter Windows wird im Batch-Modus als Anmeldebildschirm die Maske (Map) LOGONM1 statt der Dialogbox GLOGONM1 angezeigt.

Passwortänderung im Batch-Modus

Um das Passwort im Batch-Modus zu ändern, muss die Eingabe beim Kommando LOGON wie folgt vorgenommen werden:

Auf Großrechnern im Delimiter-Modus (IM=D) und auf allen anderen Plattformen:

```
%*
library-ID,user-ID,password,new-password
%*
,,,new-password
```

Auf Großrechnern im Forms-Modus (IM=F)

```
library-ID user-ID
%*
password new-password
%*
new-password
```

Im Forms-Modus müssen Bibliothekskennung *library-ID* und Passwort *password* 8 Bytes lang sein. Sind sie kürzer, müssen die restlichen Bytes mit Leerzeichen aufgefüllt werden. Dem neuen Passwort (*new-password*) in der letzten Zeile müssen 8 Leerzeichen vorangestellt werden.

Automatische Anmeldung im Batch-Modus

Wenn Sie die automatische Anmeldung (Natural-Profilparameter AUTO=ON) im Batch-Modus verwenden, wird der Wert der Natural-Systemvariablen *INIT-USER als Benutzerkennung verwendet. Standardmäßig enthält *INIT-USER im Batch-Modus den Namen des Batch-Jobs, unter dem die Natural-Sitzung läuft. Ein Benutzersicherheitsprofil für diesen Batch-Job-Namen muss in Natural Security definiert werden. Eine Anmeldung mit einer anderen Benutzerkennung ist nicht möglich.

Auf Großrechnern unter z/OS wird der Wert von *INIT-USER durch den Parameter USERID in der Natural z/OS-Batch-Schnittstelle bestimmt. Je nach Einstellung dieses Parameters kann dieser Wert vom Security Access Control Block (ACEE) des verwendeten Sicherheitspakets (z.B. RACF oder ACF2) oder vom USER-Parameter in der Jobkarte geliefert werden.

Startup-Transaktion im Batch-Modus

Wenn Sie sich im Batch-Modus bei einer Bibliothek anmelden, bestimmt die Einstellung des Schalters **Batch execution** im Bibliothekssicherheitsprofil, ob die im Bibliothekssicherheitsprofil angegebene Starttransaktion ausgeführt wird oder nicht. Einzelheiten finden Sie unter **Transactions** (unter *Bestandteile eines Bibliothekssicherheitsprofils* im Kapitel *Bibliotheken verwalten*).

Mailboxen im Batch-Modus

Wenn Sie sich im Batch-Modus anmelden, hängt es von der Einstellung der allgemeinen Option **Suppress mailboxes in batch mode** (siehe *Administrator Services*) ab, ob Mailboxen angezeigt werden oder nicht.

Batch-Benutzersicherheitsprofile

Neben dem Anlegen von Sicherheitsprofilen für Benutzer der Typen `A`, `P`, `M`, `G` und `T` können Sie auch Benutzersicherheitsprofile vom Typ `B` (für Batch) anlegen. Sie werden auf die gleiche Weise angelegt wie andere Benutzersicherheitsprofile (siehe ***Neuen Benutzer anlegen*** im Kapitel *Benutzer verwalten*). Die Benutzerkennung eines solchen Batch-Benutzers können Sie dann in das Feld **Batch User ID** eines Benutzersicherheitsprofils eintragen.

Bevor eine Batch-Benutzerkennung in ein Benutzersicherheitsprofil eingegeben werden kann, muss ein Sicherheitsprofil für diese Batch-Benutzerkennung definiert worden sein.

Mehrere Benutzer können sich dieselbe Batch-Benutzerkennung teilen, d. h. dieselbe Batch-Benutzerkennung kann in die Sicherheitsprofile mehrerer Benutzer eingetragen werden. Dadurch können für mehrere Benutzer im Batch-Modus dieselben Benutzungsbedingungen gelten, die nur einmal definiert werden müssen.

Eine Batch-Benutzerkennung kann nicht für eine Anmeldung im Online-Modus verwendet werden.

Im Batch-Modus meldet sich ein Benutzer mit seiner „normalen“ Benutzerkennung und seinem Passwort an. Natural Security verwendet dann die im Sicherheitsprofil des Benutzers angegebene Batch- Benutzerkennung, und es gelten die für diese Batch-Benutzerkennung definierten Nutzungsbedingungen.

Wenn im Sicherheitsprofil des Benutzers keine Batch-Benutzerkennung angegeben ist, werden die im Sicherheitsprofil des Benutzers angegebenen Privilegierten Gruppen (Privileged Groups) in der Reihenfolge ihres Eintrags auf eine Batch-Benutzerkennung überprüft. Wenn auch keine der privilegierten Gruppen eine Batch-Benutzerkennung hat, wird die eigene Benutzerkennung des Benutzers verwendet.

Ein Batch-Benutzersicherheitsprofil kann nicht direkt mit einer Bibliothek verlinkt werden, sondern muss über eine Gruppe (Group) verlinkt werden, d. h. es muss in einer Gruppe enthalten sein, und die Gruppe muss mit der Bibliothek verlinkt sein.

Gegenzeichnungen im Batch-Modus

Gegenzeichnungen können im Batch-Modus nicht verarbeitet werden. Das bedeutet, dass Sicherheitsprofile, die eine Gegenzeichnung für die Verwaltungserlaubnis erfordern, von der Verarbeitung im Batch-Modus ausgeschlossen sind.

24 Sicherheitsdaten in eine andere Systemdatei übertragen

- Allgemeine Informationen zur Übertragung von Sicherheitsdaten 426
- SECULD2 verwenden 427
- SECLOAD verwenden 431
- Daten auf eine andere Hardware-Plattform übertragen 433
- Benutzerdaten von einem externen Sicherheitssystem übertragen 434
- Datenübertragung im Batch-Modus 435

In diesem Kapitel wird beschrieben, wie Sie Sicherheitsdaten (Natural Security-Daten) von einer Systemdatei in eine andere übertragen können. Die folgenden Themen werden behandelt:

Allgemeine Informationen zur Übertragung von Sicherheitsdaten

Die Übertragung von Natural-Security-Daten von einer Systemdatei in eine andere ist nur relevant, wenn Sie mehr als eine Natural Security-Systemdatei verwenden.

Eine Natural Security-Systemdatei wird mit dem Natural-Profilparameter `FSEC` angegeben (siehe Natural-*Parameter-Referenz*-Dokumentation).

Die Bibliothek `SYSSEC` enthält zwei Programme für die Übertragung von Natural Security-Daten von einer Systemdatei in eine andere: `SECULD2` und `SECLOAD`:

- `SECULD2` wird zum Entladen von Daten aus einer Systemdatei in eine Arbeitsdatei verwendet.
- `SECLOAD` dient dazu, die Daten aus der Arbeitsdatei in die andere Systemdatei zu laden.

Die Auswahl der zu übertragenden Daten erfolgt mit `SECULD2`. `SECLOAD` wird immer versuchen, die komplette Arbeitsdatei zu übertragen. Allerdings prüft `SECLOAD`, ob die zu übertragenden Daten mit den bereits in der Systemdatei gespeicherten Daten konsistent sind. Inkonsistente Daten werden nicht geladen.

Die von Ihnen verwendeten Programme `SECULD2` und `SECLOAD` müssen beide die gleiche Version von Natural Security haben. Außerdem wird empfohlen, die neueste verfügbare Version von `SECULD2` und `SECLOAD` zu verwenden.

Eine FSEC-Systemdatei kann von allen unterstützten Natural-Security-Versionen gemeinsam genutzt werden. Das bedeutet, dass Sie eine bestehende FSEC-Datei weiterverwenden können und keine neue FSEC-Datei für eine neue Natural Security-Version erstellen müssen. Sollten Sie sich jedoch für die Verwendung einer neuen FSEC-Datei für eine neue Version von Natural Security entscheiden und bestehende Sicherheitsdaten in diese neue Datei übertragen wollen, müssen Sie die Daten mit dem Standardübertragungsverfahren `SECULD2`/`SECLOAD` entladen/laden.

Sowohl `SECULD2` als auch `SECLOAD` können nur *innerhalb* der Bibliothek `SYSSEC` aufgerufen werden.

SECULD2 verwenden

Um SECULD2 aufzurufen, müssen Sie das Kommando SECULD2 in der Kommandozeile eines beliebigen Natural Security-Bildschirms eingeben. Das **SECULD2**-Menü wird angezeigt.

Um die Art der zu übertragenden Daten auszuwählen, müssen Sie im **SECULD2**-Menü einen der folgenden Funktionscodes eingeben:

Funktionscode	Typ der zu entladenden Daten
*	Alle Sicherheitsdaten.
D	Alle Sicherheitsdaten, mit Löschung (alle Daten werden in die Arbeitsdatei geladen und in der Systemdatei gelöscht).
O	In Natural Security definierte Objekte (Benutzer, Bibliotheken, Versorgungsprofile usw.).
L	Links zwischen Benutzern und Objekten.
F	Links zwischen Bibliotheken und Dateien (diese Funktion ist nur auf Großrechnern verfügbar).
C	Bestandteile von Bibliothekssicherheitsprofilen (diese Funktion ist auf Großrechnern nicht verfügbar).
P	Standardprofile (Benutzer- oder Dienstprogramm-Profile).
W	**Arbeitsplan** verarbeiten.

Zusätzlich zum Funktionscode können Sie im Menü **SECULD2** folgende Angaben machen:

Transfer Format	Übertragungsformat. Mit dieser Option legen Sie fest, in welche Arbeitsdatei die ausgewählten Daten geschrieben werden sollen: ■ Y = Die Daten werden in alphanumerischer Form in Work File 1 geschrieben (dies ist die Standardeinstellung für Nicht-Großrechnerumgebungen). Work File 1 kann für jede von SECULD2/SECLOAD unterstützte Form der Übertragung verwendet werden. Dies setzt voraus, dass die Arbeitsdatei im Textformat (ASCII) vorliegt und eine Dateierweiterung hat. Hätte sie keine Dateierweiterung (oder die Dateierweiterung .sag), würden die Daten in binärer Form geladen und könnten von SECLOAD nicht verarbeitet werden. ■ N = Die Daten werden in binärer Form in Work File 5 geschrieben (dies ist der Standard für Großrechnerumgebungen). Work File 5 kann nur verwendet werden, wenn die Daten in eine andere Systemdatei auf derselben Hardwareplattform übertragen werden sollen.
Object Type	Objekttyp. Wenn Sie den Funktionscode O, L oder P wählen, müssen Sie auch den Typ des zu entladenden Objekts/Links angeben. Wenn Sie den Funktionscode C wählen, müssen Sie auch den Typ der zu entladenden Bestandteile (DDM-Sicherheitsprofile) angeben.

	Um eine Auswahlliste der möglichen Typen aufzurufen, können Sie in diesem Feld ein Fragezeichen (?) eingeben. Wenn Sie den Funktionscode W wählen, müssen Sie in diesem Feld die Kennung (ID) des Arbeitsplans (Workplan) angeben.
Start Value	Startwert. Sie können eine Kennung (ID) angeben, um ein bestimmtes Objekt oder einen Bereich von Objekten zu entladen. Siehe auch **Range** unten. **Start Value** ist nicht anwendbar bei den Funktionscodes * und D.
Range	Bereich. Dieses Feld bestimmt, wie der im Feld **Start Value** angegebene Wert behandelt werden soll: ■ Wenn Sie das Feld **Range** leer lassen, wird der Wert im Feld **Start Value** als tatsächlicher Startwert behandelt, d.h. der Bereich der zu entladenden Objekte beginnt mit demjenigen, dessen Objektkennung mit dem als Startwert im Feld **Start Value** angegebenen Wert beginnt. ■ Wenn Sie in das Feld **Range** einen Stern (*) eingeben, umfasst der Bereich der zu entladenden Objekte nur die Objekte, deren Objektkennung mit dem als Startwert im Feld **Start Value** angegebenen Wert beginnt. ■ Wenn Sie in das Feld **Range** ein Pluszeichen (+) eingeben, besteht der Bereich der zu entladenden Objekte nur aus denjenigen, deren Objektkennung mit dem als Startwert im Feld **Start Value** angegebenen Wert beginnt - bzw. im Falle von Links nur aus denjenigen, deren Objektkennung mit dem als Startwert im Feld **Start Value** angegebenen Wert beginnt.
Link ID	Link-Kennung. Dieses Feld kann nur in Verbindung mit dem Funktionscode L verwendet werden. Sie können eine Benutzerkennung angeben, um nur Links eines bestimmten Benutzers oder eines bestimmten Bereichs von Benutzern zu entladen. Um einen Bereich von Links auszuwählen, können Sie das Feld **Range** verwenden (siehe unten).
Range	Bereich. Dieses Feld kann nur in Verbindung mit dem Funktionscode L verwendet werden. Es bestimmt, wie der im Feld **Link ID** (Link-Kennung) angegebene Wert behandelt werden soll: ■ Wenn Sie das Feld **Range** leer lassen, wird der Wert im Feld **Link ID** als tatsächlicher Startwert behandelt, d.h. der Bereich der zu entladenden Links beginnt mit demjenigen, dessen Benutzerkennung dem als Link-Kennung im Feld **Link ID** angegebenen Wert entspricht. ■ Wenn Sie in das Feld **Range** einen Stern (*) eingeben, umfasst der Bereich der zu entladenden Links nur diejenigen, deren Benutzerkennung mit dem als Link-Kennung im Feld **Link ID** angegebenen Wert beginnt. ■ Wenn Sie in das Feld **Range** ein Pluszeichen (+) eingeben, umfasst der Bereich der zu entladenden Links nur diejenigen, deren Benutzerkennung mit dem als Link-Kennung im Feld **Link ID** angegebenen Wert übereinstimmt.
Number	Anzahl. Sie können die Anzahl der zu übertragenden Objekte angeben. (Diese Option ist nicht anwendbar bei den Funktionscodes * und D.)

Date from/to	Datum von/bis. Sie können zwei Datumsangaben machen, um nur Objekte zu entladen, die in diesem Zeitraum erstellt/zuletzt geändert wurden. (Diese Option ist nicht anwendbar bei Funktionscode `D`.)
Work File	Arbeitsdatei. Geben Sie den Namen der Arbeitsdatei an, in die die Daten geschrieben werden sollen. Wenn Sie Work File 5 verwenden, muss der Name der Arbeitsdatei mit `.sag` enden. Dieses Feld ist auf Großrechnern nicht verfügbar.
Ty	Der Typ der Arbeitsdatei: ■ `D` = Default. ■ `N` = Entire Connection Work File. Dieses Feld ist auf Großrechnern nicht verfügbar.

Arbeitsplan verwenden

Wenn Sie den gleichen Entladevorgang in regelmäßigen Abständen durchführen müssen, können Sie einen so genannten Arbeitsplan (Workplan) verwenden. Anstatt jedes Mal alle Angaben zum Entladen im Menü **SECULD2** machen zu müssen, brauchen Sie diese nur einmal in einem Arbeitsplan zu machen. Sie verwenden dann den Funktionscode `W` und geben im Menü **SECULD2** im Feld **Object type** nur die Kennung (ID) des Arbeitsplans an.

Ein Arbeitsplan ist ein Natural-Objekt vom Typ Text, das in der Bibliothek `SYSSEC` enthalten sein muss.

