

# **Entire Net-Work Administration LUW Documentation**

## **Entire Net-Work Administration LUW Installation and Administration Guide**

Version 1.4.1

November 2017

---

This document applies to Entire Net-Work Administration LUW Version 1.4.1 and all subsequent releases.

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

Copyright © 2017 Software AG, Darmstadt, Germany and/or Software AG USA, Inc., Reston, VA, USA, and/or its subsidiaries and/or its affiliates and/or their licensors.

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

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

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

Use, reproduction, transfer, publication or disclosure is prohibited except as specifically provided for in your License Agreement with Software AG.

**Document ID: WCB-OWCBDOC-141-20171109**

## Table of Contents

Preface .....	vii
1 Entire Net-Work Administration LUW Concepts .....	1
2 Release Notes .....	3
Enhancements .....	4
End of Maintenance .....	4
Documentation and Other Online Information .....	4
3 Installing and Uninstalling Entire Net-Work Administration LUW .....	7
System Requirements .....	8
Configuration Considerations .....	11
Before You Begin .....	12
Installation Steps .....	12
Configuring Product Components for Windows Personal Firewall .....	14
Uninstallation Steps .....	15
Installing Fixes Using Software AG Update Manager .....	15
Uninstalling Fixes Using Software AG Update Manager .....	17
4 About the System Management Hub .....	19
Accessing the System Management Hub .....	20
Leaving the System Management Hub .....	21
Using the Refresh Button in the System Management Hub .....	22
Getting Help .....	22
5 Performing Adabas Directory Server Administration .....	23
Accessing the Directory Server Area of System Management Hub .....	24
Refreshing SMH Displays .....	25
6 Maintaining Directory Server Links .....	27
Listing Linked Directory Servers .....	28
Adding a Link to a Directory Server .....	29
Modifying a Directory Server Link Definition .....	30
Listing Directory Server Parameters .....	32
Deleting a Link to a Directory Server .....	33
7 Maintaining Partitions .....	35
Listing the Partitions .....	36
Adding a Partition .....	37
Changing a Partition Name .....	37
Deleting a Partition .....	38
8 Maintaining Targets .....	41
Listing the Targets .....	42
Adding Targets .....	43
Maintaining Qualified URLs .....	47
Setting the Target Type .....	70
Changing the Target Name .....	72
Changing the Host .....	73
Changing the Protocol .....	73
Deleting a Target .....	75

9	Changing Hosts .....	77
10	Entire Net-Work Client Administration .....	79
11	The Entire Net-Work Client SMH Administration Area .....	81
12	About Client Configurations .....	83
13	Listing, Selecting, and Reviewing Client Configurations .....	85
14	Identifying the Client Configuration to Your Application .....	89
	Specifying the Configuration by Environment Variable .....	90
	Specifying the Configuration in Your Application .....	90
15	Setting Service Parameters .....	91
16	Adding Client Configurations .....	95
17	Deleting Client Configurations .....	97
18	Maintaining Client Configuration Parameters .....	99
19	Migrating Entire Net-Work Client Configurations .....	105
20	Controlling Client Access to Databases .....	107
	Maintaining Adabas Access Definitions .....	108
	Maintaining Additional Database Access Parameters .....	114
21	Managing Entire Net-Work Client Log Files .....	119
	Viewing the Current Entire Net-Work Client Log File .....	120
	Starting a New Entire Net-Work Client Log File .....	120
	Specifying the Client Log File Location .....	121
22	Accessing Secured z/OS Host Resources .....	125
	Specifying the External Security Method and Appropriate Adabas SAF Security Kernel Parameters .....	126
	Accessing z/OS Resources Using the Online Security Application .....	128
	Accessing z/OS Resources Using the Security Exit .....	131
23	Using ADALNK User Exits .....	133
	Specifying the User Exit File and Function Names .....	134
	Modifying the User Exit Code .....	136
24	Changing the Adabas Directory Server .....	137
	Changing the Adabas Directory Server for the Client Machine .....	138
	Changing the Adabas Directory Server for a Specific Client .....	139
25	Tracing Entire Net-Work Client Processing .....	141
	Managing Client Service Tracing .....	142
	Managing Client Tracing .....	144
	Managing Software AG Transport Services Tracing .....	146
	Managing Software AG Communications Tracing .....	148
26	Starting and Stopping Entire Net-Work Client .....	151
	Automatically Starting Entire Net-Work Client .....	152
	Manually Starting Entire Net-Work Client .....	152
	Stopping Entire Net-Work Client .....	153
27	Entire Net-Work Server Administration .....	155
28	The Entire Net-Work Server SMH Administration Area .....	157
	Accessing the Entire Net-Work Server SMH Administration Area .....	158
	Getting Help .....	159
	Refreshing the Displays .....	159

29 Managing Entire Net-Work Servers .....	161
30 Listing, Selecting, and Reviewing Installed Entire Net-Work Server .....	163
31 Adding Kernel Configuration Definitions .....	167
32 Migrating Kernel Configurations .....	173
33 Setting Entire Net-Work Server Parameters .....	175
34 Setting the Trace Level for an Entire Net-Work Server .....	179
35 Managing Entire Net-Work Server Log Files .....	181
Viewing the Entire Net-Work Server Log File .....	182
Starting a New Entire Net-Work Server Log File .....	182
Specifying the Entire Net-Work Server Log File Location .....	184
36 Changing the Adabas Directory Server .....	187
37 Shutting Down the Entire Net-Work Server .....	189
38 Managing Kernels .....	191
39 Listing, Selecting, and Reviewing Kernel Definitions .....	193
Listing, Selecting, and Reviewing Permanent Definitions .....	194
Listing, Selecting, and Reviewing Dynamic Definitions .....	196
40 Reviewing the Kernel Parameter Summary .....	199
41 Starting a Kernel .....	201
42 Shutting Down a Kernel .....	203
Shutting Down a Kernel Using Its Permanent Definition .....	204
Shutting Down a Kernel Using Its Dynamic Definition .....	205
43 Deleting a Kernel .....	207
44 Setting Basic Kernel Parameters .....	209
45 Setting Advanced Kernel Parameters .....	215
46 Specifying Kernel Scalability .....	219
47 Maintaining Kernel Filters .....	221
48 Changing the Adabas Directory Server .....	225
49 Maintaining Access Definitions .....	227
Listing Access Definitions .....	228
Adding Access Definitions .....	229
Modifying Access Definitions .....	233
Deleting Access Definition .....	234
50 Reviewing Kernel Access Status .....	237
51 Maintaining Connection Definitions .....	239
Listing Connection Definitions .....	240
Adding Connection Definitions .....	241
Modifying Connection Entries .....	247
Deleting Connection Entries .....	248
52 Reviewing Kernel Outgoing Connection Status .....	249
53 Reviewing Kernel Statistics .....	251
54 Dynamically Collecting Detailed Statistics .....	253
55 Generate a Kernel Configuration Dump .....	255
56 Checking Kernel Databases .....	257
57 Pinging Databases and Classic Nodes .....	259
Pinging Databases .....	260

Pinging Classic Nodes .....	261
58 Dynamically Connecting and Disconnecting a Connection .....	263
Dynamically Connecting .....	264
Dynamically Disconnecting .....	265
59 Dynamically Managing Kernel Clients and Adabas Contexts .....	267
Listing Kernel Clients and Adabas Contexts .....	268
Viewing Kernel Client and Adabas Context Statistics .....	269
Dynamically Disconnecting Kernel Clients .....	270
Dynamically Deleting Adabas Contexts .....	271
60 Dynamically Managing Kernel Client Hosts .....	273
Listing Client Hosts .....	274
Viewing Client Host Statistics .....	274
Dynamically Disconnecting All Clients and Contexts of a Client Host .....	275
61 Reviewing Kernel Status .....	277
62 Managing Kernel Log Files .....	279
Viewing the Kernel Log File .....	280
Starting a New Kernel Log File .....	280
Specifying the Kernel Log File Location .....	282
63 Tracing Kernel Processing .....	285
Managing Kernel Tracing .....	286
Managing Software AG Transport Services Tracing .....	290
Managing Software AG Communications Tracing .....	292
64 Entire Net-Work Utility Functions for the Directory Server (checkadi and setadi) .....	295
The checkadi Utility .....	296
The setadi Utility .....	297
65 Port Number Reference .....	299
Port Overview and General Assignments .....	300
Changing the Adabas Directory Server Port Number .....	301
About System Management Hub Ports .....	303
Index .....	305

---

## Preface

---

This document describes Entire Net-Work Administration LUW and explains how to install and use it.

Entire Net-Work Administration LUW is intended for system administrators in your enterprise.

This document is organized as follows:

<i>Entire Net-Work Administration LUW Concepts</i>	Introduces you to Entire Net-Work Administration LUW.
<i>Release Notes</i>	Describes the new and changed features in this version of the Entire Net-Work Administration LUW.
<i>Installing and Uninstalling Entire Net-Work Administration LUW</i>	Describes the prerequisites of the Entire Net-Work Administration LUW how to install and uninstall it.
<i>About the System Management Hub</i>	Introduces you to the System Management Hub and explains how to access it and leave it.
<i>Performing Adabas Directory Server Administration</i>	Describes administrative tasks you can perform for the Adabas Directory Server.
<i>Entire Net-Work Client Administration</i>	Describes administrative tasks you can perform for Entire Net-Work Client.
<i>Entire Net-Work Server Administration</i>	Describes administrative tasks you can perform for Entire Net-Work Server.
<i>Port Number Reference</i>	Lists the port numbers in use by Adabas products.
<i>Glossary</i>	Provides a glossary of terms in use for Adabas and Entire Net-Work products.





# 1 Entire Net-Work Administration LUW Concepts

---

Entire Net-Work Administration LUW is the product component that provides the System Management Hub (SMH) as well as the SMH agents necessary to perform Entire Net-Work, Entire Net-Work Client, Adabas Directory Server, and Adabas Administration Services management tasks.

The System Management Hub (SMH) provides centralized management of all Software AG products installed in the enterprise, using a Web-based graphical user interface. 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.

SMH can be used 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.



**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, Entire Net-Work Client, Adabas Directory Server, or Adabas Administration Services.

If SMH is not installed in your enterprise, it will be installed when you install Entire Net-Work Administration LUW.

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 the installation for Entire Net-Work Administration LUW on the machine on which SMH is installed to ensure that the appropriate product agents required for SMH are installed.

For more information about the management tasks that can be performed using Entire Net-Work Administration LUW, read the remaining chapters of this guide.



## 2 Release Notes

---

■ Enhancements .....	4
■ End of Maintenance .....	4
■ Documentation and Other Online Information .....	4

This chapter describes the new and changed features of the 1.4 SP1 version of Entire Net-Work Administration LUW.

## Enhancements

---

The primary enhancement is a roll up of previous fixes to Entire Net-Work Administration LUW the previous version. No changes in functionality are introduced in this release. Please see the product ReadMe file for last minute information.

As of this release, fixes to Entire Net-Work Administration LUW will be delivered using Software AG Update Manager. For more details, see section *Installing and Uninstalling Entire Net-Work Administration LUW* of this documentation.

## 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.

## Documentation and Other Online Information

---

The following online resources are available for you to obtain up-to-date information about your Software AG products:

- [Software AG Documentation Website](#)
- [Software AG TECHcommunity](#)

- [Software AG Empower Product Support Website](#)

## Software AG Documentation Website

You can find documentation for all Software AG products on the Software AG Documentation website at <http://documentation.softwareag.com>. This site requires Empower credentials. 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) or you can also use the TECHcommunity website to access the latest documentation.

## Software AG TECHcommunity

You can find documentation and other technical information on the Software AG TECHcommunity website at <http://techcommunity.softwareag.com>. You can:

- Access product documentation, if you have TECHcommunity credentials. If you do not, you will need to register and specify "Documentation" as an area of interest. If you already have TECHcommunity credentials, you can adjust your areas of interest on the TECHcommunity website by editing your TECHcommunity profile. To access documentation in the TECHcommunity once you are logged in, select **Documentation** from the **Communities** menu.
- Access articles, demos, and tutorials.
- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.
- Link to external websites that discuss open standards and web technology.

## Software AG Empower Product Support Website

You can find product information on the Software AG Empower Product Support website at <https://empower.softwareag.com>. This site requires Empower credentials. 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).

To submit feature/enhancement requests, get information about product availability, and download products and certified samples, select **Products & Documentation** from the menu once you are logged in.

To get information about fixes and to read early warnings, technical papers, and knowledge base articles, select **Knowledge Center** from the menu once you are logged in.



# 3 Installing and Uninstalling Entire Net-Work Administration

## LUW

---

■ System Requirements .....	8
■ Configuration Considerations .....	11
■ Before You Begin .....	12
■ Installation Steps .....	12
■ Configuring Product Components for Windows Personal Firewall .....	14
■ Uninstallation Steps .....	15
■ Installing Fixes Using Software AG Update Manager .....	15
■ Uninstalling Fixes Using Software AG Update Manager .....	17

Entire Net-Work Administration LUW is installed using the Software AG Installer. It does not require a license key.

You can download the Software AG Installer from the Software AG Empower website at <https://empower.softwareag.com/>.

This chapter provides product-specific instructions for installing Entire Net-Work Administration LUW. It is intended for use with *Using the Software AG Installer*, which explains how to prepare your machine to use the Software AG Installer and how to use the Software AG Installer and Software AG Uninstaller to install and uninstall your products. The most up-to-date version of *Using the Software AG Installer* is always available in the webMethods product documentation located on the Software AG Empower website (<https://empower.softwareag.com/>).

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.



**Important:** Please apply CUP 9.8 Fix1 using the Software AG Update Manager if you are installing the Administration component from the 2016 October release, which includes the installation of the System Management Hub. For information on using the Software AG Update Manager, please refer to the document *Using the Software AG Update Manager* in Software AG's Online Documentation Center on Software AG's **Empower** web site.

This chapter covers the following topics:

## System Requirements

---

This section describes the system requirements of Entire Net-Work Administration LUW.

- [Supported Operating System Platforms](#)
- [Supported Hardware](#)
- [Supported Browsers](#)
- [Space Requirements](#)
- [Windows Requirements](#)



## ■ Firewall Requirements

### Supported Operating System Platforms

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

For information regarding Software AG product compatibility with IBM platforms and any IBM requirements for Software AG products, please review the [Product Compatibility for IBM Platforms](#) web page.

Before attempting to install this product, ensure that your host operating system is at the minimum required level. For information on the operating system platform versions supported by Software AG products, complete the following steps.

1. Access Software AG's Empower web site at <https://empower.softwareag.com>.
2. Log into Empower. Once you have logged in, you can expand **Products & Documentation** in the left menu of the web page and select **Product Version Availability** to access the Product Version Availability screen.
3. Use the fields on the top of this screen to filter its results for your Software AG product. When you click the **Search** button, the supported Software AG products that meet the filter criteria are listed in the table below the filter criteria.

This list provides, by supported operating system platform:

- the Software AG general availability (GA) date of the Software AG product;
- the date the operating system platform is scheduled for retirement (OS Retirement);
- the Software AG end-of-maintenance (EOM) date for the product; and
- the Software AG end-of-sustained-support (EOSS) date for the product.



**Note:** Although it may be technically possible to run a new version of your Software AG product on an older 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 one listed on the Product Version Availability screen described above, consult Software AG technical support to determine whether support is possible, and under what circumstances.

## Supported Hardware

For general information regarding Software AG product compatibility with other platforms and their requirements for Software AG products, visit Software AG's [Hardware Supported](#) web page.

## Supported Browsers

The System Management Hub requires an Internet browser. For information on supported browsers, see the *webMethods System Requirements* documentation on the Empower web site.

## Space Requirements

The following table displays the minimum disk space requirements on Windows and UNIX systems for various Adabas LUW and Entire Net-Work LUW products, including the Adabas Directory Server:

Product	Space Requirement
Entire Net-Work Administration LUW	5 MB
Entire Net-Work Client	25 MB
Entire Net-Work Server	30 MB
Adabas Directory Server	20 MB

## Windows Requirements

In Windows environments, be sure to install Microsoft Visual Studio 2008 Redistributable Package.

## Firewall Requirements

If you attempt to install and use this software in a system with a firewall in place, be sure that your system administrator has set up the firewall so that the component applications can access the ports they need (including the Adabas Directory Server port and any ports Entire Net-Work dynamically assigns during its own processing). For more information about port usage, read the *Port Number Reference* found elsewhere in this documentation.

## Configuration Considerations

---

This section describes configuration issues you should consider before you install the Entire Net-Work Administration LUW.

- [How Many Entire Net-Work Administration LUWs Should You Install?](#)
- [Where Should You Install Entire Net-Work Administration LUW?](#)
- [Port Number Considerations](#)

### How Many Entire Net-Work Administration LUWs Should You Install?

If Entire Net-Work Administration LUW and the System Management Hub (SMH) are already installed in your enterprise, they should not be installed again. Only one SMH is required to manage all Software AG products that require it. SMH is used to perform administration on Adabas Administration Services, Entire Net-Work Client, Entire Net-Work Server, and the Adabas Directory Server.

If SMH is not installed in your enterprise, you must install it when you install Entire Net-Work Administration LUW.

### Where Should You Install Entire Net-Work Administration LUW?

Although you can install the Entire Net-Work Administration LUW on the same machines as your other Software AG products, Software AG does not recommend it. The primary reason is simply that your system performance could be impacted.

### Port Number Considerations

Port numbers used by Adabas LUW and Entire Net-Work LUW products are described in the [Port Number Reference](#), elsewhere in this guide. If the System Management Hub is being installed with Entire Net-Work Administration LUW, it requires its own set of port numbers. For more information about any System Management Hub installation issues, read *Installing webMethods Products* in the webMethods product documentation located on the Software AG Empower website (<https://empower.softwareag.com/>).

## Before You Begin

---

Before you begin installing this product, ensure that the following prerequisites have been met:

1. Software AG strongly recommends that you create an installation image of your existing Software products and store the image on your internal network. You should create an image for each operating system on which you plan to run the installation (for example, 32-bit, 64-bit, or both). This will help you reduce WAN traffic and speed up installation and will ensure consistency across installations over time, since the Software AG Installer provides only the latest release of each product.
2. Close (stop) all open applications, especially those applications interacting with or depending on your Adabas databases. This includes Natural, Adabas Manager, the Adabas DBA Workbench, and prior releases of any other Adabas products. To be on the safe side, also shut down all Software AG services.



**Important:** For some Software AG products, the Software AG Uninstaller will not be able to remove key files that are locked by the operating system if the associated Software AG products are not shut down.

3. Disable any antivirus software.
4. Ensure the target computer is connected to the network.
5. If this product requires a license key file, verify the license key file is copied somewhere in your environment. Products requiring license key files will not run without valid license keys. For more information, read *The License Key*, elsewhere in this section.
6. Verify your environment supports the system requirements for this product, as described in *System Requirements*, elsewhere in this section.

## Installation Steps

---

Entire Net-Work Administration LUW is installed using the Software AG Installer. This installation documentation provides a brief description on how to install the Entire Net-Work Administration LUW directly on the target machine using the installer wizard. For detailed information on the installer wizard, read *Using the Software AG Installer*.



**Note:** Read *Using the Software AG Installer* also if you want to use console mode, or if you want to install using an installation script or installation image.

➤ **To install Entire Net-Work Administration LUW, complete the following steps:**

- 1 Start the Software AG Installer as described in *Using the Software AG Installer*.

- 2 When the first page of the Software AG Installer wizard (the Welcome panel) appears, choose the **Next** button repeatedly, specifying all required information on the displayed panels, until the panel containing the product selection tree appears.

All Adabas-related products (including Adabas Directory Server) can be selected for installation within the **Adabas Family** product selection tree.

In addition to the **Adabas Family** product selection tree, two other trees, **Event-Driven Architecture** and **Infrastructure** (which includes the System Management Hub installation) are available for installation. The **Infrastructure** tree must be selected for all Software AG products; it provides the necessary Java runtime environment for the Software AG Installer.

- 3 To install Entire Net-Work Administration LUW, select (check) the Entire Net-Work Administration LUW entry from the **Adabas Family** product selection tree.



**Note:** When you select Entire Net-Work Administration LUW, the appropriate **Event-Driven Architecture** and **Infrastructure** entries, including the System Management Hub, are also selected unless they are already installed on the machine. You can opt to install other Software AG products from this list at the same time. This section just describes the installation of Entire Net-Work Administration LUW.

- 4 On the License panel, read the license agreement and select the check box to agree to the terms of the license agreement and then click **Next** to continue. If you do not accept the license agreement, the installation will stop.
- 5 A series of **Configure** panels may appear in the installation on which you specify:
  - The port numbers that should be used for the System Management Hub. For more information about any System Management Hub installation issues, including port number settings, read *Installing webMethods Products* in the webMethods product documentation located on the Software AG Empower website (<https://empower.softwareag.com/>).
  - The URL and port number for the Directory Server that should be used for this installation. The default is `tcpip://localhost:4952`.

For complete information on the ports used by Adabas LUW and Entire Net-Work LUW products, read [Port Number Reference](#), elsewhere in this guide.

Click **Next** to continue.

- 6 On the last panel, review the items you have selected for installation. If the list is correct, choose the **Next** button to start the installation process. Software AG Directory Server Installation and Administration Guide

## Configuring Product Components for Windows Personal Firewall

If you have the default Microsoft Windows personal firewall enabled on a PC and you would like to install and run Adabas and 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.

- [Allow Ports for a Specific Executable Program](#)
- [Open a Specific Port](#)



**Note:** If you attempt to install Adabas or Entire Net-Work in a system with a firewall in place, be sure that your system administrator has opened the firewall for the Adabas 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 Adabas and Entire Net-Work component files that might need to be allowed if Windows personal firewall is enabled:

Component Name	Path and File Name
Entire Net-Work Client Service	<i>&lt;your-installation-location&gt;\EntireNetWorkClient\bin\wclservice.exe</i>
Entire Net-Work Kernel program	<i>&lt;your-installation-location&gt;\EntireNetWorkServer\bin\wcpkernel.exe</i>
Entire Net-Work Server Service	<i>&lt;your-installation-location&gt;\EntireNetWorkServer\bin\wcpSERVICE.exe</i>
Adabas Directory Server Service	<i>&lt;your-installation-location&gt;\SoftwareAG\SoftwareAgDirectoryServer\bin\xtsdssvcadi.exe</i>
System Management Hub (SMH) CSLayer Service	<i>&lt;your-installation-location&gt;\InstanceManager\bin\argsrv.exe</i>
System Management Hub (SMH) EventLayer Service	<i>&lt;your-installation-location&gt;\InstanceManager\bin\argevsrv.exe</i>

To remove the Adabas or 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 an Adabas or 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.

## Uninstallation Steps

---

You uninstall this product using the Software AG Uninstaller. For information on how to use the uninstaller, read the *Using the Software AG Installer* guide.

## Installing Fixes Using Software AG Update Manager

---

Entire Net-Work Administration LUW is updated using the Software AG Update Manager (SUM).

You can download the Software AG Update Manager from the Software AG Empower website at <https://empower.softwareag.com/>.

This SUM installation documentation on Empower provides a brief description on how to update Software AG products directly on the target machine using the Update Manager wizard. The SUM

documentation also includes instructions on how to apply updates in console mode or using scripts.

➤ **To update Entire Net-Work Administration LUW, complete the following steps:**

- 1 Download and install Software AG Update Manager for your platform from Empower.
- 2 Shut down any running instances of the product. Updates cannot successfully apply if the application is active.
- 3 From a console prompt in the SUM */bin* directory, enter `UpdateManagerGUI.bat` (`UpdateManagerGUI.sh` on UNIX/Linux).
- 4 On the opening page of the SUM tool, select **Install Fixes from Empower**, enter your SAG product directory root location and provide your Empower User ID and password. Click **Next**.
- 5 Expand through the **Adabas Family** product selection tree to find the entry for this product.



**Tip:** If the product is not shown in the tree, there is either no update available or the product is not installed in the location you specified.

- 6 Select (check) the **Entire Net-Work Administration LUW** entry in the product selection tree. Click **Next**.



**Tip:** You can select more than one product to update before proceeding.

- 7 The next screen presents a summary of products that are about to be updated. If any of them require manual pre-installation steps, they will be highlighted in red and you will be directed to read the update readme file for that product before proceeding.

Complete any pre-installation steps outlined in the readme file and check the box next to **Pre-installation steps have been completed**. Click **Next**.



**Note:** If any pre-installation steps are required, the **Next** button will be unavailable until you confirm these steps have been completed.

- 8 The tool will apply updates to all selected products and present you with a final screen confirming updates have been applied. Click **Close** to exit SUM or **Home** to return to the tool's starting panel.



## Uninstalling Fixes Using Software AG Update Manager

---

➤ To remove an installed update, complete the following steps:

- 1 Shut down any running instances of the product.
- 2 Start Software AG Update Manager.
- 3 On the opening page, select **Uninstall Fixes** from the selection panel. Click **Next**.
- 4 If any product selected for uninstall requires manual steps, you will be directed to review the update readme and confirm you have performed any pre-uninstallation steps. Click **Next**.
- 5 The fix(es) you selected for uninstall will be removed and the product(s) returned to their previous state. Click **Close** to exit SUM or **Home** to return to the tool's starting panel.



## 4 About the System Management Hub

---

■ Accessing the System Management Hub .....	20
■ Leaving the System Management Hub .....	21
■ Using the Refresh Button in the System Management Hub .....	22
■ Getting Help .....	22

The System Management Hub (SMH) is a Web-based graphical user interface (GUI) you can use to perform administrative tasks for some Software AG products, including Adabas Directory Server, Adabas Administration Services, and Entire Net-Work. It runs in a standard Web browser.

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, available on Empower.

This chapter provides a high-level overview of the System Management Hub.

