

Entire Net-Work Administration

Entire Net-Work Client Installation and Administration

Version 1.4

May 2011

This document applies to Entire Net-Work Administration Version 1.4.

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

Copyright © 2011 Software AG, Darmstadt, Germany and/or Software AG USA, Inc., Reston, VA, United States of America, and/or their licensors.

Detailed information on trademarks and patents owned by Software AG and/or its subsidiaries is located at <http://documentation.softwareag.com/legal/>.

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

This software may include portions of third-party products. For third-party copyright notices and license terms, please refer to "License Texts, Copyright Notices and Disclaimers of Third-Party Products". This document is part of the product documentation, located at <http://documentation.softwareag.com/legal/> and/or in the root installation directory of the licensed product(s).

Table of Contents

1 Entire Net-Work Client Installation and Administration	1
2 Conventions	3
3 Concepts	5
Entire Net-Work Client	6
Directory Server	7
System Management Hub (SMH)	8
SSL Support	9
4 Understanding Partitioning	11
5 Understanding Filtering	13
Filtering in Client Configurations	14
Filtering in Kernel Definitions	14
6 Enhancements	17
Increased Trace Granularity	18
Statistics Integrated into webMethods Optimize for Infrastructure	18
Support for Adabas 28-byte Session ID	18
Adabas Contexts Reestablished after Disconnection	19
Support for 64-bit Adabas	19
Windows Server 2008 Support	19
Simplified Installation	19
License Requirement Changes	19
Coexistence of Entire Net-Work Releases on the Same Machine	20
New Entire Net-Work Command Line Utility	20
New Entire Net-Work Batch Directory Server Utility Functions	20
7 Migration Considerations	21
8 Dropped Features	23
9 Future Plans	25
10 End of Maintenance	27
11 Documentation	29
Allowing Active Content in Windows Environments	30
12 Platform Coverage, Prerequisites, and Restrictions	33
Supported Platforms	34
Space and Memory Requirements	35
Firewall Requirements	35
Prerequisite Software AG Products	35
Browser Requirements	36
Restrictions	36
13 Configuration Considerations	37
14 Installing and Setting Up Software AG Products on UNIX	39
General Information	40
Before Installing Your Software AG Product	41
Installing the Contents of the Installation Medium to Disk	42
15 Installing Entire Net-Work on UNIX in Batch Mode	47
Root Authentication	48

Example	49
16 Installing and Running Entire Net-Work Component Services as System Services on UNIX	51
Prerequisites	52
System Service Installation and Autostarting	52
Manually Starting Entire Net-Work Services	53
Manually Stopping Entire Net-Work Services	54
17 UNIX System Resource Usage Considerations	55
Entire Net-Work Client System Resource Usage	56
Entire Net-Work Kernel System Resource Usage	57
System Management Hub (SMH) System Resource Usage	57
Software AG Directory Server System Resource Usage	57
System Resource Usage Summary Table	58
18 Installing Management Components	59
Software AG Directory Server Installation	60
Entire Net-Work Administration Open Systems Installation	65
Uninstalling Entire Net-Work Administration Open Systems or the Directory Server	69
19 Entire Net-Work Client Installation	73
20 Installation Prerequisites	75
21 Entire Net-Work Client Installation Steps	77
Installing Entire Net-Work Client on Windows Platforms	78
22 Entire Net-Work Client Silent Installation Steps	81
23 Uninstalling Entire Net-Work Client	83
Uninstalling Entire Net-Work Client on Windows	84
24 Required Post-Installation Updates for Simple Connection Line Driver Support	87
25 Configuring Entire Net-Work Components for Windows XP Personal Firewall	89
Allow Ports for a Specific Executable Program	90
Open a Specific Port	190
26 Starting and Stopping Entire Net-Work Client	93
Automatically Starting Entire Net-Work Client	94
Manually Starting Entire Net-Work Client	94
Stopping Entire Net-Work Client	95
27 About the System Management Hub	97
Accessing the System Management Hub	98
Leaving the System Management Hub	99
Using the Refresh Button in the System Management Hub	100
Getting Help	100
28 Entire Net-Work Client Administration	101
29 The Entire Net-Work Client SMH Administration Area	103
30 About Client Configurations	105
31 Listing, Selecting, and Reviewing Client Configurations	107
32 Identifying the Client Configuration to Your Application	111
Specifying the Configuration by Environment Variable	112
Specifying the Configuration in Your Application	112

33	Setting Service Parameters	113
34	Adding Client Configurations	117
35	Deleting Client Configurations	119
36	Maintaining Client Configuration Parameters	121
37	Migrating Entire Net-Work Client 1.3 Configurations	127
38	Controlling Client Access to Databases	129
	Maintaining Adabas Access Definitions	131
	Maintaining Additional Database Access Parameters	136
39	Managing Entire Net-Work Client Log Files	141
	Viewing the Current Entire Net-Work Client Log File	142
	Starting a New Entire Net-Work Client Log File	142
	Specifying the Client Log File Location	143
40	Accessing Secured z/OS Host Resources	145
	Specifying the ESI Method and Appropriate Adabas SAF Security Kernel Parameters	146
	Accessing z/OS Resources Using the ESI Online Application	148
	Accessing z/OS Resources Using the ESI Security Exit	151
41	Using ADALNK User Exits	153
	Specifying the User Exit File and Function Names	154
	Modifying the User Exit Code	156
42	Changing the Software AG Directory Server	159
	Changing the Software AG Directory Server for the Client Machine	160
	Changing the Software AG Directory Server for a Specific Client	161
43	Tracing Entire Net-Work Client Processing	163
	Managing Client Service Tracing	164
	Managing Client Tracing	166
	Managing Software AG Transport Services Tracing	168
	Managing Software AG Communications Tracing	170
44	Entire Net-Work Service Function Utility (wcpadmin)	173
	Syntax	174
	Special Character Use	176
	Examples	176
45	Using the Entire Net-Work User Exit Interface	183
	Writing User Exits	184
	Storing User Exit Library Files	185
	User Exit Processing and Functions in Windows Environments	185
	User Exit Processing and Functions in UNIX Environments	196
46	Port Number Reference	201
	Port Overview and General Assignments	202
	Changing the Software AG Directory Server Port Number	203
47	Directing Log Files to a Shared Server	205
	Step 1. Specify the Log File Locations	206
	Step 2. Configure the Entire Net-Work and Entire Net-Work Client Windows Services	206
48	Entire Net-Work Configuration Parameters	209

Configuration Parameter List	210
Configuration Tools	213
49 Entire Net-Work Directory Server Utility Functions (checkadi and setadi)	217
The checkadi Utility	218
The setadi Utility	219
Index	221

1 Entire Net-Work Client Installation and Administration

The Entire Net-Work Client is a Software AG product option that allows you to access Adabas databases across the network. This documentation is provided for administrators and users of Entire Net-Work Client.

This document is organized as follows:

• <i>Entire Net-Work Client Installation</i>	Describes the installation of Entire Net-Work Client in Windows and UNIX environments.
• <i>Required Post-Installation Updates for Simple Connection Line Driver Support</i>	Describes the required post-installation updates you must make to support the Simple Connection Line Driver.
• <i>Starting and Stopping Entire Net-Work Client</i>	Describes how to start and stop Entire Net-Work Client.
• <i>Entire Net-Work Client Administration</i>	Describes management tasks for Entire Net-Work Client.
• <i>Entire Net-Work Service Function Utility (wcpadmin)</i>	Describes how to use the Entire Net-Work Service Function Utility (wcpadmin) to perform some of the Entire Net-Work service functions in batch mode.
• <i>Using the Entire Net-Work User Exit Interface</i>	Explains the Entire Net-Work user exit interface in open systems.
• <i>Software AG Directory Server Documentation</i>	Describes how to use the Software AG Directory Server.
• <i>Port Number Reference</i>	Describes the ports that are needed by Entire Net-Work to perform its processing and how they can be assigned.
• <i>Directing Log Files to a Shared Server</i>	Describes the process of directing your Entire Net-Work log files to a shared server.
• <i>Entire Net-Work Configuration Parameters</i>	Lists the Entire Net-Work configuration parameters and describes batch and application program tools available for you to set them.

2 Conventions

Notation *vrs* or *vr*: When used in this documentation, the notation *vrs* or *vr* stands for the relevant version, release, and system maintenance level numbers. For further information on product versions, see *version* in the *Glossary*.

3 Concepts

- Entire Net-Work Client 6
- Directory Server 7
- System Management Hub (SMH) 8
- SSL Support 9

Entire Net-Work Client includes its own code as well as making use of a number of other Software AG products to achieve its goals: the Directory Server and the System Management Hub (which installs Software AG's Base Technology Layer).

Once you have installed the Entire Net-Work Client components, you must manually make updates in the System Management Hub to support the Simple Connection Line Driver. For more information, read [Required Post-Installation Updates for Simple Connection Line Driver Support](#), elsewhere in this guide.

Entire Net-Work Client

An Entire Net-Work Client uses the Entire Net-Work 7 e-business message protocol to access Adabas databases. A Kernel does not need to be installed on the same system as a client.

Simply install an Entire Net-Work Client on any machine from which you wish to access Adabas databases. Only one Entire Net-Work Client installation is needed on the machine. Assuming the appropriate Kernels have been defined in your enterprise and the Software AG Directory Server entries have been migrated for Entire Net-Work, your client should be immediately able to access the Adabas databases it needs.

When you install Entire Net-Work Client, its Windows service or UNIX daemon is installed. Using the System Management Hub, you can define multiple client configurations within Entire Net-Work Client. Multiple client configurations allow you to control how clients use your network. Each client configuration can have its own partition, filter, database, trace, user exit, and Directory Server settings. In other words, by directing client requests to particular client configurations, you can control which databases are accessible and what trace and user exit settings are used for the client request. For more information about client configuration parameters, read [About Client Configurations](#) and [Maintaining Client Configuration Parameters](#), elsewhere in this guide. For information about using partitioning and filtering, read [Understanding Partitioning](#) and [Understanding Filtering](#), elsewhere in this guide.

When you receive your Entire Net-Work Client package, it includes installation code for:

- **The System Management Hub (SMH)**
- **The Software AG Directory Server**
- Entire Net-Work Client and the code necessary to maintain it in SMH
- A default client configuration.



Note: If you attempt to install and use Entire Net-Work Client in a system with a firewall in place, be sure that your system administrator has set up the firewall so that the Entire Net-Work Client component applications can access the ports they need (including the Software AG Directory Server port and those Entire Net-Work dynamically assigns during its own processing). For more information about Entire Net-Work ports, read . For inform-

ation about configuring Entire Net-Work components for Windows XP personal firewall, read .

Directory Server

Entire Net-Work uses information stored in a Directory Server to send and receive messages from the client to the database and back. The Directory Server contains an entry for each Kernel and database in the network.



Caution: The Directory Server is critical to the functions of Entire Net-Work 7. It should be on a dedicated system that is operational 24 hours a day, with a UPS. The location of the Directory Server must be specified to the Kernel and clients when they are installed. In addition, the location of the default Directory Server may be defined in the SAGXTSDSHOST entry in the DNS. You may need to consult with your Information Technology department to make updates to the DNS. If no Directory Server can be found for your enterprise, Entire Net-Work cannot function.

All Directory Server data is stored in the form of a Universal Resource Locator (URL) that is familiar to any Internet user. The Directory Server allows complex URLs to contain management data for Entire Net-Work using this standard industry-wide syntax. More importantly, an Entire Net-Work Kernel can dynamically add, modify, or delete client access URLs in the Directory Server.

Entire Net-Work 7 also supports communications using Secure Sockets Layer (SSL) target entries in the Software AG Directory Server. For more information about target entries in the Directory Server, read *Directory Server Target Entries* in the *Software AG Directory Server Administration Guide*. In addition, an SSL Toolkit is provided that allows you to set up a certificate authority that you can use to create security certificates for test purposes only. For more information about the SSL Toolkit, read *Using the SSL Toolkit* in the *Encryption for Entire Net-Work User's Guide*, available from your Software AG support representative.

An Entire Net-Work Client only needs to be able to extract the location of the Adabas database it is trying to access from the Directory Server. Consequently, a single Directory Server URL is required for each database in the enterprise in order for all e-business clients to access that database. If Entire Net-Work partitioning is used, more than one Directory Server entry may exist for a given database. For more information, read [Understanding Partitioning](#), later in this guide.

When operational changes occur for a database (startups, shutdowns, and movement between machines), the Entire Net-Work Kernel automatically maintains the URLs in the Directory Server: it adds a URL to the Directory Server when it discovers a database (and can accept Adabas calls intended for that database); likewise it can remove the same URL when a database becomes unavailable.

At least one Software AG Directory Server should be installed in your enterprise; we recommend that you install only one Directory Server to ensure centralized administration. However, your

enterprise network configuration may require more than one. For example, you may want to install more than one Directory Server to fully direct requests to specific databases. While partitioning can also be used to restrict database access, all entries (in all partitions) of a Directory Server can be maintained via the System Management Hub, so restriction is not complete. If, however, you use multiple System Management Hubs, you can limit what entries are available for viewing in the Directory Server portion of the System Management Hub.

Directory Server administration is performed using the System Management Hub. The Directory Server administration function allows you to populate this directory with entries that identify the address of each target in your network.



Note: If you attempt to install Entire Net-Work in a system with a firewall in place, be sure that your system administrator has opened the firewall for the Software AG Directory Server port or the installation may not complete successfully.

The port number used by the Directory Server can be changed, but must be changed with care. For complete information on changing the Directory Server port used by Entire Net-Work 7 components, read .

System Management Hub (SMH)

The System Management Hub (SMH) provides centralized management of all Software AG products installed in the enterprise, using a Web-based graphical user interface. The use of SMH eliminates the need for a system administrator to visit individual machines or maintain multiple product windows on the desktop. Only one SMH system should be defined for your enterprise.



Caution: SMH should be on a dedicated system that is operational 24 hours a day. If an SMH is not available, you cannot maintain and control Entire Net-Work or the Software AG Directory Server.

SMH is used by Entire Net-Work 7 to manipulate configuration information. Using SMH, you can easily change the URLs stored in the Directory Server without fully understanding the syntax. In addition, the Entire Net-Work Servers and Entire Net-Work Clients can be examined and controlled via SMH. The status of classic nodes and databases for which connections have been defined can be determined. Statistics can be examined and various control functions, such as node disconnection, Kernel shutdown, and trace settings can be performed.

For more information about performing these tasks, read [Entire Net-Work Client Administration](#) in the Entire Net-Work Administration Guide.

SSL Support

Entire Net-Work 7 also supports communications using Secure Sockets Layer (SSL). This support is provided using SSL protocol target entries in the Software AG Directory Server. For more information about target entries in the Directory Server, read *Directory Server Target Entries* in the *Software AG Directory Server Administration Guide*.

In addition, Software AG has an SSL Toolkit you can use, for testing purposes, to set up a certificate authority. You can then use the certificate authority to create security certificates for test purposes only. For more information about the SSL Toolkit, read *Using the SSL Toolkit* in the *Encryption for Entire Net-Work User's Guide*, available from your Software AG support representative.



Note: Due to export restrictions, the SSL Toolkit is not included on the installation CD. If you plan to use SSL in your enterprise and want to use the SSL Toolkit, please contact your Software AG support representative.

4 Understanding Partitioning

Entire Net-Work supports partitioning of Software AG Directory Server entries. Partitioning enhances your ability to use one Directory Server for your whole enterprise, rather than separate Directory Servers for different departments within your enterprise. The partitions each need to be managed separately, but only one Directory Server needs to be installed.

Once you have defined an Entire Net-Work Client or Entire Net-Work Kernel, you can assign it to a specific partition. If you specify one for an Entire Net-Work Kernel, the Directory Server entries created for that Kernel are stored in a partition by that name in the Directory Server configuration or in the Entire Net-Work Kernel configuration file (depending on where the partition is defined); the entries in the partition are maintained separately from the other entries in the appropriate configuration. The Kernel is only able to direct requests to databases, classic Entire Net-Work nodes, and other Kernels that have entries in this partition. Likewise, when you specify a partition name for an Entire Net-Work Client, the client can only direct requests to databases for which there are Directory Server entries in the specified partition.

Here are some of the advantages of partitioning:

- You can use partitioning to direct Entire Net-Work Clients and Kernels to specific databases.
- If you have created Adabas databases with identical database IDs, you can use partitioning to correctly identify which client calls get directed to which Adabas database.
- You can use partitioning to group client calls to an Adabas database, thus reducing the number of actual connections required for that database. This can be especially useful if you are using an Entire Net-Work mainframe product to access a specific Adabas database. It also provides you with some level of client control: if you want to remove access to a specific database for clients in a given partition, simply remove the access URL entry for that database (using the System Management Hub) or stop the Kernel in that partition.
- Using SSL, you can use impose real security requirements on calls made by clients in specific partitions.

For complete information about partitioning, including an example, read *Partitioning a Directory Server* in the *Software AG Directory Server Administration Guide*.

5 Understanding Filtering

- Filtering in Client Configurations 14
- Filtering in Kernel Definitions 14

Entire Net-Work supports filtering of Entire Net-Work Client configurations and Entire Net-Work Kernel definitions by Adabas database ID. In this way, individual Entire Net-Work Client configuration definitions and Entire Net-Work Kernel definitions can apply to only specific databases.

Filtering is set up in the System Management Hub for both client configurations and for Kernels.

Filtering in Client Configurations

For Entire Net-Work Client configurations, database filtering is specified on the **Client Parameters** panel and allows you to identify databases that can be accessed by the client. If no databases are listed in the **ACCEPTED_DBIDS** field, all databases defined in the Software AG Directory Server can be accessed except those listed in the **REJECTED_DBIDS** field. Likewise, if no databases are listed in the **REJECTED_DBIDS** field, all databases in the Directory Server can be accessed, unless a specific list is provided in the **ACCEPTED_DBIDS** field.

For more information on setting these Entire Net-Work Client configuration parameters, read .

Filtering in Kernel Definitions

You can filter Kernels by requests made:

- made to specific Adabas database IDs
- relayed to other Kernels
- submitted from other Kernels, by Kernel name
- submitted to and from specific machines, by machine name
- submitted from other clients, by client name

This section covers the following topics:

- [Filtering Requests to Adabas Databases](#)
- [Filtering Relay Requests to Other Kernels](#)
- [Filtering Requests from Other Kernels](#)
- [Filtering Requests to and from Specific Machines](#)

- [Filtering Requests to and from Specific Clients](#)

Filtering Requests to Adabas Databases

For Entire Net-Work Kernel definitions, database filtering is specified on the **Kernel Filters** panel and allows you to identify databases for which service requests should be processed by the Kernel. If no databases are listed in the **ACCEPTED_DBIDS** field, the Kernel will process all requests to all databases defined in the Software AG Directory Server, except those listed in the **REJECTED_DBIDS** field. Likewise, if no databases are listed in the **REJECTED_DBIDS** field, the Kernel will process all requests to all databases defined in the Software AG Directory Server, unless a specific list is provided in the **ACCEPTED_DBIDS** field.

For more information on setting these Kernel parameters, read *Maintaining Kernel Filters*, in your Entire Net-Work Server documentation.

Filtering Relay Requests to Other Kernels

In the basic Kernel parameters, you can use the **RELAY_TRAFFIC** parameter to restrict whether or not requests *to* other Kernels in the network should be relayed by the Kernel. If the value of the **RELAY_TRAFFIC** field is "YES", requests are relayed to other Kernels; if the value is "NO", they are not.

For more information on setting these Kernel parameters, read *Maintaining Kernel Filters*, in your Entire Net-Work Server documentation.

Filtering Requests from Other Kernels

A combination of Kernel parameters can be used to filter requests to the Kernel:

- In the advanced Kernel parameters, you can use the **UNSOLICITED** parameter to indicate whether or not the Kernel will process service requests *from* other Kernels it has not included in its Kernel filter list. If "YES" is specified, Kernel filtering is ignored and any Kernel can submit service requests to the Kernel. If "NO" is specified, only Kernels included on the Kernel filter list can submit requests to the Kernel; all other unsolicited requests are ignored. The Kernel filter list parameters are governed by the **ACCEPTED_KERNELS** and **REJECTED_KERNELS** parameters.

If the **UNSOLICITED** advanced Kernel parameter is set to "YES", any Kernel can submit service requests to this Kernel, except Kernels listed in the **REJECTED_KERNELS** filter parameter on the Kernel filter list. If the **UNSOLICITED** advanced Kernel parameter is set to "NO", all unsolicited Kernel service requests are ignored, except for the Kernels listed in the **ACCEPTED_KERNELS** filter parameter on the Kernel filter list.

For more information on setting the **UNSOLICITED** parameter, read *Maintaining Kernel Filters*, in your Entire Net-Work Server documentation.

- You can create a Kernel filter list to identify the Kernels from which service requests to the Kernel will be processed. The Kernel filter list is specified using the **ACCEPTED_KERNELS** and **REJECTED_KERNELS** parameters. Using these parameters, you can list Kernel names that should be accepted (service requests from these Kernels will be processed) or rejected (services requests from these Kernels will be rejected).

For complete information on the Kernel filter list and maintaining its parameters, read *Maintaining Kernel Filters*, in your Entire Net-Work Server documentation.

Filtering Requests to and from Specific Machines

You can create a host machine filter list list to identify the host machines from which service requests to the Kernel will be processed and to which the Kernel can send service requests. The host machine filter list is specified using the **ACCEPTED_HOSTS** and **REJECTED_HOSTS** parameters. Using these parameters, you can list machines names that should be accepted (service requests from and to these machines will be processed) or rejected (services requests from and to these machines will be rejected).

For complete information on the host machine filter list and maintaining its parameters, read *Maintaining Kernel Filters*, in your Entire Net-Work Server documentation.

Filtering Requests to and from Specific Clients

You can create a client filter list to identify the Enter Net-Work Clients from which service requests to the Kernel will be processed. The client filter list is specified using the **ACCEPTED_CLIENTS** and **REJECTED_CLIENTS** parameters. Using these parameters, you can list Entire Net-Work Client names that should be accepted (service requests from these clients will be processed) or rejected (services requests from these clients will be rejected).

For complete information on the client filter list and maintaining its parameters, read *Maintaining Kernel Filters*, in your Entire Net-Work Server documentation.

6 Enhancements

- Increased Trace Granularity 18
- Statistics Integrated into webMethods Optimize for Infrastructure 18
- Support for Adabas 28-byte Session ID 18
- Adabas Contexts Reestablished after Disconnection 19
- Support for 64-bit Adabas 19
- Windows Server 2008 Support 19
- Simplified Installation 19
- License Requirement Changes 19
- Coexistence of Entire Net-Work Releases on the Same Machine 20
- New Entire Net-Work Command Line Utility 20
- New Entire Net-Work Batch Directory Server Utility Functions 20

This chapter describes the enhancements that have been made to this release.

Last-minute information on problems that have been addressed by this release are described in the *ReadMe* file.

Increased Trace Granularity

The ability to control the level of the traces you request for Entire Net-Work has been enhanced in this release. More specific tracing options are now available, making it possible for you to increase or decrease the size of the tracing log (and thus making problem analysis more specific and efficient). For complete information, read about Entire Net-Work Client traces, Entire Net-Work Server traces, and Kernel traces at one of the following links:

- *Managing Client Service Tracing and Managing Client Tracing*, in the *Entire Net-Work Client Installation and Administration Guide*
- *Setting the Trace Level for a Server*, in the *Entire Net-Work Server Installation and Administration Guide*
- *Managing Kernel Tracing*, in the *Entire Net-Work Server Installation and Administration Guide*.

Statistics Integrated into webMethods Optimize for Infrastructure

In this release, Entire Net-Work key performance indicator (KPI) statistics are now provided to webMethods Optimize for Infrastructure. Using the Optimize component of webMethods Optimize for Infrastructure, you can monitor the status of these statistics as well as the overall status of your system. This support is available in version 8.2 (and later versions) of webMethods Optimize for Infrastructure.

Support for Adabas 28-byte Session ID

This release supports the Adabas 6.2 expansion of the Adabas session ID from 20 to 28 bytes. The Adabas session ID now includes an eight-byte timestamp that ensures that the session ID is unique.

Adabas Contexts Reestablished after Disconnection

In this release, you no longer need to restart your clients when an Adabas database is shutdown and restarted. Instead, the client contexts to the Adabas database are now reestablished once the database is restarted.

Support for 64-bit Adabas

Support for 64-bit Adabas has been added to this release. This release supports both 32- and 64-bit Adabas.

Windows Server 2008 Support

Windows Server 2008 64-bit support has been added in this release.

Simplified Installation

The installation for Entire Net-Work open systems and its components have been simplified in this release. Separate installations are provided for the Software AG Directory Server, Entire Net-Work Administration Open Systems, Entire Net-Work Server, and Entire Net-Work Client. For more information, read the installation documentation.

License Requirement Changes

With this release, no license is required for Entire Net-Work Client 1.4 installations, although a license is still required for Entire Net-Work Server 7.4.

Coexistence of Entire Net-Work Releases on the Same Machine

The migration between Entire Net-Work 7.3 and 7.4 has been simplified primarily because the two releases can now coexist on the same machine. You can set up and test Entire Net-Work 7.4 on a machine while running 7.3 on the same machine in production.

Likewise, the migration between Entire Net-Work Client 1.3 and 1.4 has been simplified primarily because the two releases can now coexist on the same machine.

New Entire Net-Work Command Line Utility

A new batch utility is provided, `wcadmin`, that allows you to perform some of the Entire Net-Work service functions in batch mode. For complete information, read [.](#)

New Entire Net-Work Batch Directory Server Utility Functions

Two new Entire Net-Work utility functions with focus on the Software AG Directory Server availability and settings are now provided for you to use in batch mode:

- Use the `checkadi` utility function to check for a Directory Server.
- Use the `setadi` utility function to set Directory Server access parameters for Entire Net-Work and Entire Net-Work Client.

For complete information, read [.](#)

7 Migration Considerations

If the Software AG Directory Server is installed and used by a prior version this product, be sure to use the existing Software AG Directory Server port number setting for this installation. You can change the port number after this product is installed. For complete information on changing the Directory Server port number used, read .



Note: You cannot use the System Management Hub (SMH) agents installed with an earlier version of Entire Net-Work Client or Entire Net-Work Server to manage this version of Entire Net-Work Client or Entire Net-Work Server. You must use the SMH agents distributed with this version instead. These agents are installed as part of the Entire Net-Work Administration Open Systems installation.

To migrate from an older version of Entire Net-Work Client to this one, you need only install this newer version. If you want to use your older Entire Net-Work Client configurations in this new version, you must migrate them. For complete information on migrating older Entire Net-Work Client configurations, read .

To migrate from an older version of Entire Net-Work Server to this one, you need only install this newer version. If you want to use your older Entire Net-Work Server Kernel configurations in this new version, you must migrate them. For complete information on migrating older Kernel configurations, read .



Caution: Once a Kernel configuration has been migrated to 7.4, it cannot be migrated back to 7.3. If you really need to do so, contact your Software AG technical support representative for assistance. Once a client configuration has been migrated to 1.4, it cannot be migrated back to 1.3; there is no procedure to do so.

When you install this version of Entire Net-Work Client or Entire Net-Work Server on a Windows system running an older version of the product, the older installation is automatically uninstalled. However, on UNIX systems, the older installation must be removed manually. Once your testing and migration to this new version is complete (and before you attempt to use it in your licensed

production environments), you must uninstall any Entire Net-Work version 2 products you have installed on the same machine.

8 Dropped Features

The following features have been dropped in this release:

- Support has been dropped for Entire Net-Work 2.1 and 2.6. These products are no longer provided by Software AG.
- Support has been dropped for Entire Net-Work 7.2. This product is no longer provided by Software AG. This means that the maintenance and use of Entire Net-Work 7.2 nodes has also been dropped.
- Support for the Windows Vista and Windows 2003 operating systems has been dropped in this release.
- Support for 32-bit Linux environments has also been dropped.

9

Future Plans

Support and documentation for OpenVMS systems is planned.

In a future version, support for the following platforms will be dropped:

- HP-UX on PA-RISC processors
- Windows XP

10

End of Maintenance

For information on how long a product is supported by Software AG, access Software AG's Empower web site at <https://empower.softwareag.com>.

Log into Empower. Once you have logged in, you can expand **Products** in the left menu of the web page and select **Product Version Availability** to access the Product Version Availability application. This application allows you to review support information for specific products and releases.

11 Documentation

- Allowing Active Content in Windows Environments 30

The documentation for this product is new with this release. When additional updated versions of the documentation are created, you can review them by linking to the Software AG documentation web site: <http://documentation.softwareag.com/>. If you have an Empower account, updated and past versions of the documentation can also be reviewed and downloaded by linking to the Software AG Empower web site: <https://empower.softwareag.com>. If you do not have an Empower user ID and password yet, you will find instructions for registering on this site (free for customers with maintenance contracts).

This documentation includes:

- online HTML topics describing all aspects of the product;
- Adobe Acrobat Reader Portable Document Format (PDF) files created from the HTML topics;
- Adobe Acrobat Reader Portable Document Format (PDF) files of appropriate books (guides) created from the HTML topics.

Documentation for the Software AG Directory Server can be found in *Software AG Directory Server Documentation* in the *Software AG Directory Server Administration Guide*.

The System Management Hub documentation can be found in the System Management Hub installation. For example, if SMH is installed in Windows at `C:\Program Files\Software AG\System Management Hub`, then the SMH documentation can be found in: `C:\Program Files\Software AG\System Management Hub\help\doc\overview.htm`. Likewise, in UNIX environments, if the SMH installation is located at `$SAG/common/arg`, then the SMH documentation can be found in `$SAG/common/arg/help/doc/overview.htm`.

No hard-copy documentation is provided, but you can print the PDF and HTML files on your local printer.

Allowing Active Content in Windows Environments

With Service Pack 2 (SP2) for Windows XP and Service Pack 1 (SP1) for Server 2003 and later Windows releases, Microsoft introduced a range of powerful new security features that restrict active content that runs locally on your computer. Active content includes ActiveX controls, Java applets, and JavaScript. Software AG's documentation web pages contain some JavaScript, and the SEARCH, INDEX and CONTENTS capabilities are implemented as Java applets. As a result, when viewing documentation web pages that reside on your PC using Internet Explorer and Mozilla Firefox under Windows XP SP2, note that active content is blocked. You must explicitly and repeatedly allow active content if you want to make use of the documentation's full navigation features. Note that this behavior is only observed when reading web pages installed locally on your PC, including those on CD in the PC's CD-ROM drive.

The active content for which Software AG is responsible, that is, the JavaScript code in our HTML documentation pages, will not harm your computers. The risk in using the navigation applets is negligible: Software AG has received no reports from users concerning any harm caused to a

computer by the applets. We therefore suggest that when reading Software AG documentation in a local context, you should allow active content via the Security settings in the browser (with Internet Explorer, usually found under Tools > Internet Options > Advanced).

Full details of alternatives can be found on the home page of the suppliers of the navigation applets: <http://www.phdcc.com/xpsp2.htm>.