Der Inhalt des Text-Members muss wie folgt aussehen:

```
- START-SECULD-WORKPLAN
UNLOAD       ________
TRANSFER     _
OBJECT-TYPE  ________
OBJECT-ID    ____________________________________
OBJECT-RANGE _
LINK-ID      ____________________________________
LINK-RANGE   _
NUMBER       __
DATE-FROM    __________
DATE-TO      __________
- END-SECULD-WORKPLAN
```

`SECULD2` wertet den nach den Schlüsselwörtern angegebenen Text - gekennzeichnet durch die obigen Zeilen - wie folgt aus:

Schlüsselwort	Erläuterung
- START-SECULD-WORKPLAN	Gibt den Beginn der Textdaten an, die von SECULD2 verarbeitet werden sollen.
UNLOAD	Sie können eine der folgenden Angaben machen: ■ ALL = entspricht dem Funktionscode *. ■ DELETE = entspricht dem Funktionscode D. ■ OBJECT = entspricht dem Funktionscode O. ■ LINK = entspricht dem Funktionscode L. ■ FILE = entspricht dem Funktionscode F. ■ PROFILE = entspricht dem Funktionscode P.
TRANSFER	Entspricht dem **SECULD2**-Menüfeld **Transfer Format**.
OBJECT-TYPE	Entspricht dem **SECULD2**-Menüfeld **Object Type**.
OBJECT-ID	Entspricht dem **SECULD2**-Menüfeld **Start Value**.
OBJECT-RANGE	Entspricht dem **SECULD2**-Menüfeld **Range** für Objekte.
LINK-ID	Entspricht dem **SECULD2**-Menüfeld **Link ID**.
LINK-RANGE	Entspricht dem **SECULD2**-Menüfeld **Range** für Links.
NUMBER	Entspricht dem **SECULD2**-Menüfeld **Number**.
DATE-FROM	Sie können eine der folgenden Angaben machen: ■ ein Datum (im Format YYYY-MM-DD) wie im **SECULD2**-Menüfeld **Date from**, ■ TODAY = es wird das aktuelle Datum verwendet, ■ LAST *nnn* = Objekte, die in den letzten *nnn* Tagen erstellt/geändert wurden; d.h. der aktuelle Tag plus die *nnn* vorhergehenden Tage. *nnn* kann 1 bis 999 sein.
DATE-TO	Sie können ein Datum (im Format YYYY-MM-DD) wie im **SECULD2**-Menüfeld **Date to** angeben. Wenn TODAY oder LAST *nnn* nach DATE-FROM angegeben wird, wird jede Angabe nach DATE-TO ignoriert.
- END-SECULD-WORKPLAN	SECULD2. Gibt das Ende der Textdaten an, die von SECULD2 verarbeitet werden sollen.

Wenn Sie mehrere Entladevorgänge mit einem einzigen Arbeitsplan durchführen wollen, geben Sie mehrere Gruppen von Schlüsselwörtern/Texten nach - START-SECULD-WORKPLAN und vor - END-SECULD-WORKPLAN an:

```
- START-SECULD-WORKPLAN
UNLOAD       _________
TRANSFER     _
etc. ...
UNLOAD       _________
TRANSFER     _
etc. ...
- END-SECULD-WORKPLAN
```

Ein Beispiel-Workplan `T-WPLAN1` ist in der Bibliothek `SYSSEC` vorhanden.

SECLOAD verwenden

Um SECLOAD aufzurufen:

1 Geben Sie das Kommando `SECLOAD` in der Kommandozeile eines beliebigen Natural Security-Bildschirms ein.

2 Sie werden dann aufgefordert, die folgenden Angaben zu machen:

Load NSC Data in Transfer Format from Work File 1	NSC-Daten im Transferformat aus Work File 1 laden ■ `Y` = Die Daten werden im Übertragungsformat aus der Work File 1 gelesen (dies ist die Standardeinstellung für Nicht-Großrechnerumgebungen). ■ `N` = Die Daten werden aus Work File 5 gelesen (dies ist die Standardeinstellung für Großrechnerumgebungen).
User-Defined Conversion Table	Benutzerdefinierte Umwandlungstabelle Sie können festlegen, ob eine Umwandlungstabelle verwendet werden soll oder nicht (`Y/N`). Die verwendete Umwandlungstabelle wird von dem API-Subprogramm `NSCCONV` bereitgestellt, das in der Bibliothek `SYSSEC` enthalten ist. Sie können die Tabelle an Ihre Bedürfnisse anpassen. Einzelheiten finden Sie im Quellcode von `NSCCONV`.
Simulate Loading	Laden simulieren Mit dieser Option können Sie feststellen, ob alle Daten aus der Arbeitsdatei geladen werden können, bevor Sie sie tatsächlich laden. Beim Ausführen dieser Funktion werden die Daten in die Systemdatei geladen und nach Beendigung der Funktion sofort wieder daraus gelöscht. Beim Aktivieren dieser Funktion wählen Sie aus, welche Art von Ladereport Sie als Ergebnis der Simulation wünschen: ■ `N` = Simulation nicht aktiv.

	■ A = Simulation mit Ladereport, der alle Datensätze auflistet. ■ R = Simulation mit Ladereport, der nur abgelehnte (Rejected) Datensätze auflistet. ■ L = Simulation mit Ladereport, der nur ladbare (Loadable) Datensätze auflistet.
Work File	Arbeitsdatei Geben Sie den Namen der Arbeitsdatei an, aus der die Daten geschrieben werden sollen. Dieses Feld ist auf Großrechnern nicht verfügbar.
Type of Work File	Typ der Arbeitsdatei ■ D = Default. ■ N = Entire Connection Work File. Dieses Feld ist auf Großrechnern nicht verfügbar.
Expire passwords for loaded user profiles	Passwörter für geladene Benutzersicherheitsprofile ablaufen lassen Diese Option kann verwendet werden, um das Ablaufen des Passworts für geladene Benutzersicherheitsprofile (Benutzertypen A, P, M) zu erzwingen. ■ Y = Die Passwörter für geladene Benutzersicherheitsprofile werden so zurückgesetzt, dass sie mit den entsprechenden Benutzerkennungen identisch sind. Bei der nächsten Anmeldung müssen diese Benutzer ihre Passwörter ändern. ■ N = In Verbindung mit dem Laden von Benutzersicherheitsprofilen wird kein Ablaufen des Passworts angewendet. Diese Option gilt nicht für geladene Benutzersicherheitsprofile, bei denen die Option **Change after** *nnn* **days** auf 999 gesetzt ist. Für diese sind die bestehenden Passwörter weiterhin gültig.
Import from file of external security system	Import aus Datei eines externen Sicherheitssystems Mit dieser Option können Sie Benutzersicherheitsdaten aus einem externen Sicherheitssystem in eine Datei des Natural Security-Systems laden. Siehe *Benutzerdaten von einem externen Sicherheitssystem übertragen* unten.

Anmerkung: Daten, die inkonsistent sind oder die bereits in der Zielsystemdatei vorhanden sind, werden nicht geladen. Warum die Daten nicht geladen wurden, können Sie dem Ladebericht entnehmen.

Daten auf eine andere Hardware-Plattform übertragen

Mit SECULD2 und SECLOAD können Sie auch Sicherheitsdaten von einer Hardwareplattform auf eine andere übertragen.

Dazu:

1 Geben Sie im **SECULD2**-Menü im Feld **Transfer Format** ein Y ein.

2 Durch Drücken von PF4 können Sie dann ein zusätzliches Fenster aufrufen, in dem Sie die folgenden optionalen Parameter angeben können:

Target Environment	Zielumgebung Das Betriebssystem (wie in der Natural-Systemvariablen *OPSYS) der Zielumgebung.
Target FSEC DBID/FNR	Ziel-FSEC-Datei Die Datenbankkennung und Dateinummer der FSEC-Systemdatei, in die die Daten übertragen werden sollen. SECLOAD vergleicht diese Angaben mit der DBID/FNR der jeweiligen FSEC-Datei, in die die Daten geladen werden sollen. Wenn sie nicht übereinstimmen, können die Daten nicht geladen werden. Auf diese Weise können Sie ein unkontrolliertes Laden von Sicherheitsdaten verhindern. Andernfalls könnte jeder, der sich der Arbeitsdatei bemächtigt hat, diese überallhin laden.
Conversion EBCDIC-ASCII	Umwandlung EBCDIC-ASCII Sie können festlegen, ob eine EBCDIC-ASCII-Umwandlung durchgeführt werden soll (Y/N). Die Umwandlung wird von dem API-Subprogramm NSCCONV durchgeführt, das in der Bibliothek SYSSEC enthalten ist. Einzelheiten siehe Quellcode von NSCCONV.
User-Defined Conversion Table	Benutzerdefinierte Umwandlungstabelle Sie können festlegen, ob eine Umwandlungstabelle verwendet werden soll oder nicht (Y/N). Die verwendete Umwandlungstabelle wird von dem API-Subprogramm NSCCONV bereitgestellt, das in der Bibliothek SYSSEC enthalten ist. Sie können die Tabelle an Ihre Bedürfnisse anpassen. Einzelheiten siehe Quellcode des Subprogramms NSCCONV.

Die Daten werden dann in alphanumerischer Form in Work File 1 geschrieben, von wo sie mit SECLOAD geladen werden können.

Anmerkung: Wenn Daten von einer Großrechnerplattform auf eine andere Plattform übertragen werden, prüft SECLOAD auch, ob die Bibliothekskennungen mit den Namenskonventionen für Bibliotheken übereinstimmen (wie beim Systemkommando LOGON in der Natural-*Systemkommandos*-Dokumentation beschrieben).

Benutzerdaten von einem externen Sicherheitssystem übertragen

Diese Option ist auf Großrechnern nicht verfügbar.

Mit `SECLOAD` können Sie auch Benutzeridentifikationsdaten aus einem externen Sicherheitssystem importieren und in eine Natural Security-Systemdatei laden.

Dies ist möglich für externe Daten von einem LDAP-Server (Informationen zu LDAP finden Sie unter *Authentifizierungsoptionen (LDAP)*).

Um externe Benutzerdaten zu importieren:

1 Geben Sie im Menü **SECLOAD** Folgendes an

Load NSC Data in Transfer Format from Work File 1	NSC-Daten im Transferformat aus Work File 1 laden Markieren Sie diese Option mit `Y`.
Work File	Arbeitsdatei Geben Sie den vollständigen Pfad der zu importierenden Arbeitsdatei an. Die angegebene Datei muss die Endung `.ldif` haben, sie muss mit dem Kommando `ldapsearch` erstellt worden sein, und sie muss die Zeichenfolge `dn: uid=` enthalten.
Import from file of external security system	Import aus Datei eines externen Sicherheitssystems Markieren Sie diese Option mit `Y`.

Optional können Sie die Option **Simulate loading** verwenden, wenn Sie prüfen wollen, ob die Daten aus der Arbeitsdatei importiert werden können, bevor Sie sie tatsächlich importieren.

Die anderen Einträge im Menü **SECLOAD** werden für den Import von externen Benutzerdaten ignoriert.

2 Es wird der Bildschirm **External Security Data (LDAP)** importieren angezeigt, in dem Sie folgende Angaben machen können:

Result report	Ergebnisreport Die Importfunktion erstellt einen Ergebnisreport. Wählen Sie aus, wie dieser Report ausgegeben werden soll: ■ `DI` = Online anzeigen. ■ `DW` = Online anzeigen und in Work File 2 schreiben. ■ `WW` = In Work File 2 schreiben.

Work file 2	Arbeitsdatei 2 Der Name der Arbeitsdatei, in die der Ergebnisreport geschrieben werden soll.
User default profile	Benutzer-Standardprofil Wenn die Benutzerdaten importiert werden, wird für jede importierte Benutzerkennung automatisch ein Natural Security-Benutzersicherheitsprofil erstellt. Alle diese Benutzersicherheitsprofile werden mit demselben Standardprofil als Vorlage erstellt. In diesem Feld müssen Sie die Kennung (ID) des zu verwendenden Standardprofils angeben. Um eine Auswahlliste von Standardprofilen aufzurufen, können Sie in dieses Feld ein Fragezeichen (?) oder einen Startwert in Stern-Notation eingeben. Informationen zu Standardprofilen finden Sie unter *Benutzer-Standardprofile - User Default Profiles*.
User ID prefix	Benutzerkennung-Präfix Wenn im verwendeten LDAP-Sicherheitsprofil die Option **Support user names as IDs** gesetzt ist, werden die Benutzerkennungen aus dem externen Sicherheitssystem als *Benutzernamen* in die angelegten Natural Security-Benutzersicherheitsprofile geschrieben. Die 8-stelligen Natural Security-*Benutzerkennungen* (User IDs) für diese Benutzersicherheitsprofile werden von Natural Security generiert, wobei ein Präfix gefolgt von einer generierten Zahl verwendet wird. In diesem Feld müssen Sie ein Präfix mit 1 bis 3 Zeichen angeben.

Datenübertragung im Batch-Modus

SECULD2/SECLOAD im Batch-Modus auf Großrechnern

Nachfolgend sind Beispiel-Jobs für die Ausführung von `SECULD2` und `SECLOAD` im Batch-Modus auf Großrechnern abgebildet.

Beispiel 1 für SECULD2 Job:

In diesem Beispiel werden alle Benutzer, deren Kennungen mit ADE beginnen und die zwischen dem 1. Januar und 10. Juni 2008 zuletzt geändert wurden, sowie die Bibliothek `TESTLIB` in die Arbeitsdatei `CMWKF05` übertragen.

```
//SECULD2 JOB DEMO,CLASS= ,MSGCLASS= ,REGION=2048K
//*********************************************************
//ULD      EXEC PGM=NATBATnn,
// PARM='DBID=10,FNR=5,FSEC=(,8),FDIC=(,9),IM=D,MT=0,MAXCL=0,MADIO=0'
//STEPLIB  DD DISP=SHR,DSN=NATURAL.Vnn.LOAD
//         DD DISP=SHR,DSN=ADABAS.Vnn.ADALOAD
//DDCARD   DD *
ADARUN PROGRAM=USER,SVC=249,DATABASE=10,MODE=MULTI
/*
//CMPRINT  DD SYSOUT=*
//CMWKF05  DD UNIT=TAPE,VOL=SER=NATSEC,DSN=NSC.ULD,
// DCB=(RECFM=VB,LRECL=4624,BLKSIZE=4628,DEN=3),DISP=(,KEEP)
//CMSYNIN  DD *
SYSSEC,DBA,PASSWORD
SECULD2
O,N,US,ADE,*,,,,2008-01-01,2008-06-10
O,N,LI,TESTLIB,1
.
FIN
/*
```

Beispiel 2 für SECULD2 Job:

In diesem Beispiel werden alle Benutzer, deren Kennungen mit ADE beginnen, in die Arbeitsdatei `CMWKF01` übertragen. Wenn bei der Option **Transfer** ein `Y` angegeben wird, muss der Job eine Zeile für zusätzliche Parameter enthalten (siehe *Daten auf eine andere Hardware-Plattform übertragen* oben). In diesem Beispiel sind keine zusätzlichen Parameterangaben gemacht worden (d.h. sie sind entweder nicht angegeben oder auf `N` gesetzt worden).

```
//SECULD2 JOB DEMO,CLASS= ,MSGCLASS= ,REGION=2048K
//*********************************************************
//ULD      EXEC PGM=NATBATnn,
// PARM='DBID=10,FNR=5,FSEC=(,8),FDIC=(,9),IM=D,MT=0,MAXCL=0,MADIO=0'
//STEPLIB  DD DISP=SHR,DSN=NATURAL.Vnn.LOAD
//         DD DISP=SHR,DSN=ADABAS.Vnn.ADALOAD
//DDCARD   DD *
ADARUN PROGRAM=USER,SVC=249,DATABASE=10,MODE=MULTI
/*
//CMPRINT  DD SYSOUT=*
//CMWKF01  DD UNIT=TAPE,VOL=SER=NATSEC,DSN=NSC.ULD,
// DCB=(RECFM=VB,LRECL=4624,BLKSIZE=4628,DEN=3),DISP=(,KEEP)
//CMSYNIN  DD *
SYSSEC,DBA,PASSWORD
SECULD2
O,Y,US,ADE,*
,,,N,N
.
FIN
/*
```

Beispiel 3 für SECULD2 Job:

In diesem Beispiel sollen alle Bibliotheken, deren Kennungen mit SF beginnen, in die Arbeitsdatei `CMWKF01` übertragen werden. Die Zielumgebung ist ein PC, und die Datenbankkennung (DBID) und die Dateinummer (FNR) der FSEC-Zielsystemdatei sind 89 und 356.

```
//SECULD2 JOB DEMO,CLASS= ,MSGCLASS= ,REGION=2048K
//*********************************************************
//ULD      EXEC PGM=NATBATnn,
// PARM='DBID=10,FNR=5,FSEC=(,8),FDIC=(,9),IM=D,MT=0,MAXCL=0,MADIO=0'
//STEPLIB  DD DISP=SHR,DSN=NATURAL.Vnn.LOAD
//         DD DISP=SHR,DSN=ADABAS.Vnn.ADALOAD
//DDCARD   DD *
ADARUN PROGRAM=USER,SVC=249,DATABASE=10,MODE=MULTI
/*
//CMPRINT  DD SYSOUT=*
//CMWKF01  DD UNIT=TAPE,VOL=SER=NATSEC,DSN=NSC.ULD,
// DCB=(RECFM=VB,LRECL=4624,BLKSIZE=4628,DEN=3),DISP=(,KEEP)
//CMSYNIN  DD *
SYSSEC,DBA,PASSWORD
SECULD2
0,Y,LI,SF,*
WNT-X86,89,356,N,N
.
FIN
/*
```

Beispiel 1 für SECLOAD Job:

In diesem Beispiel werden die Daten aus Work File 5 (`CMWKF05`) gelesen.

```
//SECLOAD JOB  DEMO,MSGCLASS= ,CLASS= ,REGION=2048K
//*************************************************
//LOAD     EXEC PGM=NATBATnn,
// PARM='DBID=7,FNR=23,FSEC=(,24),FDIC=(,25),EJ=OFF,MT=0,IM=D,MADIO=0,MAXCL=0'
//STEPLIB  DD DSN=NATURAL.Vnn.LOAD,DISP=SHR
//         DD DSN=ADABAS.Vnn.ADALOAD,DISP=SHR
//CMPRINT  DD SYSOUT=*
//DDCARD   DD *
ADARUN PROGRAM=USER,SVC=249,DATABASE=7,MODE=MULTI
/*
//CMWKF05  DD UNIT=TAPE,VOL=SER=NATSEC,DSN=NSC.ULD,DISP=SHR
//CMSYNIN  DD *
SYSSEC,DBA,PASSWORD
SECLOAD
N,N,N,N
FIN
/*
```

Beispiel 2 für SECLOAD Job:

In diesem Beispiel werden die Daten aus Work File 1 (CMWKF01) gelesen.

```
//SECLOAD JOB  DEMO,MSGCLASS= ,CLASS= ,REGION=2048K
//************************************************
//LOAD     EXEC PGM=NATBATnn,
// PARM='DBID=7,FNR=23,FSEC=(,24),FDIC=(,25),EJ=OFF,MT=0,IM=D,MADIO=0,MAXCL=0'
//STEPLIB  DD DSN=NATURAL.Vnn.LOAD,DISP=SHR
//         DD DSN=ADABAS.Vnn.ADALOAD,DISP=SHR
//CMPRINT  DD SYSOUT=*
//DDCARD   DD *
ADARUN PROGRAM=USER,SVC=249,DATABASE=7,MODE=MULTI
/*
//CMWKF01  DD UNIT=TAPE,VOL=SER=NATSEC,DSN=NSC.ULD,DISP=SHR
//CMSYNIN  DD *
SYSSEC,DBA,PASSWORD
SECLOAD
Y,N,N,N
FIN
/*
```

SECULD2/SECLOAD im Batch-Modus unter Linux

Um SECULD2 und SECLOAD im Batch-Modus unter Linux auszuführen, müssen Sie die Eingaben in den Batch-Modus-Dateien wie folgt vornehmen:

Die CMSYNIN zugewiesene Eingabedatei muss Folgendes enthalten:

```
SECULD2
FIN
```

In der Eingabedatei, die CMOBJIN zugewiesen ist, müssen Sie die zu übertragenden Daten angeben, z. B:

```
SYSSEC,DBA,PASSWORD,,
O,Y,US,ADE*,,,,,2008-02-01,2008-02-28
,,,N,N
.
```

Dieses Beispiel geht davon aus, dass die Sitzung mit AUTO=OFF gestartet wurde. Bei AUTO=ON lassen Sie die Benutzerkennung und das Passwort in der ersten Zeile weg.

Das Ergebnis der Datenübertragung wird in der Ausgabedatei angezeigt, die CMPRINT zugewiesen ist.

Allgemeine Informationen finden Sie im Kapitel *Natural in Batch Mode* in der Natural *Operations* Documentation for Linux.

25 User Exits

- Anmeldungsrelevante User Exits 442
- RPC-relevanter User Exit 445
- Andere User Exits 446

In diesem Kapitel werden die in Natural Security verfügbaren User Exits beschrieben. Es enthält Informationen über:

Anmeldungsrelevante User Exits

Die folgenden anmeldungsrelevanten User Exits stehen zur Verfügung:

- LOGONEX0
- LOGONEX1
- LOGONEX2
- LOGONEX3
- LOGONEX5
- LOGONSX1

Anmerkung: Der User Exit LOGONEX4 steht nicht im Zusammenhang mit der normalen Anmeldebehandlung von Natural Security, sondern ist nur in Verbindung mit der Anmeldung eines RPC Client bei einem Natural RPC Server in einer RPC-Umgebung relevant. Er wird unter *RPC-relevanter User Exit* weiter unten beschrieben.

Allgemeine Informationen zu Quellcodes und Objekten

LOGONEX0, LOGONEX1, LOGONEX2, LOGONEX3, LOGONEX5 und LOGONSX1 sind Natural-Subprogramme, die in der Bibliothek SYSLIB gespeichert sein müssen, damit sie aufgerufen werden können.

Die entsprechenden Quellcodes und Objektmodule dieser User Exits sind in der Bibliothek SYSSEC unter den folgenden Namen verfügbar:

User Exit in SYSLIB	Quellcodes und Objektmodule in SYSSEC
LOGONEX0	NOGONEX0
LOGONEX1	NOGONEX1
LOGONEX2	NOGONEX2
LOGONEX3	NOGONEX3
LOGONEX4	NOGONEX4
LOGONEX5	NOGONEX5
LOGONSX1	NOGONSX1

Sie können jeden der User Exits an Ihre Bedürfnisse anpassen. Dazu müssen Sie eine Kopie von NOGONEX*n* (*n* = 0, 1, 2, 3 oder 5) erstellen, diese unter dem Namen LOGONEX*n* speichern, Ihre Anpassungen vornehmen und sie dann in die Bibliothek SYSLIB kopieren.

Damit die User Exits immer in SYSLIB vorhanden sind, geht Natural Security wie folgt vor: Bei der Installation wird nach dem Laden aller Module in ihre jeweiligen Bibliotheken geprüft, ob in SYSLIB bereits ein Subprogramm LOGONEX*n* enthalten ist. Ist dies der Fall, dann bleibt es unberührt.

Ist dies nicht der Fall, wird das Objektmodul von LOGONEX*n* automatisch von SYSSEC nach SYSLIB kopiert und dort unter dem Namen LOGONEX*n* gespeichert. Damit ist gleichzeitig sichergestellt, dass Ihre angepassten Versionen der User Exits nicht versehentlich durch einen Installationsvorgang überschrieben werden.

Das oben Gesagte gilt auch für den User Exit LOGONSX1/NOGONSX1.

LOGONEX0

Wenn in *Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values* die Option **Password phrases active** auf Y oder A gesetzt ist, wird LOGONEX0 (anstelle von LOGONEX1) vom Natural Security-Anmeldeprogramm aufgerufen.

Wenn LOGONEX0 nicht geändert wird, ruft es den Natural Security-Anmeldebildschirm auf (Map LOGONMX1 oder Dialogfenster GLOGONMX1, siehe *Anmeldebildschirm / Anmeldedialogfenster*). Durch Ändern von LOGONEX0 können Sie Ihre eigenen Anmeldebildschirme aufrufen.

LOGONEX0 unterstützt die Verwendung von *Passphrasen*, d.h. Passwörter, die länger als 8 Zeichen sind.

LOGONEX1

Wenn in den *Voreingestellte Benutzersicherheitsprofilwerte - User Preset Values* die Option **Password phrases active** auf N gesetzt ist, wird LOGONEX1 (anstelle von LOGONEX0) vom Natural Security-Anmeldeprogramm aufgerufen.

Wenn LOGONEX1 nicht geändert wird, ruft es den Natural Security-Anmeldebildschirm auf (Map LOGONM1 oder Dialogfenster GLOGONM1, siehe *Anmeldebildschirm / Anmeldedialogfenster*). Durch Ändern von LOGONEX1 können Sie Ihre eigenen Anmeldebildschirme aufrufen.

LOGONEX1 unterstützt nur die Verwendung „normaler“ Passwörter mit bis zu 8 Zeichen.

LOGONEX2

LOGONEX2 wird vom Natural Security-Anmeldeprogramm unter einer der folgenden Bedingungen aufgerufen:

- Wenn # als Bibliothekskennung (ID) eingegeben wird (oder von LOGONEX1 als Bibliothekskennung übergeben wird),
- wenn keine Bibliothekskennung für die Anmeldung angegeben wurde und weder eine Standardbibliothek noch eine private Bibliothek existiert, die hätte aufgerufen werden können (siehe auch *Anmeldung ohne Bibliothekskennung* im Kapitel *Anmeldung (Logon)*).

Beim Aufruf von LOGONEX2 wurden die Benutzerkennung und das Passwort bereits vom Anmeldeprogramm geprüft und für gültig befunden. Zu diesem Zeitpunkt enthält die Natural-Systemvariable *USER einen gültigen Wert, der verwendet werden kann.

Sofern nicht geändert, besteht LOGONEX2 lediglich aus einem END-Statement. Bei der Rückkehr zum Anmeldeprogramm muss eine gültige Bibliothekskennung (ID) an das Anmeldeprogramm übergeben werden, sonst wird die Anmeldung zurückgewiesen. Außerdem ist es möglich, eine von möglicherweise mehreren Kennungen (IDs) zurückzugeben, über die ein Benutzer mit einer Bibliothek verbunden ist.

Da die Gültigkeit der benutzerspezifischen Anmeldedaten zum Zeitpunkt des Aufrufs von LOGONEX2 bereits durch die Prüfung der Benutzerkennung und des Passworts festgestellt wurde, kann LOGONEX2 verwendet werden, um zusätzliche benutzerspezifische Verfahren zu implementieren oder benutzerspezifische Daten abzufragen. So kann beispielsweise die Anwendungsprogrammierschnittstelle SECNOTE aufgerufen werden, um Sicherheitsvermerke des Benutzers zu lesen.

Wenn das Anmeldeprogramm LOGONEX1 oder LOGONEX2 aufruft, übergibt es die Parameter PUSERDUMMY1 und PUSERDUMMY2 an die Subprogramme. Beide Parameter sind für Ihre Verwendung vorgesehen. Ihr Format/Länge ist A8. Sie können diesen Parametern in LOGONEX1 Werte zuweisen und diese Werte anschließend in LOGONEX2 verwenden, da sie unverändert von einem Subprogramm an das andere übergeben werden.

LOGONEX3

LOGONEX3 wird vom Natural Security-Anmeldeprogramm unter einer der folgenden Bedingungen aufgerufen:

- Wenn es Mailboxen gibt, die angezeigt werden sollen,
- wenn mindestens einer der Parameter PUSERDUMMY1 oder PUSERDUMMY2, die von LOGONEX1 bzw. LOGONEX2 übergeben werden, nicht leer ist.

LOGONEX3 wird unmittelbar nach einer erfolgreichen Anmeldung und vor der Übergabe der Kontrolle vom Anmeldeprogramm an die aufgerufene Bibliothek aufgerufen. Mit dem Aufruf von LOGONEX3 ist die Anmeldeverarbeitung bis auf die Anzeige der Mailboxen abgeschlossen.

Wenn LOGONEX3 unverändert gelassen wird, führt es die für die Anzeige der Mailboxen erforderlichen Subprogrammaufrufe aus.

Sie können LOGONEX3 für einen der folgenden Zwecke ändern:

- Um die Anzeige von Mailboxen zu unterdrücken,
- um eine nicht bibliotheksspezifische Verarbeitung unmittelbar nach einer erfolgreichen Anmeldung, aber vor der Ausführung bibliotheksspezifischer Transaktionen durchführen zu lassen.

LOGONEX5

LOGONEX5 wird vom Natural Security-Anmeldeprogramm aufgerufen, wenn das Systemkommando LOGOFF ausgeführt wird.

LOGONSX1

Dieser User Exit ist nur unter Linux und Windows verfügbar.

Wenn **Authentication Type** im **LDAP-Sicherheitsprofil** auf LDAP eingestellt ist, wird LOGONSX1 - anstelle von LOGONEX1 - vom Natural Security-Anmeldeprogramm aufgerufen.

Wenn LOGONSX1 nicht geändert wird, ruft es den Natural Security-Anmeldebildschirm auf (Map LOGONSM1 oder Dialogfenster GLOGONS1, siehe *Anmeldebildschirm / Anmeldedialogfenster*).

Durch Ändern von LOGONSX1 können Sie Ihre eigenen Anmeldebildschirme aufrufen.

RPC-relevanter User Exit

Der User Exit LOGONEX4 ist ein Natural-Subprogramm, das nur in einer RPC-Umgebung verwendet wird. Er wird vom RPC-Anmeldeprogramm von Natural Security nach einer erfolgreichen Anmeldung eines RPC Client an einem Natural RPC Server aufgerufen.

Anmerkung: Die Anmeldung eines RPC-Clients bei einem Natural RPC Server führt nicht dazu, dass einer der unter *Anmeldungsrelevante User Exits* (siehe oben) beschriebenen User Exits aufgerufen wird.

Der Aufruf von LOGONEX4 ist immer die letzte Aufgabe, die das Anmeldeprogramm ausführt, wenn alle anderen Anmeldevorgänge abgeschlossen sind und bevor ein RPC-Dienst ausgeführt wird. Zu diesem Zeitpunkt sind die Benutzerkennung und das Passwort bereits vom Anmeldeprogramm geprüft und für gültig befunden worden, und die Natural-Systemvariablen *USER und *LIBRARY-ID enthalten gültige Werte, die verwendet werden können.

Im konversationellen Modus wird der User Exit beim Start der Konversation aufgerufen.

Die Eingabeparameter für den User Exit sind die Bibliothekskennung (Library ID) und der Subprogrammname. Der Ausgabeparameter des User Exit ist ein Rückgabecode. Dieser kann verwendet werden, um die RPC-Anmeldung mit einem Rückgabecode ungleich Null zu beenden. Ist dies der Fall, gibt Natural den Fehler NAT1696 mit dem Reason Code 10 aus.

Ein Beispiel-Quellcode-Modul für LOGONEX4 ist in der Bibliothek SYSSEC unter dem Namen NOGONEX4 verfügbar. Um den User Exit aufzurufen, muss sein Objektmodul unter dem Namen LOGONEX4 in der Bibliothek SYSTEM in der dem RPC Server zugewiesenen FNAT-Systemdatei gespeichert werden. Nach dem Kopieren in diese Bibliothek muss der RPC Server neu gestartet werden.

Sobald der User Exit aufgerufen worden ist, bleibt er bis zum Ende der RPC Server-Sitzung aktiv.

Um den User Exit zu deaktivieren, müssen Sie zuerst den RPC Server beenden und dann das Objekt LOGONEX4 aus der Bibliothek SYSTEM entfernen.