## 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 49981) 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.

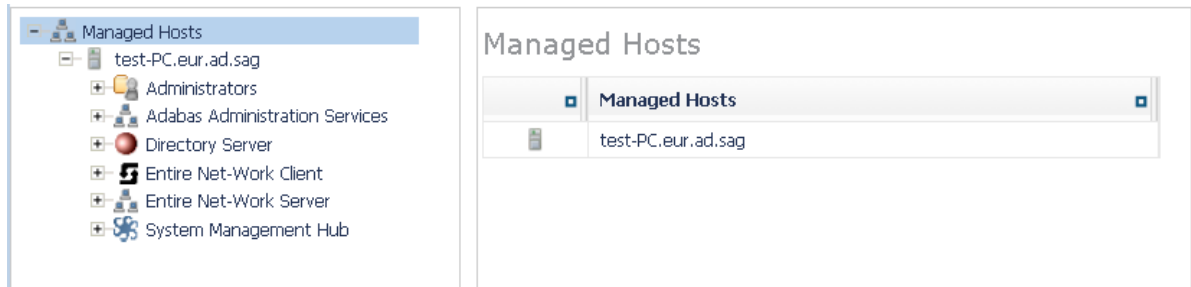
Or:

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*.

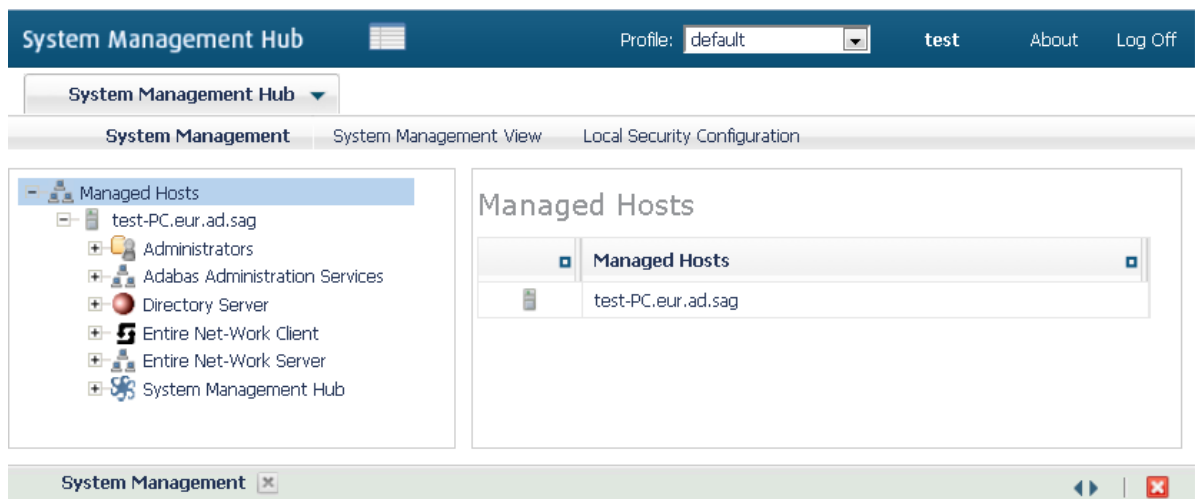
The System Management Hub main panel appears on the **System Management** tab.



## 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

---

➤ To get help on an detail-view frame:

- 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 view appears.

For complete information about the System Management Hub, read its documentation, available on Empower.

# 5

## Performing Adabas Directory Server Administration

---

■ Accessing the Directory Server Area of System Management Hub .....	24
■ Refreshing SMH Displays .....	25

Adabas Directory Server administration tasks are largely performed using the System Management Hub.



**Note:** Within SMH, two types of Directory Server administration are listed: Flat Files and Directory Servers. Software AG products do not use the **Flat File** maintenance option of the Directory Server administration. All administration tasks are performed using the **Directory Servers** maintenance option. For this reason, only the **Directory Servers** maintenance options are described in this guide.

Other sections describing Directory Server administration include:

- [Maintaining Directory Server Links](#)
- [Maintaining Partitions](#)
- [Maintaining Targets](#)
- [Changing Hosts](#)

## Accessing the Directory Server Area of System Management Hub

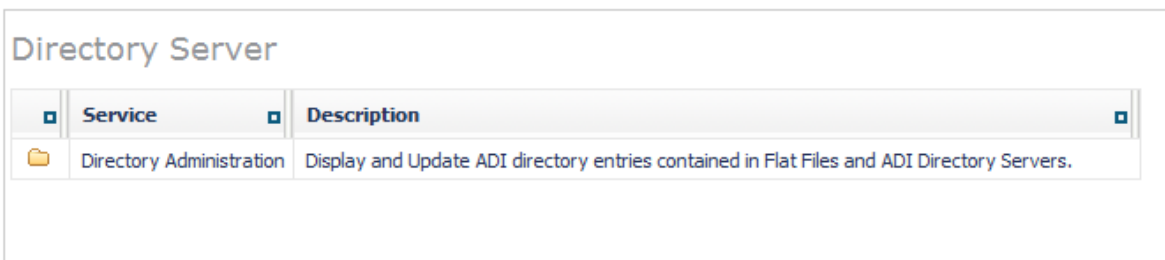
---

➤ To access the Directory Server 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 the Directory Server 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 and expand "Directory Server" in the tree-view under the managed host.

The Adabas Directory Server area of the System Management Hub becomes available to you.



- 4 Select and expand **Directory Administration** in the tree-view frame.

Two types of Adabas Directory Server administration are listed: **Flat Files** and **Directory Servers**.





**Note:** Software AG products do not use the **Flat File** maintenance option of the Adabas Directory Server administration. All administration tasks are performed using the **Directory Servers** maintenance option. For this reason, only the **Directory Servers** maintenance options are described in this section.

- 5 Select and expand Directory Servers in the tree-view frame.

The Directory Server administration area appears in the detail-view frame.



**Note:** The "No Directories have been defined!" error message displays in the detail-view frame and is expected if no directory servers have been defined.

Directory Servers			
Directory Name:	Host/IP Address	Listen Port	Status
sag-adi	localhost	4952	Unreachable

The following commands are available by right-clicking on **Directory Servers** in tree-view:



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

Command	Use this command to:
Add Directory Server	Add a new directory server, linked to this SMH.
Refresh	Refresh the screen.

## Refreshing SMH Displays

The **Refresh** command appears on the drop-down menus of the System Management Hub for many Directory Server maintenance panels. Use the **Refresh** command to refresh the display of values listed in the detail-view frame.



# 6

## Maintaining Directory Server Links

---

■ Listing Linked Directory Servers .....	28
■ Adding a Link to a Directory Server .....	29
■ Modifying a Directory Server Link Definition .....	30
■ Listing Directory Server Parameters .....	32
■ Deleting a Link to a Directory Server .....	33

To maintain your Directory Servers, they must be linked to SMH. Once linked, any of the Directory Server's parameters, targets, partitions, and other settings can be modified using the SMH screens.

To maintain your Entire Net-Work target entries, you must have an Directory Server linked to SMH. A default link, called *sag-adi*, is automatically set up during Entire Net-Work installation.

Ordinarily, Directory Servers are installed as part of another Software AG product (for example, Entire Net-Work). When this type of installation occurs, the Directory Server is automatically linked to SMH. However, there may be instances in your environment where a Directory Server is already installed in a location unknown to SMH. In these cases, you must manually create a link for the Directory Server if you want to maintain it.



**Note:** Directory Servers linked to SMH can be maintained by any user with SMH access.

Using SMH, you can add, modify, and delete SMH links to installed Directory Servers.

## Listing Linked Directory Servers

➤ To list the installed Directory Servers that are linked to SMH:

- 1 Access the Directory Server administration area, as described in [The Directory Server Administration Area](#), earlier in this section.
- 2 Select **Directory Servers** in the tree-view frame.



**Note:** The "No Directories have been defined!" error message displays in the detail-view frame and is expected if no directory servers have been defined.

The list of directory servers linked to this System Management Hub appears in the detail-view frame.

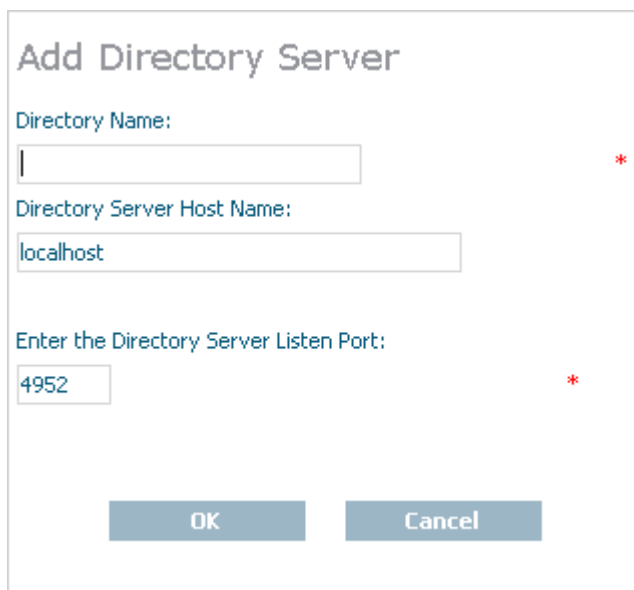
Directory Servers			
Directory Name: ▢	Host/IP Address ▢	Listen Port ▢	Status ▢
sag-adi	localhost	4952	Unreachable

## Adding a Link to a Directory Server

➤ To add a link in SMH to an installed Directory Server:

- 1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.
- 2 Right-click on **Directory Servers** in the tree-view frame and select the **Add Directory Server** in the resulting drop-down menu.

The **Add Directory Server** panel appears in the detail-view frame.



**Add Directory Server**

Directory Name:  \*

Directory Server Host Name:

Enter the Directory Server Listen Port:  \*

- 3 Specify a user-friendly name for the Directory Server in the **Directory Name** field.
- 4 Specify the host name where the Directory Server is running in the **Directory Server Host Name** field. It can be a fully qualified name.



**Note:** Host names are case-sensitive in SMH.

Or:

Enter the IP address for the Directory Server as an alternative to a host name. We do not recommend using IP addresses instead of host names because IP addresses may change

- 5 Specify the **Directory Server Listen Port** as appropriate for your site.

You can no longer specify the port number as "0". If you are using an older Directory Server installation, it may have inherited a port number of "0". While this setting for older Directory

Server versions is still supported, a setting of "0" will default to "4952". If this default is not satisfactory for your installation (if any applications you are running expect a port number other than 4952), specify the non-zero port number that should be used. In fact, Software AG recommends that you change all Directory Server port numbers that have been set to "0" to valid non-zero numbers to avoid any confusion. If you do this, however, be sure that you have also changed the values of the `XTSDSURL` and `SAGXTSDSport` environment variables and the `SAGXTSDSport` DNS entry, wherever they might be set.

For more information about setting the Directory Server port number, read *The Directory Server Port Number* in the *Software AG Directory Server Installation and Administration Guide*.

If you have problems accessing the Directory Server once it is defined, contact your system administrator for the correct port setting to use.

- 6 Click OK.

A link to the Directory Server is added and should appear in the listing of Directory Servers in both the tree-view and detail-view frames.

## Modifying a Directory Server Link Definition

---

➤ To modify the link definition in SMH for an installed Directory Server:

- 1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.
- 2 Right-click on the name of the Directory Server whose link definition you wish to modify in the tree-view frame of SMH and select **Modify Directory Server Settings** from the resulting drop-down menu.

The **Modify Directory Server Settings** panel appears in the detail-view frame.

**Modify Directory Server Settings**

Directory Name:  
test-DS \*

Directory Server Host Name:  
localhost

Enter the Directory Server Listen Port:  
4952 \*

OK Cancel

- 3 Change the name for the Directory Server in the **Directory Name** field.
- 4 Change the host name where the Directory Server is running in the **Directory Server Host Name** field. It can be a fully qualified name.



**Note:** Host names are case-sensitive in SMH.

Or:

Change the IP address for the Directory Server. We do not recommend using IP addresses instead of host names because IP addresses may change

- 5 Change the **Directory Server Listen Port** as needed.

You can no longer specify the port number as "0". If you are using an older Directory Server installation, it may have inherited a port number of "0". While this setting for older Directory Server versions is still supported, a setting of "0" will default to "4952". If this default is not satisfactory for your installation (if any applications you are running expect a port number other than 4952), specify the non-zero port number that should be used. In fact, Software AG recommends that you change all Directory Server port numbers that have been set to "0" to valid non-zero numbers to avoid any confusion. If you do this, however, be sure that you have also changed the values of the `XTSDSURL` and `SAGXTSDSport` environment variables and the `SAGXTSDSport` DNS entry, wherever they might be set.

For more information about setting the Directory Server port number, read *The Directory Server Port Number* in the *Software AG Directory Server Installation and Administration Guide*.

If you have problems accessing the Directory Server once it is defined, contact your system administrator for the correct port setting to use.

- 6 Click OK.

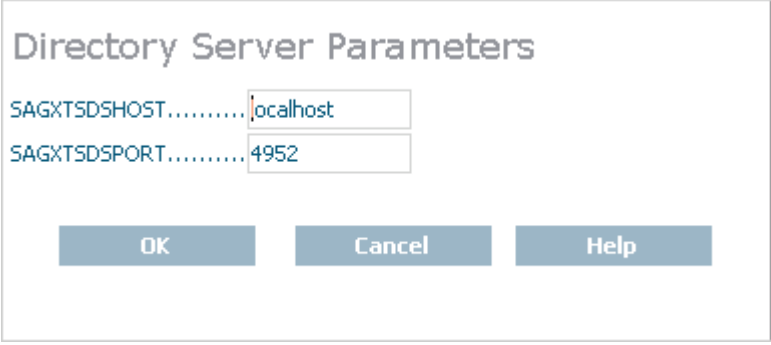
The Directory Server link definition is modified.

## Listing Directory Server Parameters

### » To display the parameters for a Directory Server:

- 1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.
- 2 Right-click on the name of the Directory Server whose parameters you wish to review in the tree-view frame of SMH and select **Display Directory Server Parms** from the resulting drop-down menu.

The **Display Directory Server Parms** panel appears in the detail-view frame.



The following table describes the parameters that are listed. These parameters are set automatically when Directory Server starts up. If you wish to change these values, contact Software AG Customer Support.

Parameter	Description
Version	A version number for internal use only.
Listen Port	The listen port used by this Directory Server. The Directory Server uses this port to listen for target access and connection requests.
Trace Settings	The trace setting for this Directory Server.
Debug Settings	The debug setting for this Directory Server.
Log Directory	The full path of the directory in which trace logs are written for this Directory Server.
Directory Type	The type of Directory Server.
Directory Parms	The full path name of the URL configuration file for this Directory Server.



## Deleting a Link to a Directory Server

---

➤ **To delete the link to an Directory Server in SMH:**

- 1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.
- 2 Click on the name of the Directory Server whose definition you wish to delete in the tree-view frame of SMH.

The targets for that Directory Server are listed in the detail-view frame.

- 3 Right-click on the name of the Directory Server whose definition you wish to delete and select **Delete Directory Server Entry** on the resulting drop-down menu.

The **Delete Directory Server Entry** panel appears in the detail-view frame.

- 4 Click OK.

The Directory Server definition is deleted.



# 7

## Maintaining Partitions

---

■ Listing the Partitions .....	36
■ Adding a Partition .....	37
■ Changing a Partition Name .....	37
■ Deleting a Partition .....	38

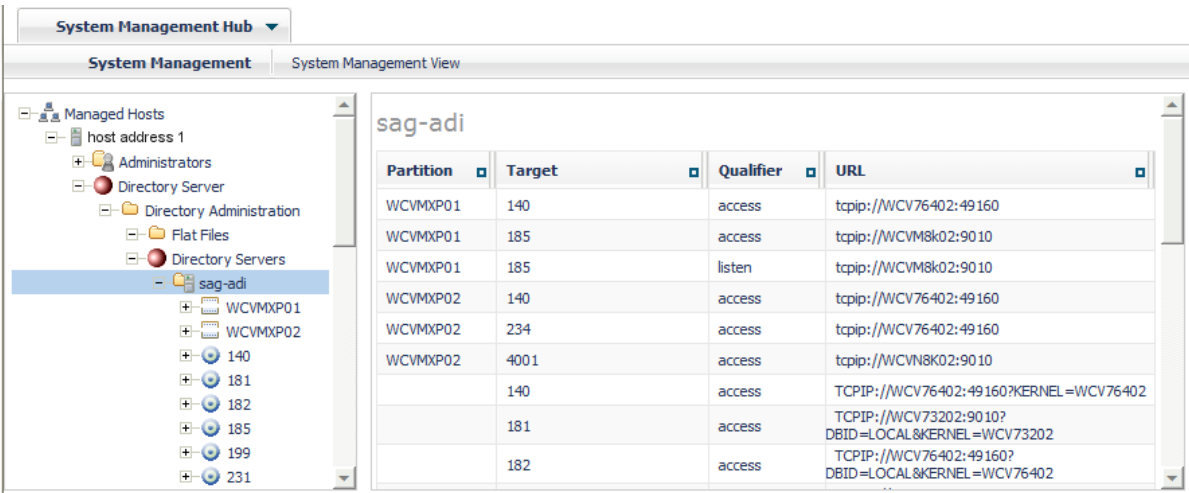
# Listing the Partitions

You can list the partitions defined for a Directory Server using the System Management Hub.

➤ **To list the partitions defined in a Directory Server:**

- 1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.
- 2 Click and expand the name of the Directory Server whose partitions you wish to review in the tree-view frame of SMH.

The targets and partitions for that Directory Server are listed in the detail-view frame and under the Directory Server name in the tree-view frame. Partitions are identified by the square icon ( ).



Targets are initially listed by partition, in the order they appear in the Directory Server. You can change the sort order of the list by clicking on the arrows in the column headings of the table in the detail-view frame. If you click on an up arrow in the column heading, the display is sorted alphabetically by the contents in that column. If you click on a down arrow in the column heading, the display is sorted in reverse alphabetic order by the contents in that column.


## Adding a Partition

You can add a partition to a Directory Server using the System Management Hub.

➤ **To add a partition in the Directory Server:**

- 1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.
- 2 In the tree-view frame of SMH, right-click on the name of the Directory Server to which you want to define partitions and select **Add Partition** from the resulting drop-down menu.

The Add Partition panel appears in the detail-view frame.

A screenshot of the 'Add Partition' dialog box. The title bar says 'Add Partition'. Inside, there is a label 'Enter the Partition Name:' followed by a text input field. A red asterisk is to the right of the input field, indicating a required field. Below the input field are two buttons: 'OK' and 'Cancel'.

- 3 Specify a name for the partition in the **Enter the Partition Name:** field.
- 4 Click OK.

The partition is added for the Directory Server and the added partition displays in the System Management Hub tree-view frame.



**Note:** No targets are defined initially for a partition. You must define them now.

## Changing a Partition Name

You can change the name of a partition defined for a Directory Server using the System Management Hub.

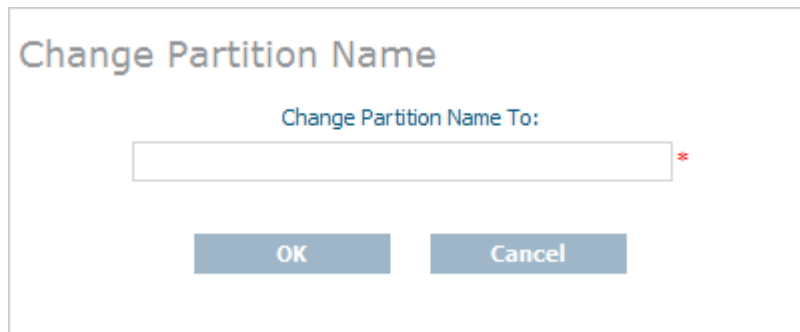


**Caution:** When you rename a partition, all of the target definitions defined for that partition remain with the partition under its new name.

➤ **To change the name of a partition:**

- 1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.
- 2 In the tree-view frame of SMH, right-click on the name of the Directory Server containing the partition you want to rename and select **Change Partition Name** from the resulting drop-down menu.

The **Change Partition Name** panel appears in the detail-view frame.



The image shows a dialog box titled "Change Partition Name". Inside the dialog, there is a label "Change Partition Name To:" followed by a text input field. A red asterisk is visible to the right of the input field, indicating a required field. Below the input field are two buttons: "OK" and "Cancel".

- 3 Specify a new name for the partition in the **Change Partition Name To** field.
- 4 Click OK.

The partition is renamed displays in the System Management Hub tree-view frame with its new name. All of its target definitions remain with the partition under its new name.

## Deleting a Partition

---

You can delete a partition defined for a Directory Server using the System Management Hub.



**Caution:** When you delete a partition, all of the target definitions defined for that partition are also deleted.

➤ **To delete a partition in a Directory Server:**

- 1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.
- 2 In the tree-view frame of SMH, click on the name of the Directory Server containing the the partition you wish to delete.

The partitions and targets for that Directory Server are listed in the detail-view frame.

- 3 Right-click on the partition you wish to delete and select **Delete Partition** from the resulting drop-down menu.

The Delete Partition panel appears in the detail-view frame.

- 4 Click OK.

The partition and all of its associated target definitions are deleted.






## 8 Maintaining Targets

---

■ Listing the Targets .....	42
■ Adding Targets .....	43
■ Maintaining Qualified URLs .....	47
■ Setting the Target Type .....	70
■ Changing the Target Name .....	72
■ Changing the Host .....	73
■ Changing the Protocol .....	73
■ Deleting a Target .....	75


Directory Server target definitions and their associated qualified URLs can be maintained using the System Management Hub.

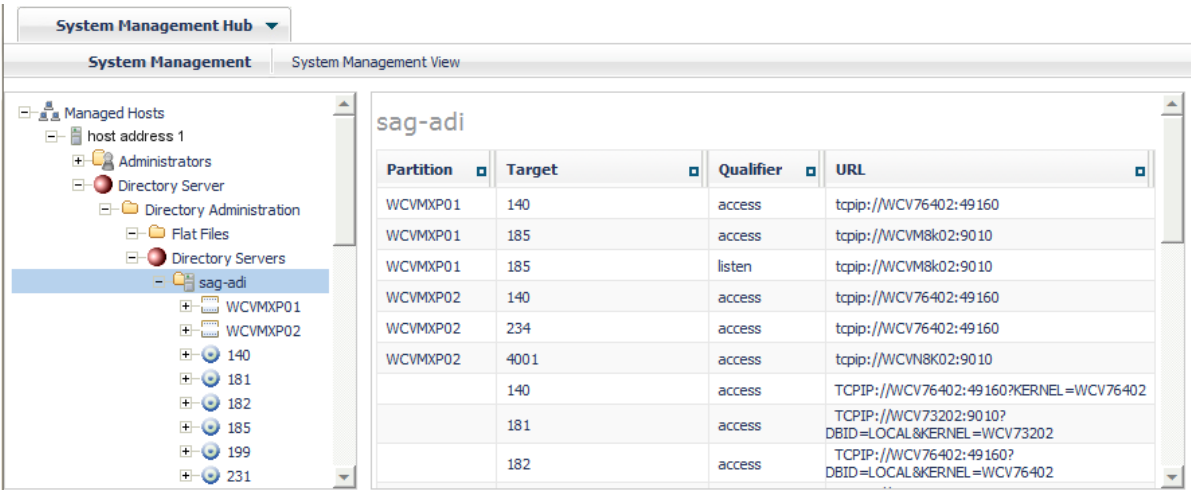
 **Note:** Some Software AG products that use the Directory Server may need to be stopped and restarted if you make changes to Directory Server qualified URLs while the Software AG product is running. One example of such a product is Entire Net-Work 7 (open systems).

## Listing the Targets

➤ To list the targets defined in a Directory Server:

- 1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.
- 2 Click and expand the name of the Directory Server or the partition within a Directory Server whose targets you wish to review in the tree-view frame of SMH.

The targets for that Directory Server are listed in the detail-view frame and under the Directory Server or partition name in the tree-view frame. Targets are identified by the red circle icon (  ).



Partition	Target	Qualifier	URL
WCVMP01	140	access	tcpip://WCV76402:49160
WCVMP01	185	access	tcpip://WCV802:9010
WCVMP01	185	listen	tcpip://WCV802:9010
WCVMP02	140	access	tcpip://WCV76402:49160
WCVMP02	234	access	tcpip://WCV76402:49160
WCVMP02	4001	access	tcpip://WCV802:9010
	140	access	TCPIP://WCV76402:49160?KERNEL=WCV76402
	181	access	TCPIP://WCV73202:9010?DBID=LOCAL&KERNEL=WCV73202
	182	access	TCPIP://WCV76402:49160?DBID=LOCAL&KERNEL=WCV76402

Targets are initially listed by partition, in the order they appear in the Directory Server. You can change the sort order of the target list by clicking on the arrows in the column headings of the table in the detail-view frame. If you click on an up arrow in the column heading, the display is sorted alphabetically by the contents in that column. If you click on a down arrow in the column heading, the display is sorted in reverse alphabetic order by the contents in that column.

## Adding Targets

You can add targets to the Directory Server directly, within a partition of the Directory Server, or both. For information on the use of partitions in a Directory Server, read *Partitioning a Directory Server* in the *Software AG Directory Server Installation and Administration Guide*.

When you add a target definition, an "access" qualified URL and a "listen" qualified URL are automatically created. In the case of ADATCP and Entire Net-Work 7.x, the "listen" URL is not required and can be deleted. For information on deleting qualified URLs, read [Deleting Qualified URLs](#), elsewhere in this section.



**Note:** ADATCP connections do not support IPv6 communication.

For information on modifying or adding additional qualified URLs for the target definition, including specifying parameters for the URL, read [Maintaining Qualified URLs](#), elsewhere in this section.

### » To add a target definition:

- 1 Access the Directory Server administration area, as described in [The Directory Server Administration Area](#), earlier in this section.
- 2 In the tree-view frame of SMH, click on the name of the Directory Server to which you want to define the target.