12 Platform Coverage, Prerequisites, and Restrictions

- Supported Platforms 34
- Space and Memory Requirements 35
- Firewall Requirements 35
- Prerequisite Software AG Products 35
- Browser Requirements 36
- Restrictions 36

This chapter describes the supported platforms, space and memory requirements, firewall requirements, prerequisite Software AG products, and restrictions of this release.

Supported Platforms

Software AG generally provides support for the operating system versions supported by their respective manufacturers; when an operating system provider stops supporting a version of an operating system, Software AG will stop supporting that operating system version.

Before attempting to install this product, ensure that your host operating system is at the minimum required level. For information on the platform versions supported by Software AG products, access Software AG's Empower web site at <https://empower.softwareag.com>.

Log into Empower. Once you have logged in, you can expand **Products** in the left menu of the web page and select **Product Version Availability** to access the Product Version Availability application. This application allows you to review the supported platforms and releases for any Software AG product.

Use the fields on this application to filter its results. When you click the **Find** button, a list of the supported Software AG products that meet the filter requirements is shown. You can clear all filter selections using the **Clear** button.



Note: Although it may be technically possible to run a new version of this product on an old operating system, Software AG cannot continue to support operating system versions that are no longer supported by the system's provider. If you have questions about support,

or if you plan to install this product on a release, version, or type of operating system other than those described in the Product Version Availability application as described above, consult Software AG technical support to determine whether support is possible, and under what circumstances.

Space and Memory Requirements

The following minimum space and memory quantities are required for this version of Entire Net-Work:

- On Windows and UNIX systems: 20 MB disk space for the Software AG Directory Server, 25MB disk space for Entire Net-Work Client, and 30 MB disk space for Entire Net-Work (with no log files)

Refer to your System Management Hub (SMH) documentation for an estimate of the space its requires.

- On all operating systems, 128MB or more RAM is required to run the components of this version of Entire Net-Work

Firewall Requirements

If you attempt to install and use Entire Net-Work in a system with a firewall in place, be sure that your system administrator has set up the firewall so that the Entire Net-Work component applications can access the ports they need (including the Software AG Directory Server port and those Entire Net-Work dynamically assigns during its own processing). For more information about Entire Net-Work ports, read [Port Number Reference](#), elsewhere in this guide. For information about configuring Entire Net-Work components for Windows XP personal firewall, read [Configuring Entire Net-Work Components for Windows XP Personal Firewall](#), elsewhere in this guide.

Prerequisite Software AG Products

Adabas 6.1 SP9 or later is a prerequisite for Entire Net-Work Server 7.4. Using older Adabas patch levels or versions may lead to hanging transactions.

Entire Net-Work uses the Software AG Directory Server as well as System Management Hub (SMH), which can be installed from the Entire Net-Work DVD as part of the Entire Net-Work Administration Open Systems installation. In addition, Entire Net-Work Server is used to provide communications with Adabas databases and as a concentrator for non-Adabas servers (such as EntireX Communicator, Tamino, and Adabas SQL Gateway). For information regarding which

releases of these Software AG products are currently supported, refer to the documentation for the appropriate product.



Note: If you attempt to install Entire Net-Work in a system with a firewall in place, be sure that your system administrator has opened the firewall for the Software AG Directory Server port or the installation may not complete successfully.

If the Software AG Directory Server is installed and used by a prior version of Entire Net-Work, be sure to use the existing Software AG Directory Server port number setting for the Entire Net-Work 7.4 installation. You can change the port number after Entire Net-Work 7.4 is installed. For complete information on changing the Directory Server port number used, read .

Browser Requirements

The System Management Hub requires an Internet browser. For information on supported browsers, see the *webMethods System Requirements* on the [Software AG Documentation](#) web site.

Restrictions

The following restrictions exist in Entire Net-Work 7:

- The MHDR protocol is not supported.
- RDA-based calls do not support two-byte database IDs; therefore access is limited to database IDs less than 256. If your application needs to access a mainframe database with an ID greater than 255, you must use Entire Net-Work e-business connections or the TCP/IP protocol with the Entire Net-Work mainframe Simple Connection (TCPX) Line Driver. For more information, read your Entire Net-Work mainframe documentation.

13 Configuration Considerations

Before you install Entire Net-Work, you must decide how you are going to configure it. To assist you in these decisions, the following table provides some questions you should answer for the installation of Entire Net-Work in your enterprise. Corresponding considerations for the questions are also provided.

Category	Question	Considerations
System Management Hub (SMH)	Is SMH already installed in your enterprise?	<p>If SMH is already installed in your enterprise, it should not be installed again. Only one SMH is required to manage all Software AG products that require it.</p> <p>If SMH is not installed in your enterprise, you must install it when you install Entire Net-Work. Read <i>Installing Management Components</i>, elsewhere in this guide, for more information.</p>
System Management Hub and Software AG Directory Server	Should you install Entire Net-Work management components on the same machine as Entire Net-Work clients?	<p>Although you are able to install management components on the same machines as Entire Net-Work clients, Software AG does not recommend it. There are two reasons for this recommendation:</p> <ul style="list-style-type: none"> ■ Your system performance could be impacted. ■ In Windows environments, problems will arise if the Entire Net-Work client service is started before the Directory Server service. The Directory Server service must be started before any Entire Net-Work service. We recommend, therefore, that the Directory Server be installed on a stable machine, separate from Entire Net-Work clients, that is not frequently rebooted.
Software AG Directory Server	Is a Directory Server already installed in your enterprise?	<p>If a Directory Server is already installed in your enterprise, you do not need to install another, although you may if you wish. Read <i>Installing Management Components</i>, elsewhere in this guide, for information on the pros and cons of installing more than one Directory Server.</p>

Category	Question	Considerations
		<p>Note: We recommend that you use only one Directory Server for all Software AG products that require it.</p> <p>If a Directory Server is not installed in your enterprise, you must install one when you install Entire Net-Work. Read <i>Installing Management Components</i>, elsewhere in this guide, for more information.</p>
	Do you want to direct specific Entire Net-Work Clients to specific databases by department or other organizational grouping?	You can create multiple Kernels and use partitioning and filtering in SMH to control which clients and Kernels have access to which databases.
	Do you need or want to change the port number used by Directory Server?	The port number used by the Directory Server can be changed, but must be changed with care. To change the Directory Server port used by Entire Net-Work 7 components, first install the Entire Net-Work 7 components, using the Directory Server port number currently in use. Then follow the instructions provided in to make the port number change.
Partitioning	Do you want to implement partitioning?	Partitioning allows you to direct specific Entire Net-Work Clients to specific databases. Partitions are defined for the Entire Net-Work Clients in the System Management Hub. For more information, read <i>Understanding Partitioning</i> , elsewhere in this guide.

14 Installing and Setting Up Software AG Products on UNIX

- General Information 40
- Before Installing Your Software AG Product 41
- Installing the Contents of the Installation Medium to Disk 42

This document contains general information which applies when installing and setting up any Software AG product on a UNIX platform.

General Information

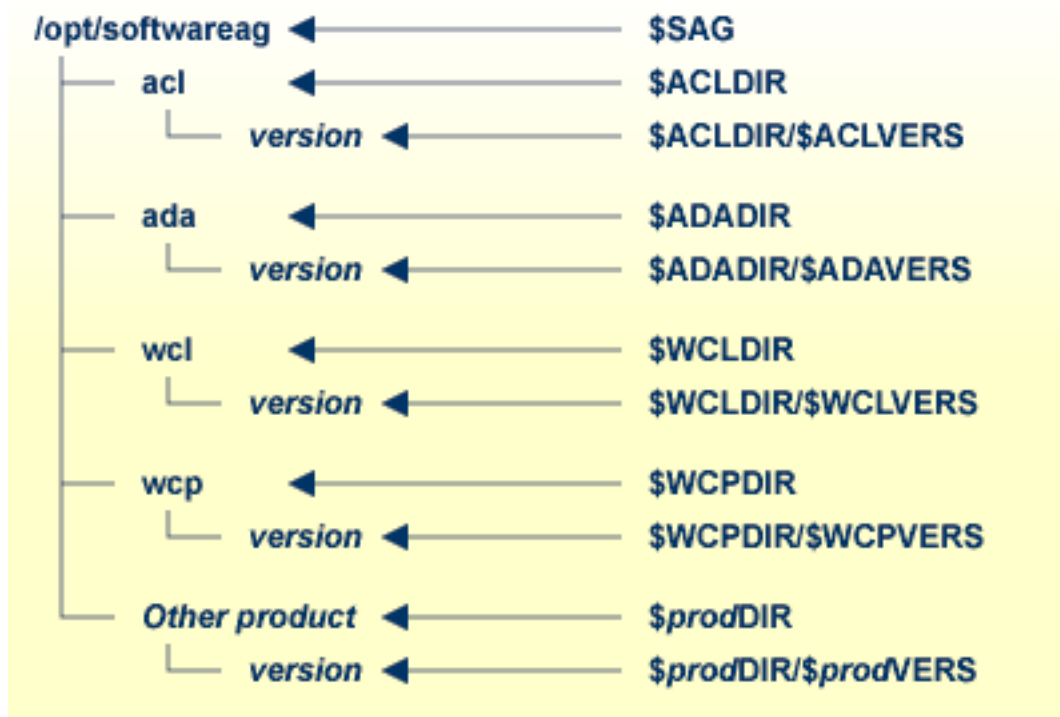
Installation Package

The installation package containing Software AG products is provided on an installation medium conforming to the ISO 9660 standard.

The installation medium contains a complete directory structure which clearly specifies product and platform.

Software AG Environment

The following figure shows the general directory structure generated during installation and the environment variables which reference the specified directories:



Note: Product code files (those that do not change after installation) are stored in the *version* subdirectories. Product data files (those that can change after installation) are stored one level higher up, in the three-character product code directories (such as *ada* or *wcp*).

The environment variable `$SAG` defines the root directory for all Software AG products. It is recommended to define `SAG=/opt/softwareag`.

For each product, the variable `$prodDIR` is set to the path of the main directory of the product specified, where `prod` is a three-letter product code in upper-case letters. For example, all files for Entire Net-Work, whose product code is WCP, are contained in the directory `$WCPDIR`.

The name of the main directory is usually the same as the product code in lower-case letters. For example, the main directory for Entire Net-Work is named `wcp` and the main directory for Entire Net-Work Client is named `wcl`.

Version-independent parts of the product, such as examples or data, are stored in a subdirectory of the product main directory. For example, all Adabas demonstration data is contained in the directory `$ADADIR/adademo`.

Version-dependent components of the product are kept in the version directory `$prodDIR/$prodVERS`. For example, the current versions of Entire Net-Work or Entire Net-Work Client is stored in the directory `$WCPDIR/$WCPVERS`.

The environment variables `prodDIR` and `prodVERS` for all products specified during installation are defined via the file `sagenv.new`. The same applies for any other environment variables needed for the various products.

Before Installing Your Software AG Product

It is recommended that you use `/opt/softwareag` as one common root directory for all of your Software AG products. For Linux systems, this location is the registered name with LANANA.

The default search path for dependent libraries of some Software AG products is `/opt/softwareag`. They are loaded from this location or using the environment variable `$LD_LIBRARY_PATH` (`$SHLIB_PATH` on HP-UX systems). If you install the product to a different location (for example, `/usr/SAG` instead of `/opt/softwareag`), you may create a symbolic link to your `$SAG` directory to get a valid default search path:

```
su
cd /opt
ln -s $SAG softwareag
```

The following activities must be performed if you are installing a Software AG product for the first time, or if your environment is not yet set correctly due to any other causes.

This section covers the following topics:

- [Creating the Administrator's Account and Group](#)

- [Backing Up Your Current Product Version](#)
- [Logging in as User "sag"](#)

Creating the Administrator's Account and Group

You must create one administrator account and one group for all Software AG products when you install your first Software AG product.

1. Define an administrator account to which all of the Software AG products installed at your site belong. Since all environment definition files for the products are written in Bourne shell syntax, the Bourne (or Korn) shell is recommended as the login shell for the administrator account. This section assumes that the administrator account is called "sag".
2. Define a group to which the administrator belongs. This section assumes that this group is also called "sag".
3. Create a login directory for the user "sag" (for example, */opt/softwareag*).
4. Make sure that the group "sag" is defined in the system file */etc/group* and the user "sag" is defined in the system file */etc/passwd*.



Note: To perform these steps, use an appropriate system administration tool.

Backing Up Your Current Product Version

When upgrading a product, it is strongly recommended that you back up your current product version.

Logging in as User "sag"

This description assumes that the user "sag" is the administrator for Software AG products. It is recommended that you log in as the user "sag".

Installing the Contents of the Installation Medium to Disk

Before performing the following steps, make sure that the administrator user and group have been created and defined.

▶ To install the contents of the installation medium to disk

- 1 Load the installation medium and mount it if this is not done automatically.

Command	Description
<code>su - root</code>	To mount an installation medium you may need to be root.
<code>mkdir /mount-dir</code>	You may need to create a mount directory for the installation medium.
<code>mount platform-specific_mount_options device-name /mount-dir</code>	Execute the mount command (see the table below for operating system-specific mount commands).
<code>exit</code>	Return to "sag" user.

Platform-specific mount command and options to mount the installation medium as ISO9660 or High-Sierra file system:

Platform	Mount Command
AIX	<code>/usr/sbin/mount -F cdfs -o cdcase device-name /mount-dir</code>
HP-UX	<code>/usr/sbin/mount -F cdfs -o cdcase device-name /mount-dir</code>
Solaris	<code>/usr/sbin/mount -F hsfs -o ro device-name /mount-dir</code>
Linux	<code>/bin/mount -t iso9660 -o ro device-name /mount-dir</code>

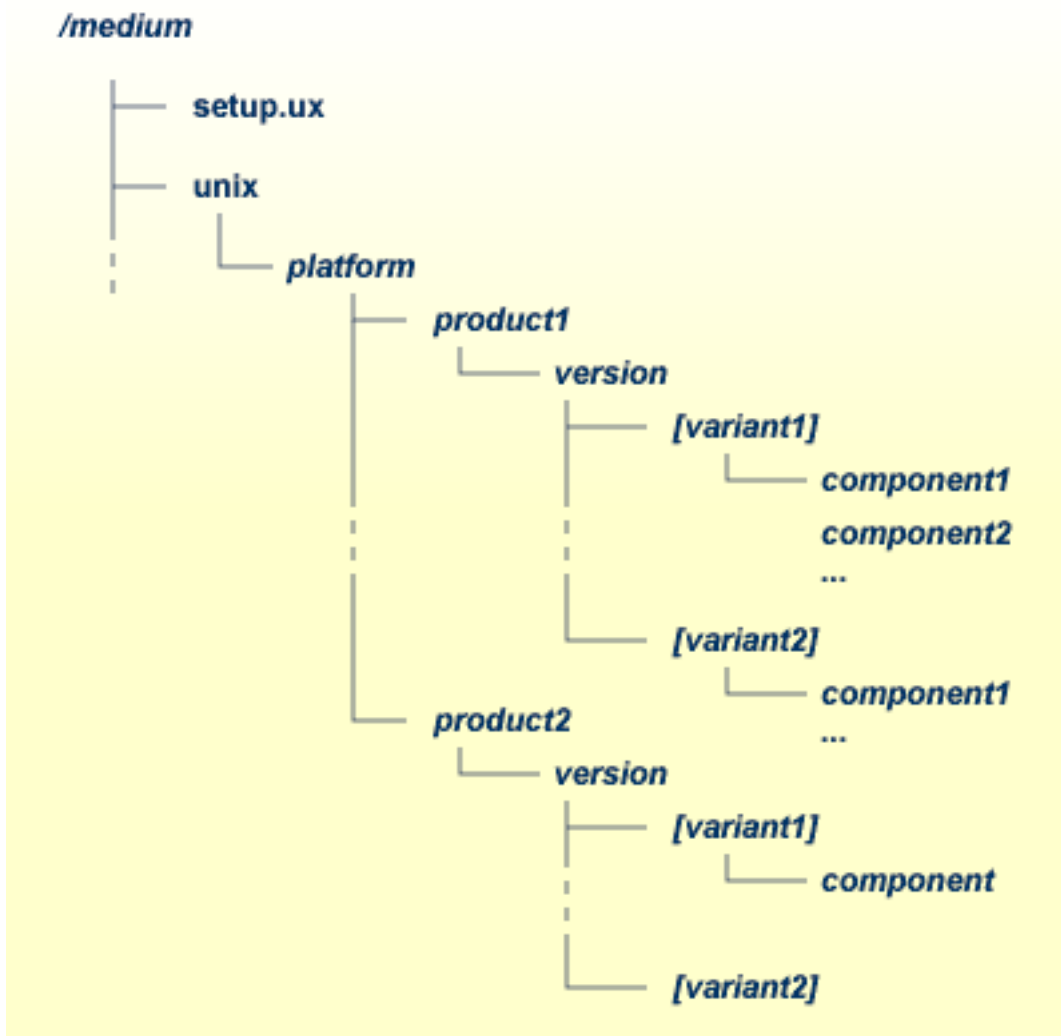


Note: On Solaris, the volume management daemon *vold* might be active. This daemon mounts the installation medium automatically.

Example for Linux:

```
/bin/mount -t iso9660 -o ro /dev/cdrom /mnt
```

- 2 Check the directory structure of the UNIX part of the installation medium. When you run an `ls(1)` command on the installation medium, you will see a structure like the following:



Note: Depending on the mount options used, the files will be all upper case or all lower case. If you mount the installation medium as a pure ISO 9660 Interchange Level I CD, you will also see a version number ;1 appended to all files. Please note this for the following steps and use the correct name format.

- 3 For Linux S/390, a single archive is provided for your convenience (for example, for Entire Net-Work this is the file *WCPv732n.tgz*). The following steps can be performed after you have loaded the installation medium on a Windows or UNIX machine that has a network connection to the Linux S/390 system:
 1. Copy the archive file (*file-name.tgz*) that is located in the root directory of the installation medium to a temporary area such as */tmp/cdrom* in your Linux S/390 environment, using for example ftp in binary mode.
 2. Unpack the archive using the command `tar -xzvf file-name.tgz`.

3. Read the installation instructions for details on how to start the installation from this media in the file *setup.txt* in this directory. Instructions of how to proceed after installing the software will be displayed at the end of the installation and also copied onto your hard disk.

- 4 Please continue reading the step-by-step installation instructions for the Software AG product being installed.

15

Installing Entire Net-Work on UNIX in Batch Mode

- Root Authentication 48
- Example 49

When Entire Net-Work is installed, the log file (*WCPvnnnInst.log*, where *nnn* is the version, release, and maintenance level, is written, and another file, *WCPvnnnInst.sh*, which contains the batch installation settings of this particular installation, is written to *\$SAG/wcp/vnnn/INSTALL*. This file can then subsequently be executed as a shell script. An example is shown elsewhere in this document.



Note: WCB (including Software AG's System Management Hub) must already be installed before you can install Entire Net-Work in batch mode.

If you install the product in character mode, the option `-batch` can be used to execute the installation program without further user interaction. If user input is required, the default values are used; if these values are not appropriate, the correct values have to be set using the corresponding options in the command line. The available command line options can be displayed by calling the installation program with the `-help` option.



Caution: Since the value of *\$SAG* cannot be set using an option, it must already have the correct value in the calling shell.

All prerequisites and parameters are checked for correctness: missing or invalid values will cause the batch installation to terminate.

Root Authentication

Installation programs that require post-installation actions executed as a superuser usually have the following three options:

Variable/Flag Name	Type	Value	Explanation
<code>-user</code>	string	()	User account of SAG user
<code>-password</code>	string	()	Root password (usage not recommended)
<code>-authcmd</code>	choice	(su sudo "")	Command used for authentication

It is possible to specify the superuser password (or the user's password in connection with `-authcmd sudo`), as the value of the `-password` option, but this should not be done, because the password would appear as readable plain text on the screen or, even worse, be stored in the calling shell script, as shown below:

```
# Unsafe method
sh /cdrom/setupux -batch -password secret
```

Instead, we recommend that you start the installation program using `su` or `sudo`, specifying the name of the SAG user (i.e. its own account) as the value of the `-user` option as shown below:

```
# Recommended method
su root -c "sh /cdrom/setup.ux -batch -user sag"
```

Example

Here is an example of a generated batch script for Entire Net-Work that was created during a custom installation. The user is "sag", the `sudo` command was used, and a password was supplied.

```
#!/usr/xpg4/bin/sh
# ----- <Start of generated batch script> -----
# -- <Adapt the following lines until end of generated> --
# ----- < batch script to your needs > -----
# Make sure that the following Internal Products are installed
# below the same $SAG, before the batch is actually started.
# - arg v361 "System Management Hub"
# You will find the batch scripts for the other installations
# in the respective INSTALL/ directories of the products.
#
# You should replace SECRET by the actual password
# or (even better) call this script with superuser privileges.
#
  SAG="/FS/fs0863/sag/products/final_wcp732"; export SAG
  /usr/xpg4/bin/sh /FS/fs0863/sag/product_cd/wcp732_final/setup.ux wcp v732 -batch
-directory a64b \
-user sag \
-authcmd sudo \
-password SECRET \
-sagenv /FS/fs0863/sag/products/final_wcp732/sagenv.new \
-installtype customized \
-license /FS/fs0863/sag/InstDir/wcp73.xml \
-rcname cp732 \
-rcsnum 65 \
-rcknum 35 \
-rcdaemon /FS/fs0863/sag/products/final_wcp732/wcp/v732/wcpservice \
-rctitle "Entire Net-Work Server Service" \
-rcexecute 1 \
-rkdir /etc/init.d \
-rcrunlevels 3 \
-packages "
  Entire Net-Work Server : on
  System Management Hub Agents : on" \
-products "
```

```
acl v6114 : on
wcp v732 : on
wcl v122 : on"
# ----- <End of generated batch script> -----
```


16 Installing and Running Entire Net-Work Component

Services as System Services on UNIX

- Prerequisites 52
- System Service Installation and Autostarting 52
- Manually Starting Entire Net-Work Services 53
- Manually Stopping Entire Net-Work Services 54

During the UNIX installation of the Software AG Directory Server, Entire Net-Work Server, and Entire Net-Work Client components of Entire Net-Work, you are prompted to indicate whether they should be installed as system services (daemons). This chapter describes the behavior and prerequisites for such installations.

Prerequisites

Only a UNIX system administrator with superuser privileges can install the Entire Net-Work component services as system services using the Entire Net-Work installation procedure. If you do not have system administrator superuser privileges while performing the installation (if you enter "none" at the prompt during the installation) and you indicate during the installation that the Entire Net-Work component services should be installed as system services, the Entire Net-Work software is not installed. However, an installation script is generated that can be run by a system administrator with superuser privileges later.

If you do not want the component services autostarted, you can install the Directory Server, Entire Net-Work Server, and Entire Net-Work Client without superuser privileges. Entire Net-Work Administration Open Systems installation always requires superuser privileges.



Note: System Management Hub (SMH) installations require superuser privileges. So, if you are also installing SMH or the Entire Net-Work component SMH agents, you will need to be logged in as a superuser.

System Service Installation and Autostarting

The installation of Entire Net-Work component services occurs when you install the rest of the software using the UNIX installation script. During the installation, you are prompted to indicate whether the component services (daemons) should be installed as system services. If you respond that they should be, the services are installed at the system level and are automatically started upon completion of the installation. Thereafter, they will also be automatically started each time the machine on which they are installed is started. When you request that the services be installed at the system level, you are also requested to specify the run level for the service.

If you specify that the Entire Net-Work component services should *not* be installed as system services, the services are installed, but not at the system level. In this case, the services will never be autostarted after a machine reboot or whenever a machine is started. However, depending on the component being installed, you may be prompted to indicate whether or not the service should be started by the installation. The following table describes:

- the default setting for whether Entire Net-Work component services should start up as system services

- the installation and service startup behavior of Entire Net-Work component services when they are *not* installed as system services:

Component Service	System Service Default Setting	Behavior when <i>not</i> installed as a system service
Directory Server	Yes (start as a system service)	The service is automatically started at the end of the installation. Thereafter, the service will need to be restarted manually each time the machine on which it is installed is started, as described in Manually Starting Entire Net-Work Services , elsewhere in this section.
Entire Net-Work Client	No (do not start as a system service)	A prompt appears asking whether you want the service started at the end of the installation. If you respond "no", the service is not started at the end of the installation; if you respond "yes", the service is started at the end of the installation. Thereafter, the service will need to be restarted manually each time the machine on which it is installed is started, as described in Manually Starting Entire Net-Work Services , elsewhere in this section.
Entire Net-Work Server	Yes (start as a system service)	A prompt appears asking whether you want the service started at the end of the installation. If you respond "no", the service is not started at the end of the installation; if you respond "yes", the service is started at the end of the installation. Thereafter, the service will need to be restarted manually each time the machine on which it is installed is started, as described in Manually Starting Entire Net-Work Services , elsewhere in this section.
Entire Net-Work Administration Open Systems	Yes (start as a system service)	A prompt appears during the installation of the System Management Hub (SMH) asking whether you want the SMH services started at the end of the installation. If you respond "no", the services are not started at the end of the installation; if you respond "yes", the service is started at the end of the installation. Thereafter, the service will need to be restarted manually each time the machine on which it is installed is started, as described in Manually Starting Entire Net-Work Services , elsewhere in this section.

Manually Starting Entire Net-Work Services

If the Entire Net-Work component services are not automatically started after a machine reboot or when a machine is started, you can manually start them using the following UNIX shell scripts:

To manually start the service for:	Use this shell script:
Directory Server	<i>adidmn.sh</i>
Entire Net-Work Client	<i>wclstart.sh</i>
Entire Net-Work Server	<i>wcpstart.sh</i>

For information on manually starting the System Management Hub (SMH) services, refer to your SMH documentation.

Manually Stopping Entire Net-Work Services

To manually stop the Entire Net-Work component services, use the following UNIX shell scripts:

To manually stop the service for:	Use this shell script:
Directory Server	<i>stopadi.sh</i>
Entire Net-Work Client	<i>wclstop.sh</i>
Entire Net-Work Server	<i>wcpstop.sh</i>

For information on manually stopping the System Management Hub (SMH) services, refer to your SMH documentation.

17 UNIX System Resource Usage Considerations

- Entire Net-Work Client System Resource Usage 56
- Entire Net-Work Kernel System Resource Usage 57
- System Management Hub (SMH) System Resource Usage 57
- Software AG Directory Server System Resource Usage 57
- System Resource Usage Summary Table 58

The Entire Net-Work service, Kernels, and clients use UNIX resources. This chapter describes the use of TCP/IP sockets, threads, and semaphores by the various Entire Net-Work components in UNIX environments.

Entire Net-Work system resources are allocated dynamically, as they are needed, not when the products are started. However, you may encounter times when Kernels are so heavily used that they cannot accept new connections, incoming clients, or System Management Hub (SMH) inquiries. This can also happen when other applications on your system are used heavily.

UNIX systems are sometimes configured with specific platform resource defaults. You must take into consideration how many resources the individual applications require and configure their systems accordingly. Bear in mind:

- Sockets that are not closed properly (for example, when applications crash) may linger in the system for a while and are not available for some time. We recommend that you set the socket linger time to a lower value.
- Consider the system resources required when a client application, the Software AG Directory Server, SMH, and Kernels run on the same system at the same time as other applications you have installed. You may find it beneficial to run them on separate systems.

This chapter provides information on Entire Net-Work component resource usage to help you do this:

Entire Net-Work Client System Resource Usage

A simple client uses the following system resources:

- Three semaphores and one thread are used for data protection.
- One thread, semaphore, and socket are required for each connection made by the client.
- If the client needs to retrieve Adabas access information from the Software AG Directory Server, another thread, semaphore, and socket are required temporarily. These are freed immediately after the information is obtained.

Bear in mind that some client applications are complex and may require multiple connections.

Entire Net-Work Kernel System Resource Usage

Entire Net-Work Kernels use the following system resources:

- Fourteen semaphores and seven threads are used for data protection. If the gateway thread count is increased from its default of five, the number of threads required for Kernel data protection is increased accordingly.
- Each access (e-business, e-business client, classic Entire Net-Work, and SMH) performed by the Kernel requires a thread, semaphore, and socket.
- Each incoming or outgoing connection (e-business and classic Entire Net-Work) performed by the Kernel requires a thread, semaphore, and socket, during the life of the connection.
- Each incoming client requires a thread, semaphore, and socket during the life of the client.
- If the Kernel needs to retrieve network information from the Software AG Directory Server, another thread, semaphore, and socket are required temporarily. These are freed immediately after the information is obtained.

System Management Hub (SMH) System Resource Usage

If SMH needs to retrieve Kernel information from the Software AG Directory Server, another thread, semaphore, and socket are required temporarily. These are freed immediately after the information is obtained.

Software AG Directory Server System Resource Usage

Software AG Directory Server clients use the following system resources:

- Six semaphores, a socket, and two threads are needed for Directory Server processing.
- Directory Server allocates a semaphore, socket, and two threads for each incoming connection, for the life of the connection.

System Resource Usage Summary Table

The following table summarizes use of system resources by the various Entire Net-Work components.

Component	System Resource Requirements			Duration of Requirement
	Sockets	Threads	Semaphores	
Client data protection	0	1	3	Life of the client.
Client connection (each connection)	1	1	1	Life of the client.
Client retrieval of Adabas access information from the Directory Server	1	1	1	Temporarily; resources freed after information is retrieved.
Kernel data protection	0	7	14	Life of the Kernel.
Kernel access (e-business, e-business client, classic Entire Net-Work, and SMH)	1	1	1	Life of the access attempt.
Kernel incoming and outgoing connection (e-business and classic Entire Net-Work)	1	1	1	Life of the connection.
Kernel incoming client	1	1	1	Life of the client.
Kernel retrieval of network information from the Directory Server	1	1	1	Temporarily; resources freed after information is retrieved.
SMH retrieval of Kernel information from the Directory Server	1	1	1	Temporarily; resources freed after information is retrieved.
Directory Server base processing	1	2	6	Life of Directory Server.
Directory Server incoming connection handling	1	2	1	Life of the connection.
Total	9	19	31	---

18

Installing Management Components

- Software AG Directory Server Installation 60
- Entire Net-Work Administration Open Systems Installation 65
- Uninstalling Entire Net-Work Administration Open Systems or the Directory Server 69

The management components used by Entire Net-Work 7 are the Entire Net-Work Administration Open Systems and the Software AG Directory Server. These components:

- Must be installed on a machine in your network that can be accessed by all machines where Entire Net-Work will be installed (both Entire Net-Work Server and Entire Net-Work Client). They should be installed on a dedicated system that is operational 24 hours a day, with a UPS.
- Can be installed together on the same machine or individually on separate machines. To reduce resource consumption, Software AG recommends that you install them on the same machine.

Once these management components are installed, you should not need to configure them much for Entire Net-Work. The defaults supplied in the Entire Net-Work installations of these components should work for most organizations. This is especially true of the Directory Server settings in SMH.

Once the appropriate management components, servers, and clients are installed and appropriate Kernels are defined, we recommend that you try to use Entire Net-Work in a test environment prior to attempting to configure it further.