Entfernen Sie LOGONEX4 *nicht*, solange eine RPC Server-Sitzung, die diese FNAT-Systemdatei verwendet, noch aktiv ist, da dies die RPC Server-Sitzung funktionsunfähig machen würde (bei der nächsten Anmeldung am RPC-Server würde der Fehler NAT0082 ausgegeben).

Andere User Exits

Die Bibliothek SYSSEC enthält mehrere andere User Exits:

User Exit	Funktion
NSC*XX*EX1	Wobei *XX* der Objekttyp ist: US = User, LI = Library, SF = Environment, DD = DDM, FI = File, UT = Utility, OB = External Object, MA = Mailbox. Der objekttypspezifische User Exit NSC*XX*EX1 wird unmittelbar nach der Durchführung einer Verwaltungsfunktion für ein Objekt dieses Typs aufgerufen.
NSCUSEX2	Dieser User Exit wird aufgerufen, wenn Sie die Funktion **Edit Group Members** verwenden und die von Ihnen vorgenommenen Änderungen mit dem Systemkommando CATALOG katalogisieren. Er zeigt eine Liste der Gruppenmitglieder an, aus der hervorgeht, welche Mitglieder in der Gruppe hinzugefügt und welche aus ihr entfernt wurden.
NSC*XX*EX3	wobei *XX* der Objekttyp ist: US = User, LI = Library, DD = DDM, FI = File, OB = External Object, MA = Mailbox. Der objekttypspezifische User Exit NSC*XX*EX3 wird aufgerufen, wenn eine Verwaltungsfunktion für ein Objekt dieses Typs aufgerufen wurde und nachdem Daten eingegeben wurden - jedoch bevor diese Daten von Natural Security validiert und verarbeitet werden.

User Exit	Funktion
	Die Quellcodes von NSC*XX*EX3 werden unter dem Namen ESC*XX*EX3 ausgeliefert. Um einen von ihnen zu aktivieren, müssen Sie ihn unter dem Namen NSC*XX*EX3 in der Bibliothek SYSSEC katalogisieren.

Die Parameter dieser User Exits sind nicht änderbar.

Einzelheiten finden Sie in den Quellcodes der User Exits.

26 Anwendungsprogrammierschnittstellen

- Allgemeines zu Subprogrammen bei NSC 450
- Subprogramme zur Zugangsberechtigungsprüfung und zur Benutzerauthentifizierung 451
- Subprogramme für Administrator Services 456
- Subprogramme zur Objektverwaltung 460
- Subprogramme für Abruf-Funktionen (Retrieval) 467

In diesem Kapitel werden die für Natural Security verfügbaren Anwendungsprogrammierschnittstellen (APIs) beschrieben:

Allgemeines zu Subprogrammen bei NSC

Natural Security bietet mehrere Anwendungsprogrammierschnittstellen (APIs). Es handelt sich um Natural-Subprogramme, die in vier Kategorien fallen:

- Subprogramme für die Zugangsprüfung und Benutzerauthentifizierung,
- Subprogramme zur Ausführung von Natural Security Administrator Services-Funktionen von außerhalb der Natural Security-Bibliothek `SYSSEC`,
- Subprogramme zur Ausführung von Natural Security-Verwaltungsfunktionen (Maintenance Functions) von außerhalb der Natural Security-Bibliothek `SYSSEC`,
- Subprogramme zur Ausführung von Natural Security-Retrieval-Funktionen von außerhalb der Natural Security-Bibliothek `SYSSEC`.

Jedes zu verwendende Subprogramm muss in die Bibliothek kopiert werden, in der es ausgeführt werden soll, oder in eine der Steplibs, die mit dieser Bibliothek verkettet sind.

Anmerkung: Die Subprogramme (mit Ausnahme von `SECNOTE`) können nicht aus einem der im Kapitel *User Exits* beschriebenen anmeldebezogenen User Exits aufgerufen werden.

Um die APIs aufzulisten:

1 Wählen Sie im Hauptmenü (**Main Menu**) die Option **Administrator Services**.

Wenn Sie Zugriff auf die Administrator Services haben, wird das **Administrator Services Menu 1** angezeigt.

2 Drücken Sie PF8.

3 Wählen Sie im **Administrator Services Menu 2** die Option **Application Programming Interfaces**.

Es wird eine Liste der Schnittstellen-Subprogramme mit Beispielen und erklärenden Online-Texten angezeigt. Sie können das Ergebnis mithilfe der folgenden Suchfelder filtern:

- **Example**
  Beispiel: Suche nach einer bestimmten Gruppe von Beispielen.
- **Interface**
  Schnittstelle: Suche nach einer benötigten Anwendungsprogrammierschnittstelle.

- **Description**
  Beschreibung: Filterung der Beispiele nach beschreibenden Stichwörtern.

Rückgabecode

Mehrere der Subprogramme enthalten das Feld `PRC`. Es enthält den Rückgabecode. Dieser ist `0` (Null), wenn die Funktion erfolgreich ausgeführt wurde. Jeder andere Rückgabecode *nnnn* entspricht entweder einer Natural Security-Fehlernummer oder, wenn ein Bindestrich (-) vorangestellt ist, einer Natural-Systemfehlernummer. Sie können die entsprechende Meldung anzeigen, indem Sie eines der folgenden Natural-Systemkommandos eingeben:

- `HELP U`*nnnn* für eine Natural Security-Meldung, in der Bibliothek `SYSSEC` oder
- `HELP` *nnnn* für eine Natural-Systemmeldung.

Subprogramme zur Zugangsberechtigungsprüfung und zur Benutzerauthentifizierung

Diese Subprogramme können für Folgendes verwendet werden:

Subprogramm	Beschreibung
Subprogramme zur Zugangsberechtigungsprüfung	
`NSC---L`	Prüfen, ob die Anmeldung bei einer Bibliothek erlaubt ist und welche Module in einer Bibliothek für einen Benutzer verfügbar sind.
`NSCCHCK`	Prüfen, ob der Zugriff auf ein externes Objekt erlaubt ist.
`NSCDEF`	Prüfen, ob das Objekt in Natural Security definiert ist.
Subprogramme zur Benutzerauthentifizierung	
`NSC---P`	Prüfen, ob das Passwort gültig ist.
`NSC----P`	Prüfen, ob das Passwort gültig ist, und es ändern.
`NSC--PH`	Prüfen, ob die Passphrase gültig ist.
`NSC--PHS`	Prüfen, ob die Passphrase gültig ist, und sie ändern.
`NSC---SP`	Prüfen, ob das Passwort gültig ist - in RPC Server-Umgebungen.
`NSCSSX`	Prüfen, ob das Passwort gültig ist - in einem LDAP-Benutzerauthentifizierungskontext.

NSC---L

Das Subprogramm NSC---L wird verwendet, um:

- zu prüfen, ob ein bestimmter Benutzer sich bei einer bestimmten Bibliothek anmelden darf,
- festzustellen, welche Module in einer Bibliothek für einen Benutzer verfügbar sind.

Es wird wie folgt aufgerufen:

```
CALLNAT 'NSC---L' PAPPLID PUSERID PRC PPARM1 PNSC-MESSAGE
```

Beispielprogramme PGM---L und PGM---LM für den Aufruf dieses Subprogramms sowie erläuternde Texte TXT---L und TXT---LM sind in der Bibliothek SYSSEC in Quellcodeform enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung
PGM---L	Prüfen, ob ein bestimmter Benutzer sich bei einer bestimmten Bibliothek anmelden darf.
PGM---LM	Prüfen, ob ein bestimmter Benutzer ein Modul in einer Bibliothek ausführen darf.

NSCCHCK

Das Subprogramm NSCCHCK wird verwendet, um zu prüfen, ob ein bestimmter Benutzer auf ein bestimmtes externes Objekt zugreifen darf.

Das Subprogramm NSCCHCK wird wie folgt aufgerufen:

```
CALLNAT 'NSCCHCK' PCLASSID PUSERID POBJID PACCESS-TYPE PRC PPARM1 PNSC-MESSAGE
```

Ein Beispielprogramm PGMCHCK für den Aufruf dieses Subprogramms und ein erläuternder Text TXTCHCK sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung	Codes
PGMCHCK	Prüfen, ob ein bestimmter Benutzer auf ein bestimmtes externes Objekt zugreifen darf.	DS, JB, ND, OP, PR, VA, VS

Code	Funktion
DS	Dataset
JB	Batch Jobs
ND	Nodes (Knoten)
OP	Operations
PR	Printers (Drucker)
VA	VTAM-Anwendungen
VS	Volume Serials (Datenträgernummer)

NSCDEF

Das Subprogramm NSCDEF wird verwendet, um zu prüfen, ob ein bestimmtes Objekt unter Natural Security definiert ist, d.h. ob ein Sicherheitsprofil für das Objekt existiert.

Das Subprogramm NSCDEF wird wie folgt aufgerufen:

```
CALLNAT 'NSCDEF' POBJID POBJTYPE PRC PNSC-MESSAGE PPARM1
```

Ein Beispielprogramm PGMDEF für den Aufruf dieses Subprogramms und ein erläuternder Text TXTDEF sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung
PGMDEF	Prüfen, ob ein bestimmtes Objekt unter Natural Security definiert ist (ob ein Sicherheitsprofil für das Objekt existiert).

NSC---P

Das Subprogramm NSC---P wird verwendet, um zu prüfen, ob das zusammen mit einer Benutzerkennung gelieferte Passwort gültig ist.

Anmerkung: Um diese Funktion in einer Natural RPC Server-Umgebung auszuführen, wird empfohlen, stattdessen NSC---SP (siehe unten) zu verwenden. Zum Prüfen einer *Passphrase* können Sie NSC--PH (siehe unten) verwenden.

Das Subprogramm NSC---P wird wie folgt aufgerufen:

```
CALLNAT 'NSC---P' PUSERID PPASSWORD PUSER_NAME PRC PNSC-MESSAGE
```

Ein Beispielprogramm PGM---P für den Aufruf dieses Subprogramms und ein erläuternder Text TXT---P sind in der Bibliothek SYSSEC in Quellcodeform enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung
PGM---P	Prüfen des Passworts eines bestimmten Natural Security-Benutzers.

Anmerkung: Bei der Ausführung dieses Subprogramms gilt die allgemeine Option **Maximum Number of Logon Attempts**, d.h. jedes ungültige Passwort wird als ein erfolgloser Anmeldeversuch gewertet.

NSC----P

Das Subprogramm NSC----P wird verwendet, um zu prüfen, ob das zusammen mit einer Benutzerkennung gelieferte Passwort gültig ist. Außerdem wird es verwendet, um das Passwort zu ändern.

Anmerkung: Um diese Funktion für eine *Passphrase* auszuführen, können Sie NSC--PHS verwenden (siehe unten).

Das Subprogramm NSC----P wird wie folgt aufgerufen:

```
CALLNAT 'NSC----P' PUSERID PPASSWORD(*) PUSER_NAME PPARM PRC PNSC-MESSAGE
```

Ein Beispielprogramm PGM----P, wie dieses Subprogramm aufgerufen werden kann, und ein erläuternder Text TXT----P sind in der Bibliothek SYSSEC in Quellcodeform enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung
PGM----P	Prüfen und ändern des Passworts eines bestimmten Natural Security-Benutzers.

Anmerkung: Bei der Ausführung dieses Subprogramms gilt die allgemeine Option **Maximum Number of Logon Attempts**, d.h. jedes ungültige Passwort wird als ein erfolgloser Anmeldeversuch gewertet.

NSC--PH

Das Subprogramm NSC--PH wird verwendet, um zu prüfen, ob die Passphrase, die zusammen mit einer Benutzerkennung angegeben wurde, gültig ist.

Es wird wie folgt aufgerufen:

```
CALLNAT 'NSC--PH' PUSERID PPASSWORD_PHRASE PUSER_NAME PRC PNSC-MESSAGE PNSC-MESSAGE_2
```

Ein Beispielprogramm PGM--PH für den Aufruf dieses Subprogramms und ein erläuternder Text TXT--PH sind in der Bibliothek SYSSEC in Quellcodeform enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung
PGM--PH	Prüfen der Passphrase einer bestimmter Benutzerkennung.

Anmerkung: Bei der Ausführung dieses Subprogramms gilt die allgemeine Option **Maximum Number of Logon Attempts**, d.h. jedes ungültige Passwort wird als ein erfolgloser Anmeldeversuch gewertet.

NSC--PHS

Das Subprogramm NSC--PHS wird verwendet, um zu prüfen, ob die zusammen mit einer Benutzerkennung gelieferte Passphrase gültig ist. Außerdem wird es verwendet, um die Passphrase zu ändern.

Das Subprogramm NSC--PHS wird wie folgt aufgerufen:

```
CALLNAT 'NSC--PHS' PUSERID PPASSWORD_PHRASE(*) PUSER_NAME PPARM PRC PNSC-MESSAGE ↩
PNSC-MESSAGE_2
```

Ein Beispielprogramm PGM--PHS für den Aufruf dieses Subprogramms und ein erläuternder Text TXT--PHS sind in der Bibliothek SYSSEC in Quellcodeform enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung
PGM--PHS	Prüfen und ändern der Passphrase eines bestimmten Natural Security-Benutzers.

Anmerkung: Bei der Ausführung dieses Subprogramms gilt die allgemeine Option **Maximum Number of Logon Attempts**, d.h. jedes ungültige Passwort wird als ein erfolgloser Anmeldeversuch gewertet.

NSC---SP

Das Subprogramm NSC---SP ist nur in Natural RPC Server-Umgebungen zu verwenden. Es entspricht im Wesentlichen NSC---P (siehe oben). Es wird verwendet, um zu prüfen, ob das zusammen mit einer Benutzerkennung angegebene Passwort gültig ist.

Das Subprogramm NSC---SP wird wie folgt aufgerufen:

```
CALLNAT 'NSC---SP' PUSERID PPASSWORD PLIBRARYID PUSERNAME
                     PPARM1 PRC PNSC-MESSAGE
```

Ein Beispielprogramm PGM---SP für den Aufruf dieses Subprogramms und ein erläuternder Text TXT---SP sind in der Bibliothek SYSSEC in Quellcodeform enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung
PGM---SP	Prüfen des Passworts eines bestimmten Natural Security-Benutzers. Diese Natural Security API kann in einer Natural-Server-Sitzung (das heisst, wenn die Natural-Systemvariable *SERVER-TYPE nicht leer ist) sowie in einer Nicht-Natural-Sitzung verwendet werden.

Anmerkung: Für die Ausführung dieses Subprogramms gilt die allgemeine Option **Maximum Number of Logon Attempts**, d.h. jedes ungültige Passwort wird als ein erfolgloser Anmeldeversuch gewertet. Außerdem verhält sich Natural Security so, als ob die Option

Lock User Option auf `X` gesetzt wäre, d.h. es merkt sich erfolglose Anmeldeversuche über Sitzungen hinweg. Anders als bei der **Lock User Option** wird bei der Sperrung von Benutzerkennungen jedoch nicht die in der Natural-Systemvariablen `*INIT-USER` enthaltene Benutzerkennung berücksichtigt. Wenn die maximale Anzahl an Anmeldeversuchen überschritten wird, wird die Natural RPC Server-Sitzung *nicht* beendet.

NSCSSX

Das Subprogramm `NSCSSX` ist nur unter Windows und Linux verfügbar. Es wird verwendet, um zu prüfen, ob das zusammen mit der Benutzerkennung übergebene Passwort gültig ist.

Voraussetzung für die Verwendung dieses Subprogramms ist, dass die Benutzerauthentifizierung über einen LDAP-Server aktiviert wurde. Siehe ***Authentifizierungsoptionen (LDAP)***.

Das Subprogramm `NSCSSX` wird wie folgt aufgerufen:

```
CALLNAT 'NSCSSX' PUSERID PPASSWORD PNSC-USERID PNSC-USERNAME PNSC-USERTYPE PPARM ↩
PRC PNSC-MESSAGE ↩
```

Ein Beispielprogramm `PGMSSX01` für den Aufruf dieses Subprogramms und ein erläuternder Text `TXTSSX01` sind in Quellcodeform in der Bibliothek `SYSSEC` enthalten. Sie enthalten Beschreibungen der einzelnen `CALLNAT`-Parameter.