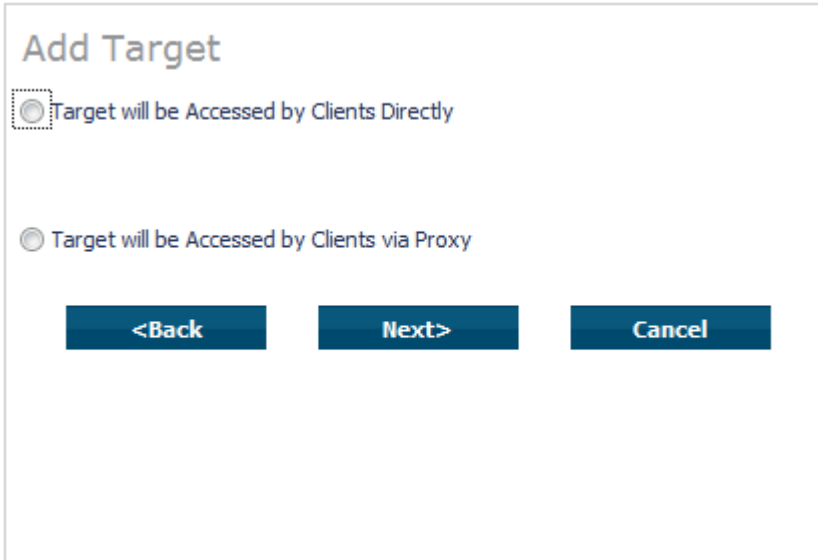
The partitions and targets already defined for that Directory Server are listed in the detail-view frame and under the Directory Server name in the tree-view frame.

- 3 Optionally, if you want to define the target to a specific partition, click and expand the a name of the partition in the tree-view frame of SMH.
- 4 Right-click on the name of the Directory Server or partition to which you wish to add the target and select **Add Target** from the resulting drop-down menu.

The first panel in the **Add Target** panel series appears in the detail-view frame. In the following sample panel, the target is being added to the Directory Server directly and not to a partition within the Directory Server.

- 5 Enter the database ID (DBID) into the **Target Name or ID** field.
- 6 Ensure that the **Server** option is selected.
  - The **Server** option is usually the option you should select.
  - The **Replicated Server** option is reserved for future use by Software AG.
  - The **Proxy** option is only applicable to configurations requiring a proxy. It is provided for compatibility with Software AG products that still require a proxy. If your Software AG product requires a proxy, refer to the documentation for your Software AG product for information about proxies and how to configure them in SMH.
  - The **Entire Net-Work (2.x, 5.x) Accessed Database via a Proxy** option is only applicable to installations that still maintain Entire Net-Work version 2 (open systems) or Entire Net-Work version 5 (mainframe) systems . This option is provided only for compatibility with these older, unsupported versions of these Software AG products; connections to these older systems must be done via a proxy.
- 7 Click **Next**.

The next panel in the **Add Target** panel series appears in the detail-view frame.




**Add Target**

☒ Target will be Accessed by Clients Directly

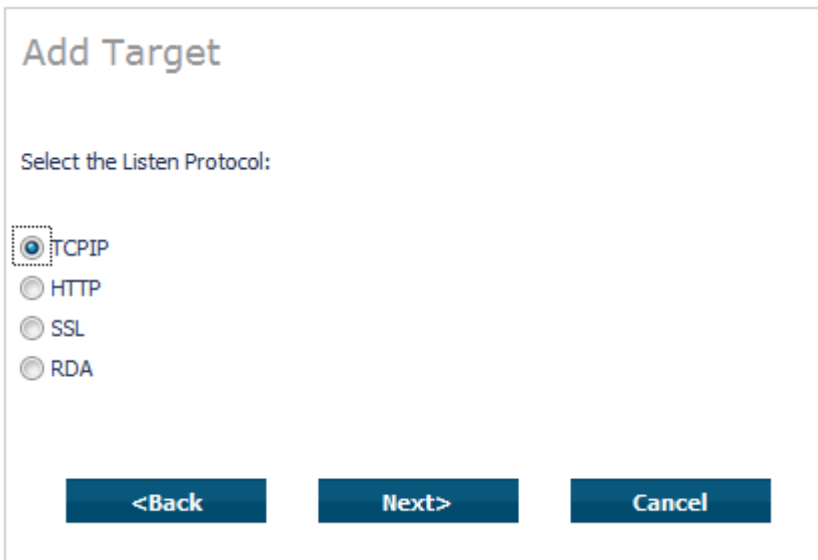
☐ Target will be Accessed by Clients via Proxy

**<Back** **Next>** **Cancel**

- 8 Select the **Target will be Accessed by Clients Directly** option, then click **Next**.

 **Note:** The **Target will be Accessed by Clients via Proxy** option is only provided for compatibility with Software AG products that still require a proxy. If your Software AG product requires a proxy, refer to the documentation for your Software AG product for information about them.

The next panel in the **Add Target** panel series appears in the detail-view frame.



**Add Target**

Select the Listen Protocol:

☒ TCPIP

☐ HTTP

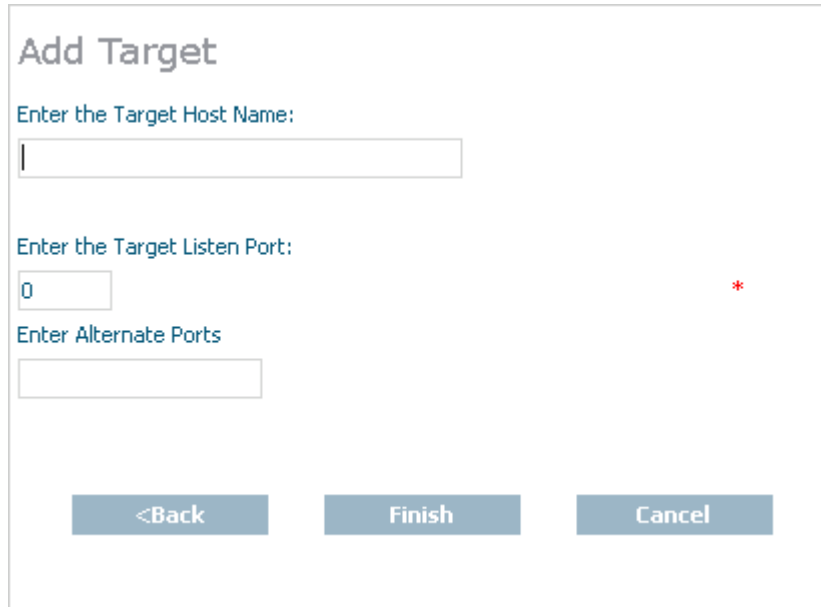
☐ SSL

☐ RDA

**<Back** **Next>** **Cancel**

- 9 Select the listen protocol, then click **Next**. In most cases, the listen protocol will be **TCPIP**. For a complete description of these protocols, read *Protocols* in the *Software AG Directory Server Installation and Administration Guide*.

The final panel in the **Add Target** panel series appears in the detail-view frame.



**Add Target**

Enter the Target Host Name:

Enter the Target Listen Port:

0 \*

Enter Alternate Ports

<Back Finish Cancel

- 10 Specify the host name of the middleware in the **Target Host Name** field. This is the Entire Net-Work version 7 or ADATCP host name.



**Note:** Host names are case-sensitive in SMH.

Or:

Specify an IP address as an alternative to a host name. We do not recommend specifying IP addresses instead of host names as the IP address may change.

- 11 Enter the middleware's listen port into the **Target Listen Port** field.



**Note:** You can leave the **Alternate Ports** field blank, unless you want to enter alternate listen ports. If the **Target Listen Port** field is set to "0", you must specify alternate listening ports.

- 12 Click **Finish**.

A message displays indicating that the new target definition was added, and the added target displays in the tree-view frame.

## Maintaining Qualified URLs

Qualifiers identify the use of a target URL. Three qualifiers are supported in the Adabas Directory Server: access, connect, and listen. For more information about each qualifier, read *Qualifiers* in the *Software AG Directory Server Installation and Administration Guide*.

Using SMH, you can add and delete qualified URLs for a target. For more information about qualified URLs, read *Qualified URL Structure* in the *Software AG Directory Server Installation and Administration Guide*.

This section covers the following topics:

- [Listing Qualified URLs](#)
- [Adding Qualified URLs for the Target](#)
- [Deleting Qualified URLs](#)
- [Maintaining Qualified URL Parameters](#)
- [Changing Protocol, Host, and Port Values of the Qualified URL](#)

### Listing Qualified URLs

#### » To list the qualified URLs of a target:

- 1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.
- 2 In the tree-view frame of SMH, click and expand the name of the Directory Server containing the qualified URLs you wish to list.

The partitions and targets for that Directory Server are listed in the detail-view frame.

- 3 Click and expand the target whose qualified URLs you wish to list. If the target is in a partition, you must first select the partition and then click on the target.

The qualified URLs for the target are listed in the detail-view frame and under the target in the tree-view frame.

## Adding Qualified URLs for the Target

When you add qualifiers (qualified URLs) for a target, the entire target entry is created, including the qualifier and full URL of the entry.

### ➤ To add a qualified URL for a target:

- 1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.
- 2 In the tree-view frame of SMH, click and expand the name of the Directory Server in which you want to add a qualifier.

The partitions and targets for that Directory Server are listed in the detail-view frame.

- 3 Click and expand the target in which you want to add a qualifier. If the target is in a partition, you must first select the partition and then click on the target.
- 4 Right-click on the name of the target to which you want to add a qualifier and select **Add Qualifier** from the resulting drop-down menu.

The first panel in the **Add Qualifier** panel series appears in the detail-view frame.

**Add Qualifier**

Select the Qualifier Type to be Built:

- access
- listen
- connect

Select 'access' to define direct client access to target.

Select 'listen' to allow connects to the target.

Select 'connect' to define a connect from this target to another target.

Next> Cancel

- 5 Select the qualifier type (URL use) to be defined for this target entry. Three types of qualifiers are supported in the Adabas Directory Server: access, connect, and listen. For complete information on these qualifiers, read *Qualifiers* in the *Software AG Directory Server Installation and Administration Guide*.
- 6 Click **Next**.



Depending on the qualifier you specified in the previous step, different SMH panels appear. The rest of this section describes how to create target URL entries for each of these different qualifiers.

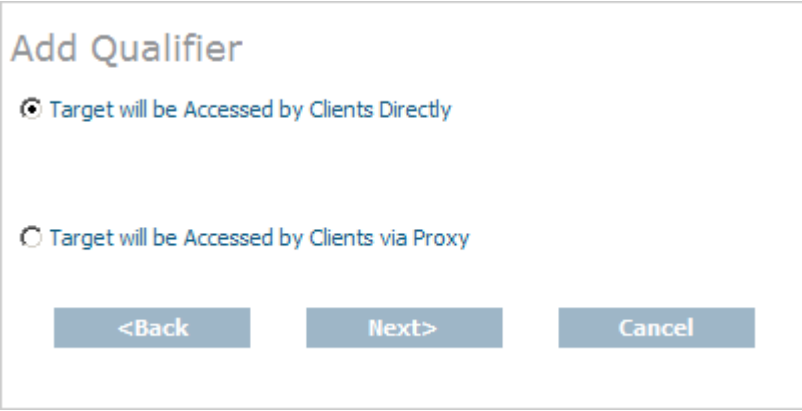
- [Creating an access URL](#)
- [Creating a connect URL](#)
- [Creating a listen URL](#)

### Creating an access URL

#### ➤ To create an access URL for a target:

- 1 Complete the first 4 steps described in [Adding Qualified URLs for the Target](#). When you get to Step 5, select **access** for the qualifier type. Then click **Next**.

A second panel appears in the detail-view frame, asking you to indicate how this target will be accessed.

A screenshot of a dialog box titled "Add Qualifier". It contains two radio button options. The first option, "Target will be Accessed by Clients Directly", is selected with a blue radio button. The second option, "Target will be Accessed by Clients via Proxy", is unselected with a grey radio button. At the bottom of the dialog, there are three buttons: "<Back", "Next>", and "Cancel".

- 2 Select the first option, **Target will be Accessed by Clients Directly**, and click **Next**.



**Note:** The **Target will be Accessed by Clients via Proxy** option is only provided for compatibility with Software AG products that still require a proxy. If your Software AG product requires a proxy, refer to the documentation for your Software AG product for information about them.

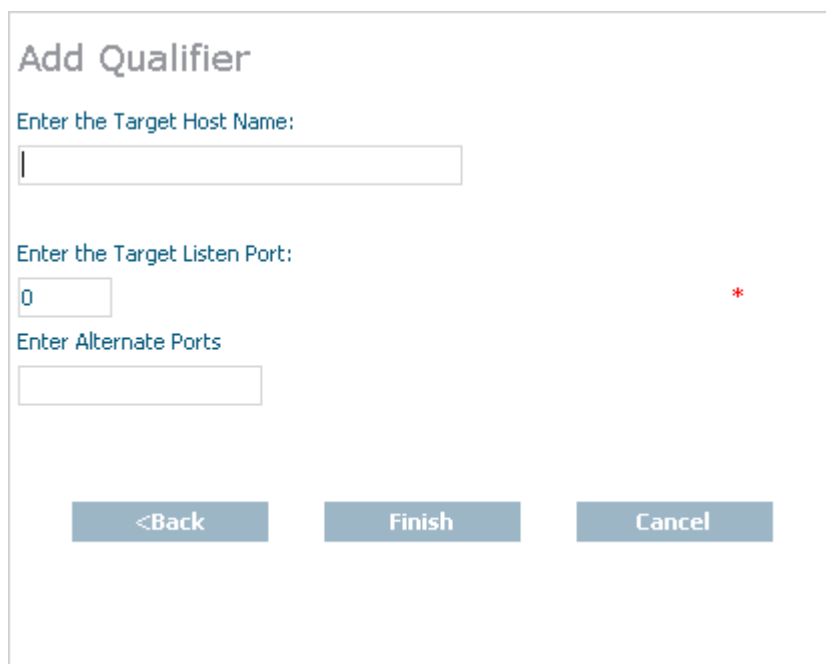
A protocol selection panel appears in the detail-view frame.



The 'Add Qualifier' dialog box has a title bar. Below the title, it says 'Select Protocol:'. There are four radio button options: TCPIP (which is selected and has a dashed box around it), HTTP, SSL, and RDA. At the bottom, there are three buttons: '<Back', 'Next>', and 'Cancel'.


- 3 Select the protocol for the qualified URL and click **Next**. In most cases, the protocol will be **TCPIP**. For more information on the supported protocols, read *Protocols* in the *Software AG Directory Server Installation and Administration Guide*.

The final panel in the **Add Qualifier** series of panels appears, requesting the host and port information for the qualified URL.



The 'Add Qualifier' dialog box shows the next step. It has three input fields: 'Enter the Target Host Name:' with a text box containing a vertical bar '|'; 'Enter the Target Listen Port:' with a text box containing '0' and a red asterisk '\*' to its right; and 'Enter Alternate Ports' with an empty text box. At the bottom, there are three buttons: '<Back', 'Finish', and 'Cancel'.

- 4 Specify the host name of the middleware in the **Target Host Name** field. This is the Entire Net-Work version 7 or ADATCP host name.

 **Note:** Host names are case-sensitive in SMH.

Or:

Specify an IP address as an alternative to a host name. We do not recommend specifying IP addresses instead of host names as the IP address may change.

- 5 Enter the middleware's listen port in the **Enter the Target Listen Port** field.

 **Note:** You can leave the **Enter Alternate Ports** field blank, unless you want to enter alternate listen ports.

- 6 Click **Finish**.

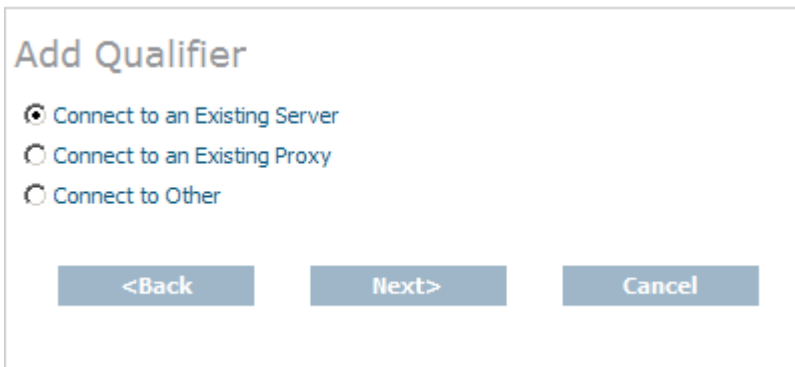
A message displays indicating that the new qualified access URL was added, and the added URL appears in the tree-view frame.

### Creating a connect URL

➤ To create a connect URL for a target:


- 1 Complete the first 4 steps described in [Adding Qualified URLs for the Target](#). When you get to Step 5, select **connect** for the qualifier type. Then click **Next**.

A second panel appears in the detail-view frame, asking you to indicate to what this target will connect.



The image shows a dialog box titled "Add Qualifier". It contains three radio button options: "Connect to an Existing Server" (which is selected), "Connect to an Existing Proxy", and "Connect to Other". At the bottom of the dialog, there are three buttons: "<Back", "Next>", and "Cancel".

- 2 Select the **Connect to an Existing Server** or **Connect to Other** option, and click **Next**.

 **Note:** The **Connect to an Existing Proxy** option is only provided for compatibility with Software AG products that still require a proxy. If your Software AG product requires a proxy, refer to the documentation for your Software AG product for information about them.

Depending on your selection, different panels appear.

- If you selected the **Connect to an Existing Server** or the **Connect to an Existing Proxy** options, a list of servers or proxies to which this target can connect is listed.

Select	Partition	Target	Protocol	Host	Port
<input checked="" type="radio"/> →		999	tcpip	localhost	9020

<Back      Finish      Cancel

Select the server or proxy for the connection definition and click **Finish**.

A message displays indicating that the new qualified connect URL was added, and the added URL appears in the tree-view frame.

- If you selected the **Connect to Other** option, a protocol selection panel appears in the detail-view frame.

Select Protocol:

☒ TCPIP  
☐ HTTP  
☐ SSL  
☐ RDA

<Back      Next>      Cancel

Select the protocol for the qualified URL and click **Next**. In most cases, the protocol will be **TCPIP**. For more information on the supported protocols, read *Protocols* in the *Software AG Directory Server Installation and Administration Guide*.

The final panel in the **Add Qualifier** series of panels appears, requesting the host and port information for the qualified URL.

**Add Qualifier**

Enter the Target Host Name:

Enter the Target Listen Port:  
 \*

Enter Alternate Ports

<Back      Finish      Cancel

Specify the host name of the middleware in the **Target Host Name** field. This is the Entire Net-Work version 7 or ADATCP host name. Alternatively, you can specify an IP address instead of a host name. We do not recommend specifying IP addresses instead of host names as the IP address may change.



**Note:** Host names are case-sensitive in SMH.

Enter the middleware's listen port in the **Enter the Target Listen Port** field.



**Note:** You can leave the **Enter Alternate Ports** field blank, unless you want to enter alternate listen ports.

If you selected the **Connect to an Existing Proxy** option, a protocol selection panel appears in the detail-view frame.

Click **Finish**.

A message displays indicating that the new qualified connect URL was added, and the added URL appears in the tree-view frame.

## Creating a listen URL

➤ To create a listen URL for a target:

- 1 Complete the first 4 steps described in [Adding Qualified URLs for the Target](#). When you get to Step 5, select **listen** for the qualifier type. Then click **Next**.

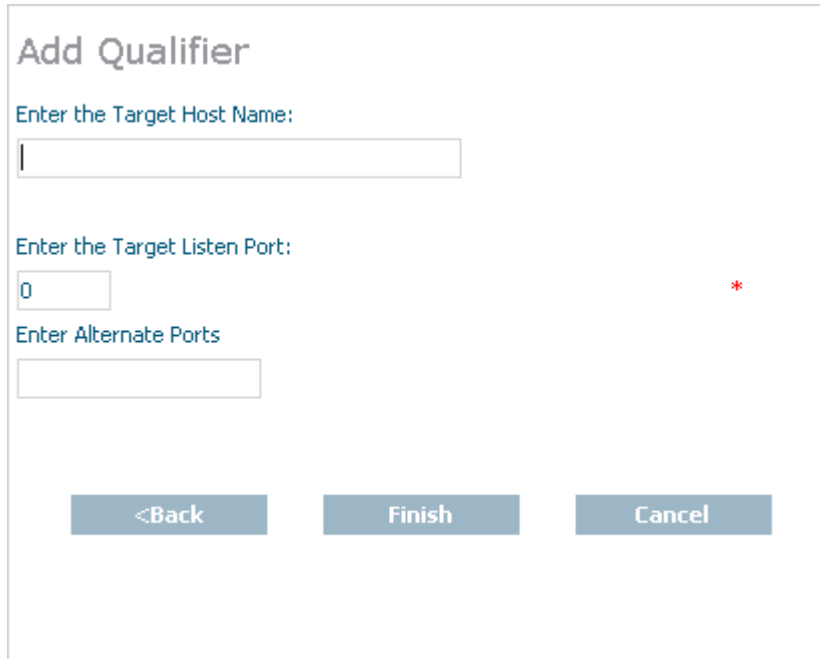
A protocol selection panel appears in the detail-view frame.



The image shows a dialog box titled "Add Qualifier". Inside the dialog, there is a label "Select Protocol:". Below this label, there are four radio button options: "TCPIP", "HTTP", "SSL", and "RDA". The "TCPIP" option is selected, indicated by a blue dot in the center of the radio button. At the bottom of the dialog, there are three buttons: "<Back", "Next>", and "Cancel".

- 2 Select the protocol for the qualified URL and click **Next**. In most cases, the protocol will be **TCPIP**. For more information on the supported protocols, read *Protocols* in the *Software AG Directory Server Installation and Administration Guide*.

The final panel in the **Add Qualifier** series of panels appears, requesting the host and port information for the qualified URL.



**Add Qualifier**

Enter the Target Host Name:

Enter the Target Listen Port:

Enter Alternate Ports

<Back Finish Cancel

- 3 Specify the host name of the middleware in the **Target Host Name** field. This is the Entire Net-Work version 7 or ADATCP host name.



**Note:** Host names are case-sensitive in SMH.

Or:

Specify an IP address as an alternative to a host name. We do not recommend specifying IP addresses instead of host names as the IP address may change.

- 4 Enter the middleware's listen port in the **Enter the Target Listen Port** field.



**Note:** You can leave the **Enter Alternate Ports** field blank, unless you want to enter alternate listen ports.

- 5 Click **Finish**.

A message displays indicating that the new qualified listen URL was added, and the added URL appears in the tree-view frame.

## Deleting Qualified URLs

### » To delete a qualifier from a target:

- 1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.
- 2 In the tree-view frame of SMH, click and expand the name of the Directory Server containing the qualifier you wish to delete.

The partitions and targets for that Directory Server are listed in the detail-view frame.

- 3 Click and expand the target containing the qualifier you wish to delete. If the target is in a partition, you must first select the partition and then click on the target.
- 4 Click on the qualifier you wish to delete.
- 5 Right-click on the name of the qualifier you wish to delete and select **Delete Qualifier** from the resulting drop-down menu.

The **Delete Qualifier** panel appears in the detail-view frame.

- 6 Click **OK**.

The qualifier definition is deleted.

## Maintaining Qualified URL Parameters

This section covers the following topics:

- [Setting Reconnect Parameters](#)
- [Setting Basic Parameters](#)
- [Setting Advanced Parameters](#)
- [Setting JSSE Parameters](#)
- [Setting OpenSSL Parameters](#)
- [Setting RDA-MHDR Parameters](#)

### Setting Reconnect Parameters

Using SMH, you can set or alter the values of the `reconnect`, `retry`, and `retryint` parameters for a qualified URL. These parameters control:

- Whether or not reconnection is attempted if the connection is disconnected due to some system failure
- The number of times the reconnection is attempted
- The interval, in seconds, between reconnection attempts.



➤ To set the reconnect parameters for a qualified URL:

- 1 Locate and list the qualified URL you want to change as described in [Listing Qualified URLs](#), elsewhere in this guide.
- 2 Click on the qualified URL whose reconnect parameters you want to change.
- 3 Right-click on the name of the qualifier and select **Set Reconnect Parms** in the resulting drop-down menu.

The **Set Reconnect Parms** panel appears in the detail-view frame of SMH.

**Set Reconnect Parms**

Attempt Reconnection on Failure

☐ Reconnect

Reconnect Retry Count:

Reconnect Retry Interval:

seconds

OK Cancel

- 4 Click the **Reconnect** check box if you want reconnection attempts to occur if the connection is disconnected due to some failure in the system. If this check box is not checked, no reconnection attempt is made.

When this check box is checked, the `reconnect` parameter appears in the qualified URL.

- 5 Specify the number of times reconnection should be attempted in the **Reconnect Retry Count** field. The valid range is "0" through "2147483648". The default value is "0" (no reconnection attempts).

When a value other than "0" is specified, the `retry` parameter appears in the qualified URL.

- 6 Specify the number of seconds to wait between reconnection attempts. The valid range is "0" through "2147483648". The default value is "60000" seconds.

When a value other than "60000" is specified, the `retryint` parameter appears in the qualified URL.

- 7 Click OK.

The reconnection parameters for the qualified URL are set.

### Setting Basic Parameters

Using SMH, you can set or alter the value of the `chirpinterval` parameter for a qualified URL. This parameter controls the interval, in seconds, at which the broadcast connection occurs. This broadcast connection is the communication mechanism used to validate the availability of the connection.

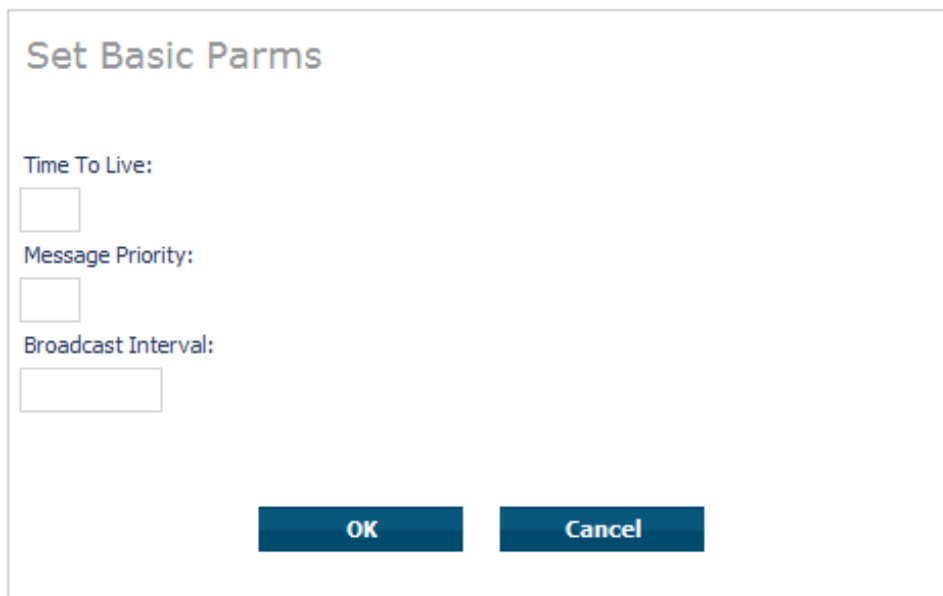


**Note:** The `ttl` (**Time To Live**) and `priority` (**Message Priority**) parameters are not available at this time. They are reserved for future use.