Software AG Directory Server Installation

One or more Directory Servers can be installed in your enterprise although Software AG recommends that you use only one Directory Server in your enterprise. However, if you elect to install more than one, remember:

- You will have to manage and administer multiple Directory Server configurations.
- You will need to be very careful about which Directory Server you select to use in your installations of Entire Net-Work Client, Entire Net-Work Server, and Entire Net-Work Administration Open Systems -- especially if other Directory Servers have been installed by other Software AG products.
- As you are restricted to a single pointer to a Directory Server in your DNS (via its SAGXTSDSHOST and SAGXTSDSPORT entries), all systems required to use a different Directory Server must be redirected using local, manual, administration. For more information on this manual administration, contact your Software AG technical support representative.

Software AG has registered port number 4952 with the Internet Assigned Numbers Authority (IANA) for use by the Software AG Directory Server. You are not required to use this port number for the Directory Server and can change it. For complete information on the port used by the Directory Server, read *The Directory Server Port Number*, in the *Software AG Directory Server Administration Guide*.

To verify the existence of the Software AG Directory Server, check with your system administrator.

If SMH has already been installed in your enterprise, you still need to run the Entire Net-Work Administration Open Systems installation supplied with the Software AG Directory Server install-

ation code. This Entire Net-Work Administration Open Systems installation for Directory Server should be run on the machine where SMH is installed. This will ensure that the Software AG Directory Server SMH agents get installed properly.

This section covers the following topics:

- [Installing Software AG Directory Server on Windows Platforms](#)
- [Installing Software AG Directory Server on UNIX Platforms](#)

Installing Software AG Directory Server on Windows Platforms

This section describes how to install Software AG Directory Server on Windows systems. .

► To install a Software AG Directory Server on Windows:

- 1 Insert the Entire Net-Work installation CD into your CD-ROM drive.

The following executable files can be found on the CD:

Executable File Name	Use to Install Component	Description
<i>ADISETUP.EXE</i>	Software AG Directory Server	Run this executable file to install the Software AG Directory Server. Entire Net-Work requires that the Directory Server be available to the installation or that it be installed as part of the installation. If the Directory Server has already been installed in your enterprise, you do not need to install it again -- although multiple installations of the Directory Server in the enterprise are allowed. If you elect to install the Software AG Directory Server, its installation must occur before any other components you might also select to install.
<i>WCPSETUP.EXE</i>	Entire Net-Work Server	Run this executable file to install Entire Net-Work Server.
<i>WCLSETUP.EXE</i>	Entire Net-Work Client	Run this executable file to install Entire Net-Work Client. The installation of Entire Net-Work Client always includes the installation of the Adabas Client software.
<i>WCBSETUP.EXE</i>	Entire Net-Work Administration Open Systems	Run this executable file to install the System Management Hub (SMH) as well as all the agents necessary to perform Directory Server maintenance. If SMH is already installed in your enterprise, it should not be installed again. Only one SMH is required to manage all Software AG products that require it. However, you should run this installation on the machine on which SMH is installed to

Executable File Name	Use to Install Component	Description
		<p>ensure that the Software AG Directory Server agents required for SMH are installed.</p> <p>Note: Installation of Entire Net-Work Administration Open Systems components requires superuser privileges.</p> <p>For more information about installing and using the Entire Net-Work management components, see Entire Net-Work Administration Open Systems Installation.</p>

- 2 Locate and run the appropriate executable file on the CD-ROM. If you only want to install Software AG Directory Server, only run *ADISETUP.EXE*.

The Welcome panel appears.

- 3 Follow the prompts on the installation panels. The following AG panels should be noted:
 - On the Choose Destination panel, use the **Browse** button to search for and identify the location where the Directory Server should be installed.
 - When the **Directory Server Port Assignment** panel appears, specify the port number of the Directory Server that should be used for this installation. For complete information on the port used by the Directory Server, read *The Directory Server Port Number*, in the *Software AG Directory Server Administration Guide*.

If the installation is not successful, you will receive one of several possible error messages. Contact your local distributor for information about customer support services. If the installation fails, it is likely that some parts of the product will have been installed. Therefore, before you attempt to install Entire Net-Work Server again, run the installation program to remove it. See [Uninstalling Entire Net-Work Administration Open Systems or the Directory Server](#), elsewhere in this guide, for instructions on removing the product.

Installing Software AG Directory Server on UNIX Platforms

This section describes how to install Software AG Directory Server on UNIX systems.

▶ To install a Software AG Directory Server on UNIX:

Shut down all open applications, especially those applications interacting with or depending on your Adabas databases. This includes Natural, the Adabas DBA Workbench, and prior releases of Entire Net-Work.

- 1 Mount the Entire Net-Work CD as described in .
- 2 Run the setup.ux command:

```
sh <cd mount dir>/setup.ux
```

where `<cd mount dir>` is the directory where the CD is mounted.

The **Welcome** panel appears.

- 3 Follow the prompts on the installation panels. The following panels should be noted:
 - Some of the installation steps must be performed as superuser. Specifically, if you want to elect to run the Entire Net-Work Server service as a system service (one of the installation panels will ask you this), you must have superuser privileges.
 - On the **Destination Location** panel, you can change the \$SAG environment variable, which identifies where your Software AG products are installed.
 - When you get to the **SAG Environment Shell** panel, verify the path and file name of the SAG environment file. The default name is *sagenv.new*. If you would like to change it, type the fully qualified name of the Software AG environment file you want used for this installation, or click the **Browse** button to locate an existing file.
 - When you get to the **Choose Programs** panel, you have the option to install four Entire Net-Work components, as described in the table below. If you only want to install Software AG Directory Server, select only "Software AG Directory Server".

Component Name	Description
Software AG Directory Server	Select this option to install the Software AG Directory Server. Entire Net-Work requires that the Directory Server be available to the installation or that it be installed as part of the installation. If the Directory Server has already been installed in your enterprise, you do not need to install it again -- although multiple installations of the Directory Server in the enterprise are allowed. If you elect to install the Software AG Directory Server, its installation must occur before any other components you might also select to install.
Entire Net-Work Server	Select this option to install Entire Net-Work Server.
Entire Net-Work Client	Select this option to install Entire Net-Work Client. The installation of Entire Net-Work Client always includes the installation of the Adabas Client software.
Entire Net-Work Administration Open Systems	Select this option to install the System Management Hub (SMH) as well as all the agents necessary to perform Directory Server maintenance. If SMH is already installed in your enterprise, it should not be installed again. Only one SMH is required to manage all Software AG products that require it. However, you should run this installation on the machine on which SMH is installed to ensure that the Software AG Directory Server agents required for SMH are installed.

Component Name	Description
	<p>Note: Installation of Entire Net-Work Administration Open Systems components requires superuser privileges.</p> <p>For more information about installing and using the Entire Net-Work management components, see Entire Net-Work Administration Open Systems Installation.</p>

- You will be prompted for the port number to use for this Directory Server installation. For complete information on the port used by the Directory Server, read *The Directory Server Port Number*, in the *Software AG Directory Server Administration Guide*.
- During the course of the installation, a panel appears prompting you to indicate whether you want the Directory Server service installed as a system service. For complete information about installing Entire Net-Work component services as system services, read [Installing and Running Entire Net-Work Component Services as System Services on UNIX](#), elsewhere in this guide.

If you do not elect to run the Directory Server service as a system service, a window will appear asking you whether the Directory Server service should be started automatically by the installation.

- We recommend that you read the post-installation README file. Click **Finish** when you done reading the file.

The installation of Software AG Directory Server is complete. However, its environment is not yet activated.

- 4 After all the Entire Net-Work components you selected on the **Choose Programs** panel have been installed and when you click **Finish** on the Readme panel for the last one, the Activate Installed Products panel appears. Select all the products listed on the panel. The Software AG environment file is called, by default, *sagenv.new* and is created for the list of products you select.

When finished with the Activate Installed Products panel, click **Next** and the full installation of the product completes. You must then activate the environment for the Software AG products you selected in the Software AG environment file. To do this, change to the installation directory and run *sagenv.new*:

```
. sagenv.new
```

The installation and deployment of the Software AG Directory Server in UNIX is complete.

Entire Net-Work Administration Open Systems Installation

Only one System Management Hub (SMH) should be installed in your enterprise. It can be used to manage all Software AG products that use it.

If SMH has already been installed in your enterprise, you still need to run the Entire Net-Work Administration Open Systems installation supplied with the Directory Server, Entire Net-Work Client and Entire Net-Work Server installations on the machine where SMH is installed to ensure that the Directory Server, Entire Net-Work Client or Entire Net-Work Server SMH agents get installed.

The use of an X-terminal or suitable software emulator is recommended for a UNIX installation of SMH. This way, if SMH is installed on a UNIX system, it can be accessed from any suitable Web browser on both Windows or UNIX systems. Software AG does not recommend a particular Web Browser for UNIX use.



Notes:

1. When installing SMH, other Software AG internal components may also be installed (if they have not already been installed by another Software AG product). SMH cannot run without these internal products.

This section covers the following topics:

- [Installing Entire Net-Work Administration Open Systems on Windows Platforms](#)
- [Installing Entire Net-Work Server on UNIX Platforms](#)

Installing Entire Net-Work Administration Open Systems on Windows Platforms

This section describes how to install Entire Net-Work Administration Open Systems on Windows systems.

▶ To install an Entire Net-Work Administration Open Systems on Windows:

- 1 Insert the Entire Net-Work installation CD into your CD-ROM drive.

The following executable files can be found on the CD:

Executable File Name	Use to Install Component	Description
<i>ADISETUP.EXE</i>	Software AG Directory Server	<p>Run this executable to install the Software AG Directory Server. Entire Net-Work requires that the Directory Server be available to the installation or that it be installed as part of the installation.</p> <p>If the Directory Server has already been installed in your enterprise, you do not need to install it again -- although multiple installations of the Directory Server in the enterprise are allowed (for more details, read <i>Software AG Directory Server Installation</i>).</p> <p>If you elect to install the Software AG Directory Server, its installation must occur before any other components you might also select to install.</p>
<i>WCPSETUP.EXE</i>	Entire Net-Work Server	Run this executable to install Entire Net-Work Server.
<i>WCLSETUP.EXE</i>	Entire Net-Work Client	<p>Run this executable to install Entire Net-Work Client.</p> <p>The installation of Entire Net-Work Client always includes the installation of the Adabas Client software.</p>
<i>WCBSETUP.EXE</i>	Entire Net-Work Administration Open Systems	<p>Run this executable to install the System Management Hub (SMH) as well as all the agents necessary to perform Entire Net-Work maintenance.</p> <p>If SMH is already installed in your enterprise, it should not be installed again. Only one SMH is required to manage all Software AG products that require it. However, you should run this installation on the machine on which SMH is installed to ensure that the Entire Net-Work agents required for SMH are installed.</p> <p>Note: Installation of Entire Net-Work Administration Open Systems components requires superuser privileges.</p>

- 2 Locate and run the appropriate executable file on the CD-ROM. If you only want to install Entire Net-Work Administration Open Systems, only run *WCBSETUP.EXE*.

The Welcome panel appears.

- 3 Follow the prompts on the installation panels. The following panels should be noted:
 - On the Installation Instructions panel, read the installation instructions and click **Yes** to continue. If you click **No**, the installation will stop.
 - On the License Agreement panel, read the installation instructions and click **Yes** to accept the license agreement and continue. If you click **No**, the installation will stop.

- When the **Directory Server Access** panel appears, specify the host name (or IP address) and port number of the Directory Server that should be used by this installation. For complete information on the port used by the Directory Server, read *The Directory Server Port Number*, in the *Software AG Directory Server Administration Guide*.

If the installation is not successful, you will receive one of several possible error messages. Contact your local distributor for information about customer support services. If the installation fails, it is likely that some parts of the product will have been installed. Therefore, before you attempt to install Entire Net-Work Server again, run the installation program to remove it. See [Uninstalling Entire Net-Work Administration Open Systems or the Directory Server](#), elsewhere in this guide, for instructions on removing the product.

Installing Entire Net-Work Server on UNIX Platforms

This section describes how to install Entire Net-Work Administration Open Systems on UNIX systems.

▶ To install an Entire Net-Work Administration Open Systems on UNIX:

Shut down all open applications, especially those applications interacting with or depending on your Adabas databases. This includes Natural, the Adabas DBA Workbench, and prior releases of Entire Net-Work.

- 1 Mount the Entire Net-Work CD as described in .
- 2 Run the `setup.ux` command:

```
sh <cd mount dir>/setup.ux
```

where `<cd mount dir>` is the directory where the CD is mounted.

The **Welcome** panel appears.

- 3 Follow the prompts on the installation panels. The following panels should be noted:
 - Some of the installation steps must be performed as superuser. Specifically, if you want to elect to run the Entire Net-Work Server service as a system service (one of the installation panels will ask you this), you must have superuser privileges.
 - On the **Destination Location** panel, you can change the `$SAG` environment variable, which identifies where your Software AG products are installed.
 - When you get to the **SAG Environment Shell** panel, verify the path and file name of the SAG environment file. The default name is `sagenv.new`. If you would like to change it, type the fully qualified name of the Software AG environment file you want used for this installation, or click the **Browse** button to locate an existing file.

- When you get to the **Choose Programs** panel, you have the option to install four Entire Net-Work components, as described in the table below. If you only want to install Entire Net-Work Administration Open Systems, select only "Entire Net-Work Administration Open Systems".

Component Name	Description
Software AG Directory Server	<p>Select this option to install the Software AG Directory Server. Entire Net-Work requires that the Directory Server be available to the installation or that it be installed as part of the installation.</p> <p>If the Directory Server has already been installed in your enterprise, you do not need to install it again -- although multiple installations of the Directory Server in the enterprise are allowed (for more details, read Software AG Directory Server Installation).</p> <p>If you elect to install the Software AG Directory Server, its installation must occur before any other components you might also select to install.</p>
Entire Net-Work Server	Select this option to install Entire Net-Work Server.
Entire Net-Work Client	<p>Select this option to install Entire Net-Work Client.</p> <p>The installation of Entire Net-Work Client always includes the installation of the Adabas Client software.</p>
Entire Net-Work Administration Open Systems	<p>Select this option to install the System Management Hub (SMH) as well as all the agents necessary to perform Entire Net-Work maintenance.</p> <p>If SMH is already installed in your enterprise, it should not be installed again. Only one SMH is required to manage all Software AG products that require it. However, you should run this installation on the machine on which SMH is installed to ensure that the Entire Net-Work agents required for SMH are installed.</p> <p>Note: Installation of Entire Net-Work Administration Open Systems components requires superuser privileges.</p>

- The **Directory Server Access** panel will appear requesting the location of the Directory Server you want used with this Entire Net-Work Administration Open Systems installation. For complete information on the port used by the Directory Server, read *The Directory Server Port Number*, in the *Software AG Directory Server Administration Guide*.
- We recommend that you read the post-installation README file. Click **Finish** when you done reading the file.

The installation of Entire Net-Work Administration Open Systems is complete. However, its environment is not yet activated.

- 4 After all the Entire Net-Work components you selected on the **Choose Programs** panel have been installed and when you click **Finish** on the Readme panel for the last one, the Activate Installed Products panel appears. Select all the products listed on the panel. The Software AG

environment file is called, by default, *sagenv.new* and is created for the list of products you select.

When finished with the Activate Installed Products panel, click **Next** and the full installation of the product completes. You must then activate the environment for the Software AG products you selected in the Software AG environment file. To do this, change to the installation directory and run *sagenv.new*:

```
. sagenv.new
```

The installation and deployment of the Entire Net-Work Administration Open Systems in UNIX is complete.

Uninstalling Entire Net-Work Administration Open Systems or the Directory Server

This section describes the uninstallation of Entire Net-Work Administration Open Systems and the Directory Server on each of the platforms on which it is supported.

- [Uninstalling Entire Net-Work Administration Open Systems or Directory Server on Windows](#)
- [Uninstalling Entire Net-Work Administration Open Systems or Directory Server on UNIX](#)

Uninstalling Entire Net-Work Administration Open Systems or Directory Server on Windows

This section describes how to uninstall Entire Net-Work Administration Open Systems or Directory Server on Windows.



Notes:

1. Uninstalling will not remove any files that were not originally installed by the Entire Net-Work Administration Open Systems or Directory Server installation tools. For example, files modified, expanded, moved, or introduced after installation must be removed manually.
2. Uninstalling will stop Entire Net-Work Administration Open Systems or Directory Server.

▶ To uninstall Entire Net-Work Administration Open Systems or the Software AG Directory Server on Windows:

- 1 If you are uninstalling the Software AG Directory Server, stop the Directory Server service before you start these steps. This uninstallation procedure will uninstall the service, but it cannot do so if the service is running. If you do not uninstall the service (or if its uninstallation fails) and you try to reinstall Directory Server later, errors will occur when you try to use your new Directory Server installation.
- 2 Go to the Control Panel.

3 In Windows XP environments, select **Add/Remove Programs**.

In Windows 7 environments, select **Uninstall or Change a Program**.

4 To uninstall Entire Net-Work Administration Open Systems, locate **Software AG Entire Net-Work Administration Open Systems v.r.m** (where *v.r.m* are the version, release, and modification levels of the Entire Net-Work Administration Open Systems code). Then:

- In Windows XP environments, click on the associated **Change/Remove** button.
- In Windows 7 environments, double-click on **Software AG Entire Net-Work Administration Open Systems v.r.m**.

To uninstall the Software AG Directory Server, locate **Software AG Directory Server**. Then:

- In Windows XP environments, click on the associated **Change/Remove** button.
- In Windows 7 environments, double-click on **Software AG Directory Server**.

The InstallShield Wizard is invoked.

5 in Windows XP environments, select **Remove** on the **Welcome** panel and click **Next**. Click **OK** for any verification messages.

In Windows 7 environments, click **OK** to start the uninstallation.

The **Setup Status** panel appears on which you can watch the progress of the uninstallation.

6 When the uninstallation has completed, the Finish panel appears. Click **Finish** to end the uninstallation.

Alternatively, when you try to install this version of the product, the InstallShield automatically detects whether another version is already installed and prompts you to remove it.

Uninstalling Entire Net-Work Administration Open Systems or Directory Server on UNIX

The Entire Net-Work Administration Open Systems or Directory Server uninstallation process will not remove any files that were not originally installed by the Entire Net-Work Administration Open Systems or Directory Server installation tools.

▶ To uninstall Software AG software on UNIX:

1 Enter `sagrm` on the command line.



Note: The executable `sagrm` file resides in the `$SAG/common/bin` directory. Ensure that this path is included in the PATH environment variable.

The Software AG deinstallation GUI is started and the **Product Selection** panel appears.

- 2 On the **Product Selection** panel, select the Software AG products in this environment that you want to uninstall. To select a product, click on the check box to the left of the product name until a check appears in the box.

When all products have been selected, click **Next**.

A subpanel appears allowing you to select specific component packages of the product you selected in **Step 1** to be uninstalled.

- 3 Select the component packages you want installed. To select a package, click on the check box to the left of the component package name until a check appears in the box.

Click **Next** when all appropriate component packages have been selected.

The component packages and products are uninstalled.

19

Entire Net-Work Client Installation

This chapter describes the installation of Entire Net-Work Client. It is organized as follows:

•	<i>Installation Prerequisites</i>	Describes the prerequisites you should meet before you install Entire Net-Work Client.
•	<i>Entire Net-Work Client Installation Steps</i>	Describes the steps necessary to install Entire Net-Work Client.
•	<i>Entire Net-Work Client Silent Installation Steps</i>	Describes the silent installation steps for Entire Net-Work Client in Windows environments.
•	<i>Uninstalling Entire Net-Work Client</i>	Describes the steps necessary to uninstall the Entire Net-Work Client components in Windows and UNIX environments.

20

Installation Prerequisites

Before you begin the Entire Net-Work Client installation, ensure that the following prerequisites have been met:

1. Close (stop) all open applications, especially those applications interacting with or depending on your Adabas databases. This includes Natural, the Adabas DBA Workbench, and prior releases of Entire Net-Work.
2. Disable any antivirus software.
3. Ensure the target computer is connected to the network.
4. Read the *Enhancements*, *Configuration Considerations*, and *Concepts* (earlier in this guide).

If you are upgrading from an Entire Net-Work Version 2 (or earlier) installation, please read the *Entire Net-Work 7 Planning Guide* for a complete description of the architectural changes that have occurred in Entire Net-Work 7, migration considerations, and answers to frequently asked questions.

5. The Entire Net-Work Administration Open Systems installation must be run on the same machine on which the System Management Hub (SMH) is installed to be sure that the Entire Net-Work Client SMH agents required to maintain Entire Net-Work Clients are also installed. If SMH has not yet been installed at your site, running the Entire Net-Work Administration Open Systems installation will install it as well.

For more information, read *Entire Net-Work Administration Open Systems Installation*, elsewhere in this guide.

6. Determine whether or not the Software AG Directory Server needs to be installed as part of this Entire Net-Work Client installation. Entire Net-Work Client requires that the Directory Server be available to the installation or that it be installed as part of the installation.

If the Directory Server has already been installed in your enterprise by other Software AG products, you do not need to install it again -- although multiple installations of the Directory

Server are allowed (for more details, read [Software AG Directory Server Installation](#), elsewhere in this guide).

21

Entire Net-Work Client Installation Steps

- Installing Entire Net-Work Client on Windows Platforms 78

The Entire Net-Work Client installation includes only the components required to run Software AG client applications (Natural and Tamino, for example) that access Adabas databases.



Notes:

1. We recommend that you use only one Directory Server for all Software AG products that require it.
2. Do not install both Entire Net-Work Client and Entire Net-Work 7.2 Client on the same machine.
3. Ideally, the installation of Entire Net-Work Client should be performed by a system administrator or someone with administrator privileges.
4. The steps provided in this chapter will install only an Entire Net-Work Client on the machine. Be aware that the sequence of steps will vary if you are installing one of the Entire Net-Work management components (SMH or the Software AG Directory Server) as well.



Note: The Adabas client package (ACL) is a subproduct that is also installed with Entire Net-Work. ACL has its own versioning.

Installing Entire Net-Work Client on Windows Platforms

This section describes how to install Entire Net-Work Client on Windows systems. Prior to attempting the installation, verify that you have met all of the requirements described in [Platform Coverage, Prerequisites, and Restrictions](#), elsewhere in this guide.

► **To install an Entire Net-Work Client on Windows:**

Shut down all open applications, especially those applications interacting with or depending on your Adabas databases. This includes Natural, the Adabas DBA Workbench, and prior releases of Entire Net-Work Client.

- 1 Insert the Entire Net-Work installation CD into your CD-ROM drive.

The following executable files can be found on the CD:

Executable File Name	Use to Install Component	Description
ADISETUP.EXE	Software AG Directory Server	Run this executable file to install the Software AG Directory Server. Entire Net-Work Client requires that the Directory Server be available to the installation or that it be installed as part of the installation. If the Directory Server has already been installed in your enterprise, you do not need to install it again -- although multiple

Executable File Name	Use to Install Component	Description
		<p>installations of the Directory Server in the enterprise are allowed (for more details, read Software AG Directory Server Installation, elsewhere in this guide).</p> <p>If you elect to install the Software AG Directory Server, its installation must occur before any other components you might also select to install.</p>
WCPSETUP.EXE	Entire Net-Work Server	Run this executable file to install Entire Net-Work Server.
WCLSETUP.EXE	Entire Net-Work Client	<p>Run this executable file to install Entire Net-Work Client.</p> <p>The installation of Entire Net-Work Client always includes the installation of the Adabas Client software.</p>
WCBSETUP.EXE	Entire Net-Work Administration Open Systems	<p>Run this executable file to install the System Management Hub (SMH) as well as all the agents necessary to perform Entire Net-Work Client maintenance.</p> <p>If SMH is already installed in your enterprise, it should not be installed again. Only one SMH is required to manage all Software AG products that require it. However, you should run this installation on the machine on which SMH is installed to ensure that the Entire Net-Work Client agents required for SMH are installed.</p> <p>Note: Installation of Entire Net-Work Administration Open Systems components requires superuser privileges.</p> <p>For more information, read Entire Net-Work Administration Open Systems Installation, elsewhere in this guide.</p>

- 2 Locate and run the appropriate executable file on the CD-ROM. If you only want to install Entire Net-Work Client, only run *WCLSETUP.EXE*.

The Welcome panel appears.

- 3 Follow the prompts on the installation panels. The following panels should be noted:
 - On the Installation Instructions panel, read the installation instructions and click **Yes** to continue. If you click **No**, the installation will stop.
 - On the License Agreement panel, read the installation instructions and click **Yes** to accept the license agreement and continue. If you click **No**, the installation will stop.
 - When the **Directory Server Access** panel appears, specify the host name (or IP address) and port number of the Directory Server that should be used by this installation. For complete information on the port used by the Directory Server, read *The Directory Server Port Number*, in the *Software AG Directory Server Administration Guide*.

If the installation is not successful, you will receive one of several possible error messages. Contact your local distributor for information about customer support services. If the installation fails, it is likely that some parts of the product will have been installed. Therefore, before you attempt to install Entire Net-Work again, run the installation program to remove it. See [Uninstalling Entire Net-Work Client](#), elsewhere in this guide, for instructions on removing the product.

22

Entire Net-Work Client Silent Installation Steps

You can perform a silent installation of Entire Net-Work Client in Windows environments. This chapter provides the steps you must perform to initiate the silent installation.

▶ **To initiate a silent installation of Entire Net-Work Client in a Windows environment, complete the following steps.**

- 1 On 64-bit systems, install the 32-bit and 64-bit runtime components required for the silent installation by entering the following statements:

```
start <cdroot>\windows\wc164\ISSetupPrerequisites\{8D61397C-2AD6-4210-8E43-C2793010DC35}\vcredist_x64.exe /qb
```

```
start <cdroot>\windows\wc164\ISSetupPrerequisites\{0BE9572E-8558-404f-B0A5-8C347D145655}\vcredist_x86.exe /qb
```

Specify the location of the installation CD for *<cdroot>*.

Or:

On 32-bit systems, install the 32-bit runtime components required for the silent installation by entering the following statement:

```
start  
<cdroot>\windows\wc1\ISSetupPrerequisites\{0BE9572E-8558-404f-B0A5-8C347D145655}\vcredist_x86.exe /qb
```

Specify the location of the installation CD for *<cdroot>*.

- 2 Create a configuration text file that includes settings for the following parameters:

Parameter	Specify
SAGXTSDSHOST	The name of the host machine for the Software AG Directory Server used by the client.
SAGXTSDSPORT	The port number for the Software AG Directory Server used by the client.
REMOTE_ADMIN	Either YES or NO. This parameter indicates whether the Entire Net-Work Client service should be started at the end of the installation or not and whether its starting should be automatic. Specify YES if the service should be started after the installation completes and automatically initiated; specify NO if the service should not be started after the installation completes and its starting should be manually initiated.

For example:

```
SAGXTSDSHOST=aaaaaa.bbb.ccc  
SAGXTSDSPORT=4952  
REMOTE_ADMIN=YES
```

- 3 On 64-bit systems, start the silent installation by entering the following statement:

```
<cdroot>\windows\wcl64\setup.exe /z"-c<config.file>"
```

Specify the location of the installation CD for *<cdroot>*. Specify the fully-qualified path and file name of the configuration file you created in the previous step for *<config.file>*.

Or:

- On 32-bit systems, start the silent installation by entering the following statement:

```
<cdroot>\windows\wcl\setup.exe /z"-c<config.file>"
```


Specify the location of the installation CD for *<cdroot>*. Specify the fully-qualified path and file name for the configuration file you created in the previous step for *<config.file>*.

The silent install is initiated.

23 Uninstalling Entire Net-Work Client

- Uninstalling Entire Net-Work Client on Windows 84

This chapter describes the uninstallation of Entire Net-Work Client on all the platforms it supports.

 **Important:** When you uninstall Entire Net-Work Client on Windows systems, the license file is deleted (Note that on UNIX systems, it is *not* deleted.) Management of the license file is, therefore, your responsibility. Make sure that you have a copy of the file before doing the uninstall.

Uninstalling Entire Net-Work Client on Windows

This section describes how to uninstall Entire Net-Work Client on Windows.

 **Notes:**

1. Uninstalling will not remove any files that were not originally installed by the Entire Net-Work Client installation tool. For example, files modified, expanded, moved, or introduced after installation must be removed manually.
2. Uninstalling will stop Entire Net-Work Client.
3. Uninstalling will remove the license file.

The *complete* uninstallation of Entire Net-Work Client on Windows involves the uninstallation of the following software:

- Entire Net-Work Client-specific software
- Software AG Directory Server software
- Entire Net-Work Administration Open Systems, System Management Hub, Software AG Common Tomcat, and Software Common Java software components. These components *must* always be uninstalled in the following order:
 1. Entire Net-Work Administration Open Systems
 2. System Management Hub (SMH)
 3. Software AG Common Tomcat Package
 4. Software AG Common Java Package

The environment variable WCPDIR is removed when you uninstall this product. The environment variable SAG_COMMON is not removed; it may or may not be used by other installed Software AG products.

 **To uninstall Entire Net-Work Client on Windows:**

- 1 If you are running the Entire Net-Work Client as a Windows service, stop the service before you start these steps. This uninstallation procedure will uninstall the service, but it cannot do

so if the service is running. If you do not uninstall the service (or if its uninstallation fails) and you try to reinstall Entire Net-Work Client later, errors will occur when you try to use your new Entire Net-Work installation.

2 Go to the Control Panel.

3 In Windows XP environments, select **Add/Remove Programs**.

In Windows 7 environments, select **Uninstall or Change a Program**.

4 Locate **Software AG Entire Net-Work Client v.r.m** (where *v.r.m* are the version, release, and modification levels of the Entire Net-Work Client code).

In Windows XP environments, click on the associated **Change/Remove** button.

In Windows 7 environments, double-click on **Software AG Entire Net-Work Client v.r.m**.

The InstallShield Wizard is invoked.

5 in Windows XP environments, select **Remove** on the **Welcome** panel and click **Next**. Click **OK** for any verification messages.

In Windows 7 environments, click **OK** to start the uninstallation.

The **Setup Status** panel appears on which you can watch the progress of the uninstallation.

6 When the uninstallation has completed, the Finish panel appears. Click **Finish** to end the uninstallation.

Alternatively, when you try to install this version of the product, the InstallShield automatically detects whether another version is already installed and prompts you to remove it.

24 Required Post-Installation Updates for Simple Connection

Line Driver Support

Once you have installed the Entire Net-Work Client components, you must add target entries in the System Management Hub (SMH) to support the Simple Connection Line Driver.

You can do this in one of two ways:

- You can add them on your local machine by adding an Adabas access definition to a client configuration in SMH. Specifically, one Adabas access definition must be added for each open systems Adabas database you want to access using the Simple Connection Line Driver. For more information, read [Adding Adabas Access Definitions](#), elsewhere in this guide.
- You can manually set up Directory Server target entries for the Adabas open systems databases in the Directory Server that the client uses. Specifically, one XTSaccess (access) target entry must be created in the Directory Server for each open systems Adabas database you want to access using the Simple Connection Line Driver. You can add these target entries using SMH.