Beispielprogramm	Beschreibung
`PGMSSX01`	Prüfen des Passworts einer bestimmten Benutzerkennung.

Anmerkung: Bei der Ausführung dieses Subprogramms gilt die allgemeine Option **Maximum Number of Logon Attempts**, d.h. jedes ungültige Passwort wird als ein erfolgloser Anmeldeversuch gewertet.

Subprogramme für Administrator Services

Mit diesen Subprogrammen können verschiedene Funktionen der Administrator Services ausgeführt werden:

Subprogramm	Beschreibung
`NSCADM`	Allgemeine Optionen anzeigen Verarbeiten von (ETID-bezogenen) Anmeldesätzen Anmelde-/Gegenzeichnungsfehlersätze verarbeiten Verwaltungs-/Wiederherstellungsabschnitten für einzelne Objekttypen entfernen/wiederherstellen Benutzer anzeigen, in deren Sicherheitsprofilen ein Wert von einem voreingestellten Wert abweicht Gesperrte Benutzerkennungen auflisten und entsperren

Subprogramm	Beschreibung
NSCSSXMN	LDAP-Sicherheitsprofil archivieren/zurückholen
NSCXLI	Eines einzelnen Verwaltungsprotokollsatz anzeigen
NSCXLO	Eine Liste von Verwaltungsprotokollsätzen anzeigen

NSCADM

Das Subprogramm NSCADM wird für folgende Zwecke verwendet:

- Einstellungen der **General Options** in den Administrator Services anzeigen.
- **Anmeldesätze** verarbeiten, was insbesondere für ETID-bezogene Anmeldesätze relevant ist.
- **Anmelde-/Gegenzeichnungsfehlersätze** verarbeiten.
- Natural Security-Verwaltungs-/Abrufabschnitte entfernen/neu einrichten: für Basis-/Verbundanwendungsprofile und RPC-Serverprofile.
- Einen voreingestellten Wert (wie in den **User Preset Values** festgelegt) mit dem entsprechenden tatsächlichen Wert in Benutzersicherheitsprofilen vergleichen, um eine Liste aller Benutzersicherheitsprofile zu erhalten, in denen der Wert vom voreingestellten Wert abweicht.
- Gesperrte Benutzerkennungen auflisten und eine gesperrte Benutzerkennung entsperren.

Das Subprogramm NSCADM wird wie folgt aufgerufen:

```
CALLNAT 'NSCADM' PVERSION PPARM PPARM1(*) PLENGTH PRC PNSC-MESSAGE
```

Beispielprogramme PGMADM01 - PGMADM07 und erläuternde Texte TXTADM01 bis TXTADM07 sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung	Codes
PGMADM01	Allgemeine Standardeinstellungen und Optionen zurückgeben.	GDO, NSF (nur unter z/OS), SSX (nur unter Linux und Windows)
PGMADM02	Anmeldedatensätze auflisten und löschen.	LR, DR
PGMADM03	Natural Security-Objekttypbeschreibungen verarbeiten (Beschreibung der Anwendungsentität löschen, Beschreibung der Anwendungsentität anzeigen, Beschreibung der Natural-RPC-Entität aktualisieren).	DI, DE, UP
PGMADM04	Liste der Natural Security-Benutzerprofile abrufen, bei denen der Wert eines Feldes vom entsprechenden voreingestellten Wert abweicht.	PR
PGMADM05	Zeitstempelbezogene ETID-Anmeldesätze verwalten. (Es ist möglich, diejenigen Anmeldungen auszuwählen, die in einer Natural RPC-Umgebung stattgefunden haben).	LR

Beispielprogramm	Beschreibung	Codes
PGMADM06	Gesperrte Benutzerkennungen auflisten und entsperren.	AE
PGMADM07	Anmelde-/Gegenzeichnungsfehlersätze auflisten und löschen.	LE, DE

Der Parameter PPARM wird als Funktionscode verwendet:

Code	Funktion
GDO	Allgemeine Optionen anzeigen.
NSF	NSF-Optionen anzeigen.
LR	Anmeldesätze auflisten.
DR	Anmeldesätze löschen.
LE	Anmelde-/Gegenzeichnungsfehler auflisten.
DE	Anmelde-/Gegenzeichnungsfehler löschen.
DI	Verwaltungs-/Abruf-Abschnitte für Basis-/Verbundanwendungsprofile und RPC-Serverprofile anzeigen.
DE	Verwaltungs-/Retrieval-Abschnitte für Basis-/Verbundanwendungsprofile und RPC-Serverprofile löschen.
PR	Vorgabewert vergleichen.
LI	Gesperrte Benutzerkennungen auflisten.
UL	Eine gesperrte Benutzerkennung entsperren.

NSCSSXMN

Das Subprogramm NSCSSXMN ist nur unter Windows und Linux verfügbar. Es wird verwendet, um ein LDAP-Sicherheitsprofil zur archivieren und zurückzuholen.

Voraussetzung für die Verwendung dieses Subprogramms ist, dass das LDAP-Sicherheitsprofil in archivierter oder zurückgeholter Form existiert. Siehe *Authentifizierungsoptionen (LDAP)*.

Das Subprogramm NSCSSXMN wird wie folgt aufgerufen:

```
CALLNAT 'NSCSSXMN' PFUNCTION PPROFILE-ID PRC
```

Ein Beispielprogramm PGMSSX02 für den Aufruf dieses Subprogramms und ein erläuternder Text TXTSSX02 sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung	Codes
PGMSSX02	Authentifizierungsprofile verwalten (LDAP).	AR, RV

Der Parameter PFUNCTION dient als Funktionscode:

Code	Funktion
AR	Security-Profil archivieren.
RV	Security-Profil zurückholen.

NSCXLI

Das Subprogramm NSCXLI wird verwendet, um einen einzelnen Verwaltungsprotokolldatensatz anzuzeigen, der von Natural Security erstellt wurde, wenn die allgemeine Option **Logging of Maintenance Functions** aktiv ist.

Das Subprogramm NSCXLI wird wie folgt aufgerufen:

```
CALLNAT 'NSCXLI' PFUNCTION PSELECT-TYPE POBJ-ID POBJ-ID2 PTIMESTMP PPARM PRC ↩
PNSC-MESSAGE PLOG-HEADER XPARM1 PPARM1 XPARM2 PPARM2 XPARM3 PPARM3 XPARM4 PPARM4 ↩
XPARM5 PPARM5 XPARM6 PPARM6 XTEXT PTEXT
```

Beispielprogramme PGMXLI01 - PGMXLI10 für den Aufruf dieses Subprogramms und erläuternde Texte TXTXLI01 - TXTXLI10 sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung	Codes
PGMXLI01	Den Verwaltungsprotokolldatensatz einer Datei lesen.	RI
PGMXLI02	Den Verwaltungsprotokolldatensatz einer Datei lesen. Nur die geänderten Daten dieses Satzes anzeigen.	RI
PGMXLI03	Den Verwaltungsprotokolldatensatz einer Bibliothek lesen.	RI
PGMXLI04	Den Verwaltungsprotokolldatensatz einer Bibliothek lesen. Nur die geänderten Daten dieses Satzes anzeigen.	RI
PGMXLI05	Den Verwaltungsprotokolldatensatz einer Mailbox lesen.	RI
PGMXLI06	Den Verwaltungsprotokolldatensatz einer Mailbox lesen. Nur die geänderten Daten dieses Satzes anzeigen.	RI
PGMXLI07	Den Verwaltungsprotokolldatensatz eines Benutzers lesen.	RI
PGMXLI08	Den Verwaltungsprotokolldatensatz eines Benutzers lesen. Nur die geänderten Daten dieses Satzes anzeigen.	RI
PGMXLI09	Den Verwaltungsprotokolldatensatz eines externen Objekts lesen.	RI
PGMXLI10	Den Verwaltungsprotokolldatensatz eines externen Objekts lesen.	RI

Code	Funktion
RI	Einen Datensatz lesen.

NSCXLO

Das Subprogramm NSCXLO dient zum Lesen von Verwaltungsprotokolldatensätzen, die von Natural Security erstellt werden, wenn die allgemeine Option **Logging of Maintenance Functions** aktiv ist.

Das Subprogramm NSCXLO wird wie folgt aufgerufen:

```
CALLNAT 'NSCXLO' PFUNCTION PSELECT-TYPE PSTART-OBJ-ID PFROMTIMESTMP PTOTIMESTMP PRC ↩
PPARM PPARM1(*) PNSC-MESSAGE
```

Ein Beispielprogramm PGMXLO01 für den Aufruf dieses Subprogramms und ein erläuternder Text TXTXLO01 sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung	Code
PGMXLO01	Sicherheitsprofil-Verwaltungsprotokolle abrufen.	RI

Code	Funktion
RI	Einen Datensatz lesen.

Subprogramme zur Objektverwaltung

Mit diesen Subprogrammen können Verwaltungsfunktionen für Sicherheitsprofile verschiedener Objekttypen durchgeführt werden:

Subprogramm	Beschreibung
NSCFI	Verwaltungsfunktionen für Dateien
NSCLI	Verwaltungsfunktionen für Bibliotheken
NSCMA	Verwaltungsfunktionen für Mailboxen
NSCOB	Verwaltungsfunktionen für externe Objekte
NSCUS	Verwaltungsfunktionen für Benutzer
NSCUT	Verwaltungsfunktionen für Dienstprogramme (Utilities)

Die Verwendung der Subprogramme für die Objektpflege wird über die allgemeine Option **Free Access to Functions via APIs** gesteuert (siehe Kapitel *Administrator Services*).

NSCFI

Das Subprogramm NSCFI ist nur in einer z/OS-Umgebung verfügbar und kann nur auf Dateisicherheitsprofile angewendet werden. Für DDM-Sicherheitsprofile können Sie das Subprogramm NSCLI verwenden (siehe unten).

Das Subprogramm NSCFI wird verwendet, um Verwaltungs-/Abruf-Funktionen für Dateisicherheitsprofile von außerhalb der Bibliothek SYSSEC durchzuführen.

Es wird wie folgt aufgerufen:

```
CALLNAT 'NSCFI' PFUNCTION PFILEID PFILEID2 PRC PPFKEY(*) PPARM PPARM1 PPARM2 PTEXT(*) ↩
PNSC-MESSAGE
```

Ein Beispielprogramm PGMFI001 für den Aufruf dieses Subprogramms und ein erläuternder Text TXTFI001 sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Das Beispielprogramm ist nur in einer z/OS-Umgebung verfügbar.

Beispielprogramm	Beschreibung	Codes
PGMFI001	Dateiverwaltungsfunktionen ausführen.	AD, CL, CO, DE, DI, MO, RE, UP

Der erste Parameter (PFUNCTION) muss mit dem Funktionscode für die gewünschte Funktion gefüllt werden. Die folgenden Funktionen sind verfügbar:

Code	Funktion
AD	Datei anlegen
CL	Verlinkung zwischen Bibliothek und Datei aufheben
CO	Datei kopieren
DE	Datei löschen
DI	Datei anzeigen
MO	Datei ändern (einschließlich aller **Bestandteile** des Sicherheitsprofils)
RE	Lese-Link zwischen Bibliothek und Datei herstellen
UP	Update-Link zwischen Bibliothek und Datei herstellen

NSCLI

Das Subprogramm NSCLI wird verwendet, um Verwaltungs-/Abruf-Funktionen für Bibliothekssicherheitsprofile von außerhalb der Bibliothek SYSSEC auszuführen.

Es wird wie folgt aufgerufen:

```
CALLNAT 'NSCLI' PFUNCTION PLIBID PLIBID2 PLIBTYPE PRC PPFKEY(*) PPARM PPARM1 PPARM2 ↩
PTEXT(*) PPARM3 PPARM4 PPARM5 PPARM6 POPRB(*) PNSC-MESSAGE
```

Beispielprogramme PGMLI001 - PGMLI006 für den Aufruf dieses Subprogramms und erläuternde Texte TXTLI001 - TXTLI006, sowie Beispielprogramme PGMDDM01 - PGMDDM02, wie es mit dem Funktionscode MD aufzurufen ist, und entsprechende erläuternde Texte TXTDDM01 - TXTDDM02 sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Die Beispielprogramme PGMDDM01 und PGMDDM02 sind nur unter Windows und Linux verfügbar.

Beispielprogramm	Beschreibung	Codes
PGMLI001	Bibliotheksprofil verwalten (allgemeine Optionen).	AD, CO, DI, DL, MO, LK, RE, SL, TL
PGMLI002	Bibliotheksprofil verwalten (Verknüpfung Benutzer-Bibliothek aufheben, Bibliothek löschen, ETID abfragen).	CL, DE, ET
PGMLI003	Module erlauben und nicht erlauben.	DM, MM
PGMLI004	Bibliotheksprofil verwalten (Kommandoprozessoren).	AC, DC, LC, MC, MK, UC
PGMLI005	Steplib-Eintragstabelle sowie *STEPLIB verwalten.	ST
PGMLI006	Bibliotheksprofile mit Adabas-Passwort abrufen und verwalten.	SL, MO
PGMDDM01	Bibliotheksprofile mit Adabas-Passwort abrufen und verwalten.	MD
PGMDDM02	DDM-Sicherheitsprofil verwalten.	MD, LD

Der erste Parameter (PFUNCTION) muss mit dem Funktionscode für die gewünschte Funktion gefüllt werden. Die folgenden Funktionen sind verfügbar:

Code	Funktion
AD	Bibliothek anlegen
CL	Verlinkung zwischen Benutzer und Bibliothek aufheben
CO	Bibliothek kopieren
DE	Bibliothek löschen
DI	Bibliothek anzeigen
DL	Special-Link zwischen Benutzer und Bibliothek anzeigen

Code	Funktion
DM	Erlaubte/nicht erlaubte Module anzeigen
ET	Bibliothekskennung (Library ID) über ETID abfragen
LK	Benutzer mit Bibliothek verlinken
MD	DDM-Profil verwalten; siehe auch unten (diese Funktion ist unter z/OS nicht verfügbar)
MM	Erlaubte/nicht erlaubte Module ändern
MO	Bibliothek ändern (einschließlich aller **Bestandteile** ihres Sicherheitsprofils)
SL	Special-Link zwischen Benutzer und Bibliothek herstellen
TL	Link zwischen Benutzer und Bibliothek vorübergehend sperren
UC	Alle *geänderten* Kommandoprozessoren in der Bibliothek aktualisieren

Wenn PFUNCTION mit dem Funktionscode MD gefüllt ist, muss der PSUBFUNC-Abschnitt des Parameters PPARM mit dem Code für die gewünschte Unterfunktion gefüllt werden. Die folgenden Unterfunktionen sind verfügbar:

Code	Unterfunktion
AD	DDM-Profil anlegen
CL	Link zwischen Bibliotheksprofil und DDM-Profil aufheben
CO	DDM-Profil kopieren
DE	DDM-Profil löschen
DI	DDM-Profil anzeigen
MO	DDM-Profil ändern
RE	Lesen-Link zwischen Bibliotheksprofil und DDM-Profil herstellen
UP	Update-Link zwischen Bibliotheksprofil und DDM-Profil herstellen

NSCMA

Das Subprogramm NSCMA wird verwendet, um Verwaltungs-/Abruf-Funktionen für Mailbox-Sicherheitsprofile von außerhalb der Bibliothek SYSSEC durchzuführen.