#### ➤ To set the basic parameters for a qualified URL:

- 1 Locate and list the qualified URL you want to change as described in [Listing Qualified URLs](#), elsewhere in this guide.
- 2 Click on the qualified URL whose reconnect parameters you want to change.
- 3 Right-click on the name of the qualifier and select **Set Basic Parm**s from the resulting drop-down menu.

The **Set Basic Parm**s panel appears in the detail-view frame of SMH.



The image shows a dialog box titled "Set Basic Parm". It contains three input fields, each with a label to its left: "Time To Live:", "Message Priority:", and "Broadcast Interval:". Each label is in a blue font. The input fields are empty text boxes. At the bottom of the dialog box, there are two buttons: "OK" and "Cancel", both in white text on a dark blue background.



**Note:** The `ttl` (**Time To Live**) and `priority` (**Message Priority**) parameters are not available at this time. They are reserved for future use.

- 4 Specify the number of seconds to wait between broadcast connection attempts in the **Broadcast Interval** field. The valid range is "0" through the maximum integer that can be stored by your operating system. The default value is "300"seconds (5 minutes). A value of "0" implies the default, "300". This broadcast connection is the communication mechanism used to validate the availability of the connection specified by the URL.

When a value other than "300" is specified, the `chirpinterval` parameter appears in the qualified URL.

- 5 Click OK.

The basic parameters for the qualified URL are set.

### Setting Advanced Parameters

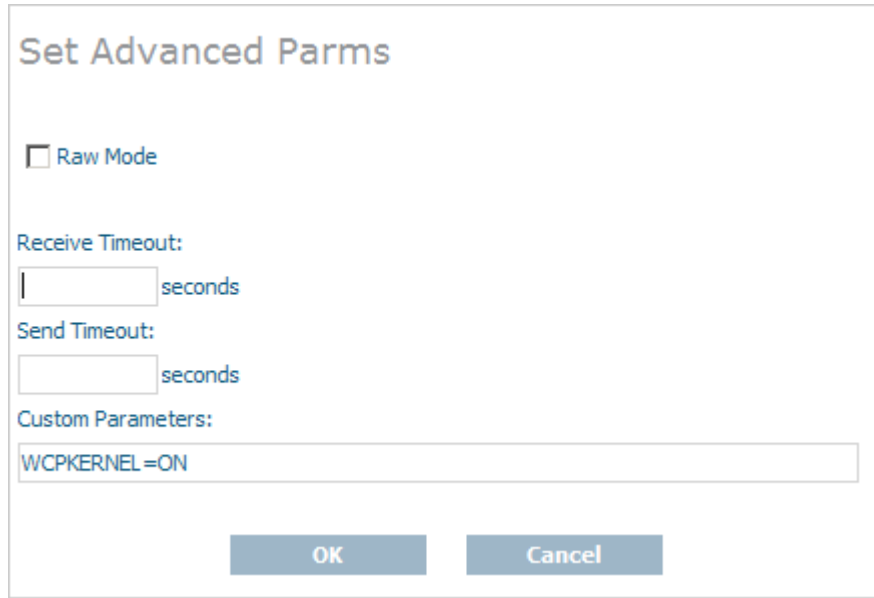
Using SMH, you can set or alter the values of advanced parameters `raw`, `recvtimeout`, `sendtimeout`, and various custom parameters for a qualified URL. These parameters control:

- Whether transport subsystem headers are sent
- The timeout value in seconds to receive messages on this connection
- The timeout value in seconds to send messages on this connection
- Other custom parameter either set automatically by the Software AG application for the qualified URL or with assistance from Software AG Customer Support.

#### ➤ To set the advanced parameters for a qualified URL:

- 1 Locate and list the qualified URL you want to change as described in [Listing Qualified URLs](#), elsewhere in this guide.
- 2 Click on the qualified URL whose reconnect parameters you want to change.
- 3 Right-click on the name of the qualifier and select **Set Advanced Parms** from the resulting drop-down menu.

The **Set Advanced Parms** panel appears in the detail-view frame of SMH.



The image shows a dialog box titled "Set Advanced Params". It contains a checkbox labeled "Raw Mode". Below it are two text input fields: "Receive Timeout:" and "Send Timeout:", each followed by a text box and the word "seconds". Below these is a "Custom Parameters:" label followed by a text box containing the text "WCPKERNEL=ON". At the bottom are "OK" and "Cancel" buttons.

- 4 Click the **Raw Mode** check box if you want transport subsystem headers sent with messages on this connection. If this check box is checked, proxy operations are not possible.

When this check box is checked, the `raw` parameter appears in the qualified URL.

- 5 Specify the number of seconds to wait before timing out a message being received on this connection in the **Receive Timeout** field. The valid range is "0" through the maximum integer that can be stored by your operating system. The default value is "60" seconds. A value of "0" implies the default, "60".

When a value other than "0" or "60" is specified, the `recvtimeout` parameter appears in the qualified URL.

- 6 Specify the number of seconds to wait before timing out a message being sent on this connection in the **Send Timeout** field. The valid range is "0" through the maximum integer that can be stored by your operating system. The default value is "60" seconds. A value of "0" implies the default, "60".

When a value other than "0" or "60" is specified, the `sendtimeout` parameter appears in the qualified URL.

- 7 Specify other custom parameters in the **Custom Parameters** field, as directed by Software AG Customer Support.



**Note:** Some custom parameters are specified automatically when the qualified URL is initially defined.

These custom parameters appear in the qualified URL.

- 8 Click OK.

The advanced parameters for the qualified URL are set.

### Setting JSSE Parameters

Using SMH, you can set or alter the values of the Java security `KEYSTORE`, `KEYSTORE_PASSWD`, `TRUSTSTORE`, `TRUSTSTORE_PASSWD`, `VERSION`, and `VERIFY` parameters for a qualified URL. These parameters control:

- The Java keystore to use for the SSL connection
- The password for the Java keystore
- The Java truststore to use for the SSL connection
- The password for the Java truststore
- The SSL version that should be used for the SSL connection
- The verification processing level for the SSL connection.

#### ➤ To set the JSSE parameters for a qualified URL:

- 1 Locate and list the qualified URL you want to change as described in [Listing Qualified URLs](#), elsewhere in this guide.
- 2 Click on the qualified URL whose reconnect parameters you want to change.
- 3 Right-click on the name of the qualifier and select **Set JSSE Params** on the resulting drop-down menu.

The **Set JSSE Params** panel appears in the detail-view frame of SMH.

## Set JSSE Parms

Browse File Pattern:

Browse and Select Java Keystore File

Browse...

☐ Trim File Path

Java KeyStore Password:

Browse and Select Java Truststore File

Browse...

☐ Trim File Path

Java TrustStore Password:

Version:

TLSv1 - Defaults to TLSv1

Verification Level:

0 - Defaults to 0

OK

Cancel

- 4 Optionally specify a browse file pattern in the **Browse File Pattern** field. This pattern is used to initially list files in the specified pattern when you click on any of the **Browse** buttons on this panel. However, once you get to the **Choose a File** panel produced by clicking on a **Browse** button, you can change the pattern if you choose.
- 5 Click in the **Browse and Select Java Keystore File** field and specify the name of the Java keystore. You can click the **Browse** button for this field to locate and select the Java keystore file using a **Choose a File** panel.



**Note:** The **Trim File Path** checkbox, when checked, will trim off the path if you specify a fully qualified path and file name.

When a value is specified, the `keystore` parameter appears in the qualified URL.

- 6 Click in the **Java KeyStore Password** field and specify the password required to extract information from the Java keystore.

When a value is specified, the `keystore_passwd` parameter appears in the qualified URL.

- 7 Click in the **Browse and Select Java Truststore File** field and specify the name of the Java truststore. You can click the **Browse** button for this field to locate and select the Java truststore file using a **Choose a File** panel.



**Note:** The **Trim File Path** checkbox, when checked, will trim off the path if you specify a fully qualified path and file name.

When a value is specified, the `truststore` parameter appears in the qualified URL.

- 8 Click in the **Java TrustStore Password** field and specify the password required to extract information from the Java truststore.

When a value is specified, the `truststore_passwd` parameter appears in the qualified URL.

- 9 Select the version of SSL that should be used by selecting one from the drop-down list provided for the **Version** field. The default is "TLSv1".

When a value other than "TLSv1" is specified, the `version` parameter appears in the qualified URL.

- 10 Specify the certificate processing level by selecting one from the drop-down list provided for the **Verification Level** field. The default is "0".

For Java applications, valid values are:

0 (No peer verification occurs. This is the default value.)

1 (The application requests that the peer certificate be verified.)

2 (The application requests that the peer certificate be verified. A fatal condition occurs if there is no certificate.)

Values 4 and 8 are not valid for Java.

When a value is specified, the `verify` parameter appears in the qualified URL.

- 11 Click OK.

The JSSE parameters for the qualified URL are set.

### Setting OpenSSL Parameters

Using SMH, you can set or alter the values of the OpenSSL security `VERSION`, `VERIFY`, `RANDOM_FILE`, `CAPATH`, `CAFILE`, `CERT_FILE`, `KEY_FILE`, and `CERT_PASSWD` parameters for a qualified URL. These parameters control:

- The SSL version that should be used for the SSL connection
- The verification processing level for the SSL connection
- The random file to use for the SSL connection
- The path for the Certificate Authority file that stores the trusted CA certificates

- The name of the Certificate Authority file that stores the trusted CA certificates
- The name of the file containing the participant's certificate
- The name of the file containing the server's private key
- The password for extracting information from the participant's certificate.

➤ **To set the OpenSSL parameters for a qualified URL:**

- 1 Locate and list the qualified URL you want to change as described in *Listing Qualified URLs*, elsewhere in this guide.
- 2 Click on the qualified URL whose reconnect parameters you want to change.
- 3 Right-click on the name of the qualifier and select **Set OpenSSL Parms** on the resulting drop-down menu.

The **Set OpenSSL Parms** panel appears in the detail-view frame of SMH.



### Set OpenSSL Parms

Version:

TLSv1
▼

- Defaults to TLSv1

Verification Level:

0
▼

- Defaults to 0

Browse and Select Random File

Browse...

☐ Trim File Path

Browse and Select Certificate Authority Path:

Browse...

Browse and Select Certificate Authority File:

Browse...

☐ Trim File Path

Browse and Select Certificate File:

Browse...

☐ Trim File Path

Browse and Select Key File:

Browse...

☐ Trim File Path

Certificate Password:

OK

Cancel

- 4 Select the version of SSL that should be used by selecting one from the drop-down list provided for the **Version** field. The default is "TLSv1".

When a value other than "TLSv1" is specified, the `version` parameter appears in the qualified URL.

- 5 Specify the certificate processing level by selecting one from the drop-down list provided for the **Verification Level** field. The default is "0".

For C applications, valid values are:

0 (No peer verification occurs. This is the default value.)

1 (The application requests that the peer certificate be verified.)

2 (The application requests that the peer certificate be verified. A fatal condition occurs if there is no certificate.)

4 (The application requests that the peer certificate be verified only once.)

8 (The application requests that the issuer name is checked against the host name.)

Values "1", "2", and "4" can be specified simultaneously, but only if you use the **Custom Parameter** field on the [Set Advanced Params](#) panel.

If no client certificate is available, certification fails.

When a value is specified, the `verify` parameter appears in the qualified URL.

- 6 Click in the **Browse and Select Random File** field and specify the name of the text file to be used by encryption routines to ensure that encryption itself occurs in a random manner. This text file contains at least 14 random characters. You can click the **Browse** button for this field to locate and select the random text file using a **Choose a File** panel.



**Note:** The **Trim File Path** checkbox, when checked, will trim off the path if you specify a fully qualified path and file name.

When a value is specified, the `random_file` parameter appears in the qualified URL.

- 7 Click in the **Browse and Select Certificate Authority Path** field and specify the path where the Certificate Authority file that stores the trusted CA certificates resides. You can click the **Browse** button for this field to locate and select the path using a **Choose a File** panel.

When a value is specified, the `capath` parameter appears in the qualified URL.

- 8 Click in the **Browse and Select Certificate Authority File** field and specify the name of the Certificate Authority file that stores the trusted CA certificates. You can click the **Browse** button for this field to locate and select the file using a **Choose a File** panel.



**Note:** The **Trim File Path** checkbox, when checked, will trim off the path if you specify a fully qualified path and file name.

When a value is specified, the `cafile` parameter appears in the qualified URL.

- 9 Click in the **Browse and Select Certificate File** field and specify the name of the file containing the participant's certificate. You can click the **Browse** button for this field to locate and select the file using a **Choose a File** panel.



**Note:** The **Trim File Path** checkbox, when checked, will trim off the path if you specify a fully qualified path and file name.

When a value is specified, the `cert_file` parameter appears in the qualified URL.

- 10 Click in the **Browse and Select Key File** field and specify the name of the file containing the server's private key. You can click the **Browse** button for this field to locate and select the file using a **Choose a File** panel.



**Note:** The **Trim File Path** checkbox, when checked, will trim off the path if you specify a fully qualified path and file name.

When a value is specified, the `key_file` parameter appears in the qualified URL.

- 11 Click in the **Certificate Password** field and specify the password required to extract information from the certificate file.

When a value is specified, the `cert_passwd` parameter appears in the qualified URL.

- 12 Click OK.

The OpenSSL parameters for the qualified URL are set.

### Setting RDA-MHDR Parameters

Using SMH, you can set or alter the values of the RDA `node`, `nodename`, `charset`, and `security` parameters for a qualified URL. These parameters control:

- The node ID by which this node is known to a classic Entire Net-Work installation
- The node name by which this node is known to a classic Entire Net-Work installation
- The character encoding of the classic Entire Net-Work node associated with the URL
- The name of a security file containing a list of IP addresses authorized to access this protocol..

#### ➤ To set the RDA parameters for a qualified URL:

- 1 Locate and list the qualified URL you want to change as described in [Listing Qualified URLs](#), elsewhere in this guide.
- 2 Click on the qualified URL whose reconnect parameters you want to change.
- 3 Right-click on the name of the qualifier and select **Set RDA-MHDR Parms** on the resulting drop-down menu.

The **Set RDA-MHDR Parms** panel appears in the detail-view frame of SMH.

**Set RDA-MHDR Params**

Entire Net-Work Node ID:

Entire Net-Work Node Name:

Select the Charset:

Security:

OK Cancel

- 4 Specify the node ID by which this node is known to a classic Entire Net-Work installation in the **Entire Net-Work Node ID** field.

When a value is specified for this field, the `node` parameter appears in the qualified URL.

- The name of a security file containing a list of IP addresses authorized to access this protocol..

- 5 Specify the node name by which this node is known to a classic Entire Net-Work installation in the **Entire Net-Work Node Name** field.

When a value is specified for this field, the `nodename` parameter appears in the qualified URL.

- 6 Specify the character encoding of the classic Entire Net-Work node associated with the URL in the **Select the Charset** field.

When a value is specified for this field, the `charset` parameter appears in the qualified URL.

- 7 Specify the name of a security file containing a list of IP addresses authorized to access this protocol in the **Security** field.

When a value is specified for this field, the `security` parameter appears in the qualified URL.

- 8 Click OK.

The RDA-MHDR parameters for the qualified URL are set.

## Changing Protocol, Host, and Port Values of the Qualified URL

Using SMH, you can change the protocol, host name, host IP address, port, or alternate ports for a qualified URL.

### ➤ To change these values for a qualified URL:

- 1 Locate and list the qualified URL you want to change as described in [Listing Qualified URLs](#), elsewhere in this guide.
- 2 Click on the qualified URL whose reconnect parameters you want to change.
- 3 Right-click on the name of the qualifier and select **Set Protocol, Host, and Port Values** on the resulting drop-down menu.

The **Set Protocol, Host, and Port Values** panel appears in the detail-view frame of SMH.

**Set Protocol, Host, and Port Values**

Protocol:

☒ TCPIP

☐ HTTP

☐ SSL

☐ RDA

Host Name:

WCV76402

Port:

49160 \*

Alternate Ports:

OK Cancel

- 4 Click on the appropriate protocol checkbox in the **Protocol** field. In most cases, the protocol will be **TCPIP**. For a complete description of these protocols, read *Protocols* in the *Software AG Directory Server Installation and Administration Guide*.
- 5 Specify the host name of the middleware in the **Host Name** field. This is the Entire Net-Work version 7 or ADATCP host name.



**Note:** Host names are case-sensitive in SMH.

Or:

Specify an IP address as an alternative to a host name. We do not recommend specifying IP addresses instead of host names as the IP address may change.

- 6 Enter the middleware's listen port into the **Port** field.



**Note:** You can leave the **Alternate Ports** field blank, unless you want to enter alternate listen ports.

- 7 Click OK.

The protocol, host, and port values for the qualified URL are set.

## Setting the Target Type

---

You can globally change the target type of a target definition using the System Management Hub. When you do this, some of the qualified URLs assigned the target definition are updated with the new target type, as appropriate for the protocol specified in the URL.

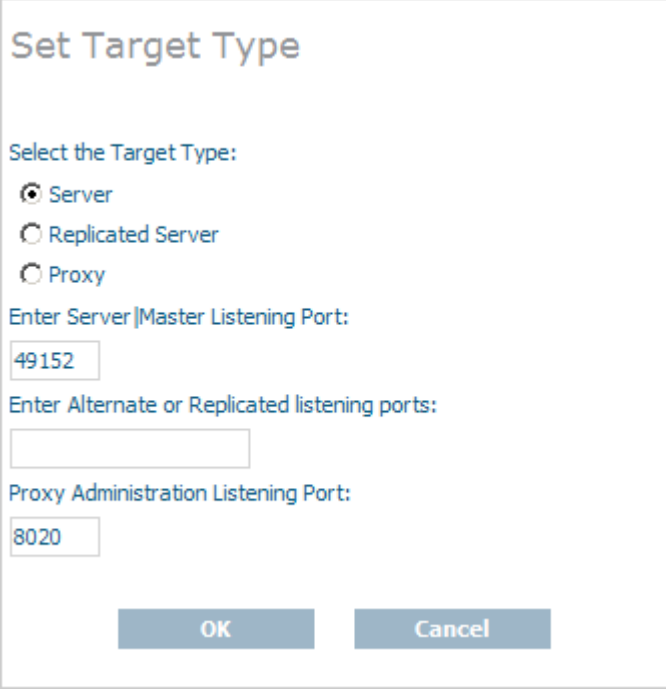
### » To change the target type of a target definition:

- 1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.
- 2 In the tree-view frame of SMH, click and expand the name of the Directory Server containing the target definition you want to modify.

The partitions and targets already defined for that Directory Server are listed in the detail-view frame and under the Directory Server name in the tree-view frame.

- 3 Click on the target you want to modify. If the target is in a partition, you must first select the partition and then click on the target.
- 4 Right-click on the name of the target and select **Set Target Type** from the resulting drop-down menu.

The **Set Target Type** panel appears in the detail-view frame.



**Set Target Type**

Select the Target Type:

☒ Server

☐ Replicated Server

☐ Proxy

Enter Server|Master Listening Port:

49152


Enter Alternate or Replicated listening ports:

Proxy Administration Listening Port:

8020

OK Cancel

- 5 Select the appropriate option in the **Select the Target Type** area for the target type you want used for the target definition.
  - The **Server** option is usually the option you should select.
  - The **Replicated Server** option is reserved for future use by Software AG.
  - The **Proxy** option is only applicable to configurations requiring a proxy. It is provided for compatibility with Software AG products that still require a proxy. If your Software AG product requires a proxy, refer to the documentation for your Software AG product for information about proxies and how to configure them in SMH.
- 6 Optionally, change the listening ports used by the target in the **Enter Server/Master Listening Port**, **Enter Alternate or Replicated listening ports**, or **Proxy Administration Listening Port** fields.
 



**Note:** The **Proxy Administration Listening Port** field is only applicable to configurations requiring a proxy. It is provided for compatibility with Software AG products that still require a proxy. If your Software AG product requires a proxy, refer to the documentation for your Software AG product for information about them.
- 7 Click **OK**.

The target type is changed for the target definition and the qualified URLs of the target definition are updated with the new target type, depending on the protocol specified in each URL.

## Changing the Target Name

---

You can change the name of a target definition using the System Management Hub. When you do this, all of the qualified URLs assigned the target definition are updated with the new name.

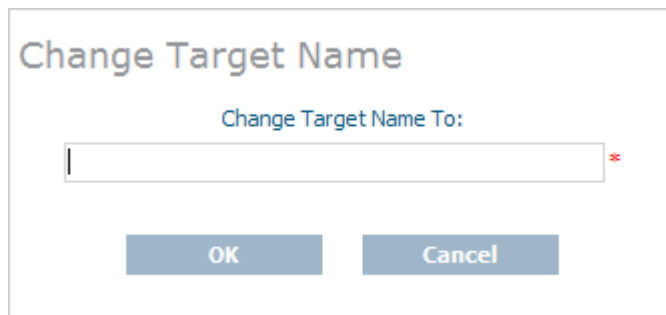
➤ **To change the name of a target:**

- 1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.
- 2 In the tree-view frame of SMH, click and expand the name of the Directory Server containing the target definition you want to modify.

The partitions and targets already defined for that Directory Server are listed in the detail-view frame and under the Directory Server name in the tree-view frame.

- 3 Click on the target you want to modify. If the target is in a partition, you must first select the partition and then click on the target.
- 4 Right-click on the name of the target and select **Change Target Name** from the resulting drop-down menu.

The **Change Target Name** panel appears in the detail-view frame.

A screenshot of a dialog box titled "Change Target Name". Inside the dialog, there is a label "Change Target Name To:" followed by a text input field. A red asterisk is positioned to the right of the input field, indicating a required field. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

- 5 Specify a new target name in the **Change Target Name To** field.



**Note:** Target names are case-sensitive.

- 6 Click **OK**.

The name of the target definition is changed and all of its qualified URLs are updated with the new name.



## Changing the Host

---

You can globally change the host setting of URLs in a target definition using the System Management Hub. For information on doing this, read [Changing Hosts](#), elsewhere in this guide.

## Changing the Protocol

---

You can globally change the protocol settings of URLs in a target definition using the System Management Hub.

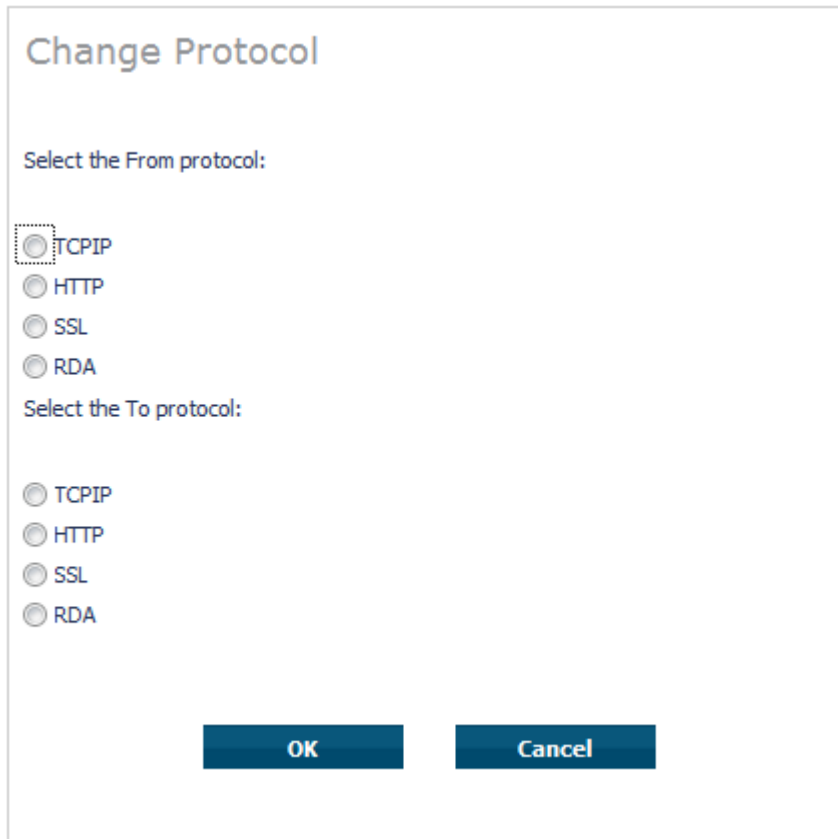
➤ **To change the protocol settings of URLs in a target definition:**

- 1 Access the Directory Server administration area, as described in [The Directory Server Administration Area](#), earlier in this section.
- 2 In the tree-view frame of SMH, click and expand the name of the Directory Server containing the target definition you want to modify.

The partitions and targets already defined for that Directory Server are listed in the detail-view frame and under the Directory Server name in the tree-view frame.

- 3 Click on the target you want to modify. If the target is in a partition, you must first select the partition and then click on the target.
- 4 Right-click on the name of the target and select **Change Protocol** from the resulting drop-down menu.

The **Change Protocol** panel appears in the detail-view frame.



The dialog box is titled "Change Protocol". It contains two sections for protocol selection. The first section, "Select the From protocol:", has four radio buttons: TCPIP (which is selected and highlighted with a dashed box), HTTP, SSL, and RDA. The second section, "Select the To protocol:", also has four radio buttons: TCPIP, HTTP, SSL, and RDA. At the bottom of the dialog are two buttons: "OK" and "Cancel".

- 5 Click on the checkbox in the **Select the From protocol** area for the protocol you want to change. All URLs for the target definition using this protocol will be changed when these steps are completed.
- 6 Click on the checkbox in the **Select the To protocol** area for the protocol you want to use instead. The URLs using the protocol you specified in the previous step will be changed to use the protocol you select in this step.
- 7 Click **OK**.

A URLs in the target definition with the protocol selected in the **Select the From protocol** area are changed to use the protocol selected in the **Select the To protocol** area.