For example, if you needed to access database 5 on the host machine named BHOST at port 2504, your access entry might look like this:

```
XTSaccess.5[0]=tcpip://bhost:2504
```


For complete instructions on creating target entries in the Directory Server, read *Maintaining Targets* in the *Software AG Directory Server Administration Guide*. For general information about target entries, read *Directory Server Target Entries* in the *Software AG Directory Server Administration Guide*.

25 Configuring Entire Net-Work Components for Windows

XP Personal Firewall

- Allow Ports for a Specific Executable Program 90
- Open a Specific Port 190

If you have the default Microsoft Windows XP personal firewall enabled on a PC and you would like to install and run Entire Net-Work components on that PC, you will need to allow communications through the firewall on certain ports. You can do this in one of two ways: you can allow ports for a specific executable program or you can open specific ports.

 **Note:** If you attempt to install Entire Net-Work in a system with a firewall in place, be sure that your system administrator has opened the firewall for the Software AG Directory Server port or the installation may not complete successfully.

Allow Ports for a Specific Executable Program

You can allow a specific executable program to open a port. To do so, issue the following command:

```
C:\>netsh firewall add allowedprogram program="<path and file name>"
name="<component-name>" profile=ALL
```

where *<path and file name>* is the path and file name of the file you want to allow and *<component-name>* is a user-specified name to identify the file you are allowing. The following table lists the common Entire Net-Work component files that might need to be allowed if Windows XP personal firewall is enabled:

Component Name	Default Path and File Name
Entire Net-Work Kernel program	C:\Program Files\Software AG\Entire Net-Work Server\731\wcpkernel.exe
Entire Net-Work Client Service	C:\Program Files\Software AG\Entire Net-Work Client\wclservice.exe
Entire Net-Work Server Service	C:\Program Files\Software AG\Entire Net-Work Server\731\wcp-service.exe
Software AG Directory Server Service	C:\Program Files\Software AG\Directory Server\xtsdssvcadi.exe
System Management Hub (SMH) CSLayer Service	C:\Program Files\Software AG\System Management Hub\bin\argsrv.exe
System Management Hub (SMH) EventLayer Service	C:\Program Files\Software AG\System Management Hub\bin\argevsrv.exe
System Management Hub (SMH) MILayer Service	C:\Program Files\Software AG\System Management Hub\bin\argmlsrv.exe

To remove the Entire Net-Work component as an allowed program, issue the following command:


```
C:\>netsh firewall delete allowedprogram program="<path and file name>"  
profile=ALL
```

where *<path and file name>* is the path and file name of the file you want to disallow.

Open a Specific Port

To open a specific port for use by a Entire Net-Work component in the firewall, issue the following command:

```
C:\>netsh firewall add portopening protocol=TCP port=nnnn  
name="<component-name>" profile=ALL
```

where *nnnn* is the port number you want to open and *<component-name>* is a user-specified name to identify the port you are allowing.

To avoid port number conflicts, read [Port Number Reference](#), later in this guide, for a general list of the ports used by Software AG products.

To close a specific port in the firewall, issue the following command:

```
C:\>netsh firewall delete portopening protocol=TCP port=nnnn profile=ALL
```

where *nnnn* is the port number you want to close.

26 Starting and Stopping Entire Net-Work Client

- Automatically Starting Entire Net-Work Client 94
- Manually Starting Entire Net-Work Client 94
- Stopping Entire Net-Work Client 95

This chapter describes what you need to do to start and stop Entire Net-Work Client.

During installation of Entire Net-Work Client, you indicate whether or not the Entire Net-Work Client service or daemon should be started automatically when the computer is started.



Note: The Windows Entire Net-Work Client service is for the Entire Net-Work Client alone and is named "Entire Net-Work Client Service". If a given system does not have Entire Net-Work Client installed, no service will be available in Windows.

Once the Entire Net-Work Client service is started, you can use the System Management Hub (SMH) to configure the client.

Automatically Starting Entire Net-Work Client

If, during installation of the Entire Net-Work Client, you elected to have its service or daemon started automatically at system startup, you need do nothing to start the client. It will start up automatically when the system starts.



Note: You must manually stop the Entire Net-Work Client service before you can uninstall Entire Net-Work Client.

Manually Starting Entire Net-Work Client

If, during installation of the Entire Net-Work Client on Windows systems, you elected not to have its service or daemon started automatically at system startup, you need to manually start it after system startup.

▶ To manually start the Entire Net-Work Client service on Window systems:

- Start it from the Windows Services window (usually located under Administrative Tools on the Control Panel). For more information on the Windows Services window, refer to the documentation for your Windows system.



Note: You must manually stop the Entire Net-Work Client Windows service before you can uninstall Entire Net-Work Client.

The Entire Net-Work Client Windows service is started.

Stopping Entire Net-Work Client

You can shut down (stop) the Entire Net-Work Client Windows service using SMH or using the Windows Services window. This section describes all methods.

▶ **To stop the Entire Net-Work Client Windows service from the Windows Services window:**

- Stop it from the Windows Services window (usually located under Administrative Tools on the Control Panel). For more information on the Services window, refer to the documentation for your Windows system.

The Entire Net-Work Client service is stopped.

▶ **To stop the Entire Net-Work Client service from the System Management Hub (SMH):**

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

The list of client nodes managed by this installation of the System Management Hub appears.

- 3 Right-click on the client node you want in the list and select **Shutdown** from the resulting drop-down menu..

Or:

Select the client node you want and then select **Shutdown** from the **Commands** menu of SMH.

The Entire Net-Work Client service or daemon is shut down (stopped).

To subsequently restart it, follow the procedures described in [Manually Starting Entire Net-Work Client](#), elsewhere in this section, or reboot your machine if you have elected to have the Entire Net-Work Client service or daemon automatically started when the machine is started.

27

About the System Management Hub

- Accessing the System Management Hub 98
- Leaving the System Management Hub 99
- Using the Refresh Button in the System Management Hub 100
- Getting Help 100

The System Management Hub is a Web-based graphical user interface (GUI) you can use to perform administrative tasks for Entire Net-Work and the Software AG Directory Server.

Before you start using the System Management Hub, you must set up an administrative user for the product. To do so, consult the Add Administrator section of the System Management Hub documentation. The System Management Hub (SMH) is the standard, GUI-based, central point of administration for Software AG's products. It runs in a standard Web browser. Please refer to the System Management Hub documentation for further information.

This chapter provides an overview of the System Management Hub and describes its interface elements as they pertain to Entire Net-Work and Software AG Directory Server administration tasks.

Accessing the System Management Hub

▶ To access the System Management Hub:

- 1 Type the following URL into your Web browser:

```
http://smh-mil-node:smh-mil-http-port/smh/login.htm
```

where *smh-mil-node* is the name of the machine where the System Management Hub (SMH) is running (normally this is "localhost") and *smh-mil-http-port* is the port number (the default is 9991) for the SMH MIL (Management Independent Layer) server.



Note: If SMH has been installed on an Apache Web server, replace *smh-mil-http-port* with the port number of the Apache Web server (the default is 80) rather than the SMH MIL server.

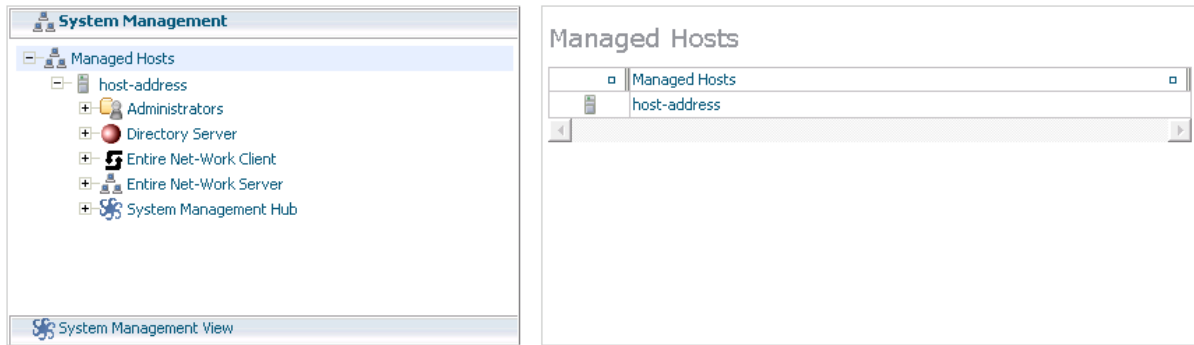
Or:

Select **System Management Hub** on the **Software AG Base Technology** Start Programs submenu (Windows only) and then select **Web Interface** on the resulting submenu.

The login screen for the System Management Hub (SMH) appears.

- 2 Login to the System Management Hub, as described in the section entitled *Internal HTTP Server* under *System Management Hub Web Interface* in *System Management Hub Interfaces and Tools* .

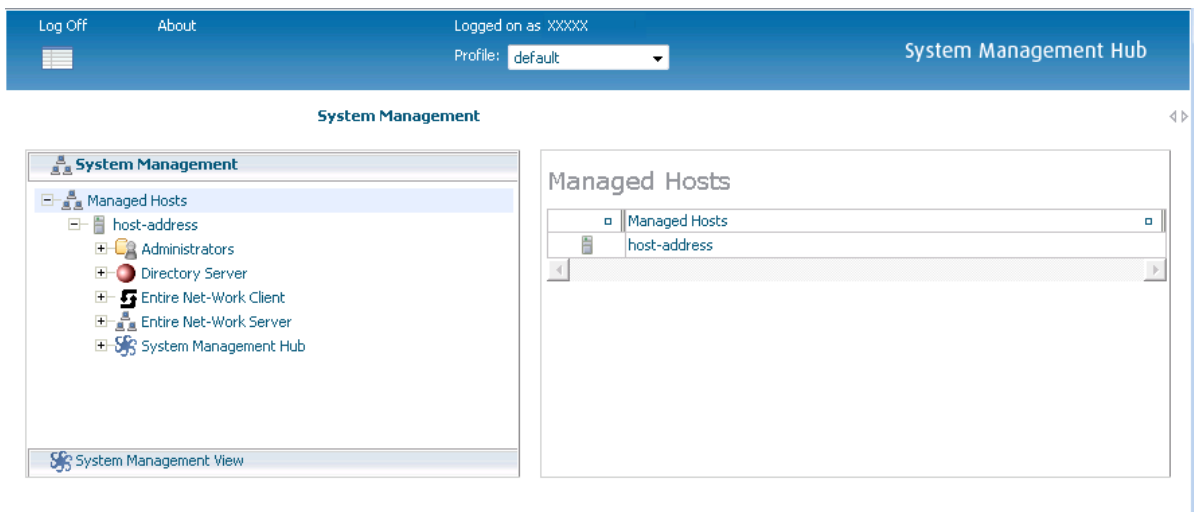
The System Management Hub main panel appears.



Leaving the System Management Hub

► To leave the System Management Hub:

- Click the Log Off command at the top of the screen.



Or:

Close the Browser window.

The System Management Hub window is closed.

Using the Refresh Button in the System Management Hub

Refresh buttons appear in the command frame of the System Management Hub for many panels. Use the **Refresh** button to update the values of items listed in the detail-view frame.

Getting Help

You can get help for any area in the System Management Hub.

▶ **To get help on an area:**

- Click the **Documentation** button in the command frame of the System Management Hub or, if it is available, click the **Help** button in the detail-view frame of the System Management Hub screen.

The documentation pertaining to that System Management Hub area appears.

28

Entire Net-Work Client Administration

This chapter describes the administration tasks you can perform for Entire Net-Work Clients using the System Management Hub (SMH). It is organized as follows:

• <i>The Entire Net-Work Client SMH Administration Area</i>	Describes the section of SMH in which you can manage Entire Net-Work Client services and client configurations.
• <i>About Client Configurations</i>	Describes the concept of a client configuration.
• <i>Listing, Selecting, and Reviewing Client Configurations</i>	Describes how to list, select, and review client configurations.
• <i>Identifying the Client Configuration to Your Application</i>	Describes how to identify which client configuration should be used by your application.
• <i>Setting Service Parameters</i>	Describes how to set general parameters for all client configurations of a client machine.
• <i>Adding Client Configurations</i>	Describes how to add a client configuration.
• <i>Deleting Client Configurations</i>	Describes how to delete a client configuration.
• <i>Maintaining Client Configuration Parameters</i>	Describes the parameters of a client configuration and how to maintain them.
• <i>Migrating Entire Net-Work Client 1.3 Configurations</i>	Describes how to migrate Entire Net-Work Client 1.3 configurations to Entire Net-Work Client 1.4 configurations.
• <i>Controlling Client Access to Databases</i>	Describes how you can use the System Management Hub to control client access to databases.
• <i>Managing Entire Net-Work Client Log Files</i>	Describes how to manage the Entire Net-Work Client log files.
• <i>Accessing Secured z/OS Host Resources</i>	Describes how to use the Entire Net-Work Client External Security Interface (ESI) to access secured Adabas resources on a z/OS host.
• <i>Using ADALNK User Exits</i>	Describes how to use the ADALNK user exits provided with Entire Net-Work Client.

• <i>Changing the Software AG Directory Server</i>	Provides instructions for changing the Software AG Directory Server for an Entire Net-Work Client service and for specific client configurations.
• <i>Tracing Entire Net-Work Client Processing</i>	Describes Entire Net-Work Client trace processing.
• <i>Using the Entire Net-Work User Exit Interface</i>	Explains the Entire Net-Work user exit interface in open systems.

29

The Entire Net-Work Client SMH Administration Area

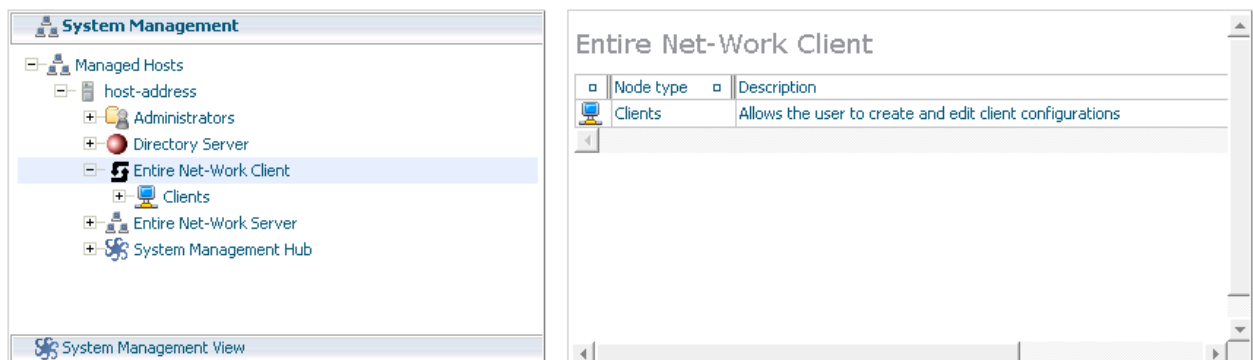
▶ To access the Entire Net-Work Client administration area of the System Management Hub (SMH):

Make sure you have started and logged into the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Client is installed.
- 2 Expand the tree-view frame for the managed host by clicking on the plus sign (+) to the left of its name.
- 3 Select "Entire Net-Work Client" in the tree-view under the managed host.

The Entire Net-Work Client administration area of the System Management Hub becomes available to you.

The Entire Net-Work Client administration area lists the clients you can manage.



The following commands are available in the command menu of the Entire Net-Work Client administration area or by right-clicking on "Entire Net-Work Client" in tree-view:

 **Note:** You must have **Entire Net-Work Client** selected in the tree-view frame to see these commands.

Command	Use this command to:
Help	Link to help for your use of SMH as it pertains to the Entire Net-Work Client administration area.
Refresh	Refresh the screen.

30

About Client Configurations

A *client configuration* provides settings that define a client and how it should operate in the network. Each configuration includes settings for:

- The Software AG Directory Server that should be used by the client in its attempts to work with Adabas databases.
- The databases that should be included or excluded for use by the client.
- Specific database access definitions for the client, including any additional access parameters that should be used.
- XTS (communication service) and ADALNK trace levels used for the client.
- Any user exit used for the client.

These client configuration settings are stored in an *Entire Net-Work Client configuration file*. When you first install Entire Net-Work Client, a default client (named "default") is already defined and can be maintained. When a client is added to the System Management Hub (SMH), a new Entire Net-Work Client configuration file is created to contain the settings for that client. When a client is deleted from SMH, its associated Entire Net-Work Client configuration file is also deleted.

By default, all client configuration files are stored in one of the following locations:

- **In Windows XP environments (up to XP Server 2003):** Documents and Settings\All Users\Application Data\Software AG\Entire Net-Work Client\
Users\Application Data\Software AG\Entire Net-Work Client\
Users\Application Data\Software AG\Entire Net-Work Client\
- **In Windows 7 environments:** ProgramData\Software AG\Entire Net-Work Client\
ProgramData\Software AG\Entire Net-Work Client\
ProgramData\Software AG\Entire Net-Work Client\
- **In UNIX environments:** \$SAG\wc1\.

However, you can elect to store a client configuration file in a different location by specifying the location when you create the client configuration. For more information, read [Adding Client Configurations](#), elsewhere in this guide. Once the configuration is created, you cannot change the path; you must delete and recreate the client configuration to do so.

Client configurations cannot be stored on a server; they can only be stored on the local machine. If you want to share a client configuration with multiple clients, define it in a directory on the local machine and then share that directory with the other clients, being sure to specify the path to the client configuration when you identify the client configuration to your application. For more information, read *Identifying the Client Configuration to Your Application*, elsewhere in this guide.

In general, the filenames of Entire Net-Work Client configuration files are the same as the name of the client you specify when you add the client in SMH. For example, a client named "TEST" will create a configuration file also named "TEST".



Note: We do not recommend that you maintain client configuration files using a text editor. Instead, we recommend that you use SMH to perform all maintenance to Entire Net-Work Clients and their configuration files.

Comparison With Directory Server Configuration

You can also use Directory Server configuration settings to define how a client should operate in the network. Directory Server configuration settings affect all clients that use the Directory Server. Entire Net-Work Client configuration settings only affect the individual client. Entire Net-Work Client configurations can be very useful, therefore, if you want to test a configuration before publishing it for additional clients in the Directory Server.

For example, you might use the following procedure to test a configuration prior to publishing it in the Directory Server:

1. Test the Entire Net-Work Client configuration settings against a copy of an Adabas database on a local machine.
2. Once these first tests run correctly, you might then test the Entire Net-Work Client configuration settings against the actual Adabas database available to all users on the network. The only client affected by the Entire Net-Work Client configuration settings would be the client to which they apply.
3. Only after these second set of tests run correctly would you publish the Entire Net-Work Client configuration settings by defining the same settings in the Directory Server.

31 Listing, Selecting, and Reviewing Client Configurations

▶ To list and review the **Entire Net-Work Client configurations** managed by SMH:

Make sure you have accessed the System Management Hub.

- 1 Select (left-click on) and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select (left-click on) and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

The following commands are available for this client list:



Note: You must have **Clients** selected in the tree-view frame to see these commands.

Command	Use this command to:
Help	Link to help for your use of SMH as it pertains to the Entire Net-Work Client administration area.
Refresh	Refresh the screen.

- 3 Select (left-click on) and expand the client machine you want from the list.

The client configuration section becomes available in tree-view, listing all the clients defined for the client machine.

The following Entire Net-Work commands are available for each client machine, when you right-click on the client machine name:



Note: You must have a client machine selected in the tree-view frame to see these commands.

Command	Use this command to:
Add Client Configuration	Add a client to be maintained by SMH. For more information, read Adding Client Configurations , elsewhere in this chapter.
Add to Browser Favorites	Add a node in tree-view to your browser favorites.
Add to View	Add a node in tree-view to System Management View. For more information about System Management View, read your System Management Hub documentation.
Help	Link to help for your use of SMH as it pertains to the Entire Net-Work Client administration area.
Migrate WCL13 Client Configuration	Migrate the client configurations you set up in Entire Net-Work Client 1.3. This process converts them to Entire Net-Work Client 1.4 client configurations. For more information, read Migrating Entire Net-Work Client 1.3 Configurations , elsewhere in this chapter.
New Log File	Close the current Entire Net-Work Client log file and start a new one. For more information, read Managing Entire Net-Work Client Log Files , elsewhere in this chapter.
Refresh	Refresh the screen.
Remove from View	Remove a node in tree-view from System Management View. For more information about System Management View, read your System Management Hub documentation.
Set Service Parameters	Change the parameters used by the client machine, including the Directory Server used by the client machine. For more information, read Setting Service Parameters , elsewhere in this chapter.
Set Service Trace Granularity	Set the Entire Net-Work Client trace level for all clients. For more information, read Tracing Entire Net-Work Client Processing , elsewhere in this chapter.
Shutdown	Shut down the Entire Net-Work Client service. For more information, read Stopping Entire Net-Work Client , elsewhere in this chapter.
View Log File	View the current Entire Net-Work Client log file. For more information, read Managing Entire Net-Work Client Log Files , elsewhere in this chapter.

- 4 Select (left-click on) and expand a client.

A list of Entire Net-Work Client parameter settings for the client appears in detail view. For more information about these settings, read [Maintaining Client Configuration Parameters](#), elsewhere in this chapter.

The following Entire Net-Work commands are available for each client, when you right-click on the name of the client:



Note: You must have a client selected in the tree-view frame to see these commands.

Command	Use this command to:
Add Adabas Access	Add an access definition for an Adabas database to the client.
Add Additional Access Parameters	Add additional access parameters for an Adabas database to the client.
Add to Browser Favorites	Add a node in tree-view to your browser favorites.
Add to View	Add a node in tree-view to System Management View. For more information about System Management View, read your System Management Hub documentation.
Delete Client	Delete the client definition from SMH. For more information, read Deleting Client Configurations , elsewhere in this chapter
Help	Link to help for your use of SMH as it pertains to the Entire Net-Work Client administration area.
Refresh	Refresh the screen.
Remove from View	Remove a node in tree-view from System Management View. For more information about System Management View, read your System Management Hub documentation.
Set ADASAF Parameters	Specify parameters to support the External Security Interface (ESI) supplied with Entire Net-Work Client. ESI allows you to access secured z/OS host resources. For more information, read Accessing Secured z/OS Host Resources , elsewhere in this chapter.
Set Client Configuration Parameters	Maintain the parameters for the client configuration. For more information, read Maintaining Client Configuration Parameters , elsewhere in this chapter.
Set Client Trace Granularity	Set the client trace level. For more information, read Managing Client Tracing , elsewhere in this chapter.
Set Directory Server	Change the Software AG Directory Server used by the client. For more information, read Changing the Software AG Directory Server for the Client , elsewhere in this chapter.
Set LNK User Exit Parameters	Specify the user exit file and function names that should be called before and after ACB and ACBX direct calls, if the Adabas interface supports user exits. For more information, read Using ADALNK User Exits , elsewhere in this chapter.

In addition to these commands, other standard browser commands such as **Refresh** or **Add to Browser Favorites** are also available.

32 Identifying the Client Configuration to Your Application

- Specifying the Configuration by Environment Variable 112
- Specifying the Configuration in Your Application 112

When your application attempts to access a database, it needs to know which client configuration it should use for its communications with the database. You can specify which client configuration should be used by your application in one of two ways:

- You can set an environment variable that identifies the client configuration.
- You can specify the client configuration in your application.

Specifying the Configuration by Environment Variable

▶ To specify the client configuration using an environment variable:

- In your list of system environment variables, add a `WCPCONFIG` environment variable that is set to the name of the client configuration file. Do not specify the path to this file; Entire Net-Work knows where to find it. For information on specifying environment variables in Windows, refer to your Windows documentation and UNIX, refer to the documentation for those environments.

Specifying the Configuration in Your Application

▶ To specify the client configuration in your application:

- Use the `AdaSetParameter` function in your application to specify the client configuration name prior to accessing the database. The syntax of the `AdaSetParameter` function is:

```
AdaSetParameter ("WCPCONFIG=configname")
```

-- where *configname* is the name of the configuration.

33

Setting Service Parameters

You can set parameters for the client machine, including the default Software AG Directory Server used by the client, as well as the client name, host name, and port number.

▶ **To set parameters for the client machine:**

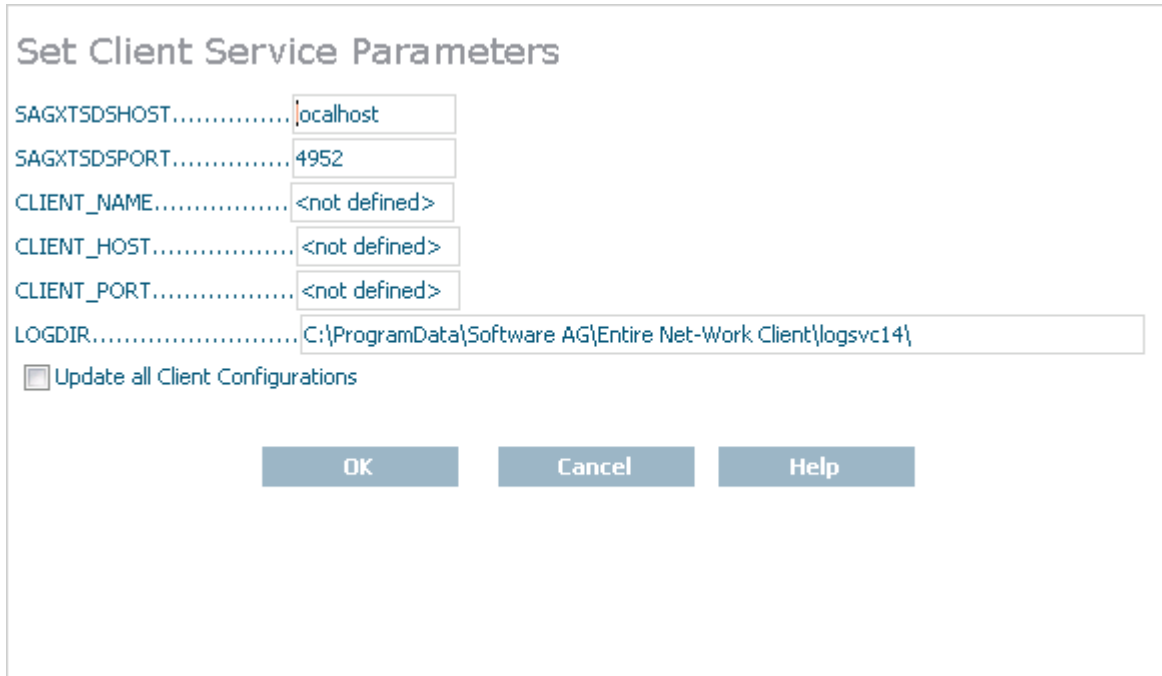
Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and right-click on the client machine on which the client is defined. Then select the **Set Service Parameters** option from the resulting drop-down menu.

The **Set Client Service Parameters** panel appears in detail-view.



- 4 Modify the parameters on the **Set Client Service Parameters** panel, as described in the following table.

Parameter	Description
SAGXTSDSHOST	Specify the Software AG Directory Server host name you want to use for this client machine.
SAGXTSDSPORT	Specify the port number of the Software AG Directory Server you specified in the SAGXTSDSHOST parameter.
CLIENT_NAME	Normally, the client machine name is the machine name. However, for cosmetic reasons only, you can change the client machine name. If a client name is specified in this parameter, the new client name is changed in the access entries in the local Entire Net-Work Client configuration file.
CLIENT_HOST	Normally, the host name for a client is the client machine name. However, you may want to select a different host name for the client machine. For example, you might want to specify the fully qualified host name (such as, "user.aaa.com") or physical address (such as, "10.124.221.36") of the machine instead. If a client host name is specified in this parameter, the new host name is changed in the access entries in the local Entire Net-Work Client configuration file.
CLIENT_PORT	Normally, port numbers are dynamically assigned by Entire Net-Work when the client is started, as follows: <ul style="list-style-type: none"> ■ Entire Net-Work searches for the first available port starting from port 49152 through 65535. (The starting search port number, 49152, is the IANA-recommended value from which to start.).

Parameter	Description
	<ul style="list-style-type: none"> ■ Once an available port number is found, it is assigned to the client in its Software AG Directory Server entry. <p>You can optionally assign a port number to a client using this parameter. If you do, the new port number is changed in the access entries in the local Entire Net-Work Client configuration file.</p>
LOGDIR	Specify the fully-qualified path of the directory where Entire Net-Work Client log files should be written. For more information, read Specifying the Log File Location , elsewhere in this chapter.

- 5 Optionally, select the **Update all Client Configurations** checkbox if you want all of the client configurations defined for this client machine to have these parameters applied to them. If you do not select the **Update all Client Configurations** checkbox, only new client configurations you define will have these parameters applied.
- 6 When all parameters are set as you want, click OK.

The client machine parameters are updated.

34 Adding Client Configurations

Using the System Management Hub (SMH), you can add client configurations for a client machine. Once added, the configuration can be maintained in SMH. Adding a client configuration will create a new client configuration file. For more information, read *About Client Configurations*, elsewhere in this chapter.



Note: We do not recommend that you maintain client configuration files using a text editor. Instead, we recommend that you use SMH to perform all maintenance to Entire Net-Work configuration files.

▶ **To add a client configuration definition to SMH:**

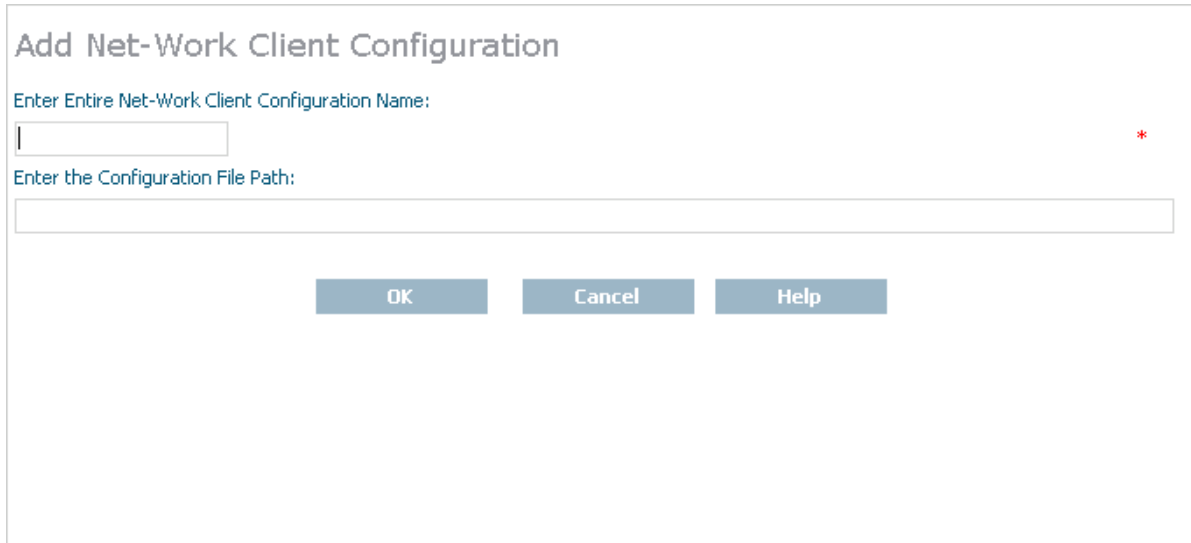
Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Right-click on the client machine you want in the list and select **Add Client Configuration** from the resulting drop-down menu.