Es wird wie folgt aufgerufen:

```
CALLNAT 'NSCMA' PFUNCTION POBJID POBJID2 PRC PPFKEY(*) PPARM PPARM1 PPARM2 PTEXT1(*) ↩
PTEXT2(*) PNSC-MESSAGE
```

Beispielprogramme PGMMA001 - PGMMA002 für den Aufruf dieses Subprogramms und erläuternde Texte TXTMA01 - TXTMA02 sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung	Codes
PGMMA001	Mailbox-Profil verwalten.	AD, DI, MO, CO, RE
PGMMA002	Mailbox-Profil löschen.	DE

Der erste Parameter (PFUNCTION) muss mit dem Funktionscode der gewünschten Funktion gefüllt werden. Die folgenden Funktionen sind verfügbar:

Code	Funktion
AD	Mailbox-Profil anlegen
CO	Mailbox-Profil kopieren
DE	Mailbox-Profil löschen
DI	Mailbox-Profil anzeigen
MO	Mailbox-Profil ändern (einschließlich aller **Bestandteile** des Sicherheitsprofils)
RE	Mailbox-Profil umbenennen

NSCOB

Das Subprogramm NSCOB ist nur in einer z/OS-Umgebung verfügbar. Es wird verwendet, um Verwaltungs-/Abruf-Funktionen für externe Objektsicherheitsprofile von außerhalb der Bibliothek SYSSEC durchzuführen.

Es wird wie folgt aufgerufen:

```
CALLNAT 'NSCOB' PFUNCTION PCLASSID POBJID POBJID2 PRC PPFKEY(*) PPARM PPARM1 PPARM2 ↩
PTEXT(*) PNSC-MESSAGE
```

Beispielprogramme PGMOB001 - PGMOB002 für den Aufruf dieses Subprogramms und erläuternde Texte TXTOB001 - TXTOB002 sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung	Codes
PGMOB001	Externes Objektprofil verwalten (allgemeine Optionen).	AD, CO, CL, DE, DI, DL, LK, MO
PGMOB002	Externes Objektprofil verwalten (Link zwischen externem Objekt und Benutzer aufheben, externes Objektprofil löschen).	CL, DE

Der erste Parameter (PFUNCTION) muss mit dem Funktionscode für die gewünschte Funktion gefüllt werden. Die folgenden Funktionen sind verfügbar:

Code	Funktion
AD	Externes Objekt anlegen
CL	Link zwischen Benutzer und externem Objekt aufheben
CO	Externes Objekt kopieren
DE	Externes Objekt löschen
DI	Externes Objekt anzeigen
DL	Link zwischen Benutzer und externem Objekt anzeigen
LK	Benutzer mit externem Objekt verlinken
MO	Externes Objekt ändern (einschließlich aller **Bestandteile** seines Sicherheitsprofils)

NSCUS

Das Subprogramm NSCUS wird verwendet, um Verwaltungs-/Abruf-Funktionen für Benutzersicherheitsprofile von außerhalb der Bibliothek SYSSEC durchzuführen.



Anmerkung: NSCUS kann nicht für private Bibliotheken verwendet werden, die an Benutzersicherheitsprofile angehängt sein können. Für die Verwaltung/das Abrufen von privaten Bibliotheken können Sie das Subprogramm NSCLI verwenden.

Das Subprogramm NSCUS wird wie folgt aufgerufen:

```
CALLNAT 'NSCUS' PFUNCTION PUSERID PUSERID2 PRC PPFKEY(*) PPARM PPARM1 PPARM2 PTEXT(*) ↩
PPARM3 PPARM4 PNSC-MESSAGE
```

Beispielprogramme PGMUS001 - PGMUS004 für den Aufruf dieses Subprogramms und erläuternde Texte TXTUS001 - TXTUS001 sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung	Codes
PGMUS001	Benutzerprofil verwalten (allgemeine Optionen).	AD, AM, CO, CP, DI, MO, RE
PGMUS002	Benutzerprofil verwalten (Benutzerprofil löschen, Benutzer über ETID suchen).	DE, ET
PGMUS003	Benutzergruppen verwalten	AD, DE, LI
PGMUS004	Benutzer über Default-Profil verwalten.	AD, CO, DE, DI, MO

Der erste Parameter (PFUNCTION) muss mit dem Funktionscode der gewünschten Funktion gefüllt werden. Die folgenden Funktionen sind verfügbar:

Code	Funktion
AD	Benutzer anlegen
AM	Mehrere Benutzer anlegen
CO	Benutzer kopieren
DE	Benutzer löschen
DI	Benutzer anzeigen
EG	Gruppenmitglieder editieren
ET	Benutzerkennung über ETID abfragen
MO	Benutzer ändern (einschließlich aller **Bestandteile** seines Sicherheitsprofils)



Anmerkung: Die Benutzerverwaltungsfunktion *Links des Benutzers kopieren* (**Copy User's Links**) ist über NSCUS nicht verfügbar.

Für den Funktionscode EG sind die folgenden Unterfunktionen verfügbar:

Code	Unterfunktion
AD	Benutzer zu einer Gruppe hinzufügen
DE	Benutzer aus einer Gruppe löschen
LI	Gruppenmitglieder auflisten

NSCUT

Das Subprogramm NSCUT wird verwendet, um Verwaltungs-/Abruf-Funktionen für Dienstprogramm-Sicherheitsprofile (**Utility Security Profiles**) von außerhalb der Bibliothek SYSSEC durchzuführen.

Es wird wie folgt aufgerufen:

```
CALLNAT 'NSCUT' PFUNCTION PUTILITY PUSER PLIBRARY PRC PPFKEY(*) PPARM PPARM1 PPARM2 ↩
PTEXT(*) PNSC-MESSAGE
```

Ein Beispielprogramm PGMUT001 für den Aufruf dieses Subprogramms und ein erläuternder Text TXTUT001 sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung	Codes
PGMUT001	Verwalten eines bibliotheksspezifischen Dienstprogrammprofils, eines benutzerspezifischen Dienstprogrammprofils, oder Anzeigen eines Default-Dienstprogrammprofils.	AD, DE, DI, MO

Der erste Parameter (PFUNCTION) muss mit dem Funktionscode der gewünschten Funktion gefüllt werden. Die folgenden Funktionen sind verfügbar:

Code	Unterfunktion
AD	Dienstprogramm anlegen
DE	Dienstprogramm löschen
DI	Dienstprogramm anzeigen
MO	Dienstprogramm ändern (einschließlich aller **Bestandteile** seines Sicherheitsprofils)

Beachten Sie, dass die Bestandteile der Sicherheitsprofile für jedes Dienstprogramm unterschiedlich sind. Siehe auch den Quellcode von PGMUT001.

Subprogramme für Abruf-Funktionen (Retrieval)

Diese Subprogramme können verwendet werden, um verschiedene Arten von Informationen zu erhalten:

Subprogramm	Beschreibung
NSCDA	Anzeige des Bibliothekssicherheitsprofils
NSCDA-C	Anzeige der Kommandoeinschränkungen des Bibliothekssicherheitsprofils
NSCDA-P	Anzeige der Sicherheitsoptionen, Sicherheitslimits und Session-Parameter des Bibliothekssicherheitsprofils
NSCDA-S	Anzeige der Statement-Einschränkungen des Bibliothekssicherheitsprofils
NSCDAU	Anzeige des Special-Link-Sicherheitsprofils
NSCDAUC	Anzeige der Kommandoeinschränkungen des Special-Link-Sicherheitsprofils
NSCDAUP	Anzeige der Sicherheitsoptionen, Sicherheitslimits und Session-Parameter des Special-Link-Sicherheitsprofils
NSCDAUS	Anzeige der Statement-Einschränkungen des Special-Link-Sicherheitsprofils
NSCDU	Anzeige des Benutzersicherheitsprofils
NSCONE	Anzeige des NaturalONE-Profils
NSCXR	Cross-Referenz-Funktionen
NSCXRIER	Anzeige einzelner Anmeldefehlersätze
NSCXRUSE	Anzeige von Benutzern mit Anmeldefehlerzählern und nicht verwendeten Benutzerkennungen
NSCXRUTC	Anzeige der für einen Benutzer erlaubten Dienstprogrammfunktionen
SECNOTE	Anzeige der Sicherheitsvermerke eines Benutzers, einer Bibliothek oder eines Special-Link-Sicherheitsprofils
NSCFI, NSCLI, NSCMA, NSCOB, NSCUS, NSCUT	Die Anzeigefunktionen (Funktionscode DI - Sicherheitsprofil anzeigen) dieser Subprogramme werden als Abruf-Funktionen (Retrieval) betrachtet.

Die Verwendung der Subprogramme für das Abrufen wird über die allgemeine Option **Free Access to Functions via APIs** gesteuert (siehe *Administrator Services*).

NSCDA

Das Subprogramm `NSCDA` wird zur Anzeige des Sicherheitsprofils einer Bibliothek verwendet.

Das Subprogramm `NSCDA` wird wie folgt aufgerufen:

```
CALLNAT 'NSCDA' PAPPLID PPARM PRC PTYPE PPARM1 PPARM2 PPARM3 PTEXT(*) PNSC-MESSAGE
```

Ein Beispielprogramm `PGMDA` für den Aufruf dieses Subprogramms und ein erläuternder Text `TXTDA` sind in Quellcodeform in der Bibliothek `SYSSEC` enthalten. Sie enthalten Beschreibungen der einzelnen `CALLNAT`-Parameter.

Beispielprogramm	Beschreibung
`PGMDA`	Anzeigen des Sicherheitsprofils einer Anwendung oder einer privaten Bibliothek

NSCDA-C

Das Subprogramm `NSCDA-C` wird verwendet, um den Abschnitt **Command Restrictions** (Kommandoeinschränkungen) eines Bibliothekssicherheitsprofils anzuzeigen.

Das Subprogramm `NSCDA-C` wird wie folgt aufgerufen:

```
CALLNAT 'NSCDA-C' PAPPLID PRC PTYPE PPARM1 PNSC-MESSAGE
```

Ein Beispielprogramm `PGMDA-C` für den Aufruf dieses Subprogramms und ein erläuternder Text `TXTDA-C` sind in Quellcodeform in der Bibliothek `SYSSEC` enthalten. Sie enthalten Beschreibungen der einzelnen `CALLNAT`-Parameter.

Beispielprogramm	Beschreibung
`PGMDA-C`	Anzeigen der Kommandoeinschränkungen in der Sicherheitsdefinition einer Bibliothek oder einer privaten Bibliothek

NSCDA-P

Das Subprogramm `NSCDA-P` wird verwendet, um die Abschnitte **Security Options**, **Security Limits** und **Session Parameters** eines Bibliothekssicherheitsprofils anzuzeigen.

Das Subprogramm `NSCDA-P` wird wie folgt aufgerufen:

```
CALLNAT 'NSCDA-P' PAPPLID PRC PTYPE PPARM1 POPRBS(*) PNSC-MESSAGE
```

Ein Beispielprogramm `PGMDA-P` für den Aufruf dieses Subprogramms und ein erläuternder Text `TXTDA-P` sind in Quellcodeform in der Bibliothek `SYSSEC` enthalten. Sie enthalten Beschreibungen der einzelnen `CALLNAT`-Parameter.

Beispielprogramm	Beschreibung
PGMDA-P	Anzeigen der Sicherheitsoptionen, Limits und Session-Parameter in der Sicherheitsdefinition einer Anwendung oder einer privaten Bibliothek

NSCDA-S

Das Subprogramm NSCDA-S wird verwendet, um den Abschnitt **Statement Restrictions** (Statement-Einschränkungen) eines Bibliothekssicherheitsprofils anzuzeigen.

Das Subprogramm NSCDA-S wird wie folgt aufgerufen:

```
CALLNAT 'NSCDA-S' PAPPLID PRC PTYPE PPARM1 PNSC-MESSAGE
```

Ein Beispielprogramm PGMDA-S für den Aufruf dieses Subprogramms und ein erläuternder Text TXTDA-S sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung
PGMDA-S	Anzeigen der Statement-Einschränkungen in der Sicherheitsdefinition einer Anwendung oder einer privaten Bibliothek

NSCDAU

Das Subprogramm NSCDAU dient zur Anzeige eines Special-Link-Sicherheitsprofils.

Das Subprogramm NSCDAU wird wie folgt aufgerufen:

```
CALLNAT 'NSCDAU' PAPPLID PUSERID PRC PPARM1 PPARM2 PPARM3 PTEXT(*) PNSC-MESSAGE
```

Ein Beispielprogramm PGMDAU für den Aufruf dieses Subprogramms und ein erläuternder Text TXTDAU sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung
NSCDAU	Anzeigen des Sicherheitsprofils eines Special-Link.

NSCDAUC

Das Subprogramm NSCDAUC wird verwendet, um den Abschnitt **Command Restrictions** (Kommando-Einschränkungen) eines Special-Link-Sicherheitsprofils anzuzeigen.

Das Subprogramm NSCDAUC wird wie folgt aufgerufen:

```
CALLNAT 'NSCDAUC' PAPPLID PUSERID PRC PPARM1 PNSC-MESSAGE
```

Ein Beispielprogramm PGMDAUC für den Aufruf dieses Subprogramms und ein erläuternder Text TXTDAUC sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung
NSCDAUC	Anzeigen des Sicherheitsprofils eines Special-Link.

NSCDAUP

Das Subprogramm NSCDAUP wird verwendet, um die Abschnitte **Security Options**, **Security Limits** und **Session Parameters** eines Special-Link-Sicherheitsprofils anzuzeigen.

Das Subprogramm NSCDAUP wird wie folgt aufgerufen:

```
CALLNAT 'NSCDAUP' PAPPLID PUSERID PRC PPARM1 POPRBS(*) PNSC-MESSAGE
```

Ein Beispielprogramm PGMDAUP für den Aufruf dieses Subprogramms und ein erläuternder Text TXTDAUP sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung
NSCDAUP	Anzeigen der Sicherheitsoptionen, Limits und Session-Parameter in der Sicherheitsdefinition eines Special-Link.

NSCDAUS

Das Subprogramm NSCDAUS wird verwendet, um den Abschnitt **Statement Restrictions** (Statement-Einschränkungen) eines Special-Link-Sicherheitsprofils anzuzeigen.

Das Subprogramm NSCDAUS wird wie folgt aufgerufen:

```
CALLNAT 'NSCDAUS' PAPPLID PUSERID PRC PPARM1 PNSC-MESSAGE
```

Ein Beispielprogramm PGMDAUS für den Aufruf dieses Subprogramms und ein erläuternder Text TXTDAUS sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung
NSCDAUS	Anzeigen der Statement-Einschränkungen in der Sicherheitsdefinition eines Special-Link.

NSCDU

Das Subprogramm NSCDU wird verwendet, um ein Benutzersicherheitsprofil anzuzeigen.

Es wird wie folgt aufgerufen:

```
CALLNAT 'NSCDU' PUSERID PPARM PRC PPARM1 PPARM2 PPARM3 PTEXT(*) PNSC-MESSAGE
```

Ein Beispielprogramm PGMDU für den Aufruf dieses Subprogramms und der erläuternde Text TXTDU sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung
NSCDU	Anzeigen eines Benutzersicherheitsprofils.

NSCONE

Das Subprogramm NSCONE dient zur Anzeige eines NaturalONE-Profils, d. h. der Optionen und Aktionen, die in der Natural-Server-Ansicht und der Eclipse-Navigator-Ansicht für eine bestimmte Bibliothek und einen bestimmten Benutzer erlaubt/nicht erlaubt sind.

Es wird wie folgt aufgerufen:

```
CALLNAT 'NSCONE' PFUNCTION PUSER PGROUP PLIBRARY PFUSER(*) PRC PPARM PPARM1 PPARM2 ↩
PPARM3 PNSC-MESSAGE ↩
```

Ein Beispielprogramm PGMONE01 für den Aufruf dieses Subprogramms und ein erläuternder Text TXTONE01 sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung	Code
PGMONE01	Anzeigen eines NaturalONE-Profils für eine bestimmte Bibliothekskennung und Benutzerkennung.	DI

Code	Funktion
DI	Anzeigen eines NaturalONE-Profils

NSCXR

Das Subprogramm NSCXR wird verwendet, um Cross-Referenz-Funktionen für Sicherheitsprofile von außerhalb der Bibliothek SYSSEC auszuführen.