## Deleting a Target

---

➤ To delete a target definition:

- 1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.
- 2 In the tree-view frame of SMH, click on the name of the Directory Server containing the the target definition you wish to delete.

The partitions and targets for that Directory Server are listed in the detail-view frame.

- 3 Click on the target you wish to delete. If the target is in a partition, you must first select the partition and then click on the target.
- 4 Right-click on the name of the target and select **Delete Target** from the resulting drop-down menu.

The **Delete Target** panel appears in the detail-view frame.

- 5 Click OK.

The target definition is deleted.



## 9 Changing Hosts

---

You can globally change the host setting of URLs in a target definition using the System Management Hub.

You can change the host setting for the URLs in a given:

- Directory Server
- partition within a Directory Server
- target

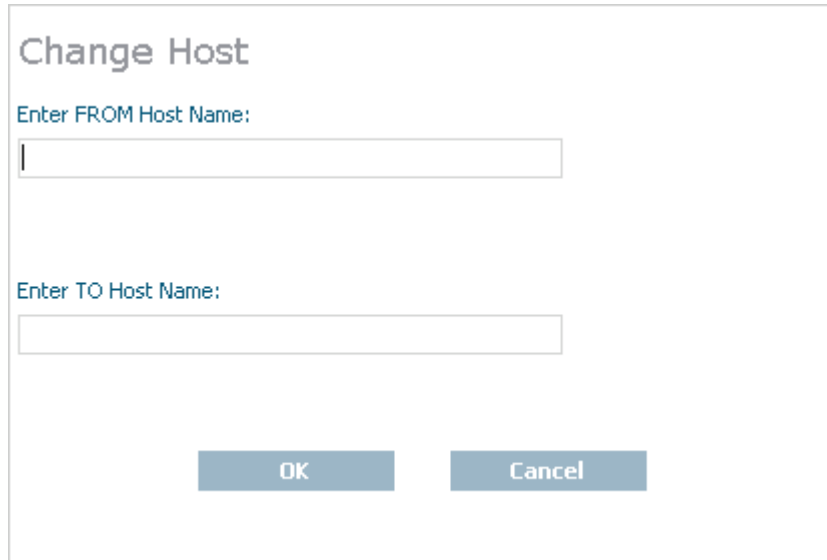


**Note:** If you want to change the host name in a specific qualified URL definition, read *Changing Protocol, Host, and Port Values of the Qualified URL*, elsewhere in this chapter.

➤ **To change the host setting for URLs in a Directory Server, partition, or target definition:**

- 1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this chapter.
- 2 Navigate to the administration area for the particular Directory Server, partition, or target containing the URLs you want to change. For example, if you want to change the host name for the URLs in a particular target, navigate through the SMH screens until you have selected that target in the tree-view frame.
- 3 Right-click on the name of the Directory Server, partition, or target and select **Change Host** on the resulting drop-down menu.

The **Change Host** panel appears in the detail-view frame.



The image shows a 'Change Host' dialog box. It has a title bar at the top. Below the title, there are two text input fields. The first field is labeled 'Enter FROM Host Name:' and the second field is labeled 'Enter TO Host Name:'. At the bottom of the dialog, there are two buttons: 'OK' and 'Cancel'.

- 4 Specify the original host name in the **Enter FROM Host Name** field. Any URLs in the Directory Server, partition, or target with the host name specified in this field will be changed by this procedure.



**Note:** Host names are case-sensitive in SMH.

- 5 Specify the new host name in the **Enter TO Host Name** field. The host names for any URLs in the Directory Server, partition, or target with the host name specified in the previous step will be changed to the name you specify in this step.



**Note:** Host names are case-sensitive in SMH.

- 6 Click OK.

All URLs in the selected Directory Server, partition, or target with the host name specified in the **Enter FROM Host Name** field will be changed to use the host name specified in the **Enter TO Host Name** field.

# 10

## 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 Configurations</i>	Describes how to migrate Entire Net-Work Client 1.3 and 1.4 configurations to Entire Net-Work Client 1.5 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 Adabas Directory Server</i>	Provides instructions for changing the Adabas 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.



# 11 The Entire Net-Work Client SMH Administration Area

---

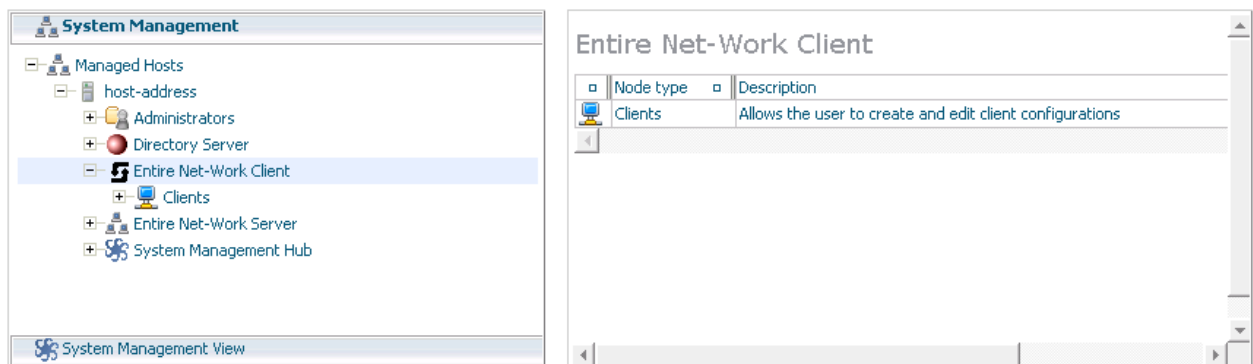
➤ To access the Entire Net-Work Client administration area of the System Management Hub (SMH):

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.

# 12

## About Client Configurations

---

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

- The Adabas 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 . 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\
- **In Windows 7 environments:** 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.

# 13

## 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:
<b>Add to Browser Favorites</b>	Add a node in tree-view to your browser favorites.
<b>Add to View</b>	Add a node in tree-view to System Management View. For more information about System Management View, read your System Management Hub documentation.
<b>Help</b>	Link to help for your use of SMH as it pertains to the Entire Net-Work Client administration area.
<b>Refresh</b>	Refresh the screen.
<b>Remove from View</b>	Remove a node in tree-view from System Management View. For more information about System Management View, read your System Management Hub documentation.

- 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:
<b>Add Client Configuration</b>	Add a client to be maintained by SMH. For more information, read <a href="#">Adding Client Configurations</a> , elsewhere in this chapter.
<b>Add to Browser Favorites</b>	Add a node in tree-view to your browser favorites.
<b>Add to View</b>	Add a node in tree-view to System Management View. For more information about System Management View, read your System Management Hub documentation.
<b>Help</b>	Link to help for your use of SMH as it pertains to the Entire Net-Work Client administration area.
<b>Migrate WCL13 Client Configuration</b>	Migrate the client configurations you set up in Entire Net-Work Client 1.3. This process converts them to Entire Net-Work Client 1.5 client configurations. For more information, read <a href="#">Migrating Entire Net-Work Client Configurations</a> , elsewhere in this chapter.
<b>Migrate WCL14 Client Configuration</b>	Migrate the client configurations you set up in Entire Net-Work Client 1.4. This process converts them to Entire Net-Work Client 1.5 client configurations. For more information, read <a href="#">Migrating Entire Net-Work Client Configurations</a> , elsewhere in this chapter.
<b>New Log File</b>	Close the current Entire Net-Work Client log file and start a new one. For more information, read <a href="#">Managing Entire Net-Work Client Log Files</a> , elsewhere in this chapter.
<b>Refresh</b>	Refresh the screen.
<b>Remove from View</b>	Remove a node in tree-view from System Management View. For more information about System Management View, read your System Management Hub documentation.
<b>Set Service Parameters</b>	Change the parameters used by the client machine, including the Directory Server used by the client machine. For more information, read <a href="#">Setting Service Parameters</a> , elsewhere in this chapter.
<b>Set Service Trace Granularity</b>	Set the Entire Net-Work Client trace level for all clients. For more information, read <a href="#">Tracing Entire Net-Work Client Processing</a> , elsewhere in this chapter.
<b>Shutdown</b>	Shut down the Entire Net-Work Client service. For more information, read <a href="#">Stopping Entire Net-Work Client</a> , elsewhere in this chapter.
<b>View Log File</b>	View the current Entire Net-Work Client log file. For more information, read <a href="#">Managing Entire Net-Work Client Log Files</a> , 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 <a href="#">Deleting Client Configurations</a> , 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 <a href="#">Accessing Secured z/OS Host Resources</a> , elsewhere in this chapter.
Set Client Configuration Parameters	Maintain the parameters for the client configuration. For more information, read <a href="#">Maintaining Client Configuration Parameters</a> , elsewhere in this chapter.
Set Client Trace Granularity	Set the client trace level. For more information, read <a href="#">Managing Client Tracing</a> , elsewhere in this chapter.
Set Directory Server	Change the Adabas Directory Server used by the client. For more information, read <a href="#">Changing the Adabas Directory Server for the Client</a> , elsewhere in this chapter.
Set LNK User Exit Parameters	Specify the ADALNK 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 <a href="#">Using ADALNK User Exits</a> , elsewhere in this chapter.

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



# 14

## Identifying the Client Configuration to Your Application

---

- Specifying the Configuration by Environment Variable ..... 90
- Specifying the Configuration in Your Application ..... 90

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

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

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

# 15

## Setting Service Parameters

---

You can set parameters for the client machine, including the default Adabas 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.

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

Parameter	Description
SAGXTSDSHOST	Specify the Adabas Directory Server host name you want to use for this client machine.
SAGXTSDSPORT	Specify the port number of the Adabas 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	<p>Normally, port numbers are dynamically assigned by Entire Net-Work when the client is started, as follows:</p> <ul style="list-style-type: none"> <li>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.).</li> </ul>

Parameter	Description
	<p>■ Once an available port number is found, it is assigned to the client in its Adabas Directory Server entry.</p> <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 <a href="#">Specifying the Log File Location</a> , 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.



# 16

## 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:**

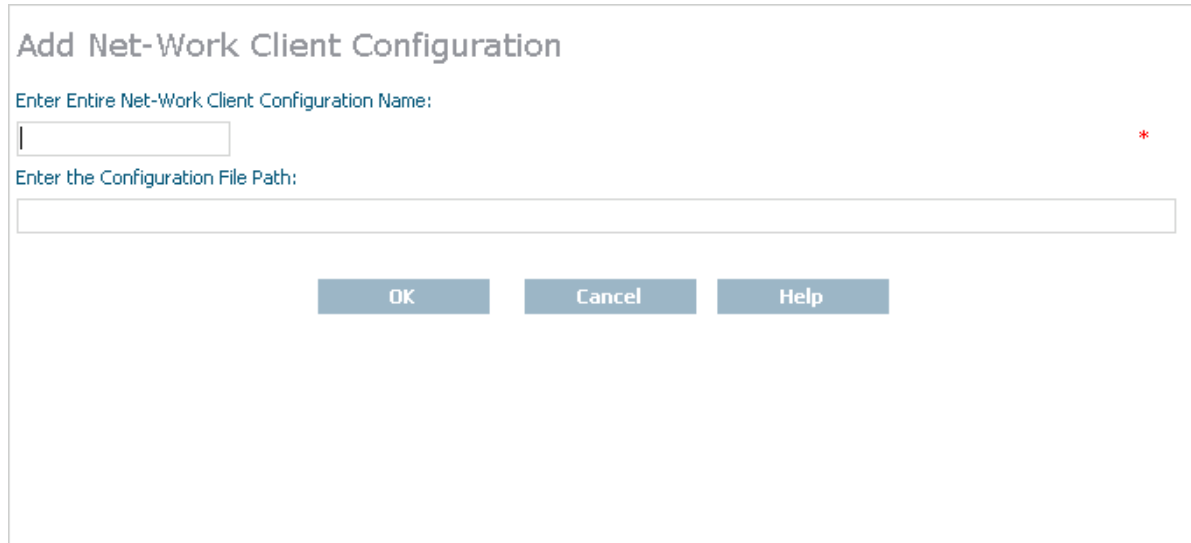
Make sure you have accessed the System Management Hub.

- 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.



# 17

## 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.



# 18

## 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.

## 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>  
MULTIPLEX ..... <not defined>  
NOLOCAL ..... <not defined>  
NOREMOTE ..... <not defined>  
Protocol Family  
☐ Unspecified  
☐ IPV4 Only  
☐ IPV6 Only

- 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 .	No	All defined databases can be accessed.

Parameter	Description	Required?	Default
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 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.
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"> <li>■ In Windows XP environments (up to XP Server 2003): Documents and Settings\All Users\Application Data\Software AG\Entire Net-Work Client\.</li> <li>■ In Windows 7 environments: ProgramData\Software AG\Entire Net-Work Client\logsvc15.</li> <li>■ In UNIX environments: \$SAG\wc1\.</li> </ul>
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	No	00

Parameter	Description	Required?	Default
	<p>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>		
MULTIPLEX	<p>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.</p> <p>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).</p>	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
Protocol Family	Select the TCP/IP protocol family used for this client. Click (check) <b>Unspecified</b> , <b>IPV4 Only</b> , or <b>IPV6 Only</b> . If you select <b>IPV4 Only</b> or <b>IPV6 Only</b> , only the selected protocol is used for communications with this client. If you select <b>Unspecified</b> , the domain name server (DNS) will determine which protocol is used; <b>Unspecified</b> is the default.	No	Unspecified

Parameter	Description	Required?	Default
	<b>Caution:</b> We recommend that you use the default value ( <b>Unspecified</b> ) for this parameter, allowing the DNS to determine which communication protocol is appropriate. If you do specify a specific protocol, calls to this client via the other protocol type are ignored.		
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 .	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 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 Adabas Directory Server is installed.  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.	No	No
USER_EXITS	This field is supplied only to support compatibility with previous Entire Net-Work Client releases. New Entire Net-Work user exits are no longer supported. Specify the name of the user exit DLL file that should be used with this client in this field. .	No	No user exit is used with this client.

Parameter	Description	Required?	Default
WCPARTITION	Specify the partition in which the client is assigned, if any. For more information, read .	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 <a href="#">Tracing Entire Net-Work Client Processing</a> , elsewhere in this guide.</p>	No	0000

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



# 19

## Migrating Entire Net-Work Client Configurations

---

If you want to use your client configurations from earlier versions of Entire Net-Work Client in this version, you must convert them to them to current Entire Net-Work Client configurations. This chapter describes how to do this.



**Caution:** Once a client configuration has been migrated to the most recent version of Entire Net-Work Client, it cannot be migrated back to an earlier Entire Net-Work Client version.

» **To convert an Entire Net-Work Client configuration to configuration used by the current version of Entire Net-Work 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 Right-click on the client machine on which the 1.3 client is defined and select **Migrate 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:...

Enter Entire Net-Work Client Configuration Location:

☒ Version 1.3  
☐ Version 1.4  
☐ Version 1.5

OK Cancel Help

- 4 In the **Enter the Net-Work Client Configuration Name** field, specify the name of the older client configuration definition you want to migrate.
- 5 In the **Enter the Net-Work Client Configuration Location** field, specify the fully qualified path name of the location of the older client configuration definition you want to migrate.
- 6 Select (click on) the radio button associated with version number of the older client configuration definition you want to migrate.
- 7 When all fields been specified, click **OK** to convert the older client configuration to a current client configuration.

The configuration is converted.

# 20

## Controlling Client Access to Databases

---

■ Maintaining Adabas Access Definitions .....	108
■ Maintaining Additional Database Access Parameters .....	114

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 Adabas Directory Server definitions. These definitions are stored in the Directory Server configuration file, wherever the Adabas 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 .

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 the *Software AG Directory Server Installation and 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:  \*

Reconnect ☐ Retry Count:  Retry Interval:

Enter Additional Parameters:

OK Cancel Help

- 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 Installation and 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.

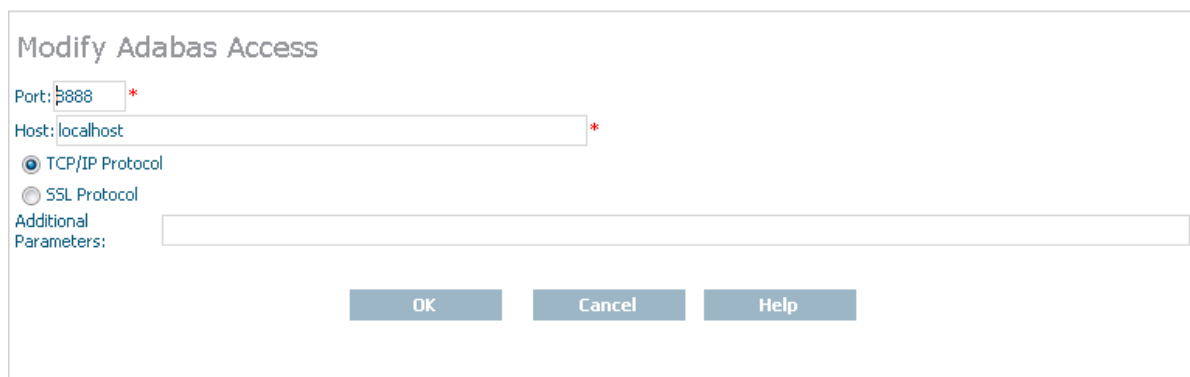
Options for the Adabas access and additional access parameter definitions appear in tree-view.

- 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.



Modify Adabas Access

Port: 8888 \*

Host: localhost \*

☒ TCP/IP Protocol

☐ SSL Protocol

Additional Parameters:

OK Cancel 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 Installation and 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.

- 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 of the Software AG Directory Server Installation and 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 Installation and 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.

# 21

## Managing Entire Net-Work Client Log Files

---

■ Viewing the Current Entire Net-Work Client Log File .....	120
■ Starting a New Entire Net-Work Client Log File .....	120
■ Specifying the Client Log File Location .....	121

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\logsvc15*
- 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\logsvc15`
- In UNIX environments: `$SAG\wcl\`.



**Note:** If you want to put your Entire Net-Work log files on a shared server, read . 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.

**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>

MULTIPLEX ..... <not defined>

NOLOCAL ..... <not defined>

NOREMOTE ..... <not defined>

Protocol Family

☐ Unspecified

☐ IPV4 Only

☐ IPV6 Only

**OK** **Cancel** **Help**

- 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.



## 22      Accessing Secured z/OS Host Resources

---

- Specifying the External Security Method and Appropriate Adabas SAF Security Kernel Parameters ..... 126
- Accessing z/OS Resources Using the Online Security Application ..... 128
- Accessing z/OS Resources Using the Security Exit ..... 131

Entire Net-Work Client includes an external security interface 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.

Before you can use ADASAF to access secured Adabas resources on a z/OS host, your access information (user ID and password) must be supplied to ADASAF. You can do this using one of the following methods:

1. In Windows environments only, you can supply your access information using the online security application and the External Security Interface Logon dialog. Read [Accessing z/OS Resources Using the Online Security Application](#) for more information.
2. In any environment, you can supply your access information by modifying and using a provided security exit. This method should be used where you want full control of obtaining the logon information. A sample security exit is provided in the Adabas Client libraries included with Entire Net-Work Client called *lnkxsaf*. For more information, read [Accessing z/OS Resources Using the Security Exit](#).

## Specifying the External Security Method and Appropriate Adabas SAF Security Kernel Parameters

---

To select the external security method you prefer to use, you must set some parameters in the System Management Hub. In addition, regardless of the 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 the external security method and the 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	<p>This parameter is available for Windows systems only.</p> <p>Indicate whether the external security online application should be used to supply the logon information 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).</p>	No	No
LNKADASAF	<p>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:</p> <div style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;">library function</div> <p>If no names are specified, ("&lt;not defined&gt;" is listed) and the value "lnkxsaf lnkxsaf" is used. (The lnkxsaf library is either <i>lnkxsaf.dll</i> or <i>lnkxsaf.so</i>).</p>	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 Online Security Application

---

When you elect to use the online security application to access Adabas secured resources, your access information (user ID and password) must be supplied via an external security interface logon dialog. The user ID and password you specify on the logon dialog are encrypted and stored on the local node to confirm that you have logged on. 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 external security interface online application by setting the LNKADAESI parameter (or environment variable) to "YES". For more information, read [Specifying the External Security Method and Appropriate Adabas SAF Security Kernel Parameters](#), elsewhere in this section.



### Notes:

1. Software AG strongly recommends that you modify the encryption/decryption method used to encrypt your security 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.
2. To access z/OS resources using the online security application the SAF Security fix AX822004 must be installed. This fix is available on Empower.

This section covers the following topics:

- [Accessing the External Security Interface Logon Dialog](#)
- [Automatic Logoff](#)
- [Encryption Method Modifications](#)

### Accessing the External Security Interface Logon Dialog

You can access the external security interface logon dialog either manually or dynamically.

If you elect to access the 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 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 logon dialog are encrypted and stored on the local node to confirm that you have logged on. 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.

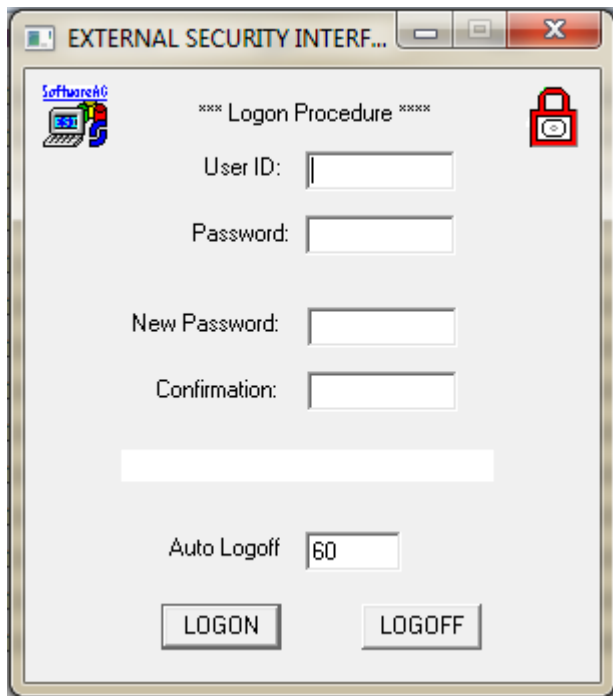
➤ If you elect to access the logon dialog manually, complete the following steps:

- 1 Run the *adaesi.exe* executable file in the Adabas Client directories of your installation (usually *\Program Files (x86)\Software AG\Adabas Client Package\vx.x.x\opt\bin*).



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

The External Security Interface Logon dialog appears, as shown below.



- 2 Supply a valid user ID and password in the **User ID** and **Password** fields and then click **LOGON**.

The user ID and password may be case-sensitive, depending on how the external security package is configured. In addition, the user ID and password must correspond to those known to the external security package on the z/OS node.

Once you have clicked **LOGON**, your logon access information is encrypted and stored. The user ID and password are not validated; the green symbol that appears on this dialog only indicates that a user ID and password combination has been supplied. Validation occurs when the user ID and password are actually used.

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

## Automatic Logoff

Once you have specified logon information for the external security interface, 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 external security interface logon 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", no automatic logoff occurs.

## Encryption Method Modifications

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



### 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 Entire Net-Work's external security interface, 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 external security interface logon dialog information:

- 1 Locate and edit the *adacrypt.c* file supplied in the Adabas Client directories included with your Entire Net-Work Client installation. This user exit file, the encryption and decryption source code, and the files required to compile and link the source code are provided in the Adabas Client directories (usually the *\ProgramData\Software AG\Adabas Client Package\vx.x.x\examples\adaesi* directory of the installation).
- 2 Modify the encryption and decryption code in *adacrypt.c* as required and then compile and link it using the files in the same Adabas Client 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 Security Exit

---

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

➤ **To modify and use the security exit:**

- 1 Locate and edit the user exit (the *lnkxsaf.c* file) supplied in the Adabas Client directories included 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 Adabas Client directories (usually the `\ProgramData\Software AG\Adabas Client Package\vx.x.x\examples\adasaf` directory of the installation).
- 2 Modify the *lnkxsaf.c* user exit as required and then compile and link it using the files in the same Adabas Client directory.



# 23

## Using ADALNK User Exits

---

- Specifying the User Exit File and Function Names ..... 134
- Modifying the User Exit Code ..... 136

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

---

This section describes how to specify the user exit file and function names using the System Management Hub.



**Note:** You can also specify them as environment variables instead.

### ➤ To specify the user exit file and function names using the System Management Hub:

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.

**Set LNK User Exit Parameters**

LNKUEX\_0..... <not defined>

LNKUEX\_1..... <not defined>

LNKUEX\_ACBX\_0..... <not defined>

LNKUEX\_ACBX\_1..... <not defined>

OK Cancel Help

- 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 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 ACB command is sent to the database.

Parameter	Description	Required?	Default
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 in the Adabas Client directories included with your Entire Net-Work Client installation. The sample user exit and the files required to compile and link the source code are usually provided in the Adabas Client installation directory `\ProgramData\Software AG\Adabas Client Package\vx.x.xx\examples\client`.

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

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



# 24

## Changing the Adabas Directory Server

---

- Changing the Adabas Directory Server for the Client Machine ..... 138
- Changing the Adabas Directory Server for a Specific Client ..... 139

Using SMH, you can change the Adabas 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 Adabas Directory Server to ensure centralized administration.

## Changing the Adabas Directory Server for the Client Machine

---

Using SMH, you can change the Adabas 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 Adabas Directory Server to ensure centralized administration.

### ➤ To change the Adabas 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 Adabas Directory Server host name you want to use for this client machine.
- 5 In the SAGXTSDSPORT parameter, specify the port number of the Adabas 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 Adabas Directory Server.

## Changing the Adabas Directory Server for a Specific Client

Using SMH, you can change the Adabas 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 Adabas Directory Server to ensure centralized administration.