The **Add Net-Work Client Configuration** panel displays in detail-view.



Add Net-Work Client Configuration

Enter Entire Net-Work Client Configuration Name: *

Enter the Configuration File Path:

OK Cancel Help

- 4 Enter the name of the client configuration in **Enter Entire Net-Work Client Configuration Name** field on the **Add Net-Work Client Configuration** panel. The maximum number of characters allowed for a client configuration name is 16.
- 5 Optionally, enter the path where the client configuration should be stored and click **OK**. The directory listed in the path must exist before you try to specify it in the configuration. Once the configuration is created, you cannot change the path; if you want to change the path, you must delete and recreate the client configuration.

The client configuration cannot be stored in shared directories; it can only be stored on the local machine. For more information about using an individual client configuration for multiple clients, read [About Client Configurations](#), elsewhere in this guide.



Note: If no path is specified, the client configuration file is stored wherever Entire Net-Work Client is installed.

The client is added to SMH and a new Entire Net-Work Client configuration file is created.

35

Deleting Client Configurations

Using the System Management Hub (SMH), you can delete a client definition from a client machine. Deleting a client configuration deletes its associated client configuration file from the system. For more information, read *About Client Configurations*, elsewhere in this chapter.



Note: We do not recommend that you maintain client configuration files using a text editor. Instead, we recommend that you use SMH to perform all maintenance to Entire Net-Work configuration files.

▶ To delete a client configuration in SMH:

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and expand the client machine on which the client is defined.

The client configuration section becomes available in tree-view.

- 4 Right-click on the client you want to delete and select **Delete Client** from the resulting drop-down menu.

A panel appears in tree-view verifying that you want to delete the client.

- 5 Click **OK** to confirm deletion of the client.

The client is deleted from SMH and its associated configuration file is removed from the system.

36

Maintaining Client Configuration Parameters

You can modify the configuration parameters set for a specific client using SMH. These parameters are stored in the appropriate client configuration file on the local machine. For more information, read *About Client Configurations*, elsewhere in this chapter.



Note: We do not recommend that you maintain client configuration files using a text editor. Instead, we recommend that you use SMH to perform all maintenance to Entire Net-Work configuration files.

▶ **To maintain the configuration parameters for a client in SMH:**

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and expand the client machine on which the client is defined.

The client configuration section becomes available in tree-view.

- 4 Right-click on the client configuration whose parameters you want to maintain and select **Set Client Configuration Parameters** from the resulting drop-down list.

The **Client Configuration Parameters** panel appears in detail-view.

- 5 Modify the parameters on the **Client Configuration Parameters** panel, as described in the following table. When all parameters are set as you want, click **OK** to save them.

Parameter	Description	Required?	Default
ACCEPTED_DBIDS	Specify the database IDs you want this client to be able to access. If more than one database ID is needed, separate them with commas. If a range of database numbers is needed, separate them with a dash. For example, "4,12-15,62" indicates that the client should have access to databases 4, 62, and any databases with numbers between 12 and 15 (inclusive). For more information, read Understanding Filtering , elsewhere in this guide.	No	All defined databases can be accessed.
ADABAS_TIMEOUT	Specify the number of seconds the client should wait for a response from a remote Adabas call before it times out. The default is 60 seconds; the minimum value you can specify is 5 seconds.	No	60 seconds
Full LNK Trace	Click in this checkbox to set the LNKTRACE value to obtain full tracing of ADALNK processing. Do not check this checkbox unless specifically instructed to	No	Full tracing is not performed.

Parameter	Description	Required?	Default
	do so by a Software AG Customer Support representative. If you do, your installation could be overrun with trace messages that would be meaningless to you and would likely affect system performance.		
Full XTS Trace	Click in this checkbox to set the XTSTRACE value to obtain full tracing of Software AG transport services processing. Do not check this checkbox unless specifically instructed to do so by a Software AG Customer Support representative. If you do, your installation could be overrun with trace messages that would be meaningless to you and would likely affect system performance.	No	Full tracing is not performed.
LOGDIR	Specify the fully-qualified path of the directory where Entire Net-Work Client log files should be written. For more information, read <i>Specifying the Client Log File Location</i> , elsewhere in this chapter.	No	<ul style="list-style-type: none"> ■ In Windows XP environments (up to XP Server 2003): Documents and Settings\All Users\Application Data\Software AG\Entire Net-Work Client\. ■ In Windows 7 environments: ProgramData\Software AG\Entire Net-Work Client\. ■ In UNIX environments: \$SAG\wcl\.
LNKTRACE	Set the hexadecimal ADALNK trace level using this parameter. This is the trace level for Adabas calls. Valid values are hexadecimal values ranging from "00" (no tracing) through "f1 (full tracing)". Do not specify full tracing unless specifically instructed to do so by a Software AG Customer Support representative. If you do, your installation could be overrun with trace messages that would be meaningless to you and would likely affect system performance.	No	00

Parameter	Description	Required?	Default
	For more information about Entire Net-Work Client tracing, read Tracing Entire Net-Work Client Processing , elsewhere in this guide.		
MULTIPLEX	Indicate whether a TCP/IP connection is shared by multiple Adabas open system clients connected to Entire Net-Work. Valid values are "YES" and "NO". If you specify "YES", the TCP/IP connection is shared; if you specify "NO", the TCP/IP connection is not shared. Sharing a TCP/IP connection can result in reduced speed across the network. However, it can be useful if the number of sockets available is limited (especially in UNIX environments).	No	For Adabas open systems versions 6.3 and earlier, the default is "YES". For all versions after 6.3, the default is "NO"
NOLOCAL	Indicate whether or not you want this client to use local databases. Valid values are "YES" and "NO". If you specify "YES", local databases are <i>not</i> used; if you specify "NO", they are used.	No	NO
NOREMOTE	Indicate whether or not you want this client to use remote databases. Valid values are "YES" and "NO". If you specify "YES", remote databases are <i>not</i> used; if you specify "NO", they are used.	No	NO
REJECTED_DBIDS	Specify the database IDs you do <i>not</i> want this client to be able to access. If more than one database ID is needed, separate them with commas. If a range of database numbers is needed, separate them with a dash. For example, "4,12-15,62" indicates that the client should <i>not</i> have access to databases 4, 62, and any databases with numbers between 12 and 15 (inclusive). For more information, read Understanding Filtering , elsewhere in this guide.	No	All defined databases can be accessed.
REMEMBER_DBID	Indicate whether the access entries for databases used by this client should be remembered and stored in local Entire Net-Work Client access entries in the Entire Net-Work Client configuration file as well as in the Directory Server. Valid values are "YES" and "NO". If you specify "YES", the access entry information is	No	No

Parameter	Description	Required?	Default
	<p>stored locally as well as in the Directory Server; if you specify "NO", the access entry information is available only in the Directory Server configuration file, wherever the Software AG Directory Server is installed.</p> <p>The advantage of storing access entries locally is increased client speed. If the client fails to access Adabas using the local access information, it will attempt to access Adabas using the Directory Server. If the Directory Server access is successful and its access information is new, the local information is updated.</p>		
USER_EXITS	Specify the name of the user exit DLL file that should be used with this client. For more information about Entire Net-Work Client user exits, read <i>Using the Entire Net-Work User Exit Interface</i> , elsewhere in this guide.	No	No user exit is used with this client.
WCPPARTITION	Specify the partition in which the client is assigned, if any. For more information, read <i>Understanding Partitioning</i> , elsewhere in this guide.	No	The client is not assigned a partition.
XTSTRACE	<p>Set the hexadecimal XTS trace level using this parameter. This is the trace level for Software AG transport services. Valid values are hexadecimal values ranging from "0000" (no tracing) through "FFFE" (full tracing). Do not specify full tracing unless specifically instructed to do so by a Software AG Customer Support representative. If you do, your installation could be overrun with trace messages that would be meaningless to you and would likely affect system performance.</p> <p>For more information about Entire Net-Work Client tracing, read <i>Tracing Entire Net-Work Client Processing</i>, elsewhere in this guide.</p>	No	0000

The client parameters are updated in the appropriate Entire Net-Work Client configuration file.

37

Migrating Entire Net-Work Client 1.3 Configurations

If you want to use your Entire Net-Work Client 1.3 configurations in Entire Net-Work Client 1.4, you must convert them to Entire Net-Work Client 1.4 configurations. This chapter describes how to do this.



Caution: Once a client configuration has been migrated to 1.4, it cannot be migrated back to 1.3.

► To convert an Entire Net-Work Client 1.3 configuration:

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Right-click on the client machine on which the 1.3 client is defined and select **Migrate WCL13 Client Configuration** from the resulting drop-down menu.

The **Migrate Net-Work Client Configuration** panel appears in detail-view.

Migrate Net-Work Client Configuration

Enter Entire Net-Work Client Configuration Name:

*

OK Cancel Help

- 4 Specify the name of the Entire Net-Work Client 1.3 client configuration you want to migrate in the area provided for it on the panel.
- 5 When the name has been specified, click **OK** to convert the configuration to a 1.4 configuration.

The configuration is converted.

38

Controlling Client Access to Databases

- Maintaining Adabas Access Definitions 131
- Maintaining Additional Database Access Parameters 136

You can control client access to Adabas databases in two ways:

- Locally, using local Entire Net-Work Client definitions. These definitions are stored in the Entire Net-Work Client configuration file on the local machine, and are therefore available only to the local client.
- Globally, using Software AG Directory Server definitions. These definitions are stored in the Directory Server configuration file, wherever the Software AG Directory Server is installed, and are published and available for other clients using the same Directory Server.

Updates to the Directory Server configuration affect all clients that use the Directory Server updates to the Entire Net-Work Client configuration only affect the individual client. Entire Net-Work Client configurations can be very useful, therefore, if you want to test a configuration before publishing it for additional clients in the Directory Server.

Using a local Entire Net-Work Client configuration, you can control client access to Adabas databases in two ways:

- You can use filtering to identify databases that the client can and cannot access.
- You can define local Adabas access definitions for specific databases.

The difference between the two methods is that you can specify additional connection parameters to a database in an Adabas access definition, whereas filtering controls all connections to the database. The two methods do work in conjunction. For example, if your filtering allows access to a given database, you can further qualify that access by specifying additional database access parameters, as described in this chapter. But, if your filtering does *not* allow access to a given database, no additional database access settings you may have specified are processed.

For complete information on filtering in the Entire Net-Work Client configuration, read [Understanding Filtering](#), elsewhere in this guide.

Globally, you can perform such filtering in the Directory Server configuration, using partitioning and target definitions. For more information about using the Directory Server, read *Software AG Directory Server Documentation*, in the *Software AG Directory Server Administration Guide*.

This chapter describes how to control client access to databases in the Entire Net-Work Client configuration.

Maintaining Adabas Access Definitions

You can specify access definitions for specific Adabas databases. This access definition will be used when the database is accessed by the client. However, if filtering for the client configuration does not allow access to the database, this access definition is ignored.

This section covers the following topics:

- [Adding Adabas Access Definitions](#)
- [Listing Adabas Access Definitions](#)
- [Modifying Adabas Access Definitions](#)
- [Deleting Adabas Access Definitions](#)

Adding Adabas Access Definitions

Using the System Management Hub (SMH), you can add Adabas database access definitions for a client configuration.

▶ **To add an Adabas access definition to a client configuration:**

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and expand the client machine on which the client configuration is defined.

The list of clients defined on the client machine appears.

- 4 Right-click on the client configuration to which you want to add an Adabas access definition and select **Add Adabas Access** from the resulting drop-down menu.

The **Add Adabas Access Definition** panel appears in detail-view.

Add Adabas Access Definition

Enter Adabas ID: *

Protocol Type
 TCP/IP
 SSL

Enter Host Address:

Enter Port Value: 0 *

Reconnect Retry Count: Retry Interval:

Enter Additional Parameters:

- 5 Modify the parameters on the **Add Adabas Access Definition** panel, as described in the following table. When all parameters are set as you want, click OK.

Parameter	Description	Required?	Default
Adabas ID	Specify the ID of the Adabas database to which this definition applies.	Yes	---
Protocol Type	Select the communication protocol that will be used to connect to the database: TCP/IP or SSL	Yes	---
Host Address	Specify the name of the host computer where the database runs.	Yes	---
Port Value	The port number of the host computer for the database.	Yes	---
Reconnect	Click in the checkbox if you want reconnection attempts to occur if the database connection is disconnected due to some failure in the system. If this check box is not checked, no reconnection attempt is made.	No	No reconnection attempt is made.
Retry Count	Specify the number of times reconnection should be attempted. The valid range is "0" through "2147483648". A value should only be specified for this parameter if the Reconnect parameter is turned on (checked). If no value is specified, reconnection attempts do not occur.	No	0
Retry Interval	Specify the number of seconds to wait between reconnection attempts. The valid range is "0" through "2147483648". A value should only be specified for this parameter if the	No	0

Parameter	Description	Required?	Default
	Reconnect parameter is turned on (checked). If no value is specified, reconnection attempts do not occur.		
Additional Parameters	Specify additional parameters as described in <i>Parameters</i> , in the chapter entitled <i>Directory Server Target Entries</i> of the <i>Software AG Directory Server Administration Guide</i> . Separate parameters in this field with ampersand (&) symbols.	No	---

The Adabas access definition is added to the client configuration.

Listing Adabas Access Definitions

► To list the Adabas access definitions of a client configuration:

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and expand the client machine on which the client configuration is defined.

The list of client configurations defined on the client machine appears.

- 4 In tree-view, expand the client configuration containing the Adabas access definitions you want to review.

Options for the Adabas access and additional access parameter definitions appear in tree-view.

- 5 Select and expand **Adabas Access Definitions** in the tree-view list for the client configuration.

The Adabas access definitions are listed in detail-view as well as in the tree-view list below the **Adabas Access Definitions** heading.

Modifying Adabas Access Definitions

► **To modify an Adabas access definition:**

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and expand the client machine on which the client configuration is defined.

The list of client configurations defined on the client machine appears.

- 4 In tree-view, expand the client configuration containing the Adabas access definitions you want to modify.

Options for the Adabas access and additional access parameter definitions appear in tree-view.

- 5 Select and expand **Adabas Access Definitions** in the tree-view list for the client configuration.

The Adabas access definitions are listed in detail-view as well as in the tree-view list below the **Adabas Access Definitions** heading.

- 6 In tree-view, right-click on the Adabas access definition you want to modify and select **Modify Entry** from the resulting drop-down menu.

The **Modify Adabas Access** panel appears in detail-view.

The screenshot shows a dialog box titled "Modify Adabas Access". It contains the following fields and controls:

- Port:** A text input field containing "8888" with a red asterisk to its right.
- Host:** A text input field containing "localhost" with a red asterisk to its right.
- Protocol Selection:** Two radio buttons. The first is labeled "TCP/IP Protocol" and is selected. The second is labeled "SSL Protocol".
- Additional Parameters:** A large empty text input field.
- Buttons:** Three buttons at the bottom: "OK", "Cancel", and "Help".

- 7 Modify the parameters on the **Modify Adabas Access** panel, as described in the following table. When all parameters are set as you want, click OK.

Parameter	Description	Required?	Default
Port	The port number of the host computer for the database.	Yes	---
Host	The name of the host computer on which the database is installed.	Yes	---
Protocol Type	Select the communication protocol that will be used to connect to the database: TCP/IP or SSL	No	The original communications protocol selected when the definition was created is used.
Additional Parameters	Specify additional parameters as described in <i>Parameters</i> , in the chapter entitled <i>Directory Server Target Entries of the Software AG Directory Server Administration Guide</i> . Separate parameters in this field with ampersand (&) symbols.	No	---

The Adabas access definition is modified.

Deleting Adabas Access Definitions

► To delete an Adabas access definition in a client configuration:

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and expand the client machine on which the client configuration is defined.

The list of client configurations defined on the client machine appears.

- 4 In tree-view, expand the client configuration containing the Adabas access definitions you want to delete.

Options for the Adabas access and additional access parameter definitions appear in tree-view.

- 5 Select and expand **Adabas Access Definitions** in the tree-view list for the client configuration.

The Adabas access definitions are listed in detail-view as well as in the tree-view list below the **Adabas Access Definitions** heading.

- 6 In tree-view, tight-click on the Adabas access definition you want to delete and select **Delete Entry** from the resulting drop-down menu.

A panel appears in tree-view verifying that you want to delete the access definition.

- 7 Click **OK** to confirm deletion of the Adabas access definition from the client configuration.

The definition is deleted from the configuration.

Maintaining Additional Database Access Parameters

You can specify additional access parameters for specific Adabas databases. These access parameters will be used in conjunction with any other database access specifications specified for the database when it is accessed by the client. However, if filtering for the client configuration does not allow access to the database, these database access parameters are ignored.

This section covers the following topics:

- [Adding Additional Access Parameter Definitions](#)
- [Listing Additional Access Parameter Definitions](#)
- [Modifying Additional Access Parameter Definitions](#)
- [Deleting Additional Access Parameter Definitions](#)

Adding Additional Access Parameter Definitions

Using the System Management Hub (SMH), you can specify additional access parameters for specific Adabas databases.

- ▶ **To add an additional access parameter definition to a client configuration:**

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and expand the client machine on which the client configuration is defined.

The list of client configurations defined on the client machine appears.

- 4 Right-click on the client configuration to which you want to add an Adabas access parameter definition and select **Add Additional Access Parameters** from the resulting drop-down menu.

The **Add Additional Access Parameters** panel appears in detail-view.

Add Additional Access Parameters

Enter Adabas ID: *

Reconnect Retry Count: Retry Interval:

Enter Additional Parameters:

- 5 Modify the parameters on the **Add Additional Access Parameters** panel, as described in the following table. When all parameters are set as you want, click OK.

Parameter	Description	Required?	Default
Adabas ID	Specify the ID of the Adabas database to which this definition applies.	Yes	---
Reconnect	Click in the checkbox if you want reconnection attempts to occur if the database connection is disconnected due to some failure in the system. If this check box is not checked, no reconnection attempt is made.	No	No reconnection attempts are made.
Retry Count	Specify the number of times reconnection should be attempted. The valid range is "0" through "2147483648". A value should only be specified for this parameter if the Reconnect parameter is turned on (checked). If no value is specified, reconnection attempts do not occur.	No	0
Retry Interval	Specify the number of seconds to wait between reconnection attempts. The valid range is "0" through "2147483648". A value should only be specified for this parameter if the Reconnect parameter is turned on (checked). If no value is specified, reconnection attempts do not occur.	No	0
Additional Parameters	Specify additional parameters as described in <i>Parameters</i> , in the chapter entitled <i>Directory Server Target Entries</i> of the <i>Software AG Directory Server Administration Guide</i> . Separate parameters in this field with ampersand (&) symbols.	No	---

The Adabas access parameter definition is added to the client configuration.

Listing Additional Access Parameter Definitions

► **To list the additional access parameter definitions of a client configuration:**

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and expand the client machine on which the client configuration is defined.

The list of client configurations defined on the client machine appears.

- 4 In tree-view, expand the client configuration containing the Adabas access parameter definitions you want to review.

Options for the Adabas access and additional access parameter definitions appear in tree-view.

- 5 Select and expand **Additional Access Parameters** in the tree-view list for the client configuration.

The Adabas access parameter definitions are listed in detail-view as well as in the tree-view list below the **Additional Access Parameters** heading.

Modifying Additional Access Parameter Definitions

► **To modify an additional access parameter definition:**

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and expand the client machine on which the client configuration is defined.

The list of client configurations defined on the client machine appears.

- 4 In tree-view, expand the client configuration containing the Adabas access parameter definitions you want to modify.

Options for the Adabas access and additional access parameter definitions appear in tree-view.

- 5 Select and expand **Additional Access Parameters** in the tree-view list for the client configuration.

The Adabas access parameter definitions are listed in detail-view as well as in the tree-view list below the **Additional Access Parameters** heading.

- 6 In tree-view, right-click on the Adabas access parameter definition you want to modify and select **Modify Entry** from the resulting drop-down menu.

The **Modify Additional Parameters** panel appears in detail-view.

- 7 Modify the parameters on the **Modify Additional Parameters** panel, as described in the following table. When all parameters are set as you want, click OK.

Parameter	Description	Required?	Default
Additional Parameters	Specify additional parameters as described in <i>Parameters</i> , in the chapter entitled <i>Directory Server Target Entries</i> of the <i>Software AG Directory Server Administration Guide</i> . Separate parameters in this field with ampersand (&) symbols.	No	If all additional parameter are removed, the Adabas access parameter definition is also removed.

The access parameter definition is modified.

Deleting Additional Access Parameter Definitions

- ▶ To delete an additional access parameter definition in a client configuration:

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and expand the client machine on which the client configuration is defined.

The list of client configurations defined on the client machine appears.

- 4 In tree-view, expand the client configuration containing the Adabas access definitions you want to delete.

Options for the Adabas access and additional access parameter definitions appear in tree-view.

- 5 Select and expand **Additional Access Parameters** in the tree-view list for the client configuration.

The Adabas access parameter definitions are listed in detail-view as well as in the tree-view list below the **Additional Access Parameters** heading.

- 6 In tree-view, right-click on the Adabas access parameter definition you want to delete and select **Delete Entry** from the resulting drop-down menu.

A panel appears in tree-view verifying that you want to delete the access parameter definition.

- 7 Click **OK** to confirm deletion of the Adabas access parameter definition from the client configuration.

The definition is deleted from the configuration.

39

Managing Entire Net-Work Client Log Files

- Viewing the Current Entire Net-Work Client Log File 142
- Starting a New Entire Net-Work Client Log File 142
- Specifying the Client Log File Location 143

You can view the current Entire Net-Work Client log file or start a new one. This chapter describes both processes.

Viewing the Current Entire Net-Work Client Log File

► **To list and review the current Entire Net-Work Client log file:**

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and right-click on the client machine on which the client is defined. Then select the **View Log File** option from the resulting drop-down menu.

The current log file for the client machine appears in detail-view.

Starting a New Entire Net-Work Client Log File

You can close the current Entire Net-Work Client log file and start a new one at any time. The original log file is retained, but is renamed with a name in the format *wclxxxxx.log*, where *xxxxxx* is an automatically assigned sequence number for the log file. For example, the first retained log file is assigned the name *wcl00000.log*, the second is assigned the name *wcl00001.log*, and so on. The older log files, therefore, have the lower sequence numbers. The current log file is the file named *wcl-svc.log*.

By default, Entire Net-Work Client log files are stored in the *logsvc* directory in one of the following locations:

- In Windows XP environments (up to XP Server 2003): `Documents and Settings\All Users\Application Data\Software AG\Entire Net-Work Client\`
- In Windows 7 environments: `ProgramData\Software AG\Entire Net-Work Client\`
- In UNIX environments: `$SAG\wcl\`.

For example, the default location in Windows XP environments is *Documents and Settings\All Users\Application Data\Software AG\Entire Net-Work Client\logsvc*. If you would like to specify

the location in which Entire Net-Work Client log files should be stored, read [Specifying the Client Log File Location](#), elsewhere in this section.

▶ **To close the current Entire Net-Work Client log file and start a new one:**

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and right-click on the client machine in which the client is defined. Then select the **New Log File** option from the resulting drop-down menu.

A prompt appears in detail view inquiring whether you want to close the current log file and start a new one.

- 4 Click **OK** at the prompt.

The current log file is closed and a new one is started.

Specifying the Client Log File Location

You can specify the fully-qualified path of the directory in which client log files should be stored. If you do not specify a log file location, the default location for client log files (the *logsvc* directory) will be used. By default, this directory will be stored in one of the following locations:

- In Windows XP environments (up to XP Server 2003): Documents and Settings\All Users\Application Data\Software AG\Entire Net-Work Client\
- In Windows 7 environments: ProgramData\Software AG\Entire Net-Work Client\
- In UNIX environments: \$SAG\wcl\.



Note: If you want to put your Entire Net-Work log files on a shared server, read [Directing Log Files to a Shared Server](#), elsewhere in this section. However, please be sure that the directory name you specify for the log files for each client is unique.

▶ **To specify the log file location:**

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

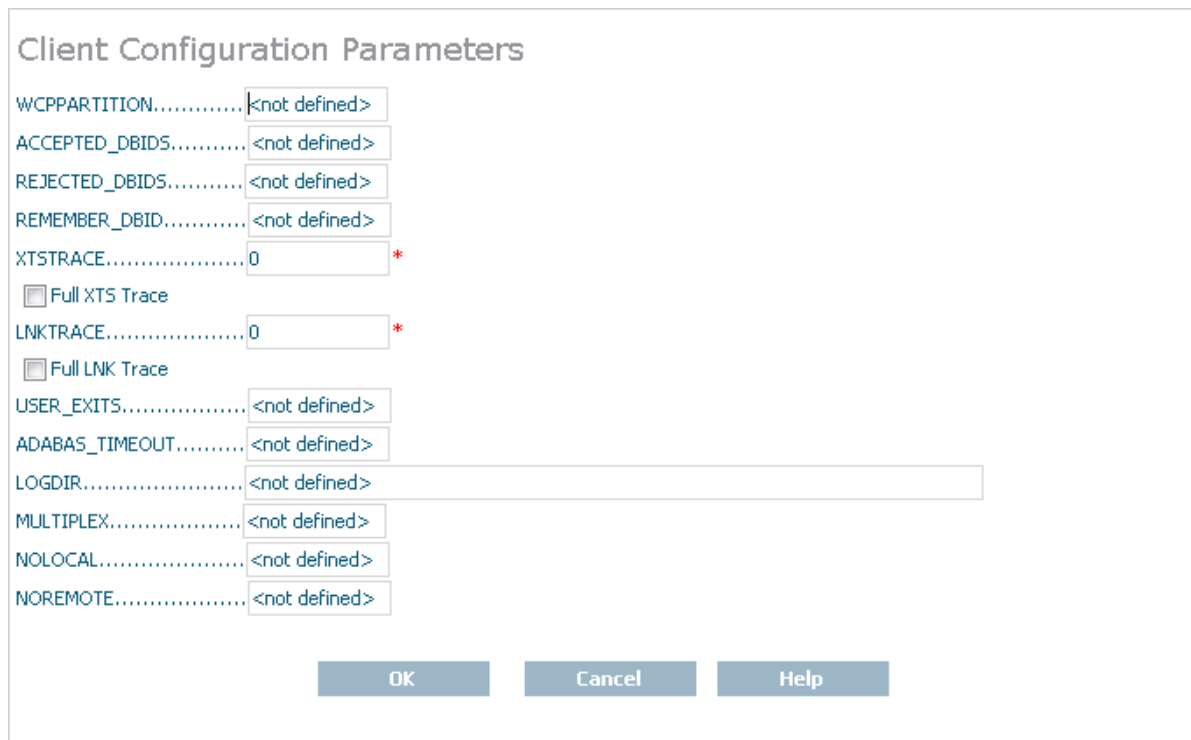
A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and expand the client machine on which the client is defined.

The client configuration section becomes available in tree-view.

- 4 Right-click on the client configuration whose log file location you want to modify and select **Set Client Configuration Parameters** from the resulting drop-down list.

The **Client Configuration Parameters** panel appears in detail-view.



- 5 Specify the fully-qualified path of the directory in which you want log files stored in the LOGDIR parameter. When all changes are made, click **OK** to save the setting.

The client parameters are updated in the appropriate Entire Net-Work Client configuration file.

40

Accessing Secured z/OS Host Resources

- Specifying the ESI Method and Appropriate Adabas SAF Security Kernel Parameters 146
- Accessing z/OS Resources Using the ESI Online Application 148
- Accessing z/OS Resources Using the ESI Security Exit 151

Entire Net-Work Client includes an External Security Interface (ESI) for ADASAF support that provides access to secured Adabas resources on a z/OS host node. To secure these resources on the host node, Adabas interacts with the Adabas SAF Security Kernel (ADASAF), an Adabas add-on product. ADASAF links Adabas to the CA-ACF2, CA-Top Secret, or RACF external security packages installed on the host system. For more information about the Adabas SAF Security Kernel, refer to its documentation.

The External Security Interface (ESI) provides two methods you can use to access secured Adabas resources on a z/OS host node:

- In Windows environments only, you can use an online application to log onto ESI.
- In any environment, you can use an ESI security exit. This method should be used in any environment where you want full control of obtaining the logon information. A sample security exit is provided with Entire Net-Work Client called *lnkxsaf*.

Specifying the ESI Method and Appropriate Adabas SAF Security Kernel Parameters

To select the External Security Interface method you prefer to use, you must set some parameters in the System Management Hub. In addition, regardless of the ESI method selected, you must set parameters that identify the Adabas SAF Security Kernel library and function that should be used for access to secured z/OS host resources.



Note: This section describes how to specify these parameters using the System Management Hub, but you can also specify them as environment variables instead.

▶ To set ESI method and Adabas SAF Security Kernel parameters:

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

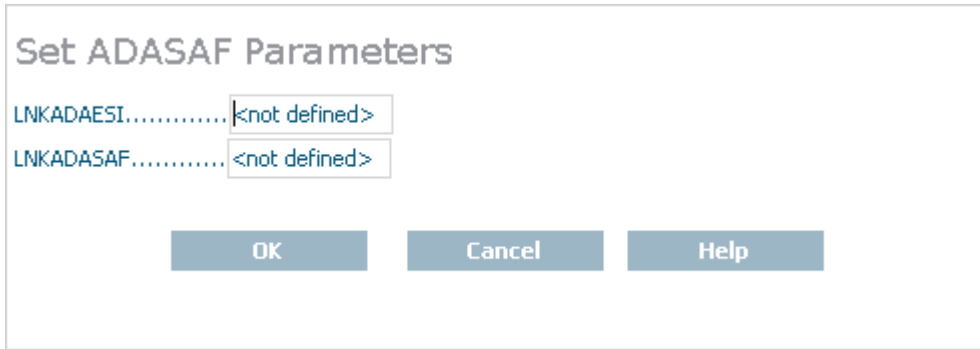
A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and expand the client machine on which the client is defined.

The client configuration section becomes available in tree-view.

- 4 Right-click on the client configuration whose parameters you want to maintain and select **Set Client Parameters** from the resulting drop-down list.

The **Set ADASAF Parameters** panel appears in detail-view.



- 5 Modify the parameters on the **ADASAF Parameters** panel, as described in the following table. When all parameters are set as you want, click **OK** to save them.

Parameter	Description	Required?	Default
LNKADAESI	This parameter is available for Windows systems only. Indicate whether the ESI online application should be used instead of a user exit. Valid values are "YES" (use the online application) or "NO" (use a user exit). The default is "NO". If LNKADAESI is set to "YES" and a value is given in LNKADASAF, the online application is used (LNKADAESI settings override LNKADASAF).	No	No
LNKADASAF	Specify the library and function names of the user exit that will provide access to the secured Adabas resource via the Adabas SAF Security Kernel (ADASAF). The library and function names should be specified with a space between them, using the following format: library function If no names are specified, ("<not defined>" is listed) and the value "lnkxsaf lnkxsaf" is used. (The lnkxsaf library is either <i>lnkxsaf.dll</i> or <i>lnkxsaf.so</i>).	No	A value of "lnkxsaf lnkxsaf" is used.