Das Subprogramm NSCXR wird wie folgt aufgerufen:

```
CALLNAT 'NSCXR' POBJ-TYPE POBJ-ID PLINK-ID PRC SUB-TYPE PPARM PPARM2(*) PNSC-MESSAGE
```

Beispielprogramme PGMXR001 - PGMXR021 für den Aufruf dieses Subprogramms und erklärende Texte TXTXR001 - TXTXR021 sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung	Codes
PGMXR001	Listet Natural Security-Objekte in alphabetischer Reihenfolge auf.	DS, DD, FI, LI, MA, JB, ND, NV, OP, PR, RP, US, UT, VS, VT
PGMXR002	Fragt Cross-Referenzdaten für eine Bibliothek ab.	LI
PGMXR003	Fragt Cross-Referenzdaten für Benutzer ab.	US
PGMXR004	Fragt Cross-Referenzdaten für Dateien und Link-Informationen ab.	FI
PGMXR005	Fragt Cross-Referenzdaten für Mailboxen ab.	MA
PGMXR006	Listet Anmeldesätze auf.	LR
PGMXR007	Listet Anmeldefehlersätze auf.	LE
PGMXR008	Fragt Cross-Referenzdaten für Steplibs ab.	ST
PGMXR009	Ruft eine Liste der Benutzer ab, die zu einer Batch-Benutzerkennung gehören.	US
PGMXR010	Ruft Cross-Referenzdaten für eine Bibliothekskennung – Benutzerkennung (Special-Link) ab.	LI
PGMXR011	Ruft Cross-Referenzdaten für eine Bibliothek ab.	LI
PGMXR012	Ruft Bibliotheken und Benutzer ab, bei denen der NCP definiert ist.	CP
PGMXR013	Ruft Cross-Referenzdaten für Dienstprogramme ab.	UT, LI, US
PGMXR014	Übersetzt den Namen eines Natural Security-Objekts in eine Natural Security-Objektkennung.	LI, US
PGMXR015	Sucht nach Bibliotheken in der aktuellen FNAT/FUSER-Systemdatei, die nicht in Natural Security definiert sind.	SF
PGMXR016	Übersetzt den zwei Zeichen langen Natural Security-Objekttypcode in den entsprechenden Natural Security-Objekttyp.	Beliebiger zwei Zeichen langer Objekttypcode.
PGMXR017	Liste für eine bestimmte Objektklasse: Natural Security-Objektkennungen oder Benutzerkennungen mit Zugriffsausnahmen.	DS, PR

Beispielprogramm	Beschreibung	Codes
PGMXR018	Ruft den Xref-Status eines bestimmten Moduls in einer Bibliothek für alle Benutzerkennungen ab, die möglicherweise Zugriff auf diese Bibliothek haben. Zusätzlich gibt es eine Option zum Auflisten der Gruppenmitglieder.	LI
PGMXR019	Ruft Cross-Referenzdaten für Benutzer ab.	US
PGMXR020	Ruft Xref-Daten für Zeitunterschied und Zeitzone ab, die in Benutzerprofilen vom Typ A, G, M, P definiert sind.	US
PGMXR021	Ruft Natural Security-Bibliothek und Natural Security-Special-Link-Profile mit FDIC- und FUSER-Zuweisungen ab.	LI

Der erste Parameter (POBJ-TYPE) muss mit dem Code für den Objekttyp gefüllt werden, für den eine Funktion ausgeführt werden soll:

Code	Objekttyp
US	Benutzer
LI	Bibliothek
DD	DDM (dieser Objekttyp ist nicht unter z/OS verfügbar)
FI	Datei (dieser Objekttyp ist nur unter z/OS verfügbar)
MA	Mailbox
LE	Anmeldefehlersatz
LR	Anmeldesatz
ST	Steplib
UT	Dienstprogramm (Utility)
CP	Kommandoprozessor
PE	Externes Predict-Objekt (dieser Objekttyp ist nur verfügbar, wenn Predict installiert ist)
PF	Predict-Funktion (dieser Objekttyp ist nur verfügbar, wenn Predict installiert ist)
PL	Predict 3GL-Bibliothek (dieser Objekttyp ist nur verfügbar, wenn Predict installiert ist)
PO	Predict-Dokumentationsobjekt (dieser Objekttyp ist nur verfügbar, wenn Predict installiert ist)
SF	Systemdatei

Auf die einzelnen oben aufgeführten Objekttypen können die folgenden Funktionen angewendet werden, indem der Parameter SUB-TYPE mit einem der folgenden Funktionscodes gefüllt wird:

Für jeden Objekttyp verfügbare Funktion:	
Code	**Funktion**
TR	Übersetzt den zweistelligen Objekttyp-Code in den entsprechenden Objekttyp.

Für einen Benutzer (US) verfügbare Funktionen:	
Code	**Funktion**
*	Alle Benutzer auflisten.
A	Alle Benutzer des Typs Administrator auflisten.
P	Alle Benutzer des Typs Person auflisten.
M	Alle Benutzer des Typs Mitglied (Member) auflisten.
T	Alle Benutzer des Typs Terminal auflisten.
G	Alle Benutzer des Typs Gruppe (Group) auflisten.
B	Alle Benutzer des Typs Batch auflisten.
GR	Alle Gruppen auflisten, zu denen der Benutzer gehört.
GP	Alle privilegierten Gruppen auflisten, zu denen der Benutzer gehört.
GM	Alle Benutzer auflisten, die in der Gruppe enthalten sind.
BU	Alle Benutzer auflisten, in deren Sicherheitsprofil die Batch-Benutzerkennung angegeben ist.
NI	Benutzerkennung abrufen (Retrieve), die zu einem bestimmten Benutzernamen gehört.
L*	Alle Benutzer und alle Bibliotheken auflisten, mit denen sie direkt verlinkt sind.
LA	Alle Bibliotheken auflisten, die dem Benutzer zur Verfügung stehen.
LL	Alle Bibliotheken auflisten, mit denen der Benutzer verlinkt ist.
LD	Alle Bibliotheken auflisten, mit denen der Benutzer direkt verlinkt ist.
LG	Alle Bibliotheken auflisten, mit denen der Benutzer über eine Gruppe verlinkt ist.
LP	Alle Bibliotheken auflisten, mit denen der Benutzer über eine privilegierte Gruppe verlinkt ist.
OW	Alle Sicherheitsprofile auflisten, bei denen der Benutzer Eigentümer ist.
DD	Alle DDMs auflisten, die dem Benutzer zur Verfügung stehen (diese Funktion ist auf Großrechnern nicht verfügbar).
DL	Alle DDMs auflisten, die dem Benutzer über einen speziellen Link zur Verfügung stehen (diese Funktion ist nicht unter z/OS verfügbar).
FI	Alle Dateien auflisten, mit denen die private Bibliothek des Benutzers verlinkt ist (diese Funktion ist nur unter z/OS verfügbar).
UT	Alle Dienstprogrammprofile auflisten, die bei dem Benutzer zutreffen.
TD	Zeitdifferenz (**Time Differential**) und Zeitzoneneinstellungen (**Time Zone**) des Sicherheitsprofils des Benutzers abrufen (Retrieve).

Für eine Bibliothek (LI) verfügbare Funktionen:	
Code	**Funktion**
*	Alle Bibliotheken und die privaten Bibliotheken der Benutzer auflisten.
L	Alle Bibliotheken auflisten.
U	Alle privaten Bibliotheken aller Benutzer auflisten.
NI	Bibliothekskennung abrufen (Retrieve), die zu einem bestimmten Bibliotheksnamen gehört.
DD	Alle DDMs auflisten, mit denen die Bibliothek verlinkt ist (diese Funktion ist unter z/OS nicht verfügbar).
LD	Alle DDMs auflisten, mit denen die Bibliothek über einen speziellen Link verlinkt ist (diese Funktion ist unter z/OS nicht verfügbar).
FI	Alle Dateien auflisten, mit denen die Bibliothek verlinkt ist (diese Funktion ist nur unter z/OS verfügbar).
NO	Erlaubte/nicht erlaubte Module auflisten.
SM	Informationen über die Zugriffsrechte der Benutzer auf ein einzelnes Modul in der Bibliothek abrufen (Retrieve).
US	Alle mit der Bibliothek verlinkten Benutzer auflisten.
UT	Alle Dienstprogrammprofile auflisten, die für die Bibliothek zutreffen.
CP	Alle Kommandoprozessoren für die Bibliothek auflisten, die einen bestimmten Status haben.
GL	Alle Bibliothekssicherheitsprofile auflisten, in denen eine FDIC- oder FUSER-Angabe gemacht wird.
GD	Alle Bibliothekssicherheitsprofile auflisten, in denen eine FDIC-Angabe gemacht wird.
GU	Alle Bibliothekprofile auflisten, in denen eine FUSER-Angabe gemacht wird.

Für ein DDM (DD) verfügbare Funktionen:	
Code	**Funktion**
*	Alle definierten DDMs auflisten (d.h. DDMs, für die Sicherheitsprofile existieren).
UN	Alle nicht definierten DDMs auflisten (d. h. DDMs, für die keine Sicherheitsprofile existieren).
DD	Alle definierten und nicht definierten DDMs auflisten.
P	Alle DDMs mit dem externen Status PUBLIC auflisten.
A	Alle DDMs mit dem externen Status ACCESS auflisten.
U	Alle DDMs mit dem externen Status PRIVATE auflisten.
ND	Alle DDM-Sicherheitsprofile auflisten, für die keine entsprechenden DDMs existieren.
LI	Alle Bibliotheken auflisten, die mit dem DDM verknüpft sind.
US	Alle Benutzer auflisten, die mit dem DDM verlinkt sind.
SL	Alle DDM-Definitionen in Special-Link-Sicherheitsprofilen auflisten.
X	Alle DDM-Definitionen in Bibliotheks- und Special-Link-Sicherheitsprofilen auflisten.

Für eine Datei (FI) verfügbare Funktionen:	
Code	**Funktion**
PU	Dateien des Typs PUBLIC auflisten.
AC	Dateien des Typs ACCESS auflisten.
UP	Dateien des Typs PRIVATE auflisten.
DD	Dateien mit vorhandenem DDM auflisten.
ND	Dateien mit nicht vorhandenem DDM auflisten.
UN	Nicht definierte Dateien auflisten.
LI	Bibliotheken auflisten, mit denen die angegebene Datei verlinkt ist.
US	Benutzer auflisten, deren private Bibliotheken mit der angegebenen Datei verlinkt sind.

Für eine Mailbox (MA) verfügbare Funktionen:	
Code	**Funktion**
LI	Alle Bibliotheken auflisten, denen die Mailbox zugewiesen ist.
US	Alle Benutzer auflisten, denen die Mailbox zugewiesen ist.

Für Anmeldefehlersätze (LR = Logon Records) verfügbare Funktionen:	
Code	**Funktion**
P	Anmeldefehlersätze auflisten - in der Reihenfolge der TP-Benutzerkennungen.
T	Anmeldefehlersätze auflisten - in der Reihenfolge der Terminalkennungen.

Für Anmeldesätze (LR = Logon Records) verfügbare Funktionen:	
Code	**Funktion**
L	Anmeldesätze auflisten - in der Reihenfolge der Bibliothekskennungen.
U	Anmeldesätze auflisten - in der Reihenfolge der Benutzerkennungen.
D	Anmeldesätze auflisten - in der Reihenfolge des Anmeldedatums.
LX	Anmeldesätze bei nicht definierten Bibliotheken auflisten - in der Reihenfolge der Bibliothekskennungen.
UX	Anmeldesätze von nicht definierten Benutzern auflisten - in der Reihenfolge der Benutzerkennungen.

Für Steplibs (ST) verfügbare Funktionen:	
Code	**Funktion**
*	Alle Steplibs auflisten.
LK	Geschützte Steplibs auflisten.
NN	Öffentliche (Public) Steplibs auflisten.
SL	Via Special-Link verlinkte Steplibs auflisten.

Für Dienstprogramme (UT) verfügbare Funktionen:	
Code	**Funktion**
LI	Alle bibliotheksspezifischen Dienstprogrammprofile auflisten, die für das Dienstprogramm definiert sind.
US	Alle benutzerspezifischen Dienstprogrammprofile auflisten, die für das Dienstprogramm definiert sind.
UT	Alle für das Dienstprogramm definierten Dienstprogrammprofile auflisten.
leer	Alle Dienstprogrammprofile auflisten, die für alle Dienstprogramme definiert sind.

Für Kommandoprozessoren (CP) verfügbare Funktionen:
Zu einem Kommandoprozessor listet NSCXR alle Bibliotheken und Benutzer für den Kommandoprozessor auf (ohne dass eine SUB-TYPE-Angabe erforderlich ist).

Für Predict-Objekte verfügbare Funktionen (PE, PF, PL, PO):
Für jeden der vier Predict-Objekttypen listet NSCXR alle Objekte dieses Typs auf (ohne dass eine SUB-TYPE-Angabe erforderlich ist).

Für für Systemdateien (SF) verfügbare Funktionen:	
Code	**Funktion**
FN	Alle Bibliotheken der aktuellen FNAT-Systemdatei auflisten, die nicht in Natural Security definiert sind.
FU	Alle Bibliotheken der aktuellen Systemdatei FUSER auflisten, die nicht in Natural Security definiert sind.

Für externe Objekte verfügbare Funktionen:	
Code	**Funktion**
LU	Alle Benutzer auflisten, die mit dem externen Objekt verlinkt sind.

NSCXRIER

Das Subprogramm NSCXRIER wird verwendet, um einzelne Anmeldefehlersätze anzuzeigen (ähnlich wie die **Logon/Countersign Errors**-Funktion **Display individual error records**).

Das Subprogramm NSCXRIER wird wie folgt aufgerufen:

```
CALLNAT 'NSCXRIER' POBJID PPARM PPARM1(*) PRC PNSC-MESSAGE
```

Ein Beispielprogramm PGMXRIER für den Aufruf dieses Programms und ein erläuternder Text TXTXRIER sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung
PGMXRIER	Natural Security-Anmeldefehlersätze auflisten.

NSCXRUSE

Das Subprogramm NSCXRUSE wird in Verbindung mit der auf X gesetzten **Lock User Option** verwendet, um eine Liste der Benutzer zu erhalten, deren Anmeldefehlerzähler größer als 0 ist.

Es wird außerdem in Verbindung mit der allgemeinen Option **Record Each User's Logon Daily** verwendet. Wenn diese Option aktiviert ist, kann NSCXRUSE verwendet werden, um die Kennungen (IDs) der Benutzer anzuzeigen, die sich seit einem bestimmten Datum nicht mehr bei Natural angemeldet haben.

Das Subprogramm NSCXRUSE wird wie folgt aufgerufen:

```
CALLNAT 'NSCXRUSE' POBJ-TYPE POBJ-ID PRC PSUBTYPE PPARM PPARM2(*) PNSC-MESSAGE
```

Ein Beispielprogramm PGMXRUSE für den Aufruf dieses Subprogramms und ein erläuternder Text TXTXRUSE sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Siehe auch das Subprogramm NSC---SP.

Beispielprogramm	Beschreibung	Codes
PGMXRUSE	Eine alphabetisch sortierte Liste der Natural Security-Benutzerprofile erstellen, bei denen der Anmeldefehlerzähler größer als 0 ist.	US

NSCXRUTC

Das Subprogramm NSCXRUTC wird verwendet, um eine Liste aller Dienstprogrammfunktionen zu erhalten, die für einen Benutzer erlaubt sind.