### ➤ To change the Adabas 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.

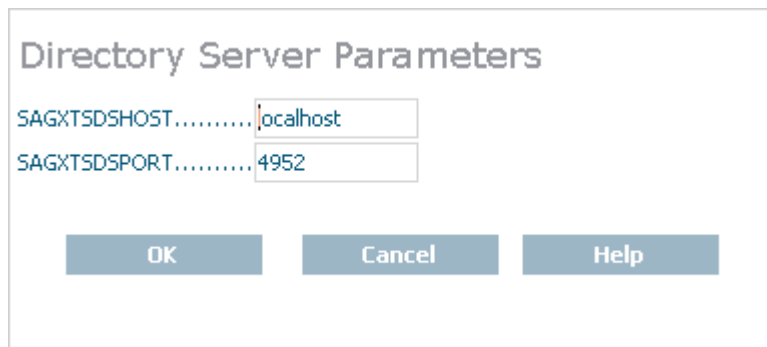
A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

- 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 Adabas Directory Server. Then select **Set Directory Server** from the resulting drop-down menu.

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



The screenshot shows a dialog box titled "Directory Server Parameters". It contains two text input fields. The first field is labeled "SAGXTSDSHOST....." and contains the text "localhost". The second field is labeled "SAGXTSDSPORT....." and contains the text "4952". Below the input fields are three buttons: "OK", "Cancel", and "Help".

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

The client will start using the requested Adabas Directory Server.

# 25

## Tracing Entire Net-Work Client Processing

---

■ Managing Client Service Tracing .....	142
■ Managing Client Tracing .....	144
■ Managing Software AG Transport Services Tracing .....	146
■ Managing Software AG Communications Tracing .....	148

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:

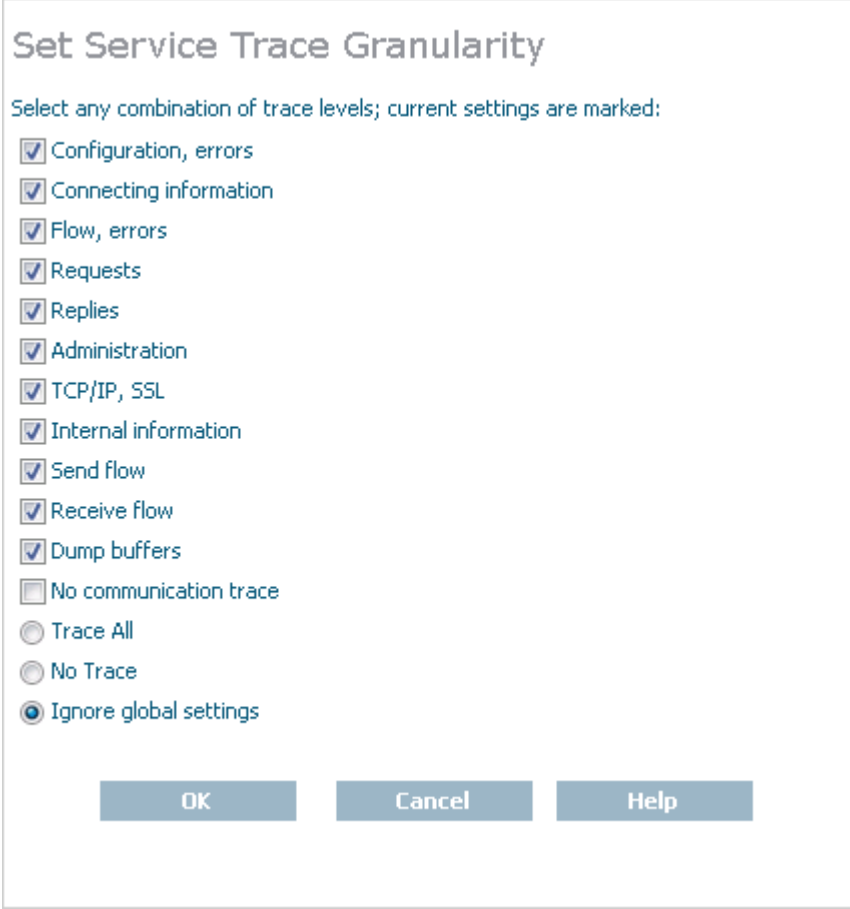
Make sure you have accessed the System Management Hub.

- 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

OK Cancel Help

- 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>  
 MULTIPLEX ..... <not defined>  
 NOLOCAL ..... <not defined>  
 NOREMOTE ..... <not defined>  
 Protocol Family  
☐ Unspecified  
☐ IPV4 Only  
☐ IPV6 Only

- 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	No	0000

Parameter	Description	Required?	Default
	are hexadecimal values ranging from "0000" (no tracing) through "FFFFE" (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.		

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>

MULTIPLEX ..... <not defined>

NOLOCAL ..... <not defined>

NOREMOTE ..... <not defined>

Protocol Family

☐ Unspecified  
☐ IPV4 Only  
☐ IPV6 Only

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	No	00

Parameter	Description	Required?	Default
	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.		

The communications trace levels are set and activated.

# 26

## Starting and Stopping Entire Net-Work Client

---

■ Automatically Starting Entire Net-Work Client .....	152
■ Manually Starting Entire Net-Work Client .....	152
■ Stopping Entire Net-Work Client .....	153

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

## Entire Net-Work Server Administration

---

This chapter describes the administration tasks you can perform for the Entire Net-Work Server using SMH. It is organized as follows:

<i>The Entire Net-Work Server SMH Administration Area</i>	Describes how to access the Entire Net-Work Server SMH administration area, how to get online help for it, and how to refresh the data that appears in the area.
<i>Managing Entire Net-Work Servers</i>	Describes management tasks for Entire Net-Work servers.
<i>Managing Kernels</i>	Describes management tasks for Entire Net-Work Kernels.



# 28

## The Entire Net-Work Server SMH Administration Area

---

■ Accessing the Entire Net-Work Server SMH Administration Area .....	158
■ Getting Help .....	159
■ Refreshing the Displays .....	159

This chapter describes how to access the Entire Net-Work Server SMH administration area, how to get online help for it, and how to refresh the data that appears in the area.

## Accessing the Entire Net-Work Server SMH Administration Area

---

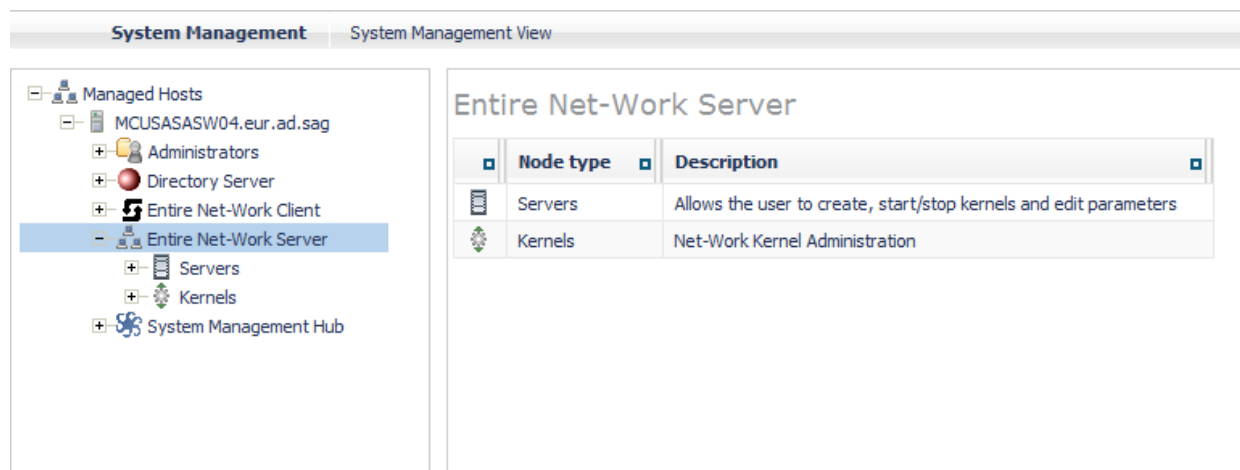
» To access the Entire Net-Work Server administration area of the System Management Hub (SMH):

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 Server 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 Server** in the tree-view under the managed host.

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

The Entire Net-Work Server administration area lists the servers and kernels and you can manage.



The following commands are available in the command menu for the Entire Net-Work Server administration area or by right-clicking on **Entire Net-Work Server** in tree-view:



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

Command	Use this command to:
<b>Add to Browser Favorites</b>	Add a node in tree-view to your browser favorites.
<b>Add to View</b>	Add a node in tree-view to System Management View. For more information about System Management View, read your System Management Hub documentation.
<b>Help</b>	Link to help for your use of SMH as it pertains to the Entire Net-Work Server administration area.
<b>Refresh</b>	Refresh the screen.
<b>Remove from View</b>	Remove a node in tree-view from System Management View. For more information about System Management View, read your System Management Hub documentation.

## Getting Help

➤ To get help on an Entire Net-Work Server management task or SMH panel:

- 1 Access the Entire Net-Work Server SMH administration area, as described in [Accessing the Entire Net-Work Server SMH Administration Area](#), elsewhere in this section.
- 2 Right-click **Entire Net-Work Server** in tree-view and select the **Help** option from the resulting drop-down menu.

Or:

Navigate to any panel within the Entire Net-Work Server SMH administration area and click the **Help** button on the panel.

Help for the panel or Entire Net-Work Server SMH administration area appears.

## Refreshing the Displays

➤ To refresh the displays in the Entire Net-Work Server SMH administration area:

- 1 Access the Entire Net-Work Server SMH administration area, as described in [Accessing the Entire Net-Work Server SMH Administration Area](#), elsewhere in this section.
- 2 Right-click **Entire Net-Work Server** or other Entire Net-Work Server SMH administration item in tree-view and select the **Refresh** option from the resulting drop-down menu.

The data for the Entire Net-Work Server SMH administration area is refreshed.

---



# 29

## Managing Entire Net-Work Servers

---

This chapter describes the administration tasks you can perform for Entire Net-Work Server using the System Management Hub.

This information is organized under the following headings:

*Listing, Selecting, and Reviewing Installed Entire Net-Work Server*

*Adding Kernel Configuration Definitions*

*Migrating Kernel Configurations*

*Setting Entire Net-Work Server Parameters*

*Setting the Trace Level for an Entire Net-Work Server*

*Managing Entire Net-Work Server Log Files*

*Changing the Adabas Directory Server*

*Shutting Down the Entire Net-Work Server*



# 30

## Listing, Selecting, and Reviewing Installed Entire Net-Work Server

---

### ➤ To list and review the Entire Net-Work Servers managed by SMH:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

The following commands are available:



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

Command	Use this command to:
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 Server administration area.
Refresh	Refresh the screen.

Command	Use this command to:
<b>Remove from View</b>	Remove a node in tree-view from System Management View. For more information about System Management View, read your System Management Hub documentation.

- Expand the name of an Entire Net-Work server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

The following commands are available for each server:



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

Command	Use this command to:
<b>Add Kernel</b>	Add a Kernel to be maintained by SMH. For more information, read <a href="#">Adding Kernel Definitions</a> , elsewhere in this chapter.
<b>Add to Browser Favorites</b>	Add a node in tree-view to your browser favorites.
<b>Add to View</b>	Add a node in tree-view to System Management View. For more information about System Management View, read your System Management Hub documentation.
<b>Help</b>	Link to help for your use of SMH as it pertains to the Entire Net-Work Server administration area.
<b>Migrate WCP73 Kernel</b>	Migrate the Kernel configuration definitions you set up in Entire Net-Work Server 7.3. This process converts them to Entire Net-Work Server 7.4 Kernel configuration definitions. For more information, read <a href="#">Migrating Kernel Configurations</a> , elsewhere in this chapter.
<b>Migrate WCP74 Kernel</b>	Migrate the Kernel configuration definitions you set up in Entire Net-Work Server 7.4. This process converts them to Entire Net-Work Server 7.5 Kernel configuration definitions. For more information, read <a href="#">Migrating Kernel Configurations</a> , elsewhere in this chapter.
<b>New Log File</b>	Close the current Entire Net-Work Server log file and start a new one. For more information, read <a href="#">Managing Entire Net-Work Server Log Files</a> , elsewhere in this chapter.
<b>Refresh</b>	Refresh the screen.
<b>Remove from View</b>	Remove a node in tree-view from System Management View. For more information about System Management View, read your System Management Hub documentation.
<b>Set Service Parameters</b>	Change the parameters used by the Entire Net-Work Server, including the default Directory Server used. For more information, read <a href="#">Setting Entire Net-Work Server Parameters</a> , elsewhere in this chapter.

Command	Use this command to:
<b>Set Service Trace Granularity</b>	Set the Entire Net-Work Server trace level. For more information, read <a href="#">Setting the Trace Level for an Entire Net-Work Server</a> , elsewhere in this chapter.
<b>Shutdown</b>	Shut down Entire Net-Work Server. For more information, read .
<b>View Log File</b>	View the current Entire Net-Work Server log file. For more information, read <a href="#">Managing Entire Net-Work Server Log Files</a> , elsewhere in this chapter.



# 31

## Adding Kernel Configuration Definitions

---

When you define a Kernel, a configuration file containing all of its access and connection definitions as well as all of its parameters is created. By default, *Kernel configuration files* are stored in one of the following locations:

- In Windows 7 environments: `ProgramData\Software AG\Entire Net-Work Server\`
- In UNIX environments: `$SAG\wcp\`.

Kernel configuration files have names in the format *name.KERNEL*, where *name* is the name you assign the Kernel definition when you add it.

### » To add a Kernel definition to an Entire Net-Work Server:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 In tree-view, right-click on the name of the server on which you want to add a Kernel and select **Add Kernel** command from the resulting drop-down menu.

The **Add Net-Work Kernel** panel appears in detail-view.

### Add Net-Work Kernel

Enter the Net-Work Kernel Name:  \*

☒ E-Business Access. Enter Port Value:  \*

Additional Parameters:

☐ E-Business SSL Access. Enter Port Value:  \*

Additional Parameters:

☒ E-Business Client Access. Enter Port Value:  \*

Additional Parameters:

☐ E-Business SSL Client Access. Enter Port Value:  \*

Additional Parameters:

☐ Classic Access. Enter Port Value:  7869 \*

Additional Parameters:

6 Fill in the fields on this panel, as described in the following table:

Field	Description	Required?
Enter the Net-Work Kernel Name	<p>The name of this Kernel definition. The Kernel name will be used as the node name for the Kernel in Entire Net-Work processing.</p> <p>Remember that node names for Entire Net-Work Version 7 Kernels are case-sensitive and must be one to eight characters long. In addition, Kernel node names should be unique, especially if they use the same Adabas Directory Server.</p>	Yes
E-Business Access parameters	<p>Select e-business access if you want this Kernel definition to include an e-business access specification for another Kernel or for a mainframe Entire Net-Work node.</p> <p>The e-business access parameters include parameters that indicate that this is an e-business Kernel access definition and identifies the port number and additional parameters that should be used for this e-business access.</p> <ul style="list-style-type: none"> <li>Click in the <b>E-Business Access</b> checkbox (a checkmark should appear) to define an e-business Kernel access definition.</li> <li>Specify the port number that should be used for e-business server access. A value of zero (0) indicates that Entire Net-Work should search for an available port and dynamically assign it. For more information about port numbers, read .</li> <li>Optionally, specify any Adabas Directory Server additional parameters needed for this e-business Kernel access definition. Additional parameters you specify are described in <i>Parameters</i>, in the chapter entitled <i>Directory Server Target Entries</i> of the <i>Software AG Directory Server Installation and Administration Guide</i>. Separate</li> </ul>	If e-business server access is required, the <b>E-Business Access</b> checkbox must be checked. No other parameters are required.



Field	Description	Required?
	parameters in this field with ampersand (&) symbols. Note that not all Directory Server parameters apply to all access types.	
E-Business SSL Access parameters	<p>Select e-business SSL access if you want this Kernel definition to include an e-business access specification for another Kernel using Secure Sockets Layer (SSL).</p> <p>The e-business SSL access parameters include parameters that indicate that this is an e-business SSL Kernel access definition and identify the port number and additional parameters that should be used for this e-business SSL Kernel access.</p> <ul style="list-style-type: none"> <li>■ Click in the <b>E-Business SSL Access</b> checkbox (a checkmark should appear) to define an e-business Kernel access definition using SSL.</li> <li>■ Specify the port number that should be used for e-business server SSL access. A value of zero (0) indicates that Entire Net-Work should search for an available port and dynamically assign it. For more information about port numbers, read .</li> <li>■ Optionally, specify any Adabas Directory Server additional parameters needed for this e-business Kernel access definition. Additional parameters you specify are described in <i>Parameters</i>, in the chapter entitled <i>Directory Server Target Entries</i> of the <i>Software AG Directory Server Installation and Administration Guide</i>. Separate parameters in this field with ampersand (&amp;) symbols. Note that not all Directory Server parameters apply to all access types.</li> </ul> <p>For assistance in setting up SSL support in Entire Net-Work, read <i>Using the SSL Toolkit</i> in the <i>Encryption for Entire Net-Work User Guide</i>, available from your Software AG support representative.</p> <p><b>Note:</b> 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.</p>	If e-business server SSL access is required, the <b>E-Business SSL Access</b> checkbox must be checked. No other parameters are required.
E-Business Client Access parameters	<p>Select e-business client access if you want this Kernel definition to include an e-business access specification for an Entire Net-Work Client.</p> <p>The e-business client access parameters include parameters that indicate that this is an e-business Entire Net-Work Client access definition and identify the port number and additional parameters that should be used for this Entire Net-Work Client e-business access.</p> <ul style="list-style-type: none"> <li>■ Click in the <b>E-Business Client Access</b> checkbox (a checkmark should appear) to define an e-business Entire Net-Work Client access definition.</li> </ul>	If e-business Entire Net-Work Client access is required, the <b>E-Business Client Access</b> checkbox must be checked. No other parameters are required.

Field	Description	Required?
	<ul style="list-style-type: none"> <li>■ Specify the port number that should be used for e-business Entire Net-Work Client access. A value of zero (0) indicates that Entire Net-Work should search for an available port and dynamically assign it. For more information about port numbers, read .</li> <li>■ Optionally, specify any Adabas Directory Server additional parameters needed for this e-business Kernel access definition. Additional parameters you specify are described in <i>Parameters</i>, in the chapter entitled <i>Directory Server Target Entries</i> of the <i>Software AG Directory Server Installation and Administration Guide</i>. Separate parameters in this field with ampersand (&amp;) symbols. Note that not all Directory Server parameters apply to all access types.</li> </ul>	
E-Business SSL Client Access parameters	<p>Select e-business Entire Net-Work Client SSL access if you want this Kernel definition to include an e-business access specification for an Entire Net-Work Client using Secure Sockets Layer (SSL).</p> <p>The e-business client SSL access parameters include parameters that indicate that this is an e-business Entire Net-Work Client SSL access definition and identify the port number and additional parameters that should be used for this e-business client SSL access.</p> <ul style="list-style-type: none"> <li>■ Click in the <b>E-Business SSL Client Access</b> checkbox (a checkmark should appear) to define an e-business Entire Net-Work Client access definition using SSL.</li> <li>■ Specify the port number that should be used for e-business Entire Net-Work Client SSL access. A value of zero (0) indicates that Entire Net-Work should search for an available port and dynamically assign it. For more information about port numbers, read .</li> <li>■ Optionally, specify any Adabas Directory Server additional parameters needed for this e-business Kernel access definition. Additional parameters you specify are described in <i>Parameters</i>, in the chapter entitled <i>Directory Server Target Entries</i> of the <i>Software AG Directory Server Installation and Administration Guide</i>. Separate parameters in this field with ampersand (&amp;) symbols. Note that not all Directory Server parameters apply to all access types.</li> </ul> <p>For assistance in setting up SSL support in Entire Net-Work, read <i>Using the SSL Toolkit</i> in the <i>Encryption for Entire Net-Work User Guide</i>, available from your Software AG support representative.</p> <p><b>Note:</b> 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.</p>	<p>If e-business Entire Net-Work Client SSL access is required, the <b>E-Business SSL Client Access</b> checkbox must be checked. No other parameters are required.</p>

Field	Description	Required?
Classic Access parameters	<p>Select classic access if you want this Kernel definition to include an access definition to a classic Entire Net-Work (Entire Net-Work 2) node.</p> <p>Classic access provides access with an Entire Net-Work 2 for open systems node, an Entire Net-Work 3 for OpenVMS node or with an Entire Net-Work 6 (mainframe) node that does not have the Simple Connection Line Driver installed.</p> <p>The classic access parameters include parameters that indicate that this is a classic access definition to an Entire Net-Work Version 2 node and identifies the port number, node ID, and additional parameters that should be used for this classic Entire Net-Work access.</p> <ul style="list-style-type: none"> <li>■ Click in the <b>Classic Access</b> checkbox (a checkmark should appear) to define an access definition to a classic Entire Net-Work node.</li> <li>■ Specify the port number that should be used for classic Entire Net-Work access. The default port number for this type of access is 7869. For more information about port numbers, read .</li> <li>■ Specify the ID of the classic Entire Net-Work node to which this Kernel will allow access.</li> <li>■ Optionally, specify any Adabas Directory Server additional parameters needed for this e-business Kernel access definition. Additional parameters you specify are described in <i>Parameters</i>, in the chapter entitled <i>Directory Server Target Entries</i> of the <i>Software AG Directory Server Installation and Administration Guide</i>. Separate parameters in this field with ampersand (&amp;) symbols. Note that not all Directory Server parameters apply to all access types.</li> </ul>	<p>If classic Entire Net-Work access is required, the <b>Classic Access</b> checkbox must be checked and a port number and node ID must be specified. No additional parameters are required.</p>

7 Click **OK**.

The Kernel configuration definition is added to the server.



# 32

## Migrating Kernel Configurations

---

If you want to use your Kernel configuration definitions from earlier versions of Entire Net-Work Server in this version, you must convert them to current Entire Net-Work Server Kernel configurations. This chapter describes how to do this.



**Caution:** Once a Kernel configuration has been migrated to the most recent version of Entire Net-Work Server, it cannot be migrated back to an earlier Entire Net-Work Server version. If you really need to do so, contact your Software AG technical support representative for assistance.

➤ **To convert Entire Net-Work Server configurations to the configuration used by the current version of Entire Net-Work Server:**

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

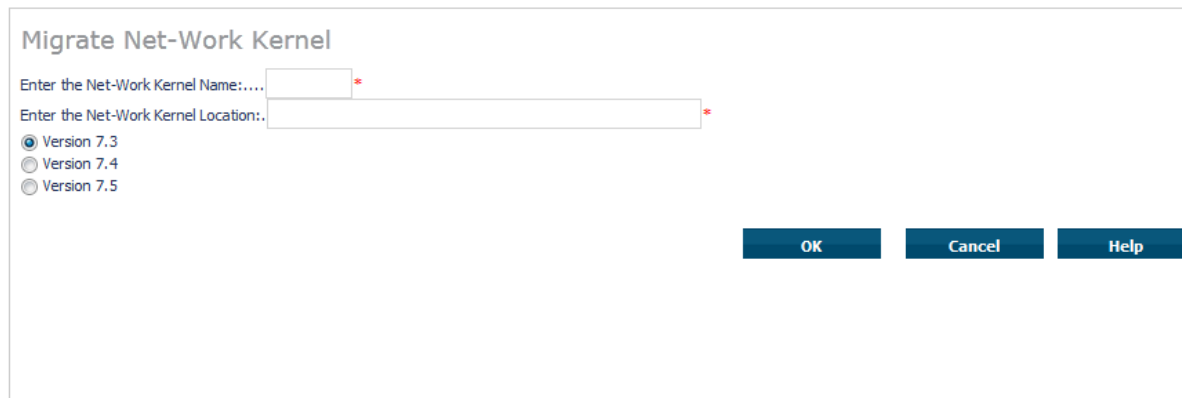
The Entire Net-Work Server administration area of the System Management Hub becomes available to you.

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 In tree-view, right-click on the name of the server on which you want to add a Kernel and select the **Migrate Kernel** command from the resulting drop-down menu.

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



**Migrate Net-Work Kernel**

Enter the Net-Work Kernel Name:.... \*

Enter the Net-Work Kernel Location:.. \*

☒ Version 7.3  
☐ Version 7.4  
☐ Version 7.5

OK Cancel Help

- 6 In the **Enter the Net-Work Kernel Name** field, specify the name of the older Kernel configuration definition you want to migrate.
- 7 In the **Enter the Net-Work Kernel Location** field, specify the fully qualified path name of the location of the older Kernel configuration definition you want to migrate.
- 8 Select (click on) the radio button associated with version number of the older Kernel configuration definition you want to migrate.
- 9 When all fields been specified, click **OK** to convert the older Kernel configuration to a current Kernel configuration.

The configuration is converted.

# 33

## Setting Entire Net-Work Server Parameters

---

You can set parameters for the Entire Net-Work Server, including the default Adabas Directory Server used by the server, as well as the server name, host name, and port number.

➤ **To set parameters for the Entire Net-Work Server:**

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Select and right-click on the server. Then select the **Set Service Parameters** option from the resulting drop-down menu.

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

**Server Parameters**

SAGXTSDSHOST ..... MCUSASASW04.eur.ad.sag

SAGXTSDSPORT ..... 4952

SERVER\_NAME ..... <not defined>

SERVER\_HOST ..... <not defined>

SERVER\_PORT ..... <not defined>

LOGDIR ..... C:\ProgramData\Software AG\Entire Net-Work Server\logsvc75\

☐ Update all Kernels

OK Cancel Help

- 6 Modify the parameters on the **Server Parameters** panel, as described in the following table.

Parameter	Description
SAGXTSDSHOST	Specify the Adabas Directory Server host name you want to use for this server.
SAGXTSDSPORT	Specify the port number of the Adabas Directory Server you specified in the SAGXTSDSHOST parameter.
SERVER_NAME	Normally, the server name is the machine name. However, for cosmetic reasons only, you can change the server name. If a name is specified in this parameter, the new name is changed in the access entries in the local Entire Net-Work Server configuration file.
SERVER_HOST	Normally, the host name for an Entire Net-Work Server is the machine name. However, you may want to select a different host name for the server. 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 host name is specified in this parameter, the new host name is changed in the access entries in the local Entire Net-Work Server configuration file.
SERVER_PORT	<p>Normally, port numbers are dynamically assigned by Entire Net-Work when the server is started, as follows:</p> <ul style="list-style-type: none"> <li>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.).</li> </ul>



Parameter	Description
	<p>■ Once an available port number is found, it is assigned to the server in its Adabas Directory Server entry.</p> <p>You can optionally assign a port number to an Entire Net-Work server using this parameter. If you do, the new port number is changed in the access entries in the local Entire Net-Work Server configuration file.</p>
LOGDIR	Specify the fully-qualified path of the directory where server log files should be written. For more information, read <a href="#">Specifying the Entire Net-Work Server Log File Location</a> , elsewhere in this chapter.