The parameters are updated in the appropriate Entire Net-Work Client configuration file.

Accessing z/OS Resources Using the ESI Online Application

When you elect to use the ESI online application to access Adabas secured resources, your ESI access information (user ID and password) must be supplied via an ESI logon dialog. The user ID and password you specify on the ESI logon dialog are encrypted and stored on the local node to confirm that you have logged onto ESI. They are then used by the Adabas SAF Security Kernel (ADASAF) when you attempt to use an application that accesses a secured Adabas resource. You can elect to use the ESI online application by setting the LNKADAESI parameter (or environment variable) to "YES". For more information, read [Specifying the ESI Method and Appropriate Adabas SAF Security Kernel Parameters](#), elsewhere in this section.



Note: Software AG strongly recommends that you modify the encryption/decryption method used to encrypt your ESI access information. The encryption/decryption algorithm you use must match the ones used on the mainframe. For more information, read [Encryption Method Modifications](#), elsewhere in this section.

This section covers the following topics:

- [Accessing the ESI Logon Dialog](#)
- [Automatic Logoff](#)
- [Encryption Method Modifications](#)

Accessing the ESI Logon Dialog

You can access the ESI logon dialog either manually or dynamically.


If you elect to access the ESI logon dialog dynamically, the Adabas SAF Security Kernel will issue a response code when you first attempt to access an Adabas secured resource. When the response code is returned, it is intercepted by Entire Net-Work Client and the ESI logon dialog appears. After supplying the logon information requested by the dialog (as explained later in this section, Entire Net-Work Client resubmits the request to the Adabas secured resource.

The user ID and password you specify on the ESI logon dialog are encrypted and stored on the local node to confirm that you have logged onto ESI. They are then used for any Adabas security checks that occur when you execute an application that requests access to Adabas-secured resources.

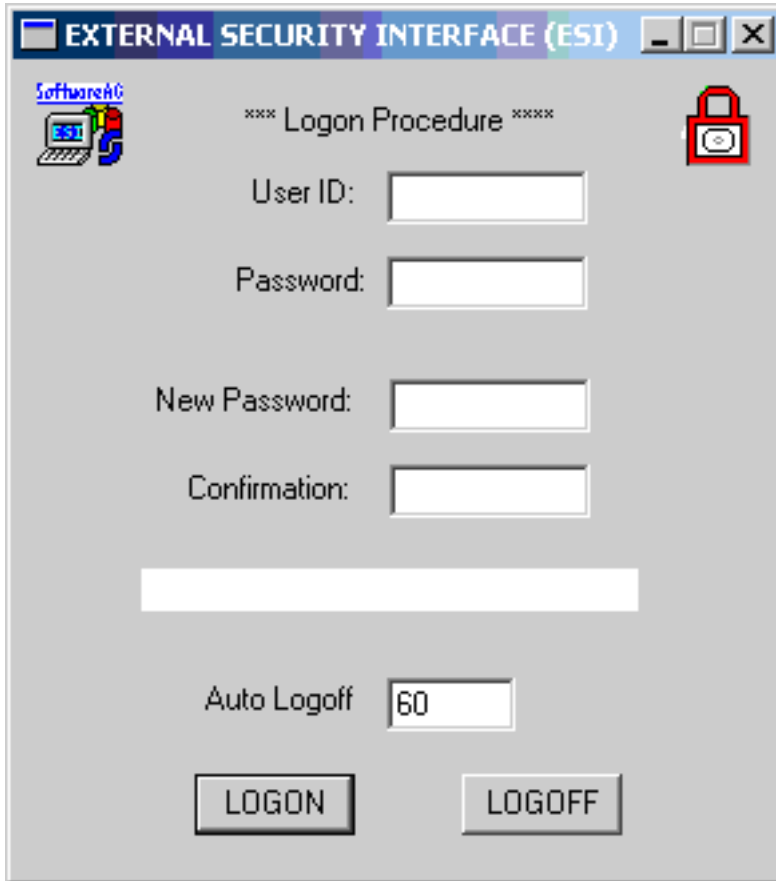
- If the security check is passed, the application is allowed to access those resources that are permitted according to your Adabas security user profile.
- If the security check is not passed, an Adabas security response code is returned to the application.

▶ **If you elect to access the ESI logon dialog manually, complete the following steps:**

- 1 Run the *ADAESI.EXE* executable file in the Entire Net-Work Client code directory.

 **Note:** You may want to add this to your *Startup* folder.

The ESI logon dialog appears, as shown below.



The screenshot shows a window titled "EXTERNAL SECURITY INTERFACE (ESI)". Inside the window, there is a "Logon Procedure" section. It includes four text input fields: "User ID:", "Password:", "New Password:", and "Confirmation:". Below these fields is a horizontal separator line. At the bottom of the window, there is an "Auto Logoff" field with the value "60" and two buttons labeled "LOGON" and "LOGOFF". A red padlock icon is located in the top right corner of the window.

- 2 Supply a valid user ID and password in the **User ID** and **Password** fields and then click **LOGON**. The user ID and password must correspond to those known to the external security package on the z/OS node.

Your ESI access information is encrypted and stored.

- 3 If your password has expired, the dialog contains the message "New Password Required" appears. Enter a new password in the **New Password** field and confirm the update in the **Confirmation** field.

Automatic Logoff

Once you have logged onto ESI, you can specify the amount of time, in minutes, that Adabas can remain inactive (no Adabas calls) before you are automatically logged out. This feature is provided to prevent unauthorized access to Adabas-secured resources when your PC is left unattended. To specify an automatic logoff time, specify a value from "0" (zero) to "1440" minutes (24 hours) in the Auto Logoff field on the ESI long dialog. The default value is 60 minutes.

- If the Auto Logoff value is "60", you are logged off of Adabas security after 60 minutes of Adabas inactivity. When you log on again, the security check is performed as if you were logging on for the first time.
- If the Auto Logoff value is "0", the automatic no automatic logoff occurs.

Encryption Method Modifications

The user ID and password you specify on the ESI logon dialog are encrypted and stored on the local node to confirm that you have logged onto ESI.



Notes:

1. Software AG strongly recommends that you modify the encryption/decryption code. The encryption/decryption algorithm you use must match the ones used on the mainframe.
2. In past versions of ESI, an *ADAESI.INI* file and ADAESIX parameter were used to modify the encryption/decryption algorithms. This file and parameter are no longer supported. Instead, you must use the procedure described in this section. In addition, Entire Net-Work Client no longer supports changing the *adacrypt.dll* library name.

▶ To modify the method used to encrypt and decrypt the ESI logon dialog information:

1. Locate and edit the user exit code supplied with your Entire Net-Work Client installation. The user exit, the encryption and decryption source code, and the files required to compile and link the source code are provided in the `\examples\adaesi_uexit` directory of the installation.
2. Modify the encryption and decryption code as required and then compile and link it using the files in the `\examples\adaesi_uexit` directory.



Note: Do not change the name of the DLL (*adacrypt.dll*) or the procedure name used in the encryption/decryption program.

Accessing z/OS Resources Using the ESI Security Exit

When you elect to use the ESI security exit to access an Adabas secured resource, the user exit must be supplied with the logon and other access information to ESI. This ESI access information is then used when you attempt to use an application that accesses a secured Adabas resource. You can elect to use the ESI online application by setting the LNKADAESI parameter (or environment variable) to blank or "NO" and specifying the ESI user exit library and function name in the LNKADASAF parameter (or environment variable). There is no default. For more information, read [Specifying the ESI Method and Appropriate Adabas SAF Security Kernel Parameters](#), elsewhere in this section.

▶ **To modify and use the ESI security exit:**

- 1 Locate and edit the user exit (the *lnkxsaf.c* file) supplied with your Entire Net-Work Client installation. The user exit and the files required to compile and link the source code are provided in the `\examples\adasaf_uexit` directory of the installation.
- 2 Modify the user exit as required and then compile and link it using the files in the `\examples\adasaf_uexit` directory.

Use the AdaSetSaf configuration tool to specify ESI access information to the user exit that will provide access to the secured Adabas resource via the Adabas SAF Security Kernel (ADASAF). This is the same information you supply using the ESI online application (read *Accessing z/OS Resources Using the ESI Online Application*, earlier in this section).

41

Using ADALNK User Exits

- Specifying the User Exit File and Function Names 154
- Modifying the User Exit Code 156

Entire Net-Work Client allows you to call user exits before and after ACB and ACBX direct calls, if the Adabas interface supports user exits.



Note: Before you attempt to use these ADALNK user exits, verify that the Adabas TP monitor interface supports user exits. If it does not, you cannot use the ACB and ACBX user exits provided with Entire Net-Work Client. If it does support user exits, you can use the exits described in this section. For more information, refer to the documentation for your Adabas TP monitor interface.

The user exits are not called for Adabas calls that are created by an Adabas utility or if the Adabas command is an internal SPT command (when the command ID starts with "SP" in the first two bytes and has "0xff" in the third byte). Note that the ADATST utility is handled as if it were a normal, non-utility Adabas user.

The before user exits (LNKUEX_0 and LNKUEX_ACBX_0) handling triggers an undocumented Natural feature; if the user exit is called and returns a non-zero response code, but the Adabas command is an RC command, the RC command is suppressed and a successful return is indicated to the calling program.

Samples of these user exits are provided with your Entire Net-Work Client installation.

This chapter describes how to set up the user exits.

Specifying the User Exit File and Function Names

To select the External Security Interface method you prefer to use, you must set some parameters in the System Management Hub. In addition, regardless of the ESI method selected, you must set parameters that identify the Adabas SAF Security Kernel library and function that should be used for access to secured z/OS host resources.



Note: This section describes how to specify these parameters using the System Management Hub, but you can also specify them as environment variables instead.

▶ To specify the user exit file and function names:

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and expand the client machine on which the client is defined.

The client configuration section becomes available in tree-view.

- 4 Right-click on the client configuration whose parameters you want to maintain and select **Set LNK User Exit Parameters** from the resulting drop-down list.

The **Set LNK User Exit Parameters** panel appears in detail-view.

- 5 Modify the parameters on the **LNK User Exit Parameters** panel, as described in the following table. When all parameters are set as you want, click **OK** to save them.



Note: Values should be specified for these parameters using the following format:

file_name;function_name

Parameter	Description	Required?	Default
LNKUEX_0	Specify the file and function names of the user exit that should be called <i>before</i> an Adabas ACB command is sent to the database. The file name is the name of a library located in the Entire Net-Work Client code directory; ADALNKX loads the library from the location you specify. LNKUEX_0 handling triggers an undocumented Natural feature; if the user exit is called and returns a non-zero response code, but the Adabas command is an RC command, the RC command is suppressed and a successful return is indicated to the calling program.	No	No user exit file and function names are called <i>before</i> an Adabas ACB command is sent to the database.
LNKUEX_1	Specify the file and function names of the user exit that should be called <i>after</i> an Adabas ACB	No	No user exit file and function names are

Parameter	Description	Required?	Default
	command is sent to the database. The file name is the name of a library located in the Entire Net-Work Client code directory; ADALNKX loads the library from the location you specify.		called <i>after</i> an Adabas ACB command is sent to the database.
LNKUEX_ACBX_0	Specify the file and function names of the user exit that should be called <i>before</i> an Adabas ACBX command is sent to the database. The file name is the name of a library located in the Entire Net-Work Client code directory; ADALNKX loads the library from the location you specify. LNKUEX_ACBX_0 handling triggers an undocumented Natural feature; if the user exit is called and returns a non-zero response code, but the Adabas command is an RC command, the RC command is suppressed and a successful return is indicated to the calling program.	No	No user exit file and function names are called <i>before</i> an Adabas ACBX command is sent to the database.
LNKUEX_ACBX_1	Specify the file and function names of the user exit that should be called <i>after</i> an Adabas ACBX command is sent to the database. The file name is the name of a library located in the Entire Net-Work Client code directory; ADALNKX loads the library from the location you specify.	No	No user exit file and function names are called <i>after</i> an Adabas ACBX command is sent to the database.

The parameters are updated in the appropriate Entire Net-Work Client configuration file.

Modifying the User Exit Code

Samples are provided of all of the Entire Net-Work Client ADALNK user exits.

► To modify and use the sample ADALNK user exits:

- 1 Locate and edit the user exit file supplied with your Entire Net-Work Client installation. The sample user exit and the files required to compile and link the source code are provided in one of the following Entire Net-Work Client installation directories:

Directory	Contains	Sample User Exit File Name
<i>\examples\acb_uexit</i>	The sample user exit and files required to compile and link the ADALNK ACB before and after user exits.	<i>lnkuex.c</i>
<i>\examples\acb_xuexit</i>	The sample user exit and files required to compile and link the ADALNK ACBX before and after user exits.	<i>lnkuexacb.c</i>

- 2 Modify the user exit as required and then compile and link it using the files in the appropriate directory.

42

Changing the Software AG Directory Server

- Changing the Software AG Directory Server for the Client Machine 160
- Changing the Software AG Directory Server for a Specific Client 161

Using SMH, you can change the Software AG Directory Server used by an Entire Net-Work Client or by a client machine. Be careful when you do this, however, so that connections used by clients are not broken.



Note: In general, Software AG recommends that you use only one Software AG Directory Server to ensure centralized administration.

Changing the Software AG Directory Server for the Client Machine

Using SMH, you can change the Software AG Directory Server used by a client machine. Be careful when you do this, however, so that connections used by the clients defined on the machine are not broken.



Note: In general, Software AG recommends that you use only one Software AG Directory Server to ensure centralized administration.

▶ To change the Software AG Directory Server for a client machine:

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and right-click on the client machine on which the client is defined. Then select the **Set Service Parameters** option from the resulting drop-down menu.

The **Set Client Service Parameters** panel appears in detail-view.

Set Client Service Parameters

SAGXTSDSHOST..... localhost

SAGXTSDSPORT..... 4952

CLIENT_NAME..... <not defined>

CLIENT_HOST..... <not defined>

CLIENT_PORT..... <not defined>

LOGDIR..... C:\ProgramData\Software AG\Entire Net-Work Client\logsvc14\

Update all Client Configurations

OK Cancel Help

- 4 In the SAGXTSDSHOST parameter, specify the Software AG Directory Server host name you want to use for this client machine.
- 5 In the SAGXTSDSPORT parameter, specify the port number of the Software AG Directory Server you specified in the SAGXTSDSHOST parameter.
- 6 When all parameters are specified, click **OK**. For more information about the other client parameters, read *Setting Client Parameters*, elsewhere in this guide.

The client machine will start using the requested Software AG Directory Server.

Changing the Software AG Directory Server for a Specific Client

Using SMH, you can change the Software AG Directory Server used by a specific client. Be careful when you do this, however, so that connections used by the client are not broken.



Note: In general, Software AG recommends that you use only one Software AG Directory Server to ensure centralized administration.

► To change the Software AG Directory Server for a specific client:

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.

- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

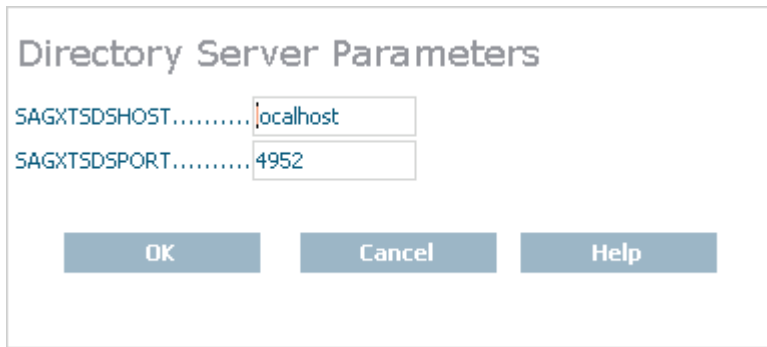
A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and expand the client machine on which the client configuration you want is defined.

The list of clients defined on the client machine appears.

- 4 Right-click on the client definition to which you want to assign an alternate Software AG Directory Server. Then select **Set Directory Server** from the resulting drop-down menu.

The **Directory Server Parameters** panel appears in detail-view.



- 5 In the SAGXTSDSHOST parameter, specify the Software AG Directory Server host name you want to use for this client.
- 6 In the SAGXTSDSPORT parameter, specify the port number of the Software AG Directory Server you specified in the SAGXTSDSHOST parameter.
- 7 When all parameters are specified, click **OK**.

The client will start using the requested Software AG Directory Server.

43 Tracing Entire Net-Work Client Processing

- Managing Client Service Tracing 164
- Managing Client Tracing 166
- Managing Software AG Transport Services Tracing 168
- Managing Software AG Communications Tracing 170


There are four kinds of trace processing that can occur when using Entire Net-Work Client:

- Traces can be performed for client service processing.
- Traces can be performed for client processing.
- Traces can be performed for Software AG transport services processing (XTSTRACE).
- Traces can be performed for Software AG communications processing (ADALNK).

Tracing should be used only for problem analysis. When you specify trace levels, large trace files will be stored on your disks and performance will be affected. Therefore, we recommend that you perform this function only under the advisement of your Software AG technical support representative.

Managing Client Service Tracing

Tracing should be used only for problem analysis. When you specify trace levels, large trace files will be stored on your disks and performance will be affected.

 **Caution:** We recommend that you perform this function only under the advisement of your Software AG support representative.

Once client configuration tracing is activated, the trace messages are written to the Entire Net-Work Client log file. For more information about the Entire Net-Work Client log file, read [Managing Entire Net-Work Client Log Files](#), elsewhere in this guide.

▶ To set the client service trace level and activate client tracing:

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Right-click the client machine you want from the list and select **Set Service Trace Granularity** from the resulting drop-down menu.

The **Set Service Trace Granularity** panel appears in detail-view.

Set Service Trace Granularity

Select any combination of trace levels; current settings are marked:

- Configuration, errors
- Connecting information
- Flow, errors
- Requests
- Replies
- Administration
- TCP/IP, SSL
- Internal information
- Send flow
- Receive flow
- Dump buffers
- No communication trace
- Trace All
- No Trace
- Ignore global settings

OK Cancel Help

- 4 Modify the trace level parameters on the **Set Service Trace Granularity** panel as requested by your Software AG technical support representative and then click **OK**.

The **Trace All**, **No Trace**, and **Ignore global settings** radio buttons are mutually exclusive selections. The **Trace All** and **No Trace** radio buttons are provided as *global* trace settings.

- If you select **Trace All**, data is collected for all of the trace levels listed on the panel, regardless of what you have selected (checked).
- If you select the **No Trace** radio button, data is collected for *none* of the trace levels listed on the panel, regardless of what you have selected (checked).
- The **Ignore global settings** radio button *must* be selected if you want to collect trace data for only some of the trace levels listed on the panel. This ensures that neither the **Trace All** and **No Trace** radio buttons are selected and indicates to Entire Net-Work that specific trace level data collection is requested.

The client service trace levels are set and activated.

Managing Client Tracing

Tracing should be used only for problem analysis. When you specify trace levels, large trace files will be stored on your disks and performance will be affected.



Caution: We recommend that you perform this function only under the advisement of your Software AG support representative.

Once client configuration tracing is activated, the trace messages are written to the Entire Net-Work Client log file. For more information about the Entire Net-Work Client log file, read [Managing Entire Net-Work Client Log Files](#), elsewhere in this guide.

▶ To set the client trace level and activate client tracing:

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and expand the client machine on which the client is defined.

The client configuration section becomes available in tree-view.

- 4 Right-click the client configuration you want from the list and select **Set Client Trace Granularity** from the resulting drop-down menu.

The **Set Client Trace Granularity** panel appears in detail-view.

Set Client Trace Granularity

Select any combination of trace levels; current settings are marked:

- Configuration, errors
- Connecting information
- Flow, errors
- Requests
- Replies
- Administration
- TCP/IP, SSL
- Internal information
- Send flow
- Receive flow
- Dump buffers
- No communication trace
- No ADABAS transactions trace
- Trace All
- No Trace
- Ignore global settings

- 5 Modify the trace level parameters on the **Set Client Trace Granularity** panel as requested by your Software AG technical support representative and then click **OK**.

The **Trace All**, **No Trace**, and **Ignore global settings** radio buttons are mutually exclusive selections. The **Trace All** and **No Trace** radio buttons are provided as *global* trace settings.

- If you select **Trace All**, data is collected for all of the trace levels listed on the panel, regardless of what you have selected (checked).
- If you select the **No Trace** radio button, data is collected for *none* of the trace levels listed on the panel, regardless of what you have selected (checked).
- The **Ignore global settings** radio button *must* be selected if you want to collect trace data for only some of the trace levels listed on the panel. This ensures that neither the **Trace All** and **No Trace** radio buttons are selected and indicates to Entire Net-Work that specific trace level data collection is requested.

The client trace levels are set and activated.

Managing Software AG Transport Services Tracing

Tracing should be used only for problem analysis. When you specify trace levels, large trace files will be stored on your disks and performance will be affected.



Caution: We recommend that you perform this function only under the advisement of your Software AG support representative.

Once Software AG transport services tracing is activated, the trace messages are written to the Entire Net-Work Client log file. For more information about the Entire Net-Work Client log file, read [Managing Entire Net-Work Client Log Files](#), elsewhere in this guide.

▶ **To set the Software AG transport services trace level and activate transport services tracing:**

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and expand the client machine on which the client is defined.

The client configuration section becomes available in tree-view.

- 4 In tree-view, under the client machine, right-click on the client configuration whose transport services trace level you want to set and select **Set Client Configuration Parameters** from the resulting drop-down list.

The **Client Configuration Parameters** panel appears in detail-view.

Client Configuration Parameters

WCPPARTITION..... <not defined>

ACCEPTED_DBIDS..... <not defined>

REJECTED_DBIDS..... <not defined>

REMEMBER_DBID..... <not defined>

XTSTRACE..... 0 *

Full XTS Trace

LNKTRACE..... 0 *

Full LNK Trace

USER_EXITS..... <not defined>

ADABAS_TIMEOUT..... <not defined>

LOGDIR..... <not defined>

MULTIPLY..... <not defined>

NOLOCAL..... <not defined>

NOREMOTE..... <not defined>

OK Cancel Help

- 5 Modify the **XTSTRACE** parameter and **Full XTS Trace** checkbox on the **Client Configuration Parameters** panel, as requested by your Software AG technical support representative. These parameters are described in the following table. When all parameters are set as you want, click **OK** to save them.

Parameter	Description	Required?	Default
Full XTS Trace	Click in this checkbox to set the XTSTRACE value to obtain full tracing of Software AG transport services processing. Do not check this checkbox unless specifically instructed to do so by a Software AG Customer Support representative. If you do, your installation could be overrun with trace messages that would be meaningless to you and would likely affect system performance.	No	Full tracing is not performed.
XTSTRACE	Set the hexadecimal XTS trace level using this parameter. This is the trace level for Software AG transport services. Valid values are hexadecimal values ranging from "0000" (no tracing) through "FFFE" (full tracing). Do not specify full tracing unless specifically instructed to do so by a Software AG Customer Support representative. If you do, your installation could be overrun with trace messages that would be meaningless to you and would likely affect system performance.	No	0000

The transport services trace levels are set and activated.

Managing Software AG Communications Tracing

Tracing should be used only for problem analysis. When you specify trace levels, large trace files will be stored on your disks and performance will be affected.



Caution: We recommend that you perform this function only under the advisement of your Software AG support representative.

Once Software AG communications tracing is activated, the trace messages are written to the Entire Net-Work Client log file. For more information about the Entire Net-Work Client log file, read [Managing Entire Net-Work Client Log Files](#), elsewhere in this guide.

▶ To set the Software AG communications trace level and activate communications tracing:

Make sure you have accessed the System Management Hub.

- 1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.
- 2 Select and expand **Clients** from the Entire Net-Work Client sublist.

A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 3 Select and expand the client machine on which the client is defined.

The client configuration section becomes available in tree-view.

- 4 In tree-view, under the client machine, right-click on the client configuration whose communications trace level you want to set and select **Set Client Configuration Parameters** from the resulting drop-down list.

The **Client Configuration Parameters** panel appears in detail-view.

Client Configuration Parameters

WCPPARTITION..... <not defined>

ACCEPTED_DBIDS..... <not defined>

REJECTED_DBIDS..... <not defined>

REMEMBER_DBID..... <not defined>

XTSTRACE..... 0 *

Full XTS Trace

LNKTRACE..... 0 *

Full LNK Trace

USER_EXITS..... <not defined>

ADABAS_TIMEOUT..... <not defined>

LOGDIR..... <not defined>

MULTIPLY..... <not defined>

NOLOCAL..... <not defined>

NOREMOTE..... <not defined>

OK Cancel Help

- 5 Modify the **LNKTRACE** parameter and **Full LNK Trace** checkbox on the **Client Configuration Parameters** panel, as requested by your Software AG technical support representative. These parameters are described in the following table. When all parameters are set as you want, click **OK** to save them.

Parameter	Description	Required?	Default
Full LNK Trace	Click in this checkbox to set the LNKTRACE value to obtain full tracing of ADALNK processing. Do not check this checkbox unless specifically instructed to do so by a Software AG Customer Support representative. If you do, your installation could be overrun with trace messages that would be meaningless to you and would likely affect system performance.	No	Full tracing is not performed.
LNKTRACE	Set the hexadecimal ADALNK trace level using this parameter. This is the trace level for Adabas calls. Valid values are hexadecimal values ranging from "00" (no tracing) through "f1 (full tracing)". Do not specify full tracing unless specifically instructed to do so by a Software AG Customer Support representative. If you do, your installation could be overrun with trace messages that would be meaningless to you and would likely affect system performance.	No	00

The communications trace levels are set and activated.

44 Entire Net-Work Service Function Utility (wcpadmin)

- Syntax 174
- Special Character Use 176
- Examples 176

The Entire Net-Work Service Function Utility allows you to perform some of the Entire Net-Work service functions in batch mode.

Syntax

The syntax of the wcpadmin function is:

```
wcpadmin {kernel-name| *} [function]
```

Specify one of the service functions (*function*) using the syntax listed in the following table.



Note: Please review the information on special character use with the wcpadmin function on Windows and UNIX systems. This is described in [Special Character Use](#), elsewhere in this section.

Function Name	Syntax	This function...
*	wcpadmin *	Displays the Entire Net-Work configuration on the machine.
add	wcpadmin kernel-name add node-name url	Allows you to add a connection to the kernel. The name of the Kernel, the node and the node's associated URL must be specified for this function.
connect	wcpadmin kernel-name connect node-name	Allows you to connect a node to the kernel. The name of the Kernel and the node name must be specified for this function.
disconnect	wcpadmin kernel-name disconnect node-name	Allows you to disconnect a node from the kernel. The name of the Kernel and the node name must be specified for this function.
showclients	wcpadmin kernel-name showclients [D R A [id]]	Allows you to view the clients on associated with the Kernel. The name of the Kernel must be supplied for this function. Optionally, supply one of the following: <ul style="list-style-type: none"> ■ D: Specify "D" to view the direct clients of the Kernel. ■ R: Specify "R"to view the relay clients of the Kernel. ■ A: Specify "A" to view the Adabas clients of the Kernel. When you specify "A", you can also specify a client ID (<i>id</i>) to view the details of a specific Adabas client.
showconnections	wcpadmin kernel-name showconnections	Allows you to view the existing connections of the Kernel and the connection status. The name of the Kernel must be specified for this function.
showdb	wcpadmin kernel-name showdb {* dbid}	Allows you to view all the databases on the Kernel or details about a specific database on the Kernel. The name of the Kernel must be supplied for this function. In

Function Name	Syntax	This function...
		addition, either an asterisk (*) or a specific database ID (<i>dbid</i>) must be specified.
showhosts	wcpadmin <i>kernel-name</i> showhosts [<i>hostname</i>]	Allows you to view the host names of known to the Kernel or statistics about a specific host. The name of the Kernel must be supplied for this function. Optionally, you can specify a specific host name (<i>hostname</i>) to view statistics about a specific host.
showlistens	wcpadmin <i>kernel-name</i> showlistens	Allows you to view the listen ports for the Kernel. The name of the Kernel must be supplied for this function.
shownodes	wcpadmin <i>kernel-name</i> shownodes [I O]	Allows you to view the Kernel's connections to nodes. The name of the Kernel must be supplied for this function. Optionally, specify "I" to view only incoming connections or "O" to view only outgoing connections. If you specify neither "I" nor "O", all connections are shown.
shownodestats	wcpadmin <i>kernel-name</i> shownodestats <i>node-name</i> {I O}	Allows you to view the Kernel connection statistics for a specific node. The name of the Kernel and the name of the node must be supplied for this function. In addition, you must specify "I" to view the statistics for the incoming connections of a node or "O" to view the statistics for the outgoing connections of a node.
showstats	wcpadmin <i>kernel-name</i> showstats	Allows you to view statistics for the Kernel. The name of the Kernel must be supplied for this function.
showstatus	wcpadmin { <i>kernel-name</i> *} showstatus	Allows you to view the status of a specific Kernel or of all Kernels. Specify either: <ul style="list-style-type: none"> ■ The name of a specific Kernel to review the status of that specific Kernel. ■ An asterisk (*) to review the status of all Kernels.
shutdown	wcpadmin { <i>kernel-name</i> *} shutdown	Shuts down (stops) a specific Kernel or all Kernels. Specify either: <ul style="list-style-type: none"> ■ The name of a specific Kernel to shut down. ■ An asterisk (*) to shut down all Kernels.
start	wcpadmin { <i>kernel-name</i> *} start	Starts a specific Kernel or all Kernels. Specify either: <ul style="list-style-type: none"> ■ The name of a specific Kernel to start. ■ An asterisk (*) to start all Kernels.
stopclients	wcpadmin <i>kernel-name</i> stopclients {D R A [<i>id</i>]}	Stops the clients of a Kernel based on type (direct clients, relay clients or Adabas clients). The name of the Kernel must be supplied for this function. In addition, supply one of the following:

Function Name	Syntax	This function...
		<ul style="list-style-type: none"> ■ D: Specify "D" to stop the direct clients of the Kernel. ■ R: Specify "R" to stop the relay clients of the Kernel. ■ A: Specify "A" to stop the Adabas clients of the Kernel. When you specify "A", you can optionally specify a client ID (<i>id</i>) to stop a specific Adabas client.
stophosts	<pre>wcpadmin kernel-name stophosts hostname</pre>	Stops all clients of a Kernel coming from a specific host. The name of the Kernel and the name of the host must be supplied for this function.

Special Character Use

In Windows environments, the ampersand [&], pipe [|] and parentheses [()] are special characters that must be preceded by the escape character [^] or passed within quotation marks ["] when they are used in arguments of the wcpadmin function.