Es wird wie folgt aufgerufen:

```
CALLNAT 'NSCXRUTC' PFUNCTION PUTILITY-ID PUSER PNEXT-VALUE PPARM PPARM-D(*) PRC ↩
PNSC-MSG
```

Ein Beispielprogramm PGMXRUTC für den Aufruf dieses Subprogramms und ein erläuternder Text TXTXRUTC sind in Quellcodeform in der Bibliothek SYSSEC enthalten. Sie enthalten Beschreibungen der einzelnen CALLNAT-Parameter.

Beispielprogramm	Beschreibung	Codes
PGMXRUTC	Eine Liste aller Dienstprogrammfunktionen erstellen, die für einen Benutzer erlaubt sind.	DI

SECNOTE

Das Subprogramm SECNOTE dient zur Anzeige des Sicherheitsvermerkteils eines Sicherheitsprofils. Es kann auf ein Benutzer-, Gruppen-, Bibliotheks- oder Special-Link-Sicherheitsprofil angewendet werden.

Das Objektmodul von SECNOTE ist in der Bibliothek SYSTEM gespeichert. Der Quellcode von SECNOTE steht nicht zur Verfügung.

Das Subprogramm SECNOTE muss mit den folgenden Parametern aufgerufen werden:

Parameter	Beschreibung
PTYPE (A1)	Mit diesem Parameter legen Sie den Typ des Objekts fest, dessen Sicherheitsvermerke (**Security Notes**) gelesen werden sollen. Gültige Werte für PTYPE sind: ■ U = User/Benutzer. Der aktuelle Inhalt der Natural-Systemvariablen *USER bestimmt, welche Sicherheitsvermerke des Benutzers gelesen werden. ■ L = Library/Bibliothek. Der aktuelle Inhalt der Natural-Systemvariablen *APPLIC-ID bestimmt, welche Sicherheitsvermerke der Bibliothek gelesen werden. ■ G = Group/Gruppe. Der aktuelle Inhalt der Natural-Systemvariablen *GROUP bestimmt, welche Sicherheitsvermerke des Benutzers/der Gruppe gelesen werden. ■ S = Special-Link. Der aktuelle Inhalt der Natural-Systemvariablen *GROUP und *APPLIC-ID bestimmt, welche Sicherheitsvermerke des Special-Link gelesen werden.
PNOTES (A60/8)	Bei der Rückkehr von SECNOTE enthält dieser Parameter die Sicherheitsvermerke (**Security Notes**).
PRC (N4)	Dieser Parameter enthält den Rückgabecode von SECNOTE: ■ 0 = Sicherheitshinweise wurden gelesen. ■ 860 = PTYPE enthält einen ungültigen Code. ■ 806 = Bibliothek existiert nicht (ist nicht in Natural Security definiert). ■ 861 = Benutzer hat keinen Special-Link zur Bibliothek. ■ 873 = Benutzer existiert nicht (ist nicht in Natural Security definiert).

Beschreibungen der oben aufgeführten Systemvariablen siehe Natural *System Variables*-Dokumentation.

27 Add-on-Produkte und Plug-ins

- Plug-Ins unter Natural Security 482
- SYSDIC unter Natural Security 483
- SYSAOS unter Natural Security 484

Dieses Kapitel enthält Informationen über den Schutz verschiedener Natural-Add-on-Produkte durch Natural Security und die Handhabung von Plug-Ins in einer Natural Security-Umgebung. Es enthält Informationen über:

Plug-Ins unter Natural Security

Die Benutzeroberfläche von Natural Studio ist durch Plug-Ins erweiterbar. Wenn Plug-Ins in einer durch Natural Security geschützten Umgebung verwendet werden, müssen die folgenden Voraussetzungen erfüllt sein:

Bibliothekssicherheitsprofile für Systembibliotheken

Für den Natural Plug-in Manager (der selbst ein Plug-in ist) und für jedes Plug-in, das verwendet werden soll, muss ein Bibliothekssicherheitsprofil definiert werden. Für Plug-ins, die zusammen mit Natural Studio ausgeliefert werden, gibt es vordefinierte Systembibliotheksprofile. Um diese zu aktivieren, können Sie die Administrator Services-Funktion **Definition of System Libraries** verwenden.

Die folgenden Plug-in-Systembibliotheken werden bereitgestellt:

Bibliothek	Inhalt
SYSEXPLG	Plug-in Example.
SYSPLCGC	Program Generation.
SYSPLMAN	Plug-in Manager.
SYSPLMFE	Mainframe Navigation.
SYSPLNEE	Metrics Calculation / Engineer Xref Viewing.
SYSPLPDC	Object Description.
SYSPLPGC	Schema Generation.
SYSPLWEB	Web Interface.
SYSPLWIZ	Application Wizard.
SYSPLXRC	Xref Evaluation.

Benutzersicherheitsprofile

Wenn ein Benutzer ein Plug-in aktiviert, startet Natural Studio eine zweite Natural-Sitzung mit automatischer Anmeldung (Profilparameter `AUTO=ON`). Damit die automatische Anmeldung erfolgreich ist, muss ein Benutzer, der ein Plug-in verwenden soll, entweder eine Standardbibliothek oder eine private Bibliothek in seinem Sicherheitsprofil angegeben haben.

Natural-Parameterdatei

Wenn ein Benutzer ein Plug-in aktiviert, startet Natural Studio eine zweite Natural-Sitzung unter Verwendung der Parameterdatei `NATPARM`. Wenn die Natural-Sitzung des Benutzers eine andere Parameterdatei als `NATPARM` verwendet, müssen die Systemdateispezifikationen für FNAT, FSEC und FUSER in der `NATPARM`-Parameterdatei mit denen der Parameterdatei übereinstimmen, die von der Benutzersitzung in einer Natural Security-Umgebung verwendet wird.

SYSDIC unter Natural Security

Auf Großrechnern kann die Predict-Bibliothek `SYSDIC` definiert und ihre Verwendung durch Natural Security kontrolliert werden.

Bibliothekssicherheitsprofil für SYSDIC

Um unter Natural Security diejenigen Predict-Funktionen nutzen zu können, die die Möglichkeiten von Adabas Online Services (AOS) nutzen, d.h. um den Natural Security-Schutz zu aktivieren, müssen Sie die folgenden Schritte durchführen:

1. Erstellen Sie ein Sicherheitsprofil für die Bibliothek `SYSDIC` (**Add Library** - Bibliothek anlegen).
2. Definieren Sie die Bibliothek `SYSDIC` als personengeschützt und verlinken Sie mit ihr die Benutzer (oder Benutzergruppen), die Predict/AOS-Administratoren sein sollen.
3. Führen Sie das Programm `NSCPRDAX` in der Bibliothek `SYSSEC` aus. Dieses Programm schreibt den User Exit `NSCPRD01` in das `SYSDIC`-Bibliothekssicherheitsprofil.
4. Rufen Sie die Funktion **Modify Library** für die Bibliothek `SYSDIC` auf. Auch wenn Sie nichts am Sicherheitsprofil ändern, müssen Sie diesen Schritt ausführen, um den Eintrag des User Exits zu bestätigen, da Natural Security die Ausführung von `NSCPRDAX` sonst als illegale Manipulation des `SYSDIC`-Sicherheitsprofils betrachten würde und sich niemand bei `SYSDIC` anmelden könnte.

Nachdem der User Exit in das Sicherheitsprofil geschrieben wurde, sind keine Predict-Funktionen mehr verfügbar, bis Predict-Sicherheitsprofile definiert sind.

Der User Exit kann nicht manuell aus dem `SYSDIC`-Bibliothekssicherheitsprofil entfernt werden. Um ihn zu entfernen, müssen Sie das Programm `NSCPRDDX` in der Bibliothek `SYSSEC` ausführen und dann die Funktion **Modify Library** zur Bestätigung aufrufen (wie bei Schritt 4 oben).

Datenbank-Sicherheitsadministratoren

Wenn Sie in den **Additional Options** des Bibliothekssicherheitsprofils von SYSDIC die Option **User Exit** wählen, wird ein zusätzlicher Bildschirm **Predict/AOS Security Profile** angezeigt. Auf diesem Bildschirm können Sie angeben, wer AOS-Sicherheitsadministrator für welche Datenbank sein soll. Die angegebenen Benutzer (oder Benutzergruppen) dürfen dann die AOS-bezogenen Predict-Funktionen für diese Datenbanken nutzen.

Für jede Datenbank können Sie nur einen AOS-Sicherheitsadministrator angeben. Dies kann ein Benutzer des Typs Administrator, Person, Mitglied (Member) oder eine Gruppe (Group) sein (es muss kein Natural Security-Administrator sein). Der Benutzer muss mit der Bibliothek SYSDIC verlinkt werden, bevor er als AOS-Sicherheitsadministrator angegeben werden kann.

Weitere Informationen zu Predict

Weitere Informationen über Predict und seine AOS-bezogenen Funktionen sowie über Predict unter Natural Security finden Sie in der *Predict*-Dokumentation.

SYSAOS unter Natural Security

Auf Großrechnern kann die Adabas Online Services-Bibliothek **SYSAOS** definiert und ihre Verwendung durch Natural Security gesteuert werden.

Bibliothekssicherheitsprofil für SYSAOS

Um den Bereich Security Maintenance der Adabas Online Services unter Natural Security nutzen zu können, d.h. um den Schutz durch Natural Security für Adabas Online Services zu aktivieren, müssen Sie folgende Schritte durchführen:

1. Erstellen Sie ein Sicherheitsprofil für die Bibliothek SYSAOS (**Add Library** - Bibliothek anlegen).
2. Definieren Sie die Bibliothek SYSAOS als personengeschützt und verlinken Sie mit ihr die Benutzer (oder Benutzergruppen), die Datenbankadministratoren der Adabas Online Services sein sollen.
3. Führen Sie das Programm NSCAOSIX in der Bibliothek SYSSEC aus. Dieses Programm schreibt den User Exit NSCAOSE1 in das SYSAOS-Bibliothekssicherheitsprofil.
4. Rufen Sie die Funktion **Modify Library** für die Bibliothek SYSAOS auf. Auch wenn Sie nichts am Sicherheitsprofil ändern, ist dieser Schritt notwendig, um den Eintrag des User Exits zu bestätigen, da Natural Security sonst die Ausführung von NSCAOSIX als illegale Manipulation des Sicherheitsprofils von SYSAOS betrachten würde und sich niemand bei SYSAOS anmelden könnte.

Nachdem der User Exit in das Sicherheitsprofil geschrieben wurde, sind keine Adabas Online Services-Funktionen mehr verfügbar, bis Adabas Online Services-Sicherheitsprofile definiert sind.

Der User Exit kann nicht manuell aus dem SYSAOS-Bibliotheks-Profil entfernt werden. Um ihn zu entfernen, müssen Sie das Programm NSCAOSDX in der Bibliothek SYSSEC ausführen und anschließend die Funktion **Modify Library** zur Bestätigung aufrufen (wie bei Schritt 4 oben).



Anmerkung: In früheren Versionen von Natural Security wurde der User Exit NSCAOS01 ausgeliefert, der weiterhin anstelle von NSCAOSE1 verwendet werden kann. Mit NSCAOS01 können jedoch nur maximal 72 Datenbankprofile mit Adabas Online Services gepflegt werden, während mit NSCAOSE1 bis zu 400 gepflegt werden können. Im Gegensatz zu NSCAOSE1 ist es bei NSCAOS01 nicht möglich, der Standarddatenbank mehr als eine Benutzergruppe als Administrator zuzuordnen (siehe unten). Das Programm, mit dem Sie NSCAOS01 in das Bibliothekssicherheitsprofil von SYSAOS schreiben, heißt NSXAOSAX. Ansonsten gilt das oben zu NSCAOSE1 Gesagte auch für NSCAOS01.

Datenbank-Sicherheitsadministratoren

Wenn Sie in den zusätzlichen Optionen des Bibliothekssicherheitsprofils von SYSAOS die Option **User Exit** wählen, wird ein zusätzlicher Bildschirm **Adabas Online Services Security Profile** angezeigt. Auf diesem Bildschirm können Sie angeben, wer Adabas Online Services-Sicherheitsadministrator für welche Datenbank sein soll. Die angegebenen Benutzer (oder Benutzergruppen) können dann den Bereich Security Maintenance von Adabas Online Services für diese Datenbanken nutzen.

Für jede Datenbank können Sie nur einen Sicherheitsadministrator für Adabas Online Services angeben. Dabei kann es sich um einen Benutzer des Typs Administrator, Person, Mitglied (Member) oder Gruppe (Group) handeln (es muss kein Natural Security-Administrator sein). Der Benutzer muss mit der Bibliothek SYSAOS verlinkt sein, bevor er als Sicherheitsadministrator für Adabas Online Services angegeben werden kann.

Adabas Online Services verwendet das Datenbankprofil für die Datenbankkennung (DBID) 999 als Standardprofil, das für alle Datenbanken gilt, für die keine individuellen Datenbankprofile definiert sind. Mit dem User Exit NSCAOSE1 können Sie der Datenbank 999 mehrere Gruppen von Adabas Online Services-Sicherheitsadministratoren zuordnen. Dazu geben Sie im SYSAOS-Bibliothekssicherheitsprofil als Administratorkennung für die Datenbank 999 acht Sterne ******** an. Die Administratoren für die Datenbank 999 werden dann über das Datenbankprofil in Adabas Online Services ermittelt. Da Sie in Adabas Online Services mehr als ein Profil pro Datenbank definieren können, können Sie für die Datenbank 999 mehrere Profile mit jeweils unterschiedlichen Administratorengruppen definieren.

Weitere Informationen

Weitere Informationen zu Adabas Online Services finden Sie in der *Adabas*-Dokumentation.

Stichwortverzeichnis

A

Administrator Services, 53
    access, 54
application
    protection, 297
application programming interface
    Natural Security, 449
authentication
    Natural Security, 74
automatic logon, 35

B

batch mode
    Natural Security, 419

C

command processor
    functional security, 410
countersignature, 399
    error, 85

D

DDM
    protection
        on Linux and Windows, 243
        on mainframe, 227
direct command
    Natural Security, 46

E

Eclipse
    protection, 325
environment
    protection, 215
    security profile, 217
        components, 219
external object
    protection, 361

F

FSEC system file
    data transfer, 425
functional security, 409

G

general options
    Natural Security, 55

L

library
    protection, 203
    security profile, 159
        components, 160
        define, 191
        preset values, 119
logon, 29
    automatic, 35
    error, 85
    in batch mode, 420
    procedure, 30
    record, 91
    user exit, 442

M

mailbox, 379
    broadcast message, 380
    ID, 382
    receive message, 381
    security profile
        components, 382
        define, 385

N

Natural Development Server
    protection, 297
Natural RPC
    protection, 339
Natural Security, 6

O

object
    external
        protection, 361
owner, 399

P

PF-keys
    Natural Security, 82
platforms
    Natural Security, 19
plug-in
    under Natural Security, 482
PROFILER utility
    security profile, 287

R

retrieval
    Natural Security, 391
RPC server
    security profile, 347
        components, 348
        define, 352

S

SECLOAD transfer program, 425
SECULD2 transfer program, 425
security
    functional, 409
security profile
    recover, 406
structure
    Natural Security, 5
SYSAOS library
    under Natural Security, 484
SYSBPM utility
    security profile, 287
SYSCP utility
    security profile, 287
SYSDB2 utility
    security profile, 287
SYSDDM utility
    security profile, 287
SYSDIC library
    under Natural Security, 483
SYSERR utility
    security profile, 288
SYSMAIN utility
    security profile, 289
SYSOBJH utility
    security profile, 290
SYSPARM utility
    security profile, 292
SYSPCI utility
    security profile, 293
SYSRPC utility
    security profile, 293

T

terminology
    Natural Security, 5

U

user
    security profile, 129
        components, 130
        define, 142
        preset values, 110
user exit
    Natural Security, 441
user interface
    Natural Security, 39
utility
    protection, 261
    security profile, 263

Z

ZIIP utility
    security profile, 293