- 7 Optionally, select the **Update all Kernels** checkbox if you want all of the Kernel definitions defined for this server to have these parameters applied to them. If you do not select the **Update all Kernels** checkbox, only new Kernel definitions will have these parameters applied.
- 8 When all parameters are set as you want, click **OK**.

The Entire Net-Work Server parameters are updated.



# 34

## Setting the Trace Level for an Entire Net-Work Server

---

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:** While you can set the trace level for an Entire Net-Work server using SMH, we recommend that you perform this function only under the advisement of your Software AG support representative.

### » To set the trace level for the server:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

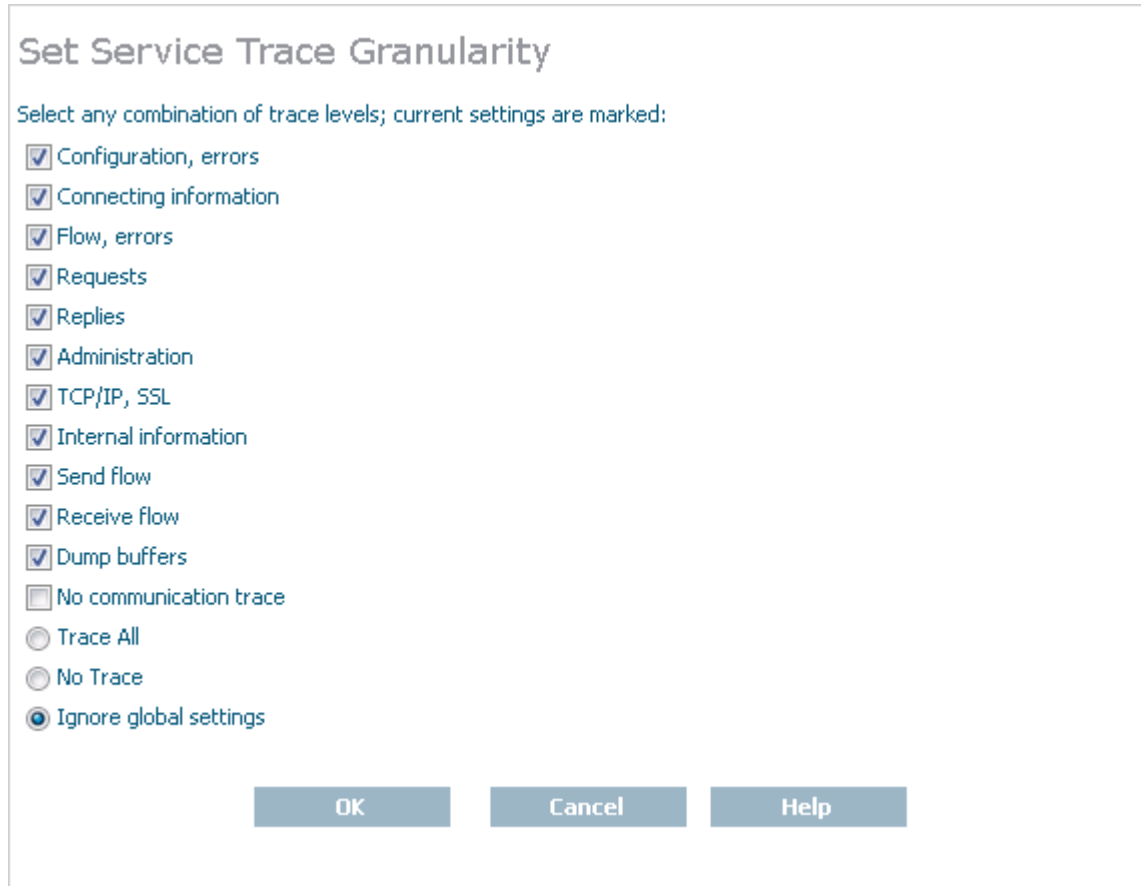
The Entire Net-Work Server administration area of the System Management Hub becomes available to you.

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 In tree-view, right-click on the name of the server for which you want to set the trace level and select **Set Service Trace Granularity** command 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

- 6 Select appropriate trace levels as requested by your Software AG support representative.

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.

- 7 Click **OK**.

The trace level is set. You must stop and restart the server in order for these settings to take effect.

# 35

## Managing Entire Net-Work Server Log Files

---

■ Viewing the Entire Net-Work Server Log File .....	182
■ Starting a New Entire Net-Work Server Log File .....	182
■ Specifying the Entire Net-Work Server Log File Location .....	184

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

## Viewing the Entire Net-Work Server Log File

---

➤ To view the log file for the Entire Net-Work Server:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 In tree-view, right-click on the name of the server whose log file you want to view and select **View Log File** command from the resulting drop-down menu.

The console log for the Entire Net-Work Server appears in detail-view.

## Starting a New Entire Net-Work Server Log File

---

You can close the current log file for an Entire Net-Work Server and start a new one at any time. When you do this, the current log file (*wcp-svc.log*) is saved under a new name and is cleared of all log entries. The name of the renamed log file is assigned in the format *wcpnnnnn.log*, where *nnnnn* is an incremental number determined by the number of the most recent log file that was renamed and saved. The log file with the name that includes the highest number is the most recently saved log file.

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

- In Windows 7 environments: `ProgramData\Software AG\Entire Net-Work Server\logsvc75`
- In UNIX environments: `$SAG\wcp\.`

If you would like to specify the location in which server log files should be stored, read [Specifying the Entire Net-Work Server Log File Location](#), elsewhere in this section.

➤ **To start a new log file for the Entire Net-Work Server:**

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

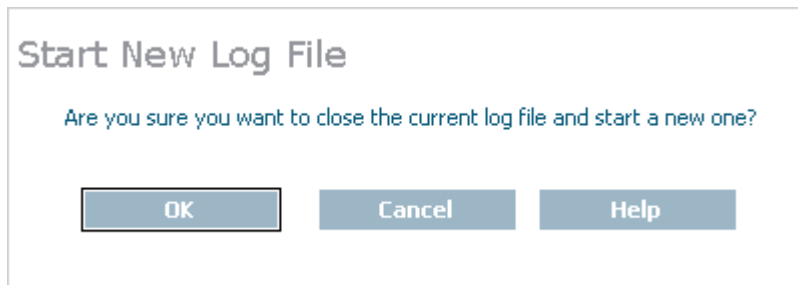
The Entire Net-Work Server administration area of the System Management Hub becomes available to you.

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 In tree-view, right-click on the name of the server for which you want to start a new log file and select **New Log File** command from the resulting drop-down menu.

The **Start New Log File** panel appears in detail-view.



- 6 Click **OK**.

A new log file is started for the Entire Net-Work Server and the old one is closed.

## Specifying the Entire Net-Work Server Log File Location

---

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

- In Windows 7 environments: `ProgramData\Software AG\Entire Net-Work Server\logsvc75`
- In UNIX environments: `$SAG\wcp\`.



**Note:** If you want to put your Entire Net-Work log files on a shared server, read . However, please be sure that the directory name you specify for the log files for each server is unique.

### ➤ To specify the log file location:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Select and right-click on the server. Then select the **Set Service Parameters** option from the resulting drop-down menu.

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



**Server Parameters**

SAGXTSDSHOST ..... MCUSASASW04.eur.ad.sag

SAGXTSDSPORT ..... 4952

SERVER\_NAME ..... <not defined>

SERVER\_HOST ..... <not defined>

SERVER\_PORT ..... <not defined>

LOGDIR ..... C:\ProgramData\Software AG\Entire Net-Work Server\logsvc75\

☐ Update all Kernels

OK Cancel Help

- 6 Specify the fully-qualified path of the directory in which you want log files stored in the **LOGDIR** parameter.
- 7 Optionally, select the **Update all Kernels** checkbox if you want all of the Kernel definitions defined for this server to have these parameters applied to them. If you do not select the **Update all Kernels** checkbox, only new Kernel definitions will have these parameters applied.
- 8 When all parameters are set as you want, click **OK**.

The Entire Net-Work Server parameters are updated.



# 36

## Changing the Adabas Directory Server

---

While you can specify that different Directory Servers be used by an Entire Net-Work Server and by its Kernel definitions, this is not recommended. The ability to do this is useful for testing only, but when your network testing is complete, we recommend that the same Directory Server be used for both.

### ➤ To change the Directory Server for the Entire Net-Work Server:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 In tree-view, right-click on the name of the server for which you want to change the Directory Server and select **Set Service Parameters** command from the resulting drop-down menu.

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

**Server Parameters**

SAGXTSDSHOST ..... MCUSASASW04.eur.ad.sag

SAGXTSDSPORT ..... 4952

SERVER\_NAME ..... <not defined>

SERVER\_HOST ..... <not defined>

SERVER\_PORT ..... <not defined>

LOGDIR ..... C:\ProgramData\Software AG\Entire Net-Work Server\logsvc75\

☐ Update all Kernels

OK Cancel Help

- 6 Fill in the **SAGXTSDSHOST** and **SAGXTSDSPORT** fields on this panel, as described in the following table:

Field	Description	Required?	Default
SAGXTSDSHOST	The host name on which the Directory Server is installed.	Yes	—
SAGXTSDSPORT	The port number assigned the Directory Server. If this field is set to zero (0) or left blank, the default will be used.	No	4952

- 7 Click **OK**.

The Directory Server is changed for the Entire Net-Work Server. You must stop and restart the server in order for these changes to take effect.

# 37

## Shutting Down the Entire Net-Work Server

---

### » To shut down the Entire Net-Work Server:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 In tree-view, right-click on the name of the server you want to shut down and select **Shutdown** command from the resulting drop-down menu.

A request to confirm that you want to shut down the server appears in detail-view.

- 6 Click **OK**.

The Entire Net-Work Server is shut down.



# 38

## Managing Kernels

---

This chapter describes the administration tasks you can perform for Entire Net-Work Kernels using the System Management Hub.

This information is organized under the following headings:

- Listing, Selecting, and Reviewing Kernel Definitions*
- Reviewing the Kernel Parameter Summary*
- Starting a Kernel*
- Shutting Down a Kernel*
- Adding Kernel Definitions*
- Deleting a Kernel*
- Setting Basic Kernel Parameters*
- Setting Advanced Kernel Parameters*
- Specifying Kernel Scalability*
- Maintaining Kernel Filters*
- Changing the Adabas Directory Server*
- Maintaining Access Definitions*
- Reviewing Kernel Access Status*
- Maintaining Connection Definitions*
- Reviewing Kernel Outgoing Connection Status*
- Reviewing Kernel Statistics*
- Setting Detailed Statistics Online*
- Generate a Kernel Configuration Dump*
- Checking Kernel Databases*
- Pinging Databases and Classic Nodes*
- Dynamically Connecting and Disconnecting a Connection*

*Dynamically Managing Kernel Clients and Adabas Contexts*

*Dynamically Managing Kernel Client Hosts*

*Reviewing Kernel Status*

*Managing Kernel Log Files*

*Tracing Kernel Processing*



# 39

## Listing, Selecting, and Reviewing Kernel Definitions

---

- Listing, Selecting, and Reviewing Permanent Definitions ..... 194
- Listing, Selecting, and Reviewing Dynamic Definitions ..... 196

You can list, select, and review Kernel definitions that are managed by SMH. These definitions are listed in two areas:

- The *permanent* definition for a Kernel is listed in the **Servers** section of the Entire Net-Work Server SMH administration area. You can maintain the definitions in this area and the changes you make are permanent (until the next time you make a change).
- The *dynamic* definition for a started Kernel is listed in the **Kernels** section of the Entire Net-Work Server SMH administration area. Statistics for the active Kernel as well as some of its parameters can be reviewed and maintained in this area. Any maintenance performed to parameters in the dynamic definition are preserved only temporarily. Once the Kernel is stopped, the changes made to the dynamic definition are lost and, if the Kernel is restarted, it starts using its permanent definition. Therefore, if you want to change the definition of a Kernel so it remains the same every time you start it, be sure to make the change to the permanent definition, not the dynamic definition.



**Note:** A Kernel must be started in the **Servers** section of the Entire Net-Work Server SMH administration area before you can see it in the **Kernels** section.

## Listing, Selecting, and Reviewing Permanent Definitions

---

➤ To list and review the permanent Kernel definitions managed by SMH:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 Select and expand the Kernel definition you want from the list.

The permanent Kernel definition section becomes available in tree-view.

The following commands are available for each Kernel:



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

Command	Use this command to:
<b>Add Connection</b>	Add a connection to other e-business Kernels or to classic Entire Net-Work installations in a Kernel definition. For more information, read <a href="#">Maintaining Connection Definitions</a> , elsewhere in this section.
<b>Add Kernel Access</b>	Add Kernel access entries to a Kernel definition. For more information, read <a href="#">Maintaining Access Definitions</a> , elsewhere in this section.
<b>Add to Browser Favorites</b>	Add a node in tree-view to your browser favorites.
<b>Add to View</b>	Add a node in tree-view to System Management View. For more information about System Management View, read your System Management Hub documentation.
<b>Delete Kernel</b>	Delete a Kernel definition. For more information, read <a href="#">Deleting a Kernel</a> , elsewhere in this section.
<b>Help</b>	Link to help for your use of SMH as it pertains to the Kernel administration area.
<b>Kernel Filters</b>	Apply a filter to the Kernels, databases, and hosts that can interact with this Kernel. For more information, read <a href="#">Maintaining Kernel Filters</a> , elsewhere in this section.
<b>Parameters Summary</b>	Review a summary of the most important parameters for the Kernel. When you select this command, the most important Kernel parameters are listed in detail-view. For more information, read <a href="#">Reviewing the Kernel Parameter Summary</a> , elsewhere in this section.
<b>Refresh</b>	Refresh the screen.
<b>Remove from View</b>	Remove a node in tree-view from System Management View. For more information about System Management View, read your System Management Hub documentation.
<b>Set Advanced Parameters</b>	Set advanced parameters for a Kernel. For more information, read <a href="#">Setting Advanced Parameters</a> , elsewhere in this section.
<b>Set Basic Parameters</b>	Set basic parameters for a Kernel. For more information, read <a href="#">Setting Basic Parameters</a> , elsewhere in this section.
<b>Set Directory Server</b>	Change the Directory Server used by the Kernel. For more information, read <a href="#">Changing the Adabas Directory Server</a> , elsewhere in this section.
<b>Set Kernel Scalability</b>	Specify settings that adjust how the Kernel is used so its performance is improved. For more information, read <a href="#">Specifying Kernel Scalability</a> , elsewhere in this section.
<b>Set Kernel Trace Granularity</b>	Set the Kernel trace level. For more information, read <a href="#">Tracing Kernel Processing</a> , elsewhere in this section.
<b>Shutdown</b>	Shut down the Entire Net-Work Server service. For more information, read <a href="#">Shutting Down a Kernel</a> , elsewhere in this section.

Command	Use this command to:
<b>Start Kernel</b>	Start a Kernel maintained by SMH. For more information, read <a href="#">Starting a Kernel</a> , elsewhere in this section.
<b>Status</b>	Review the status of a Kernel. For more information, read <a href="#">Reviewing Kernel Status</a> , elsewhere in this section.

## Listing, Selecting, and Reviewing Dynamic Definitions

### ➤ To list and review the dynamic Kernel definitions managed by SMH:

Make sure you have accessed the System Management Hub and verify that the Kernel has been started. For more information, read [Starting a Kernel](#), elsewhere in this guide.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed and started Kernels appears in detail-view.

- 5 Select and expand the Kernel definition you want from the list.

The dynamic Kernel definition section becomes available in tree-view.

The following commands are available for each Kernel:



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

Command	Use this command to:
<b>Access Status</b>	Review the status of a Kernel's access definitions. For more information, read <a href="#">Reviewing Kernel Access Status</a> , elsewhere in this section.
<b>Add Connection Online</b>	Add a dynamic outgoing connection for the Kernel. For more information, read <a href="#">Dynamically Adding a Connection</a> , elsewhere in this section.
<b>Add to Browser Favorites</b>	Add a node in tree-view to your browser favorites.
<b>Add to View</b>	Add a node in tree-view to System Management View. For more information about System Management View, read your System Management Hub documentation.

Command	Use this command to:
<b>Dump Configuration</b>	Generate a kernel configuration dump in the log file. For more information, read <a href="#">Generate a Kernel Configuration Dump</a> , elsewhere in this section.
<b>Help</b>	Link to help for your use of SMH as it pertains to the dynamic Kernel administration area.
<b>New Log File</b>	Close the current Kernel log file and start a new one. For more information, read <a href="#">Managing Kernel Log Files</a> , elsewhere in this section.
<b>Outgoing Connections Status</b>	Review the status of Kernel connections, as defined by its connection definitions. For more information, read <a href="#">Reviewing Kernel Outgoing Connection Status</a> , elsewhere in this section.
<b>Refresh</b>	Refresh the screen.
<b>Remove from View</b>	Remove a node in tree-view from System Management View. For more information about System Management View, read your System Management Hub documentation.
<b>Set Detailed Statistics Online</b>	Dynamically start collecting detailed statistics for the Kernel. For more information, read <a href="#">Dynamically Collecting Detailed Statistics</a> , elsewhere in this section.
<b>Set Trace Level Online</b>	Dynamically set the Kernel trace level. For more information, read <a href="#">Tracing Kernel Processing</a> , elsewhere in this section.
<b>Shutdown</b>	Shut down the Entire Net-Work Server service. For more information, read <a href="#">Shutting Down a Kernel</a> , elsewhere in this section.
<b>Statistics</b>	Review statistics for the running Kernel. When you select this command, the Kernel statistics are listed in detail-view. For more information, read <a href="#">Reviewing Kernel Statistics</a> , elsewhere in this section.
<b>View Log File</b>	View the Kernel log file. For more information, read <a href="#">Managing Kernel Log Files</a> , elsewhere in this section.



# 40

## Reviewing the Kernel Parameter Summary

---

### » To review a summary of Kernel parameters:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 In tree-view, right-click on the name of the Kernel for which you want to review the parameter summary and select the **Parameters Summary** command from the resulting drop-down menu.

A summary of the Kernel definition parameters appears in detail-view.

## MYKERNEL

□	Parameter	□	Value	□
✓	SAGXTSDSHOST		localhost	
✓	SAGXTSDSPORT		4952	
✓	WCPARTITION			
✓	ACCEPTED_DBIDS			
✓	REJECTED_DBIDS			
✓	RELAY_TRAFFIC		YES	
✓	NODEID		1234	
✓	WCPTRACE		0	
✓	XTSTRACE		0	
✓	LNKTRACE		0	
✓	USER_EXITS			



# 41

## Starting a Kernel

---

### ➤ To start a Kernel:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

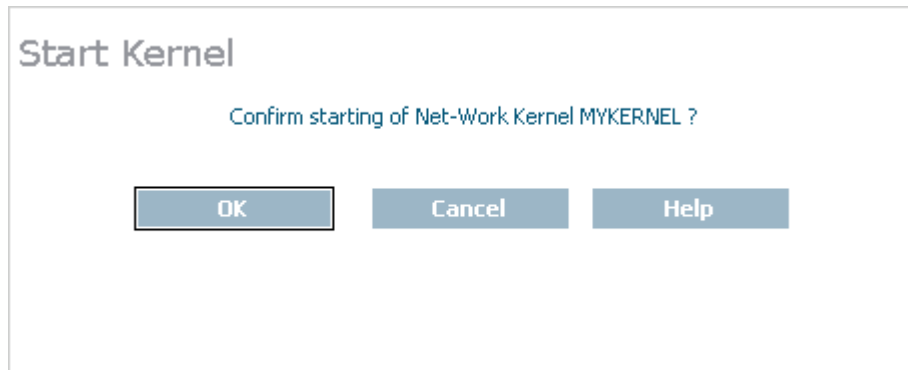
The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 In tree-view, right-click on the name of the Kernel you want to start and select the **Start Kernel** command from the resulting drop-down menu.

The **Start Kernel** panel appears in detail-view.



- 7 Click **OK**.

The Kernel is started.

# 42

## Shutting Down a Kernel

---

- Shutting Down a Kernel Using Its Permanent Definition ..... 204
- Shutting Down a Kernel Using Its Dynamic Definition ..... 205

You can shut down a Kernel from the server or from the Kernel list in SMH. There is no difference between the two methods; both methods are provided for your convenience.

### Shutting Down a Kernel Using Its Permanent Definition

---

➤ To shut down a Kernel from its permanent definition in the Entire Net-Work Server list in SMH:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

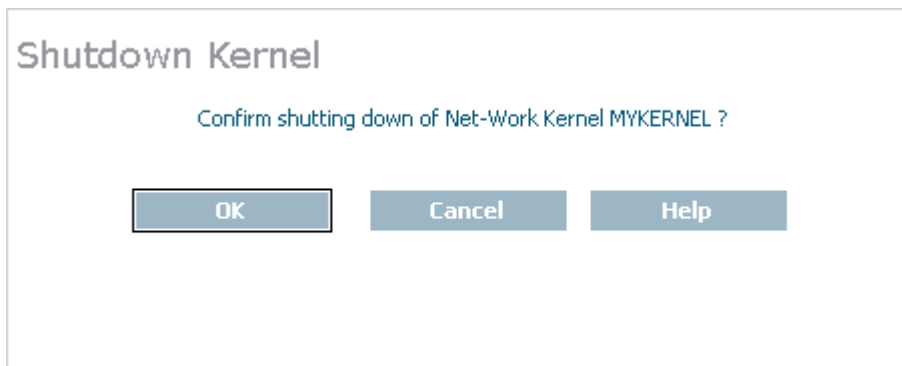
The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 In tree-view, right-click on the name of the Kernel you want to shut down and select the **Shutdown** command from the resulting drop-down menu.

The **Shutdown Kernel** panel appears in detail-view.



- 7 Click **OK**.

The Kernel is shut down.

## Shutting Down a Kernel Using Its Dynamic Definition

➤ To shut down a Kernel from its dynamic definition in the Kernel list in SMH:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

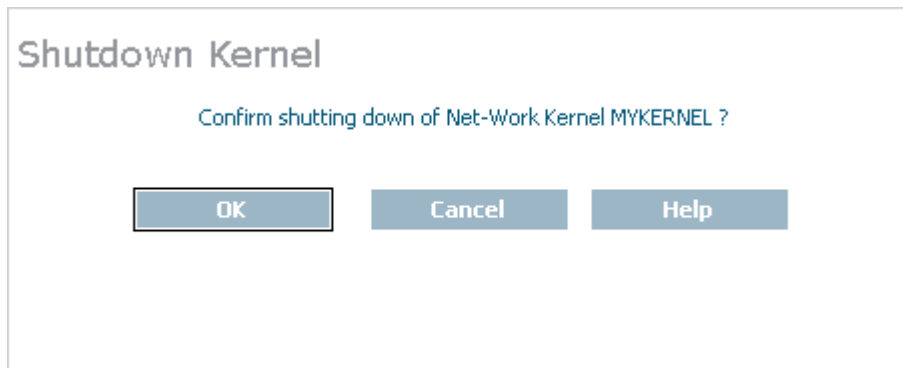
The Entire Net-Work Server administration area of the System Management Hub becomes available to you.

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of Kernels that have been started appears.

- 5 In tree-view, right-click on the name of the Kernel you want to shut down and select the **Shutdown** command from the resulting drop-down menu.

The **Shutdown Kernel** panel appears in detail-view.



- 6 Click **OK**.

The Kernel is shut down.



## 43 Deleting a Kernel

---

You cannot delete a Kernel that is started. Before you can delete a Kernel, make sure you have shut it down, as described in [Shutting Down a Kernel](#), elsewhere in this guide.

➤ **To delete a Kernel definition:**

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

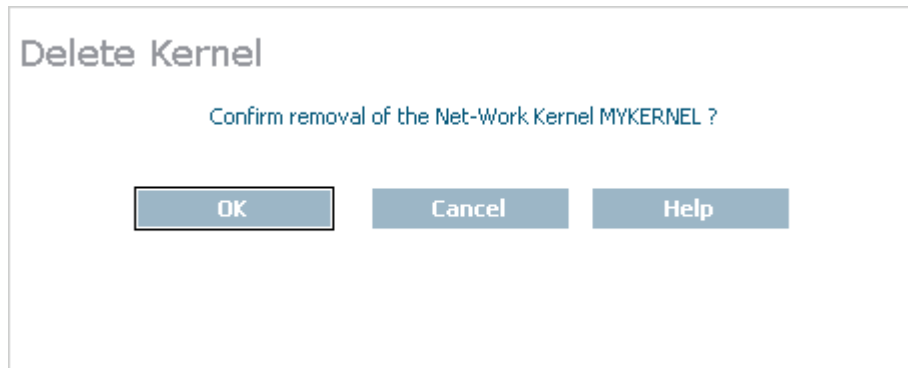
The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 In tree-view, right-click on the name of the Kernel you want to delete and select the **Delete Kernel** command from the resulting drop-down menu.

The **Delete Kernel** panel appears in detail-view.



- 7 Click **OK**.

The Kernel is deleted.



# 44

## Setting Basic Kernel Parameters

---

### » To set basic Kernel definition parameters:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 In tree-view, right-click on the name of the Kernel for which you want to set basic parameters and select the **Set Basic Parameters** command from the resulting drop-down menu.

The **Kernel Basic Parameters** panel appears in detail-view.