In UNIX environments, characters that have special meaning to the shell (such as the greater than [>], less than [<], asterisk [*], question mark [?], pipe [|], and ampersand [&] symbols) are called *metacharacters*. The list of metacharacters varies depending on the UNIX shell in use. When used in arguments of the wcpadmin function, metacharacters should be passed within single quotes or preceded by a forward slash [/]. For example, `wcpadmin '*' start` or `wcpadmin /* start` are examples of the correct use of metacharacters in wcpadmin UNIX environment processing.

Examples

Examples for each of the wcpadmin functions are given in the following table.

Function Name	Example	Sample Output
*	<code>wcpadmin *</code>	<pre>Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG SERVICE=USAXXX2 SAGXTSDSHOST=localhost SAGXTSDSPORT=12731 Kernels Available ===== FRIED XXXXX SECOND V733VIS ===== WCPadmin exiting ...</pre>

Function Name	Example	Sample Output
add	wcpadmin XXXXX add FRIED TCPIP://localhost:8000	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Add Connection to FRIED on Kernel=XXXXX WCPadmin exiting ...
connect	wcpadmin XXXXX connect SECOND	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Connect Node=SECOND on Kernel=XXXXX WCP0628I Connect procedure has been initiated WCPadmin exiting ...
disconnect	wcpadmin XXXXX disconnect SECOND	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Disconnect Node=SECOND on Kernel=XXXXX WCP0629I Disconnect procedure has been initiated WCPadmin exiting ...
showclients	wcpadmin XXXXX showclients	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Show number of clients on Kernel=XXXXX Direct Clients 2 Adabas Contexts 2 Relay Clients 0 WCPadmin exiting ...
	wcpadmin XXXXX showclients D	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Direct Clients ClientId Host Port Dbid Elapsed Time 21 usaxxx2.YYY.ww.zzz 49155 1 0h:1m:3s WCPadmin exiting ...
	wcpadmin XXXXX showclients A	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Adabas Contexts ContextId Dbid Host Port Elapsed Time 7 1 usaxxx2.YYY.WW.ZZZ 49155 0h:1m:15s WCPadmin exiting ...

Function Name	Example	Sample Output
	wcpadmin XXXXX showclients A 7	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Adabas context Dbid 1 ClientId 21 NodeName usaxxx2 User usaxxx Pid 0x86868cc4 Host usaxxx2.YYY.WW.ZZZ Port 49155 Requests 16 Replies 15 Bytes In 1468 Bytes Out 1380 Elapsed Time 0h:2m:17s WCPadmin exiting ...
showconnections	wcpadmin XXXXX showconnections	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Show connections for Kernel=XXXXX TargNode Type Protocol Port A/M Status FRIED E-business TCPIP 8000 Auto Connection defined TEST E-business TCPIP 7000 Manual Connection defined SECOND E-business TCPIP 9000 Manual Disconnected RDHP1 Classic RDA 0 Manual Connected WCPadmin exiting ...
showdb	wcpadmin XXXXX showdb *	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Show DBIDs for Kernel=XXXXX DBID Node Type Status 168 RDHP1 Classic Active 159 RDHP1 Classic Active 158 RDHP1 Classic Active 140 RDHP1 Classic Active 86 RDHP1 Classic Active 59 RDHP1 Classic Active 1 XXXXX Local Active WCPadmin exiting ...

Function Name	Example	Sample Output
	wcpadmin XXXXX showdb 168	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Show DBID=168 on Kernel=XXXXX XXXXX Current Since startup Bytes in Requests 0 0 Bytes in Replies 0 0 Number of Requests 0 0 Number of Replies 0 0 Connections 1 WCPadmin exiting ...
showhosts	wcpadmin XXXXX showhosts	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Host Connections Disconnections Elapsed Time usamih2.YYY.WW.ZZZ 10 10 0h:46m:1s WCPadmin exiting ...
	wcpadmin XXXXX showhosts usaxxx2.YYY.WW.ZZZ	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Host usamih2.YYY.WW.ZZZ Count 0 Connections 10 Disconnections 10 Requests 122 Replies 102 Bytes In 11225 Bytes Out 9384 Elapsed Time 0h:46m:20s WCPadmin exiting ...
showlistens	wcpadmin XXXXX showlistens	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Show listens for Kernel=XXXXX Name Protocol Port Status Client Access TCPIP 49155 Running E-Business Access TCPIP 8000 Running SMH Server TCPIP 49154 Running WCPadmin exiting ...

Function Name	Example	Sample Output																																						
shownodes	wcpadmin XXXXX shownodes	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Show nodes on Kernel=XXXXX <table border="1"> <thead> <tr> <th>Target</th> <th>Type</th> <th>0/I</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>SECOND</td> <td>E-Business</td> <td>I</td> <td>Active</td> </tr> <tr> <td>FRIED</td> <td>E-Business</td> <td>0</td> <td>Inactive</td> </tr> <tr> <td>TEST</td> <td>E-Business</td> <td>0</td> <td>Inactive</td> </tr> <tr> <td>SECOND</td> <td>E-Business</td> <td>0</td> <td>Inactive</td> </tr> <tr> <td>RDHP1</td> <td>Classic</td> <td>0</td> <td>Inactive</td> </tr> </tbody> </table> WCPadmin exiting ...	Target	Type	0/I	Status	SECOND	E-Business	I	Active	FRIED	E-Business	0	Inactive	TEST	E-Business	0	Inactive	SECOND	E-Business	0	Inactive	RDHP1	Classic	0	Inactive														
Target	Type	0/I	Status																																					
SECOND	E-Business	I	Active																																					
FRIED	E-Business	0	Inactive																																					
TEST	E-Business	0	Inactive																																					
SECOND	E-Business	0	Inactive																																					
RDHP1	Classic	0	Inactive																																					
shownodestats	wcpadmin XXXXX shownodestats RDHP1 0	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG XXXXX Current <table border="1"> <thead> <tr> <th colspan="2">Since Startup</th> </tr> </thead> <tbody> <tr> <td>Bytes received</td> <td>128</td> </tr> <tr> <td>0</td> <td></td> </tr> <tr> <td>Bytes sent</td> <td>128</td> </tr> <tr> <td>0</td> <td></td> </tr> <tr> <td>Requests received</td> <td>3</td> </tr> <tr> <td>0</td> <td></td> </tr> <tr> <td>Requests sent</td> <td>2</td> </tr> <tr> <td>0</td> <td></td> </tr> <tr> <td>Incoming connections</td> <td>N/A</td> </tr> <tr> <td>0</td> <td></td> </tr> <tr> <td>Outgoing connections</td> <td>N/A</td> </tr> <tr> <td>1</td> <td></td> </tr> <tr> <td>Admin msgs received</td> <td>3</td> </tr> <tr> <td>0</td> <td></td> </tr> <tr> <td>Admin msgs sent</td> <td>2</td> </tr> <tr> <td>0</td> <td></td> </tr> <tr> <td>Errors</td> <td>0</td> </tr> <tr> <td>0</td> <td></td> </tr> </tbody> </table> WCPadmin exiting ...	Since Startup		Bytes received	128	0		Bytes sent	128	0		Requests received	3	0		Requests sent	2	0		Incoming connections	N/A	0		Outgoing connections	N/A	1		Admin msgs received	3	0		Admin msgs sent	2	0		Errors	0	0	
Since Startup																																								
Bytes received	128																																							
0																																								
Bytes sent	128																																							
0																																								
Requests received	3																																							
0																																								
Requests sent	2																																							
0																																								
Incoming connections	N/A																																							
0																																								
Outgoing connections	N/A																																							
1																																								
Admin msgs received	3																																							
0																																								
Admin msgs sent	2																																							
0																																								
Errors	0																																							
0																																								
showstats	wcpadmin XXXXX showstats	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Get statistics for Kernel=XXXXX <table border="1"> <thead> <tr> <th colspan="2">Statistics for Kernel XXXXX</th> </tr> </thead> <tbody> <tr> <td>Accumulated Node Count</td> <td>4</td> </tr> <tr> <td>Databases</td> <td>1</td> </tr> <tr> <td>Adabas Calls Processed</td> <td>102</td> </tr> <tr> <td>Classic Nodes</td> <td>1</td> </tr> <tr> <td>Classic Messages</td> <td>0</td> </tr> <tr> <td>e-Business Messages</td> <td>122</td> </tr> <tr> <td>e-Business Contexts</td> <td>10</td> </tr> <tr> <td>Active Clients</td> <td>0</td> </tr> <tr> <td>Relay Messages</td> <td>0</td> </tr> <tr> <td>Memory Allocations</td> <td>64</td> </tr> </tbody> </table>	Statistics for Kernel XXXXX		Accumulated Node Count	4	Databases	1	Adabas Calls Processed	102	Classic Nodes	1	Classic Messages	0	e-Business Messages	122	e-Business Contexts	10	Active Clients	0	Relay Messages	0	Memory Allocations	64																
Statistics for Kernel XXXXX																																								
Accumulated Node Count	4																																							
Databases	1																																							
Adabas Calls Processed	102																																							
Classic Nodes	1																																							
Classic Messages	0																																							
e-Business Messages	122																																							
e-Business Contexts	10																																							
Active Clients	0																																							
Relay Messages	0																																							
Memory Allocations	64																																							

Function Name	Example	Sample Output
		Memory Frees 20 WCPadmin exiting ...
showstatus	wcpadmin XXXXX showstatus	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG XXXXX Active WCPadmin exiting ...
	wcpadmin * showstatus	Software AG Entire Net-Work Server, Copyright ©) 1997-2010 by Software AG Kernels Status FRIED Inactive XXXXX Active SECOND Inactive V733VIS Inactive ===== WCPadmin exiting ...
shutdown	wcpadmin SECOND shutdown	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Shutdown Kernel=SECOND for WCP Service=USAXXX2 Shutdown Kernel=SECOND Service=USAXXX2 has been submitted WCPadmin exiting ...
start	wcpadmin SECOND start	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Start Kernel=SECOND for WCP Service=USAXXX2 WCPadmin exiting ...
stopclients	wcpadmin XXXXX showclients D	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Direct Clients ClientId Host Port Dbid Elapsed Time 47 usamih2.XXX.wv.zzz 49155 1 0h:0m:46s WCPadmin exiting ...
	wcpadmin XXXXX stopclients D 47	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG Stop direct client=47 WCPadmin exiting ...

Function Name	Example	Sample Output
stophosts	wcpadmin XXXXX stophosts usxxx2.XXX.WW.ZZZ	Software AG Entire Net-Work Server, Copyright ©) 1997-2011 by Software AG WCPadmin exiting ...

45

Using the Entire Net-Work User Exit Interface

▪ Writing User Exits	184
▪ Storing User Exit Library Files	185
▪ User Exit Processing and Functions in Windows Environments	185
▪ User Exit Processing and Functions in UNIX Environments	196

The Entire Net-Work user exit interface supports the implementation of user-written programs that perform the following types of functions:

- Compression and decompression of message data to optimize line transmission.
- Tailored statistical information gathering.
- Encryption and decryption of message data using an independent hardware or software formula.
- Control over the connection process, both inbound and outbound, based on local security requirements.
- Detection of node disconnections so that site-specific actions can be performed; for example, activation of a watchdog security function.

Entire Net-Work user exits can be implemented on all open systems platforms where Entire Net-Work is supported. Compiled user exit code is placed in a library where it can be accessed by Entire Net-Work when required.

Writing User Exits

User exits must be written in C and must use C calling conventions. If you wish, you can use the files from the supplied user exit examples as a basis.

Note the following additional restrictions, when writing your own user exit:

1. The destination buffer cannot be larger than the source buffer. Therefore, a message that is compressed or encrypted by a user exit must not exceed the size of the original message.
2. Data that has been modified by a user exit must be restored to its original form before being processed again by another Entire Net-Work Client node. For example, if you use a user exit to encrypt a message sent from an Entire Net-Work Client, you must use a corresponding user exit to decrypt the message before it can be processed by another server.

Once your user exit has been written, it and any files it requires must be built and compiled into a user exit library (a DLL file) on Windows systems or a shared library on UNIX systems before Entire Net-Work Client can use it. Entire Net-Work Kernel and Entire Net-Work Client configurations reference user exit DLL file or shared library names in their definitions.

Storing User Exit Library Files

Windows compiled user exit libraries (DLL files) or UNIX user exit shared libraries should be stored in the installation directory wherever the other executable and library files for Entire Net-Work Server or Entire Net-Work Client are installed (as appropriate for the user exit). By default, Entire Net-Work Server and Entire Net-Work Client user exit files should be stored in one of the following locations:

- In Windows environments for Entire Net-Work Server: `Program Files\Software AG\Entire Net-Work Server\vn`, where *nn* is the release number
- In Windows environments for Entire Net-Work Client: `Program Files\Software AG\Entire Net-Work Client`
- In UNIX environments: `$SAG\ppp\vn`, where *nn* is the release number of Entire Net-Work Client or Entire Net-Work Server and *ppp* is either "wcl" (for Entire Net-Work Client) or "wcp" (for Entire Net-Work Server).

In addition, user exit libraries should be stored in the root directory; they should not be stored in the *examples* subdirectory of the Entire Net-Work Client installation.



Important: It is a good idea to keep copies of your user exit libraries in a separate location from your Entire Net-Work installations.

User Exit Processing and Functions in Windows Environments

Entire Net-Work provides a user exit entry point (UE_Y) for every Entire Net-Work Kernel definition and every Entire Net-Work Client configuration. This user exit entry point is called from the transport layer protocol. At various times during processing, Entire Net-Work calls the user exit, passing it a structure that contains a function code and various optional data elements. The user exit program performs the desired function and returns a success or error indicator to Entire Net-Work.



Note: Modification of data traffic (compression or encryption) requires processor cycles on both sending and receiving nodes. The User Exit Facility may be unsuitable in situations where processor performance is critical. Its use on relay nodes is not recommended.

This section covers the following topics:

- [Calling the User Exit](#)
- [User Exit Control Block Structure](#)
- [Windows User Exit Responses](#)
- [Windows Tracing, Debugging, or Dumping User Exit Processing](#)

- [User Exit Windows Functions](#)
- [Windows User Exit Examples](#)

Calling the User Exit

The syntax of a user exit call in Windows environments is:

```
LONG UE_Y(pUEYCB_control)
```

where *pUEYCB_control* is a pointer to the user exit control block (UEYCB).

User Exit Control Block Structure

The following table describes the user exit control block (UEYCB). For a full description of UEYCB, review the example user exit file *user_exit.h*, as described in [Windows User Exit Examples](#), elsewhere in this section. Each user exit function must comply with this control block structure.

Element	Type	Description
Function	byte	The name of user exit function being processed by the call. Valid values include "UE_INIT", "UE_CON_OUT", "UE_CON_IN", "UE_SEND", "UE_RECV", "UE_DISCON", and "UE_TERM". For more information about each of these functions, read User Exit Functions , elsewhere in this section.
LineDriver	byte	The name of the transport protocol used by the call. At this time, the only valid value is "UE_D_TCP", indicating that TCP/IP is used.
Source	pvoid	The pointer to the source buffer; that is, the buffer used to contain the data to be processed by the user exit.
Slen	long	The size of the source buffer, which equals the length of the source data.
Dest	pvoid	The pointer to the destination buffer; that is, the buffer used to return data that has been modified by the user exit. Entire Net-Work is responsible for allocation and management of this buffer. The user exit should not attempt to free it.
Context	dword	A unique identifier supplied by Entire Net-Work for each connection.
Length	long	The length of the modified data message in the destination buffer.
MaxLength	long	The maximum size of the destination buffer. The destination buffer cannot be larger than the size of the source buffer.
Domain[6+1]	char	Not used.
Host[8+1]	char	Not used.
Argument	pvoid	Not used.
LD_Data	pvoid	Not used.
Model	pvoid	Not used.



Note: The user exit must not modify the contents of the Context element in the control block. It will be required for later use in send/receive calls. For an example of a user exit source

code file, review the supplied example file *user_exit.c*, described in [Windows User Exit Examples](#), elsewhere in this section.

Windows User Exit Responses

The response from the user exit may include one of the return codes described in the table below. The specific meaning of these return codes varies, based on the user exit function you are trying to perform. To interpret these return codes, read about the user exit function you are using in [User Exit Functions](#), elsewhere in this section.

Response	Description
UE_DATAOUT	The user exit function processes a modified data message in an intermediate buffer. The control block's Length element contains the length of this message.
UE_FAILURE	The user exit function fails and a message is written to the log file.
UE_RESTRICT	The user exit connection is allowed to continue to function on a restricted basis (only the UE_DISCON function is enabled for the exit).
UE_SUCCESS	The requested user exit function is successful.

Windows Tracing, Debugging, or Dumping User Exit Processing

You can include any trace, debug, or dump information pertaining to your user exit in the Entire Net-Work log file. To do this, use one of the following Software AG Transport Subsystem trace functions listed in the user exit file *user_exit.h*, as described in [Windows User Exit Examples](#), elsewhere in this section. Each user exit function must comply with this control block structure.

- XtsDump
- XtsDump_ex
- XtsTrace
- XtsDebug

In addition to using any of these functions in your user exit, you should be sure to include the *xts2.lib* file in your user exit library. If you do not, the trace, debug, or dump processing will not occur. The *xts2.lib* file is supplied in the sample user exit supplied with Entire Net-Work. For more information, read [Windows User Exit Examples](#), elsewhere in this section.

If you need additional assistance with tracing, debugging, or dumping your user exit processing, contact your Software AG technical support representative.

User Exit Windows Functions

This section describes the available user exit functions, in order of normal use.

- UE_INIT Function
- UE_CON_OUT Function
- UE_CON_IN Function
- UE_SEND Function
- UE_RECV Function
- UE_DISCON Function
- UE_TERM Function

UE_INIT Function

The UE_INIT function is called once during Entire Net-Work startup (before remote connections are enabled) to allow the user exit to allocate resources for this session of Entire Net-Work and to describe its capabilities to Entire Net-Work. Software AG strongly recommends that a reason message be written to the log file if an initialization attempt fails.

Prior to user exit processing, the contents of the UEYCB elements should be:

pUEYCB	Contents
Function	UE_INIT
LineDriver	Zero
Source	NULL
Slen	Zero
Dest	NULL
Context	Zero
Length	Zero
MaxLength	Zero
Domain	not applicable
Host	not applicable
Argument	not applicable
LD Data	not applicable
Model	not applicable

The user exit should supply one of the following return codes to indicate processing results:

Response	Description
UE_FAILURE	Enable all future user exit calls.
UE_SUCCESS	Disable all future user exit calls (including UE_TERM) and write a message to the log file.

UE_CON_OUT Function

The UE_CON_OUT function is called once for each outbound connection attempt. The user exit can accept the connection attempt, accept the connection but restrict user exit functions, or reject the connection and terminate the connection process.

Software AG strongly recommends that a reason message be written to the log file if a connection attempt is rejected. Because rejection of an outbound connection attempt is unlikely, this function is normally used to allocate statistical recording memory and other resources. It is also the point at which DES encryption hardware is allocated, if it is being used.

Prior to user exit processing, the contents of the UEYCB elements should be:

pUEYCB	Contents
Function	UE_CON_OUT
LineDriver	Protocol type
Source	NULL
Slen	Zero
Dest	NULL
Context	Non-zero
Length	Zero
MaxLength	Zero
Domain	not applicable
Host	not applicable
Argument	not applicable
LD Data	not applicable
Model	not applicable

The user exit should supply one of the following return codes to indicate processing results:

Response	Description
UE_FAILURE	Terminate the connection process and a write a message to the log file.
UE_RESTRICT	Continue the connection process on a restricted basis and enable the exit for UE_DISCON functions, but not for the UE_SEND or UE_RECV functions.
UE_SUCCESS	Continue the connection process and enable this exit for UE_SEND, UE_RECV, and UE_DISCON functions for this node.

UE_CON_IN Function

The UE_CON_IN function is called during inbound connection processing. The user exit can accept the connection, accept the connection but restrict user exit functions, or reject the connection for security reasons.

Software AG strongly recommends that a reason message be written to the log file if a connection attempt is rejected. If the connection is accepted, the user exit should allocate the resources and memory required for the connection.

Prior to user exit processing, the contents of the UEYCB elements should be:

pUEYCB	Contents
Function	UE_CON_IN
LineDriver	Protocol type
Source	NULL
Slen	Zero
Dest	NULL
Context	Non-zero
Length	Zero
MaxLength	Zero
Domain	not applicable
Host	not applicable
Argument	not applicable
LD Data	not applicable
Model	not applicable

The user exit should supply one of the following return codes to indicate processing results:

Response	Description
UE_FAILURE	Reject the connection and write a message to the log file.
UE_RESTRICT	Accept the connection on a restricted basis and enable the user exit for UE_DISCON functions, but not for UE_SEND or UE_RECV functions.
UE_SUCCESS	Accept the connection and enable the user exit for UE_SEND, UE_RECV, and UE_DISCON functions.

UE_SEND Function

The UE_SEND function is called before a data message is transmitted to a remote node. The user exit can send the message, modify the message before sending it, or reject the message and force disconnection of the node. Software AG strongly recommends that a reason message be written to the log file if the message is rejected.

UE_INIT and either UE_CON_IN or UE_CON_OUT must have been successful (returned response "UE_SUCCESS") for this node before the UE_SEND function can be run.

Prior to user exit processing, the contents of the UEYCB elements should be:

pUEYCB	Contents
Function	UE_SEND
LineDriver	Protocol type.
Source	Pointer to the source buffer containing the data message to be transmitted.
Slen	Length of the source data.
Dest	Pointer to the destination buffer.
Context	Unique connection ID supplied by Entire Net-Work during the connection.
Length	Zero (see the "UE_DATAOUT" return code)
MaxLength	Maximum size of the user exit buffer.
Domain	not applicable
Host	not applicable
Argument	not applicable
LD Data	not applicable
Model	not applicable

The user exit should supply one of the following return codes to indicate processing results:

Response	Description
UE_DATAOUT	Send the modified data message in the destination buffer. The Length element contains the length of the message.
UE_FAILURE	Reject the message, force a disconnection of the node, and write a message to the log file.
UE_SUCCESS	Send the unmodified source data.

UE_RECV Function

The UE_RECV function is called when a data message that was modified before transmission arrives from a remote node. The user exit can accept the message for processing, modify the message, or discard the message and force disconnection of the node. Software AG strongly recommends that a reason message be written to the log file if the message is discarded.

Prior to user exit processing, the contents of the UEYCB elements should be:

pUEYCB	Contents
Function	UE_RECV
LineDriver	Protocol type
Source	Pointer to the buffer containing the data message received.
Slen	Length of the data received.
Dest	Pointer to the user exit buffer, which contains the data message when and if it is modified by the user exit.
Context	Unique connection ID supplied by Entire Net-Work during the connection.
Length	The original message length (see the UE_DATAOUT return code).
MaxLength	The maximum size of the user exit buffer.
Domain	not applicable
Host	not applicable
Argument	not applicable
LD Data	not applicable
Model	not applicable

The user exit should supply one of the following return codes to indicate processing results:

Response	Description
UE_DATAOUT	Process the modified message contained in the user exit buffer. The Length element contains the length of the message.
UE_FAILURE	Discard the message, force the disconnection of the node, and write a message to the log file.
UE_SUCCESS	Continue processing the source data.

UE_DISCON Function

The UE_DISCON function is called once immediately after a node is disconnected for any reason. The user exit can release resources allocated during a connection call, log statistical information, and initiate actions to reestablish the connection (activate a watchdog security function).

Prior to user exit processing, the contents of the UEYCB elements should be:

pUEYCB	Contents
Function	UE_DISCON
LineDriver	Protocol type
Source	NULL
Slen	Zero
Dest	NULL
Context	Unique connection ID supplied by Entire Net-Work during the connection.
Length	Zero
MaxLength	Zero
Domain	not applicable
Host	not applicable
Argument	not applicable
LD Data	not applicable
Model	not applicable

Return codes for the UE_DISCON function are ignored.

UE_TERM Function

The UE_TERM function is called once during Entire Net-Work shutdown processing. It allows the user exit to release resources allocated during UE_INIT function processing and to log statistical data prior to shutdown.

Prior to user exit processing, the contents of the UEYCB elements should be:

pUEYCB	Contents
Function	UE_TERM
LineDriver	Zero
Source	NULL
Slen	Zero
Dest	NULL
Context	Zero
Length	Zero

pUEYCB	Contents
MaxLength	Zero
Domain	not applicable
Host	not applicable
Argument	not applicable
LD Data	not applicable
Model	not applicable

Return codes for the UE_TERM function are ignored.

Windows User Exit Examples

The Entire Net-Work Client installation kit includes several example user exits in a series of sub-directories in the *examples* subdirectory:

Subdirectory	Contains
<i>acb_uexit</i>	An ADALNK user exit. This user exit is called before an Adabas call is processed (ADALNK interface) and it rejects all Adabas operator calls whose user is not SAG. In addition, it blocks N1/N2 and A1 commands for the user SAG. Response code 22 is set when any of these call restrictions in encountered.
<i>acbx_uexit</i>	An ADALNKX user exit. This user exit is called before an Adabas call is processed (ADALNKX interface) and it rejects all Adabas operator calls whose user is not SAGPC. In addition, it blocks N1/N2 and A1 commands for the user SAGPC. A return value of ADA_UEXREJ is set when any of these call restrictions in encountered.
<i>adaesi_uexit</i>	An External Security Interface (ESI) user exit you can use to modify the method used to encrypt and decrypt the ESI logon dialog information, read .
<i>adasaf_uexit</i>	An External Security Interface (ESI) user exit you can use to access secured Adabas resources on a z/OS host node. For more information, read .
<i>wcl_uexit</i>	An example user exit and a shared library stub. These are provided to assist you in creating and implementing your user exit program.

The remainder of this section describes the files and compilation method you can use to create and compile your own user exit, based on the files in the *wcl_uexit* subdirectory.

- [acb_uexit Example User Exit Files](#)
- [acbx_uexit Example User Exit Files](#)
- [wcl_uexit Example User Exit Files](#)

- [Compiling the Example User Exit Files](#)

acb_uexit Example User Exit Files

The *examples/acb_uexit* subdirectory contains all of the necessary source code files to make a working example of an ADALNK user exit program, as described in the following table:

File Name	Description
<i>adabas.h</i>	Adabas call resource file. This file lists resources files that should be included when the user exit is compiled.
<i>adabasx.h</i>	Adabas call control block file.
<i>lnkuex.c</i>	ADALNK user exit source code file.
<i>lnkuex.h</i>	ADALNK user exit control block layout file.
<i>makefile</i>	C program to be run in Windows and used to create the user exit library from the files in the user exit source code library.
<i>makefile.ux</i>	C program to be run in UNIX and used to create the user exit library from the files in the user exit source code library.
<i>mk.bat</i>	A batch file that runs nmake on the <i>makefile</i> file.

You can use these files as a model for writing your own ADALNK user exit programs. The supplied ADALNK user exit program is called before an Adabas call is processed (ADALNK interface) and it rejects all Adabas operator calls whose user is not SAG. In addition, it blocks N1/N2 and A1 commands for the user SAG. Response code 22 is set when any of these call restrictions in encountered.

acbx_uexit Example User Exit Files

The *examples/acbx_uexit* subdirectory contains all of the necessary source code files to make a working example of an ADALNKX user exit program, as described in the following table:

File Name	Description
<i>adabas.h</i>	Adabas call resource file. This file lists resources files that should be included when the user exit is compiled.
<i>adabasx.h</i>	Adabas call control block file.
<i>lnkuexacbx.c</i>	ADALNKX user exit source code file.
<i>lnkuexacbx.h</i>	ADALNKX user exit control block layout file.
<i>makefile</i>	C program to be run in Windows and used to create the user exit library from the files in the user exit source code library.
<i>makefile.ux</i>	C program to be run in UNIX and used to create the user exit library from the files in the user exit source code library.
<i>mk.bat</i>	A batch file that runs nmake/make on the <i>makefile</i> file.

You can use these files as a model for writing your own ADALNKX user exit programs. The supplied ADALNKX user exit is called before an Adabas call is processed (ADALNKX interface) and it rejects all Adabas operator calls whose user is not SAGPC. In addition, it blocks N1/N2 and A1 commands for the user SAGPC. A return value of ADA_UEXREJ is set when any of these call restrictions in encountered.

wcl_uexit Example User Exit Files

The *examples/wcl_uexit* subdirectory contains all of the necessary source code files to make a working example of a user exit program, as described in the following table:

File Name	Description
<i>user_exit.c</i>	User exit source code file.
<i>user_exit.rc</i>	User exit stub resource file. This file lists resource files that should be included when the user exit is compiled.
<i>user_exit.def</i>	User exit module definition file.
<i>user_exit.h</i>	User exit control block layout file.
<i>makefile</i>	C program used to create the user exit library from the files in the user exit source code library.
<i>xts2.lib</i>	If you need to make use of the Software AG transport subsystems's dump, trace and debug facilities in your code, include this file in your user exit library.

You can use these files as a model for writing your own user exit programs.

Compiling the Example User Exit Files

► To compile a user exit into a user exit library in Windows environments:

- Navigate to the appropriate installation directory and enter the following command:

```
nmake -f makefile
```

The appropriate user exit library (*.dll file) is generated.

User Exit Processing and Functions in UNIX Environments

The UNIX user exit shared library must contain an entry point, "ph_uexit", that will be called by the protocol handler processes.

This section covers the following topics:

- [Calling the User Exit](#)
- [UNIX User Exit Return Codes](#)
- [Processing](#)

- UNIX User Exit Examples

Calling the User Exit

The syntax of a user exit call in UNIX environments is:

```
int ph_uexit (int fct_id, char *source, int slen, char *dest, int dlen);
```



Note: The shared library's entry point function *must* be "ph_uexit".

This syntax uses the following call parameters and return codes:

Parameter	Description
int <i>fct_id</i>	The number of the user exit function to be run. Current valid values for <i>fct_id</i> are: <ul style="list-style-type: none"> ■ 0: The user exit is called by the send process before sending a buffer. ■ 1: The user exit is called by the receive process after receiving a buffer.
char * <i>source</i>	The pointer to the source buffer. The source buffer contains either original data to be sent or data just received.
int <i>slen</i>	The number of bytes in the source buffer.
char * <i>dest</i>	The pointer to a free (destination) buffer to be used by the requested user exit function to store the manipulated data from the source buffer.
int <i>dlen</i>	The size of the destination buffer (which must equal the length of the original message).

UNIX User Exit Return Codes

The response from the user exit may include one of the return codes described in the table below.

Value	Description
-1	An error occurred. The user exit call failed.
Anything greater than 0 (>0)	The user exit call was successful. The return value is the length of the data in the destination buffer.

Processing

If user exit usage is enabled, the *ph_uexit* function is called by the protocol handler processes either just before starting to send a data buffer to a remote node or just after receiving a data buffer from a remote node. The protocol handler provides the data to be manipulated by the user exit in the buffer referenced by the source pointer, and expects the user exit's output to be in the buffer referenced by the destination pointer. The sizes of these buffers is passed to the user exit in the *slen* or *dlen* parameters, as appropriate. The user exit routines must ensure that there is no address violation when accessing these buffers.

On successful completion of the user exit call, the *ph_uexit* routine must return the length of data put into the destination buffer. If an error occurs, *ph_uexit* must return -1 to indicate the failure to the calling protocol handler processes.

When the *ph_uexit* routine is called during send processing, and a value greater than zero (0) is returned, the information from the destination buffer with the length returned by the *ph_uexit* is sent instead of the information in the source buffer. At the remote (destination) node, the user exit will be called for this buffer.

UNIX User Exit Examples

The Entire Net-Work Client installation kit includes several example user exits in a series of sub-directories in the *examples* subdirectory:

Subdirectory	Contains
<i>acb_uexit</i>	An ADALNK user exit. This user exit is called before an Adabas call is processed (ADALNK interface) and it rejects all Adabas operator calls whose user is not SAG. In addition, it blocks N1/N2 and A1 commands for the user SAG. Response code 22 is set when any of these call restrictions in encountered.
<i>acbx_uexit</i>	An ADALNKX user exit. This user exit is called before an Adabas call is processed (ADALNKX interface) and it rejects all Adabas operator calls whose user is not SAGPC. In addition, it blocks N1/N2 and A1 commands for the user SAGPC. A return value of ADA_UEXREJ is set when any of these call restrictions in encountered.
<i>adasaf_uexit</i>	An External Security Interface (ESI) user exit you can use to access secured Adabas resources on a z/OS host node. For more information, read .
<i>wcl_uexit</i>	An example user exit and a shared library stub. These are provided to assist you in creating and implementing your user exit program.

The remainder of this section describes the files and compilation method you can use to create and compile your own user exit, based on the files in the *wcl_uexit* subdirectory.

- [acb_uexit Example User Exit Files](#)
- [acbx_uexit Example User Exit Files](#)
- [wcl_uexit Example User Exit Files](#)

- [Compiling the Example User Exit Files](#)

acb_uexit Example User Exit Files

The *examples/acb_uexit* subdirectory contains all of the necessary source code files to make a working example of an ADALNK user exit program, as described in the following table:

File Name	Description
<i>adabas.h</i>	Adabas call resource file. This file lists resources files that should be included when the user exit is compiled.
<i>adabasx.h</i>	Adabas call control block file.
<i>lnkuex.c</i>	ADALNK user exit source code file.
<i>lnkuex.h</i>	ADALNK user exit control block layout file.
<i>makefile</i>	C program to be run in Windows and used to create the user exit library from the files in the user exit source code library.
<i>makefile.ux</i>	C program to be run in UNIX and used to create the user exit library from the files in the user exit source code library.
<i>mk.bat</i>	A batch file that runs nmake on the <i>makefile</i> file.

You can use these files as a model for writing your own ADALNK user exit programs. The supplied ADALNK user exit program is called before an Adabas call is processed (ADALNK interface) and it rejects all Adabas operator calls whose user is not SAG. In addition, it blocks N1/N2 and A1 commands for the user SAG. Response code 22 is set when any of these call restrictions in encountered.

acbx_uexit Example User Exit Files

The *examples/acbx_uexit* subdirectory contains all of the necessary source code files to make a working example of an ADALNKX user exit program, as described in the following table:

File Name	Description
<i>adabas.h</i>	Adabas call resource file. This file lists resources files that should be included when the user exit is compiled.
<i>adabasx.h</i>	Adabas call control block file.
<i>lnkuexacbx.c</i>	ADALNKX user exit source code file.
<i>lnkuexacbx.h</i>	ADALNKX user exit control block layout file.
<i>makefile</i>	C program to be run in Windows and used to create the user exit library from the files in the user exit source code library.
<i>makefile.ux</i>	C program to be run in UNIX and used to create the user exit library from the files in the user exit source code library.

You can use these files as a model for writing your own ADALNKX user exit programs. The supplied ADALNKX user exit is called before an Adabas call is processed (ADALNKX interface)

and it rejects all Adabas operator calls whose user is not SAGPC. In addition, it blocks N1/N2 and A1 commands for the user SAGPC. A return value of ADA_UEXREJ is set when any of these call restrictions in encountered.

wcl_uexit Example User Exit Files

The *examples/wcl_uexit* subdirectory contains all of the necessary source code files to make a working example of a user exit program, as described in the following table:

File Name	Description
<i>user_exit.c</i>	User exit source code file
<i>user_exit.h</i>	User exit control block layout file
<i>makefile.ux</i>	C program used to create the user exit library from the files in the user exit source code library.

You can use these files as a model for writing your own user exit programs.

Compiling the Example User Exit Files

▶ **To compile a user exit into a user exit library in UNIX environments:**

- Navigate to the appropriate installation directory and enter the following command:

```
make -f makefile.ux
```

The appropriate user exit library (*.dll file) is generated.

46 Port Number Reference

- Port Overview and General Assignments 202
- Changing the Software AG Directory Server Port Number 203

This chapter describes the ports that are needed by Entire Net-Work to perform its processing and how they can be assigned.

Port Overview and General Assignments

The following table describes the ports that are needed by Entire Net-Work to perform its processing and any default ports assumed by Entire Net-Work. You should consider avoiding the use of these default port numbers for other applications.

Software AG Product Component	Ports Needed	Default Port Number
Software AG Directory Server	One port is needed for Entire Net-Work requests to the Directory Server	4952 (IANA port) Note: If older versions of Entire Net-Work (older than 7.3) are in use, this port number may need to be changed to 12731.
Entire Net-Work Server	One port is needed for System Management Hub (SMH) administration of Entire Net-Work Server	dynamically assigned
Entire Net-Work Kernel	A port is needed for Kernel access by clients	dynamically assigned
	A port is needed for Kernel access via e-business connections (Entire Net-Work 7 or later)	dynamically assigned
	A port is needed for Kernel access via classic RDA connections (Entire Net-Work 2)	7869
	A port is needed for System Management Hub (SMH) administration of Kernels	dynamically assigned

Note that Software AG has registered port number 4952 with the Internet Assigned Numbers Authority (IANA) for use by the Software AG Directory Server. For more information about Directory Server port number specifications, read *The Directory Server Port Number*, in the *Software AG Directory Server Administration Guide*. For information on changing the Directory Server port number for an Entire Net-Work installation, read [Changing the Software AG Directory Server Port Number](#).

In general, there are no default port numbers assigned to Entire Net-Work Kernels or clients. These are dynamically assigned by Entire Net-Work when the Kernel or client is started, unless you specify a specific port or range of ports to use when you define the Kernel or client. If you set the port number to "0", the Entire Net-Work will dynamically assign a port.

Port numbers are dynamically assigned by Entire Net-Work when the Kernel or client is started, as follows:

- Entire Net-Work searches for the first available port starting from port 49152 through 65535. (The starting search port number, 49152, is the IANA-recommended value from which to start.).
- Once an available port number is found, it is assigned to the Kernel or client in its Software AG Directory Server entry.

While defining Entire Net-Work Kernels, you can also select a specific port or specify a range or list of port numbers that Entire Net-Work should search during the process in which it dynamically assigns a port to the Kernel:

- To specify a specific port number, enter the number in the port number field when you define the Kernel.
- To specify a range of port numbers that Entire Net-Work should search to dynamically assign a port, list the starting and ending ports in the port number field when you define the Kernel, separated by a dash (-). For example, a specification of "9010-9019" would cause Entire Net-Work to search for the first available port between and including port numbers 9010 and 9019.
- To specify a list of port numbers that Entire Net-Work should search to dynamically assign a port, list the port numbers in the port number field when you define the Kernel, separated by commas (.). For example, a specification of "9010,9013,9015,9017,9019" would cause Entire Net-Work to search for the first available port from this list of ports, starting with port 9010 and working from left to right through the list.
- You can, of course, combine search ranges and lists in a port number field. For example, a specification of "9010-9019,10020,10050-10059" would cause Entire Net-Work to search for the first available port first in the 9010-9019 range (inclusive), then port 10020, and finally in the 10050-10059 range (inclusive). The first available port that Entire Net-Work encounters would be used for the Kernel.

If no available port is found in a specified range or list, an error occurs.

For more information about adding Kernels, read *Adding Kernels*, in your Entire Net-Work Server documentation.

Changing the Software AG Directory Server Port Number

▶ If you need to change the Directory Server port number for your Entire Net-Work installation, follow these steps:

- 1 Shut down the Directory Server service or daemon.

For information on shutting down the Directory Server service or daemon, read *Starting and Stopping the Software AG Directory Server*, in the *Software AG Directory Server Administration Guide*.

- 2 Modify the Directory Server installation, as appropriate for the operating system. When prompted, change the Directory Server port number to the new port number you want to use.
- 3 Start up the Directory Server service or daemon, if it is not automatically started after its installation was modified.

For information on starting up the Directory Server service or daemon, read *Starting and Stopping the Software AG Directory Server*, in the *Software AG Directory Server Administration Guide*.

47 Directing Log Files to a Shared Server

- Step 1. Specify the Log File Locations 206
- Step 2. Configure the Entire Net-Work and Entire Net-Work Client Windows Services 206

If you are using Entire Net-Work 7.3.3 or Entire Net-Work Client 1.3 or later, you can direct your Entire Net-Work log files to a shared server.



Caution: To avoid overwriting log files with the same name, log files for individual servers, Kernels, and clients should be stored in directories with unique names.

The process of directing log files to a shared server involves the steps (note that the second step is only required on Windows) described in this chapter.

Step 1. Specify the Log File Locations

Using the System Management Hub (SMH), specify the fully-qualified path of the directory in which you want to store the log files.



Caution: To avoid overwriting log files with the same name, log files for individual servers, Kernels, and clients should be stored in directories with unique names.

- For information on redirecting Entire Net-Work Client log files, read [Specifying the Client Log File Location](#), elsewhere in this guide.

Make sure that your network administrator has allowed your local machine access to the directory and server to which you are redirecting the log files. On Windows systems, you must also complete the next step to do this.

Step 2. Configure the Entire Net-Work and Entire Net-Work Client Windows Services

On Windows systems only, you must configure the Entire Net-Work and Entire Net-Work Client services so that the local host can write to the log files on the shared server.

▶ **To update the Entire Net-Work and Entire Net-Work Client Windows services appropriately, follow these steps:**

- 1 Edit the Windows service definition for the Directory Server and select the **Log On** tab.
- 2 On the **Log On** tab, select the **This account** radio button.
- 3 Enter a user account name that is known to both this host and the file server where the log files are located. This can be a domain account or a local account that is configured on both machines with the same password. The account should have full control access rights to the log file location.
- 4 Click the **OK** button.

- 5 Restart the service.

48 Entire Net-Work Configuration Parameters

- Configuration Parameter List 210
- Configuration Tools 213

Entire Net-Work configuration settings are stored in a series of parameters. Some of these you can change; some you cannot or should not. You can change these configuration settings using:

- Entire Net-Work System Management Hub (SMH) functions. For more information on this, read *Entire Net-Work Client Administration* (in the *Entire Net-Work Client Installation and Administration Guide*) and *Entire Net-Work Server Administration* (in the *Entire Net-Work Server Installation and Administration Guide*).
- Environment variables with the same names as the configuration parameter.



Caution: Future releases of Entire Net-Work will not support configuration parameter settings in environment variables. For this reason, we recommend that you do not use this method.

- Tools supplied with Entire Net-Work that can also be used in your application programs. Additional information on these tools is provided elsewhere in this chapter.

Configuration Parameter List

The following table describes each of the Entire Net-Work configuration parameters, indicating whether or not you can or should modify its setting, the platforms on which it is available, the default (if any), the name of the SMH parameter that can be used to change it, and the name of the tool that can be used to change it.

Parameter	Description	Can you change it?	Platform Availability	Default	SMH Parameter	Batch Tool
LNKADAESI	whether the ESI online application should be used instead of a user exit.	yes	Windows	NO	LNKADAESI	AdaSetParameter (set for the LNKADAESI parameter)
LNKADASAF	the library and function names of the user exit that will provide access to the secured Adabas resource via the Adabas SAF Security Kernel (ADASAF).	yes	UNIX and Windows	"lnkxsaf lnkxsaf"	LNKADASAF	AdaSetParameter (set for the LNKADASAF parameter)
LNKTIMEOUT	Global timeout for a response from a remote Adabas call.	yes	UNIX and Windows	1 minute	ADABAS_TIMEOUT	AdaSetTimeout
LNKTRACE	ADALNK and Software AG transport services trace levels.	yes	UNIX and Windows	0 (zero)	LNKTRACE and XTSTRACE	AdaSetTrace

Parameter	Description	Can you change it?	Platform Availability	Default	SMH Parameter	Batch Tool
LNKUEX_0	<p>the file and function names of the user exit that should be called before an Adabas ACB command is sent to the database.</p> <p>Note: LNKUEX_0 handling triggers an undocumented Natural feature; if the user exit is called and returns a non-zero response code, but the Adabas command is an RC command, the RC command is suppressed and a successful return is indicated to the calling program.</p>	yes	UNIX and Windows	---	LNKUEX_0	none
LNKUEX_1	<p>the file and function names of the user exit that should be called after an Adabas ACB command is sent to the database.</p>	yes	UNIX and Windows	---	LNKUEX_1	none
LNKUEX_ACBX_0	<p>the file and function names of the user exit that should be called before an Adabas ACBX command is sent to the database.</p> <p>Note: LNKUEX_ACBX_0 handling triggers an undocumented Natural feature; if the user exit is called and returns a non-zero response code, but the Adabas command is an RC command, the RC command is suppressed and a successful return is indicated to the calling program.</p>	yes	UNIX and Windows	---	LNKUEX_ACBX_0	none
LNKUEX_ACBX_1	<p>the file and function names of the user exit that should be called after an</p>	yes	UNIX and Windows	---	LNKUEX_ACBX_1	none

Parameter	Description	Can you change it?	Platform Availability	Default	SMH Parameter	Batch Tool
	Adabas ACBX command is sent to the database.					
WCLCODEDIR	the directory where the Entire Net-Work Client code is stored If you want to change the value of this configuration parameter, contact your Software AG support representative.	yes, with assistance	UNIX	local directory	none	none
WCLDATADIR	the directory where the Entire Net-Work Client data is stored If you want to change the value of this configuration parameter, contact your Software AG support representative.	yes, with assistance	UNIX	local directory	none	none
WCPCONFIG	Entire Net-Work configuration file name	yes	UNIX and Windows	local <i>xts.config</i>	none	AdaSetParameter (set for the WCPCONFIG parameter)
WCPDIR	the directory where the Entire Net-Work code is stored If you want to change the value of this configuration parameter, contact your Software AG support representative.	yes, with assistance	UNIX and Windows	local directory	none	none
WCPVERS	the Entire Net-Work version If you want to change the value of this configuration parameter, contact your Software AG support representative.	yes, with assistance	UNIX and Windows	---	none	none

Configuration Tools

This section describes the configuration tools you can use to set some of the Entire Net-Work configuration parameters.

- [AdaSetParameter Configuration Tool](#)
- [AdaSetTimeout Configuration Tool](#)
- [AdaSetTrace Configuration Tool](#)
- [AdaSetSaf Configuration Tool](#)

AdaSetParameter Configuration Tool

You can use the AdaSetParameter configuration tool to set values for the following parameters:

- LNKADAESI: Valid values are "YES" (use the ESI online application) or "NO" (use a user exit). The default is "NO". If LNKADAESI is set to "YES" and a value is given in LNKADASAF, the online application is used (LNKADAESI settings override LNKADASAF).
- LNKADASAF: Specify the library and function names of the user exit that will provide access to the secured Adabas resource via the Adabas SAF Security Kernel (ADASAF). The library and function names should be specified with a space between them, using the following format:

```
library function
```

If no names are specified, the value "lnksaf lnksaf" is used. (The lnksaf library is either *lnksaf.dll* or *lnksaf.so*).

- WPCONFIG: Valid values for WPCONFIG can be any valid file name.

The syntax of the AdaSetParameter configuration tool is:

```
AdaSetParameter("parameter=value")
```

Replace *parameter* with one of the parameter names listed above and *value* with an appropriate value for that parameter.

In the following example, the name of the Entire Net-Work configuration file to be used is set to TEST.CFG:

```
AdaSetParameter("WCPCONFIG=TEST.CFG")
```

AdaSetTimeout Configuration Tool

Use the AdaSetTimeout configuration tool to set a global time limit for a response from a remote Adabas call. The syntax of the AdaSetTimeout configuration tool is:

```
AdaSetTimeout(dbid, seconds)
```

Replace *dbid* with a valid Adabas database ID and *seconds* with the number of seconds to use for the global time limit for the specified database.

In the following example, a 60-second timeout period is defined for database 12:

```
AdaSetTimeout(12,60)
```

AdaSetTrace Configuration Tool

Use the AdaSetTrace configuration tool to set trace levels for ADALNK and Software AG transport services. The syntax of the AdaSetTrace configuration tool is:

```
AdaSetTrace(level, {TRUE | FALSE})
```

Replace *level* with a valid trace level. Trace levels must be specified in hexadecimal and in the following format:

```
0xllxxxx
```

In the trace level syntax, substitute a hexadecimal value from "00" through "f1" for *ll* to represent the ADALNK trace level. Then substitute a hexadecimal value from "0000" through "FFFE" for *xxxx* to represent the Software AG transport services trace level.

Then specify TRUE or FALSE. If you specify TRUE, the trace level is set globally for all calls; if you specify FALSE, the trace level is set only for the thread in which the call is made.

In the following example, the maximum trace level is specified for both ADALNK and Software AG transport services, but only for the thread in which the call is made:

```
AdaSetTrace(0xf1FFFE, FALSE)
```

In the following example, the maximum trace level is specified for ADALNK calls and no tracing is performed for Software AG transport services. These settings are made globally for all calls:

```
AdaSetTrace(0xf10000,TRUE)
```

AdaSetSaf Configuration Tool

Use the AdaSetSaf configuration tool to specify ESI access information to the user exit that will provide access to the secured Adabas resource via the Adabas SAF Security Kernel (ADASAF). This is the same information you supply using the ESI online application (read *Accessing z/OS Resources Using the ESI Online Application*, in *Entire Net-Work Client Installation and Administration Guide* for more information).

The syntax of the AdaSetSaf configuration tool is:

```
AdaSetSaf(PADASAF_INFO adasaf_info")
```

Replace *adasaf_info* with the name of a data structure that provides information in the following format:

```
CE_CHAR  cUserID[8];          /* UserID          */
CE_CHAR  cPassword[8];       /* Password        */
CE_CHAR  cNewPassword[8];    /* NewPassword     */
```

In the following example, the data structure "mysaf" is used to provide appropriate ESI access information to secured Adabas resources via ADASAF:

```
AdaSetSaf(PADASAF_INFO mysaf
```


49 Entire Net-Work Directory Server Utility Functions

(checkadi and setadi)

- The checkadi Utility 218
- The setadi Utility 219

Two Entire Net-Work utility functions with focus on the Software AG Directory Server availability and settings are provided for you to use in batch mode:

- Use the checkadi utility function to check for a Directory Server.
- Use the setadi utility function to set Directory Server access parameters for Entire Net-Work and Entire Net-Work Client.

This chapter describes both of these utilities.

The checkadi Utility

Use the checkadi utility to check for the existence of a Directory Server. The syntax of the checkadi function is:

```
checkadi [host=host-name] [[port=port-value]
```

Use the host or port arguments to check for the existence of a Directory Server on a specific host or port number. You can use both the host and port arguments to more specifically check for a Directory Server on a specific host and port.

Example 1

In the following example, a check is run for a Directory Server on the usaxxx2 host at port 12731:

```
checkadi host=usaxxx2 port=12731
```

The following sample output from such a check might appear:

```
Software AG Entire Net-Work, Copyright ©) 1997-2011 by Software AG
USAGE: checkadi [host=hostname] [port]=portvalue]
argv[1] host=usaxxx2
Check host=usaxxx2
argv[2] port=12731
Check port=12731
Port was set to 12731
Check Host=usaxxx2
Check Port=12731
Server is Active; check if this is a Directory Server
Select Data from Directory Server successful
Bytes ready to read=309
Response=0x010x33 0x760x310x090x720x650x730x700x6f0x6e0x730x650x090x09
Expected=          0x760x310x090x720x650x730x700x6f0x6e0x730x650x090x09
Directory Server is Active
Checkadi ending ...
```


Example 2

In the following example, a check is run to determine where a Directory Server exists:

```
checkadi
```

The following sample output from such a check might appear:

```

Software AG Entire Net-Work, Copyright ©) 1997-2011 by Software AG
USAGE: checkadi [host=hostname] [port]=portvalue]
Resolve SAGXTSDSHOST
Failure Resolve Host Name; use localhost
Port was not set, so we will use the default port=12731
Check Host=usaxxx2.YYY.ww.zzz
Check Port=12731
Server is Active; check if this is a Directory Server
Select Data from Directory Server successful
Bytes ready to read=309
Response=0x010x33 0x760x310x090x720x650x730x700x6f0x6e0x730x650x090x09
Expected=          0x760x310x090x720x650x730x700x6f0x6e0x730x650x090x09
Directory Server is Active
Checkadi ending ...

```

The setadi Utility

Use the setadi utility to set Directory Server access parameters for Entire Net-Work and Entire Net-Work Client. The syntax of the setadi function is:

```
setadi {WCP|WCL} host=host-name port=port-value [XTSTRACE={value|65534}]
```

You must specify either "WCP" (to set the access parameters for Entire Net-Work) or "WCL" (to set access parameters for Entire Net-Work Client). You should also specify the host name and port number parameters. The XTSTRACE parameter is optional; if you do not specify it, a default value of "65534" is used.



Note: While you can use setadi to change the Directory Server used, the changes only affect the configuration of the services and agents. It will not change the Directory Server assigned to any existing Kernels.

Example 1

In the following example, help for setadi is displayed, but no access parameters are set.

```
setadi
```

The following sample output from such a setadi request might appear:

```
Software AG Entire Net-Work, Copyright ©) 1997-2011 by Software AG
Usage: setadi <options...>
The following options are supported:
WCP|WCL
HOST=host name
PORT=port value
XTSTRACE=value (65534)

WCP|WCL - the user selects which product to set, WCP or WCL
```

Example 2

In the following example, an Entire Net-Work entry for host "localhost" at port "12731" is defined. The default XTSTRACE value of "65534" is used.

```
setadi WCP host=localhost port=12731
```

The following sample output from such a setadi request might appear:

```
Software AG Entire Net-Work, Copyright ©) 1997-2010 by Software AG
argv[2] host=localhost
argv[3] port=12731
Check Host=localhost
Check Port=12731
Server is Active; check if this is a Directory Server
Select Data from Directory Server successful
Bytes ready to read=309
Response=0x010x33 0x760x310x090x720x650x730x700x6f0x6e0x730x650x090x09
Expected=          0x760x310x090x720x650x730x700x6f0x6e0x730x650x090x09
Directory Server is Active
CODEPATH=C:\Program Files\Software AG\Entire Net-Work Server\v74\
DATAPATH=C:\Documents and Settings\All Users\Application Data\Software AG\Entire
Net-Work Server\
Changing C:\Documents and Settings\All Users\Application Data\Software AG\Entire
Net-Work Server\service74.config
Changing C:\Documents and Settings\All Users\Application Data\Software AG\Entire
Net-Work Server\agents\xts.config
Configuration file change successful
Setadi exiting ...
```

Index

, 69, 84, 98, 121, 186 (see Kernel configurations and client configurations) (see System Management Hub) (see user exit interface, Windows control block structure)
(see also uninstalling Entire Net-Work Client)
(see also uninstalling Entire Net-Work Server)

A

accessing
 System Management Hub, 98
accessing secured host resources, 145
ADALNK user exits, 153
AdaSetParameter configuration tool, 213
AdaSetSaf configuration tool, 215
AdaSetTimeout configuration tool, 214
AdaSetTrace configuration tool, 214
adding
 client configurations, 117
applications
 identifying client configurations, 111

C

calling the user exit
 in Windows environments, 186
 UNIX environments, 197
client configurations
 about, 105
 adding, 117
 controlling client access to databases, 129
 deleting, 119
 identifying in your applications, 111
 listing, 107
 maintaining, 121
 migrating, 127
 reviewing, 107
 selecting, 107
 setting service parameters, 113
 used for testing, 106
Clients
 installing, 77
configuration considerations, 37
configuration tools, 213
configurations, 121

D

database IDs

 filtering by, 13
databases
 controlling client access to, 129
dates, end-of-maintenance, 27
debugging user exits, 187
deleting
 client configurations, 119
Directory Server
 description, 7
 installing, 60
 uninstalling, 69, 70
documentation
 allowing active content in Windows, 30
 obtaining updates, 29
dropped features, 23
dumping user exit information, 187

E

Empower
 documentation, 29
 platform support, 34
end-of-maintenance dates, 27
enhancements, 17
Entire Net-Work
 configuration considerations, 37
 configuring components for Windows XP Personal Firewall, 89
 Entire Net-Work Client, 6
 filtering, 13
 installing management components, 59
 memory requirements, 35
 partitioning, 11
 platform coverage and prerequisites, 33
 port number reference, 201
 space requirements, 35
 starting and stopping Entire Net-Work Client, 93
 System Management Hub, 97
Entire Net-Work 7
 Directory Server, 7
 prerequisite Software AG products, 35
 SSL support, 9
 System Management Hub, 8
 UNIX installation daemons, 51
 UNIX installation in batch mode, 47
 UNIX installation system services, 51
Entire Net-Work Administration Open Systems
 installing, 65
 uninstalling, 69, 70
Entire Net-Work Client

- accessing secured z/OS host resources, 145
- changing the Software AG Directory Server, 159
- description, 6
- installation prerequisites, 75
- installing, 77
- managing client service tracing, 164
- managing client tracing, 166
- managing log files, 141
- managing Software AG communications tracing, 170
- managing Software AG transport services tracing, 168
- silent installation in Windows environments, 81
- specifying log file location, 143
- starting a new log file, 142
- tracing processing, 163
- uninstalling, 83
- viewing log files, 142

F

- filtering, 13
- functions
 - UE_CON_IN, 190
 - UE_CON_OUT, 189
 - UE_DISCON, 193
 - UE_INIT, 188
 - UE_RECV, 192
 - UE_SEND, 191
 - UE_TERM, 193
- future plans, 25

H

- help
 - System Management Hub, 100

I

- installation, 69, 84
 - batch mode on UNIX, 47
 - daemons on UNIX, 51
 - preinstallation steps, 75
 - prerequisites, 75
 - system services on UNIX, 51
- installing
 - Entire Net-Work Client, 77
 - management components, 59
- installing Directory Server, 60
 - on UNIX, 62
 - on Windows, 61
- installing Entire Net-Work Administration Open Systems, 65
 - on UNIX, 67
 - on Windows, 65

L

- listing
 - client configurations, 107
- log files
 - managing Entire Net-Work Client, 141
 - specifying Entire Net-Work Client log file location, 143
 - starting a new Entire Net-Work Client log file, 142
 - viewing Entire Net-Work Client, 142
- logging in
 - SMH, 98

M

- maintaining
 - client configurations, 121
- memory requirements, 35
- Microsoft Windows support, 34
- migrating
 - client configurations, 127
 - Entire Net-Work Client 1.3 configurations, 127
- migration considerations, 21

O

- operating system coverage, 34

P

- partitioning, 11
- platform support, 34
- port numbers, 201
- post-installation updates, 87
- preinstallation steps, 75
- product support
 - obtaining updated documentation, 29
 - supported platforms, 34

R

- Refresh button
 - System Management Hub, 100
- requirements
 - memory, 35
 - operating system coverage, 34
 - space, 35
- return codes from user exit interface, 187, 197
- reviewing
 - client configurations, 107

S

- security
 - accessing secured host resources, 145
- selecting
 - client configurations, 107
- services parameters
 - client configurations, 113
- shutting down
 - System Management Hub, 99
- Simple Connection Line Driver
 - Entire Net-Work Client post-installation updates to support, 87
- SMH, 98
- Software AG Directory Server
 - changing, 159
 - space requirements, 35
- SSL support, 9
- starting
 - Entire Net-Work Client, 93
- stopping
 - Entire Net-Work Client, 93
- storing user exit library files, 185
- support
 - obtaining updated documentation, 29
 - platforms supported, 34

- support for prior versions, 27
- supported operating systems, 34
- supported platforms, 34
- system administration
 - System Management Hub, 97
- System Management Hub
 - about, 97
 - accessing, 98
 - getting help, 100
 - logging in, 98
 - Refresh button, 100
 - shutting down, 99
- system resource usage
 - Entire Net-Work, 55
 - Entire Net-Work Client, 56
 - Entire Net-Work Kernels, 57
 - Software AG Directory Server, 57
 - summary table, 58
 - System Management Hub (SMH), 57

T

- testing network configurations, 106
- tracing
 - Entire Net-Work Client, 163
 - managing client, 166
 - managing client service, 164
 - managing Software AG communications, 170
 - managing Software AG transport services, 168
- tracing user exits, 187

U

- UE_CON_IN function, 190
- UE_CON_OUT function, 189
- UE_DATAOUT return code, 187
- UE_DISCON function, 193
- UE_FAILURE return code, 187
- UE_INIT function, 188
- UE_RECV function, 192
- UE_RESTRICT return code, 187
- UE_SEND function, 191
- UE_SUCCESS return code, 187
- UE_TERM function, 193
- UEYCB, 186
- uninstalling Directory Server
 - on UNIX, 70
 - on Windows, 69
- uninstalling Entire Net-Work Administration Open Systems
 - on UNIX, 70
 - on Windows, 69
- uninstalling Entire Net-Work Client
 - on Windows, 84
- UNIX
 - installing Directory Server, 62
 - installing Entire Net-Work Administration Open Systems, 67
 - supported platforms, 34
 - system resource usage, 55
 - uninstalling Directory Server, 70
 - uninstalling Entire Net-Work Administration Open Systems, 70
 - user exit interface processing, 196
- UNIX installation considerations

- batch mode, 47
- daemons, 51
- system services, 51
- user exit interface, 183
 - calling the user exit in UNIX, 197
 - calling the user exit in Windows, 186
 - processing in UNIX, 196, 198
 - processing in Windows, 185
 - responses, 187
 - return codes in UNIX, 197
 - return codes in Windows, 187
 - storing user exit library files, 185
 - supplied example files, 195, 196, 199, 200
 - tracing, debugging, or dumping on Windows, 187
- UE_CON_IN function, 190
- UE_CON_OUT function, 189
- UE_DISCON function, 193
- UE_INIT function, 188
- UE_RECV function, 192
- UE_SEND function, 191
- UE_TERM function, 193
- Windows control block structure, 186
- Windows functions, 188
- writing user exits, 184

W

- Windows
 - installing Directory Server, 61
 - installing Entire Net-Work Administration Open Systems, 65
 - uninstalling Directory Server, 69
 - uninstalling Entire Net-Work Administration Open Systems, 69
 - uninstalling Entire Net-Work Client, 84
 - user exit interface processing, 185
- Windows installations
 - silent installation for Entire Net-Work Client, 81
- Windows XP Personal Firewall, 89
- writing user exits, 184

Z

- z/OS host resources
 - accessing secured, 145