Kernel Basic Parameters

WCPPARTITION.....<not defined>

NODEID.....1234\*

AUTOSTART.....<not defined>

AUTOSTOP.....<not defined>

WCPTRACE.....0\*

☐ Full WCP Trace

XTSTRACE.....0\*

☐ Full XTS Trace

LNKTRACE.....0\*

☐ Full LNK Trace

LOGDIR.....C:\ProgramData\Software AG\Entire Net-Work Server\MYKERNEL\

LOGSIZE.....100

DATE\_STAMP.....<not defined>

OK

Cancel

Help

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

Parameter	Description
WCPPARTITION	Specify the partition in which the Kernel is assigned, if any. For more information, read .
NODEID	<p>Optionally, specify a unique node ID for the Kernel definition. Node IDs are required for connections between mainframe and open systems nodes, but if you do not specify one for the Kernel in this parameter, Entire Net-Work will generate one for you. In fact, whenever a new Kernel is defined, a random node ID is automatically generated for it. Any previously defined Kernels (those defined before Entire Net-Work 7.5) for which a node ID does not yet exist will be assigned the node ID "1234".</p> <p><b>Note:</b> Node IDs must be unique across the system. If two Kernels have the same node ID, network connections obtained through those Kernels may not be handled accurately. We therefore recommend that you keep a list of your node IDs and ensure that any generated (or manually specified) node IDs are unique.</p> <p>The following issues with node IDs should be considered:</p> <ul style="list-style-type: none"><li>■ Entire Net-Work generates a random node ID for a new Kernel. However, there is a small risk that a duplicate node ID might be generated with a Kernel that is</li></ul>

Parameter	Description
	<p>not started. You will want to check any generated node IDs against your node ID list to ensure the generated node ID is unique.</p> <ul style="list-style-type: none"> <li>■ Because Kernels defined in Entire Net-Work versions earlier than version 7.5 may have the node ID "1234", you should manually alter these node IDs so they are unique. You can alter them on this screen.</li> </ul>
AUTOSTART	Indicate whether or not the Kernel should automatically be started when its associated Entire Net-Work Server is started. A value of "YES", indicates that it should be automatically started; a value of "NO" indicates that it should <i>not</i> be automatically started.
AUTOSTOP	Indicate whether or not the Kernel should automatically be stopped when its associated Entire Net-Work Server is stopped. A value of "YES", indicates that it should be automatically stopped; a value of "NO" indicates that it should <i>not</i> be automatically stopped.
WCPTRACE	<p>Set the hexadecimal Kernel trace level using this parameter. Valid values are any of the following hexadecimal values:</p> <ul style="list-style-type: none"> <li>■ 0x1 - produce trace snapshot on any error code</li> <li>■ 0x2 - trace error paths only</li> <li>■ 0x4 - trace flow control only</li> <li>■ 0x8 - produce full dumps of all activity</li> <li>■ 0x10 - trace SMH-related activity</li> <li>■ 0x100 - trace ADALNKX (Adabas calls)</li> <li>■ 0x200 - trace XTS (Software AG transport services)</li> </ul> <p>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 Kernel tracing, read <a href="#">Tracing Kernel Processing</a>, elsewhere in this guide.</p>
Full WCP Trace	Click in this checkbox to set the WCPTRACE value to obtain full tracing of this Kernel's 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.
XTSTRACE	<p>Set the hexadecimal XTS trace level using this parameter. This is the trace level for Software AG transport services. Valid values are any of the following hexadecimal values:</p> <ul style="list-style-type: none"> <li>■ 0x1 - buffer the log messages</li> <li>■ 0x2 - connect calls trace</li> <li>■ 0x4 - listen calls trace</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>■ 0x8 - send calls trace</li> <li>■ 0x10 - receive calls trace</li> <li>■ 0x20 - dump send/receive buffers</li> <li>■ 0x40 - directory service trace</li> <li>■ 0x80 - miscellaneous code</li> <li>■ 0x100 - internal interface trace</li> <li>■ 0x200 - TCP driver trace</li> <li>■ 0x400 - SMP trace</li> <li>■ 0x800 - Directory Server trace</li> <li>■ 0x1000 - trace statistics</li> </ul> <p>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 Kernel tracing, read <a href="#">Tracing Kernel Processing</a>, elsewhere in this guide.</p>
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.
LNKTRACE	<p>Set the hexadecimal ADALNK trace level using this parameter. This is the trace level for Adabas calls. Valid values are the hexadecimal values "00" (no tracing) or "0x1F" (full tracing). At this time, there is no granularity to ADALNK trace levels. 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 Kernel tracing, read <a href="#">Tracing Kernel Processing</a>, elsewhere in this guide.</p>
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.
LOGDIR	Specify the fully-qualified path of the directory where Kernel log files should be written. For more information, read <a href="#">Specifying the Kernel Log File Location</a> , elsewhere in this chapter.
LOGSIZE	Specify the number of megabytes (MB) to which a Kernel log file can grow before it is automatically closed and a new log file is started. The default is 500 MB. For

Parameter	Description
	more information about Kernel log files, read <a href="#">Managing Kernel Log Files</a> , elsewhere in this guide.
DATE_STAMP	Indicate whether or not you want the date and time stamp to be added to every Entire Net-Work trace statement written. Valid values are "YES" (include the date and time stamp) or "NO" (do not include the date and time stamp). The default is "NO".

The Kernel basic parameters are updated in the appropriate Kernel definition file. You must restart the Kernel in order for these parameter changes to take effect.



# 45

## Setting Advanced Kernel Parameters

---

» To set advanced Kernel definition parameters:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 In tree-view, right-click on the name of the Kernel for which you want to set advanced parameters and select the **Set Advanced Parameters** command from the resulting drop-down menu.

The **Kernel Advanced Parameters** panel appears in detail-view.

**Kernel Advanced Parameters**

ADABAS\_TIMEOUT ..... 50

TIMER\_TIMEOUT ..... 6

STATISTICS\_DETAILS ..... NO

STATISTICS\_INTERVAL ..... 60

PING\_DB\_INTERVAL ..... 0

CHECK\_DBS\_INTERVAL ..... 20

GATEWAY\_THREADS ..... <not defined>

USER\_EXITS ..... <not defined>

CHECK\_CXT\_INTERVAL ..... <not defined>

Protocol Family

☒ Unspecified

☐ IPV4 Only

☐ IPV6 Only

OK Cancel Help

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

Parameter	Description
ADABAS_TIMEOUT	Specify the number of seconds the Kernel should wait for a response from either a local or remote Adabas call before it times out. The default is 60 seconds; the minimum value you can specify is 5 seconds.
TIMER_TIMEOUT	Specify the frequency (in seconds) at which the Kernel should check to see if it needs to run the STATISTICS_INTERVAL, PING_DB_INTERVAL, or CHECK_DBS_INTERVAL processing. The default is 6 seconds.
STATISTICS_DETAILS	Indicate whether detail statistics should be collected and displayed for clients and client hosts. Valid values for this parameter are "YES" and "NO"; the default is "NO". Note that there is the performance of your system could be affected when statistic details are collected.
STATISTICS_INTERVAL	Specify the frequency at which statistics are collected for the Kernel, in minutes. The default is 60 minutes.
PING_DB_INTERVAL	Specify the frequency at which remote databases should be pinged to determine their status, in minutes. The default is zero (0) minutes (no pinging).
CHECK_DBS_INTERVAL	Specify the frequency at which local databases should be pinged to determine their status, in seconds. The default is 20 seconds.



Parameter	Description
GATEWAY_THREADS	Specify the number of threads available for a network node. When this limit is exceeded, service requests will wait until a thread becomes available. Use this parameter to tune how your network processes requests. The default (and minimum) is 5 threads; the maximum is 1024 threads.
USER_EXITS	This field is supplied only to support compatibility with Entire Net-Work 2 releases. We recommend that user exits be used applied in Entire Net-Work Client rather than in Entire Net-Work Kernels. However, if you have a Kernel user exit that you used with Entire Net-Work Version 2.6, specify the name of the user exit DLL file that should be used with this Kernel in this field.
CHECK_CXT_INTERVAL	<p>Specify how old the Adabas contexts that are created by Entire Net-Work clients can be, in seconds. Valid values are zero (0) or an integer between 60 and 86400 seconds (24 hours). The default value is 3600 seconds (1 hour).</p> <p>Anytime a client connects with Entire Net-Work, a context (a memory table with client information) for that specific client is created. When a client disconnects, the context is deleted. In situations when clients are disconnected abnormally (for example, they crash) or they are not disconnected for a long time (for example, when navigating on a web page), the size of Entire Net-Work unused memory increases significantly, which can affect Entire Net-Work performance. To avoid such situations, you can use this parameter to indicate how long contexts should be allowed to remain.</p> <p>If CHECK_CXT_INTERVAL is not zero, an Entire Net-Work thread periodically (every minute) checks the Adabas contexts created by clients connected to Entire Net-Work. Contexts older than the time set by this parameter are deleted.</p>
Protocol Family	<p>Select the TCP/IP protocol family used for the Kernel. Click (check) <b>Unspecified</b>, <b>IPV4 Only</b>, or <b>IPV6 Only</b>. If you select <b>IPV4 Only</b> or <b>IPV6 Only</b>, only the selected protocol is used for communications with this Kernel. If you select <b>Unspecified</b>, the domain name server (DNS) will determine which protocol is used; <b>Unspecified</b> is the default.</p> <p><b>Caution:</b> We recommend that you use the default value (<b>Unspecified</b>) for this parameter, allowing the DNS to determine which communication protocol is appropriate. If you do specify a specific protocol, calls to Entire Net-Work via the other protocol type are ignored.</p>

The Kernel advanced parameters are updated in the appropriate Kernel definition file. You must restart the Kernel in order for these parameter changes to take effect.



## 46 Specifying Kernel Scalability

---

Use Kernel scalability settings to adjust the amount in which the Kernel is used as a way of improving the performance of your system.

➤ **To specify Kernel scalability settings:**

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 In tree-view, right-click on the name of the Kernel for which you want to specify the Kernel filter list and select the **Set Kernel Scalability** command from the resulting drop-down menu.

The **Kernel Scalability** panel appears in detail-view.

## Kernel Scalability

MAX\_CLIENTS..... 123  
MAX\_CPU\_THRESHOLD..... <not defined>

OK Cancel Help

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

Parameter	Description
MAX_CLIENTS	Specify the maximum number of client requests that can be processed concurrently by this Kernel, as determined by your Entire Net-Work license. When this limit is exceeded, client requests are rejected. The minimum value you can specify is "5"; the maximum value you can specify is "65535" or the number of clients allowed by your product license, whichever is lower. You can specify a value that is less than or equal to the number of clients defined by your Entire Net-Work license. The default is the number defined by your license.
MAX_CPU_THRESHOLD	Specify the maximum CPU usage (the threshold) for this Kernel that can be used by clients of this Kernel. When this CPU usage is exceeded, new clients are not accepted by the Kernel. Valid CPU usage thresholds are expressed as percentages. The minimum value you can specify is "10"; the maximum value you can specify is "99".

The Kernel scalability settings are updated in the appropriate Kernel definition file. You must restart the Kernel in order for these Kernel settings to take effect.

# 47

## Maintaining Kernel Filters

---

### » To maintain the Kernel filter list:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 In tree-view, right-click on the name of the Kernel for which you want to specify the Kernel filter list and select the **Kernel Filters** command from the resulting drop-down menu.

The **Kernel Filters** panel appears in detail-view.

### Kernel Filters

ACCEPTED\_DBIDS.....

<not defined>

REJECTED\_DBIDS.....

<not defined>

ACCEPTED\_KERNELS.....

<not defined>

REJECTED\_KERNELS.....

<not defined>

ACCEPTED\_HOSTS.....

<not defined>

REJECTED\_HOSTS.....

<not defined>

ACCEPTED\_CLIENTS.....

<not defined>

REJECTED\_CLIENTS.....

<not defined>

USE\_LOCAL\_ADABASES.....

<not defined>

UNSOLICITED.....

YES

RELAY\_TRAFFIC.....

YES

OK

Cancel

Help

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

Parameter	Description
ACCEPTED_DBIDS	<p>Specify the database IDs for which service requests should be processed by this Kernel. 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 Kernel should process service requests to databases 4, 62, and any databases with numbers between 12 and 15 (inclusive). For more information, read .</p> <p>If no databases are listed in the <b>ACCEPTED_DBIDS</b> field, the Kernel will process all requests to all databases defined in the Adabas Directory Server, except those listed in the <b>REJECTED_DBIDS</b> field.</p>
REJECTED_DBIDS	<p>Specify the database IDs for which service requests should <i>not</i> be processed by this Kernel. 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 Kernel should <i>not</i> process service requests to databases 4, 62, and any databases with numbers between 12 and 15 (inclusive). For more information, read .</p> <p>If no databases are listed in the <b>REJECTED_DBIDS</b> field, the Kernel will process all requests to all databases defined in the Adabas Directory Server, unless a specific list is provided in the <b>ACCEPTED_DBIDS</b> field.</p>

Parameter	Description
ACCEPTED_KERNELS	<p>Specify the Kernel names for which service requests should be processed by this Kernel. If more than one Kernel name is needed, separate them with commas. For more information, read .</p> <p>If the <b>UNSOLICITED</b> advanced Kernel parameter is set to "YES", any Kernel can submit service requests to this Kernel, except Kernels listed in the <b>REJECTED_KERNELS</b> filter parameter on the Kernel filter list. If the <b>UNSOLICITED</b> advanced Kernel parameter is set to "NO", all unsolicited Kernel service requests are ignored, except for the Kernels listed in the <b>ACCEPTED_KERNELS</b> filter parameter on the Kernel filter list. For complete information about the Kernel filter list, read <i>Maintaining the Kernel Filter List</i>, elsewhere in this guide.</p>
REJECTED_KERNELS	<p>Specify the Kernel names for which service requests should <i>not</i> be processed by this Kernel. If more than one Kernel name is needed, separate them with commas. For more information, read .</p> <p>If the <b>UNSOLICITED</b> advanced Kernel parameter is set to "YES", any Kernel can submit service requests to this Kernel, except Kernels listed in the <b>REJECTED_KERNELS</b> filter parameter on the Kernel filter list. If the <b>UNSOLICITED</b> advanced Kernel parameter is set to "NO", all unsolicited Kernel service requests are ignored, except for the Kernels listed in the <b>ACCEPTED_KERNELS</b> filter parameter on the Kernel filter list. For complete information about the Kernel filter list, read <i>Maintaining the Kernel Filter List</i>, elsewhere in this guide.</p>
ACCEPTED_HOSTS	Specify the host machine names from and to which service requests should be processed by this Kernel. If more than host machine name is needed, separate them with commas. For more information, read .
REJECTED_HOSTS	Specify the host machine names from and to which service requests should <i>not</i> be processed by this Kernel. If more than host machine name is needed, separate them with commas. For more information, read .
ACCEPTED_CLIENTS	Specify the Entire Net-Work Client names from which service requests should be processed by this Kernel. If more than Entire Net-Work Client name is needed, separate them with commas. For more information, read .
REJECTED_CLIENTS	Specify the Entire Net-Work Client names from which service requests should <i>not</i> be processed by this Kernel. If more than Entire Net-Work Client name is needed, separate them with commas. For more information, read .
USE_LOCAL_ADABASES	Indicate whether local Adabas databases should be used for this Kernel. Valid values are "YES" and "NO"; the default is "YES". If you only wanted this Kernel to relay calls to other Kernels on other machines and ignore the databases on the local machine, you would set this parameter to "NO". This might be useful in a test situation.

Parameter	Description
UNSOLICITED	<p>Indicate whether or not this Kernel will process service requests from other Kernels it has not included in its Kernel filter list. Valid values are "YES" and "NO", with "YES" being the default.</p> <p>If "YES" is specified, any Kernel can submit service requests to this Kernel, except Kernels listed in the <b>REJECTED_KERNELS</b> filter parameter on the Kernel filter list. If "NO" is specified, all unsolicited Kernel service requests are ignored, except for the Kernels listed in the <b>ACCEPTED_KERNELS</b> filter parameter on the Kernel filter list. For complete information about the Kernel filter list, read <a href="#">Maintaining the Kernel Filter List</a>, elsewhere in this guide.</p>
RELAY_TRAFFIC	<p>Indicate whether this Kernel should relay requests to other Kernels in the network.</p> <p>If the value of the <b>RELAY_TRAFFIC</b> field is "YES", requests to other Kernels in the network are relayed. If <b>RELAY_TRAFFIC</b> is set to "NO", requests are not relayed. The default is "YES".</p> <p>For more information, read .</p>

The Kernel filters are updated in the appropriate Kernel definition file. You must restart the Kernel in order for these Kernel filter changes to take effect.



# 48

## Changing the Adabas Directory Server

---

While you can specify that different Directory Servers be used by an Entire Net-Work Server and by its Kernel definitions, this is not recommended. The ability to do this is useful for testing only, but when your network testing is complete, we recommend that the same Directory Server be used for both.

### ➤ To change the Directory Server for the Kernel:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

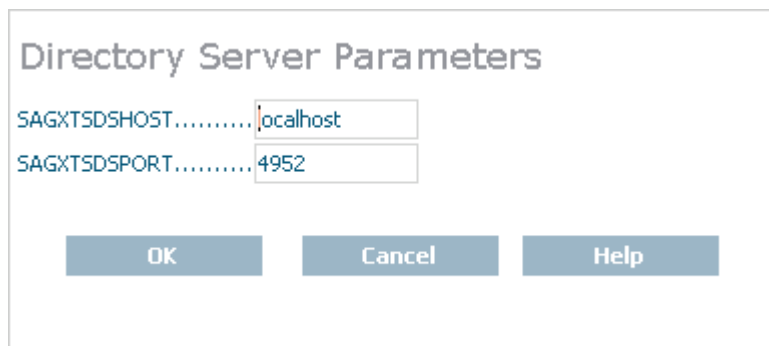
The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 In tree-view, right-click on the name of the Kernel for which you want to change the Directory Server and select **Set Directory Server** command from the resulting drop-down menu.

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



Directory Server Parameters

SAGXTSDSHOST..... localhost

SAGXTSDSPORT..... 4952

OK Cancel Help

- 7 Fill in the fields on this panel, as described in the following table:

Field	Description	Required?
SAGXTSDSHOST	The host name on which the Directory Server is installed.	Yes
SAGXTSDSPORT	The port number assigned the Directory Server. The default is 4952. If this field is set to zero (0) or left blank, the default will be used.	No

- 8 Click **OK**.

The Directory Server is changed for the Kernel. You must restart the Kernel in order for this Directory Server change to take effect.

# 49

## Maintaining Access Definitions

---

■ Listing Access Definitions .....	228
■ Adding Access Definitions .....	229
■ Modifying Access Definitions .....	233
■ Deleting Access Definition .....	234

Kernel access definitions specify how other Kernels and clients can access this Kernel definition. Ordinarily, these are specified when the Kernel is defined, but you can add additional Kernel access definitions later, as needed.

Kernel access definitions are stored as access entries in the Kernel configuration file, along with its other access and connection definitions as well as all of its parameters. The Kernel configuration file is located in the directory wherever you installed Entire Net-Work Server and has a name in the format *name.KERNEL*, where *name* is the name you assigned the Kernel definition when you added it.

This chapter describes how to maintain Kernel access definitions.

## Listing Access Definitions

---

### ➤ To review and list the access definitions of a Kernel:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 In tree-view, expand the name of the Kernel for which you want to review access definitions by clicking on the plus sign (+) to the left of its label.

The access and connection definition categories are listed beneath the Kernel name in tree-view.

- + E-Business Access
- + E-Business Client Access
- + Classic Net-Work Access
- + System Management Hub Access
- + E-Business connections
- + Classic Net-Work connections

The Kernel access definitions are listed under the category names **E-Business Access**, **E-Business Client Access** and **Classic Net-Work Access**.

Category	Description
E-Business Access	Lists the e-business (SSL and non-SSL) Kernel access definitions specified for the Kernel.
E-Business Client Access	Lists the e-business (SSL and non-SSL) client access definitions specified for the Kernel.
Classic Net-Work Access	Lists the classic access definitions specified for the Kernel.  Classic access provides access with an Entire Net-Work 2 for Open Systems node, an Entire Net-Work 3 for OpenVMS node or with an Entire Net-Work 6 (mainframe) node that does not have the Simple Connection Line Driver installed.
System Management Hub Access	Lists the System Management Hub (SMH) access definition, which uses a dynamic port number. Ordinarily, this should not be changed.

## Adding Access Definitions

### ➤ To add access definitions to a Kernel:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 In tree-view, right-click on the name of the Kernel to which you want to add access definitions and select the **Add Kernel Access** command from the resulting drop-down menu.

The **Add Kernel Access** panel appears in detail-view.

**Add Kernel Access**

☐ E-Business Access, Enter Port Value: 0 \*

Additional Parameters:

☐ E-Business SSL Access, Enter Port Value: 0 \*

Additional Parameters:

☐ E-Business Client Access, Enter Port Value: 0 \*

Additional Parameters:

☐ E-Business SSL Client Access, Enter Port Value: 0 \*

Additional Parameters:

☐ Classic Access, Enter port number: 7869 \*

Additional Parameters:

OK Cancel Help

- 7 Fill in the fields on this panel, as described in the following table:

Field	Description	Required?
E-Business Access parameters	<p>Select e-business access if you want to add an e-business Kernel access definition.</p> <ul style="list-style-type: none"> <li>■ Click in the <b>E-Business Access</b> checkbox (a checkmark should appear) to add a definition for e-business Kernel access.</li> <li>■ Specify the port number that should be used for this e-business Kernel access definition. A value of zero (0) indicates that Entire Net-Work should search for an available port and dynamically assign it. For more information about port numbers, read .</li> <li>■ Optionally, specify any Adabas Directory Server additional parameters needed for this e-business Kernel access definition. Additional parameters you specify are described in <i>Parameters</i>, in the chapter entitled <i>Directory Server Target Entries</i> of the <i>Software AG Directory Server Installation and Administration Guide</i>. Separate parameters in this field with ampersand (&amp;) symbols.</li> </ul>	If e-business server access is required, the <b>E-Business Access</b> checkbox must be checked. No other parameters are required.

Field	Description	Required?
	Note that not all Directory Server parameters apply to all access types.	
E-Business SSL Access parameters	<p>Select e-business SSL access if you to add an e-business Kernel access definition that uses Secure Sockets Layer (SSL).</p> <ul style="list-style-type: none"> <li>■ Click in the <b>E-Business SSL Access</b> checkbox (a checkmark should appear) to add a definition for e-business Kernel access via SSL.</li> <li>■ Specify the port number that should be used for this e-business Kernel SSL access definition. A value of zero (0) indicates that Entire Net-Work should search for an available port and dynamically assign it. For more information about port numbers, read .</li> <li>■ Optionally, specify any Adabas Directory Server additional parameters needed for this e-business Kernel access definition. Additional parameters you specify are described in <i>Parameters</i>, in the chapter entitled <i>Directory Server Target Entries</i> of the <i>Software AG Directory Server Installation and Administration Guide</i>. Separate parameters in this field with ampersand (&amp;) symbols. Note that not all Directory Server parameters apply to all access types.</li> </ul> <p>For assistance in setting up SSL support in Entire Net-Work, read <i>Using the SSL Toolkit</i> in the <i>Encryption for Entire Net-Work User Guide</i>, available from your Software AG support representative.</p> <p><b>Note:</b> 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.</p>	If e-business server SSL access is required, the <b>E-Business SSL Access</b> checkbox must be checked. No other parameters are required.
E-Business Client Access parameters	<p>Select e-business client access if you want to add an e-business client access definition.</p> <ul style="list-style-type: none"> <li>■ Click in the <b>E-Business Client Access</b> checkbox (a checkmark should appear) to add a definition for e-business client access.</li> <li>■ Specify the port number that should be used for this e-business client access definition. A value of zero (0) indicates that Entire Net-Work should search for an available port and dynamically assign it. For more information about port numbers, read .</li> <li>■ Optionally, specify any Adabas Directory Server additional parameters needed for this e-business Kernel access definition. Additional parameters you specify are described in <i>Parameters</i>, in the chapter entitled <i>Directory Server Target Entries</i> of the <i>Software AG Directory Server Installation and Administration Guide</i>. Separate parameters in this field with ampersand (&amp;) symbols.</li> </ul>	If e-business Entire Net-Work Client access is required, the <b>E-Business Client Access</b> checkbox must be checked. No other parameters are required.

Field	Description	Required?
	Note that not all Directory Server parameters apply to all access types.	
E-Business SSL Client Access parameters	<p>Select e-business client SSL access if you want to set up an e-business client access definition that uses Secure Sockets Layer (SSL).</p> <ul style="list-style-type: none"> <li>Click in the <b>E-Business SSL Client Access</b> checkbox (a checkmark should appear) to add a definition for e-business client access via SSL.</li> <li>Specify the port number that should be used for this e-business client SSL access definition. A value of zero (0) indicates that Entire Net-Work should search for an available port and dynamically assign it. For more information about port numbers, read .</li> <li>Optionally, specify any Adabas Directory Server additional parameters needed for this e-business Kernel access definition. Additional parameters you specify are described in <i>Parameters</i>, in the chapter entitled <i>Directory Server Target Entries</i> of the <i>Software AG Directory Server Installation and Administration Guide</i>. Separate parameters in this field with ampersand (&amp;) symbols. Note that not all Directory Server parameters apply to all access types.</li> </ul> <p>For assistance in setting up SSL support in Entire Net-Work, read <i>Using the SSL Toolkit</i> in the <i>Encryption for Entire Net-Work User Guide</i>, available from your Software AG support representative.</p> <p><b>Note:</b> 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.</p>	If e-business Entire Net-Work Client SSL access is required, the <b>E-Business SSL Client Access</b> checkbox must be checked. No other parameters are required.
Classic Access parameters	<p>Select classic access if you want to add an access definition for classic Entire Net-Work nodes.</p> <p>Classic access provides access with an Entire Net-Work 2 for open systems node, an Entire Net-Work 3 for OpenVMS node or with an Entire Net-Work 6 (mainframe) node that does not have the Simple Connection Line Driver installed.</p> <p>The classic access parameters include parameters that indicate whether this Kernel supports communication with access to Entire Net-Work Version 2 (classic) systems and, if so, the port number, node ID, and additional parameters that should be used for classic Entire Net-Work access.</p> <ul style="list-style-type: none"> <li>Click in the <b>Classic Access</b> checkbox (a checkmark should appear) to add a definition for a classic Entire Net-Work node.</li> </ul>	If classic Entire Net-Work access is required, the <b>Classic Access</b> checkbox must be checked and a port number and node ID must be specified. No additional parameters are required.



Field	Description	Required?
	<ul style="list-style-type: none"> <li>■ Specify the port number that should be used for this classic Entire Net-Work access definition. The default port number for this type of access is 7869. For more information about port numbers, read .</li> <li>■ Specify the ID of the classic Entire Net-Work node for this classic access definition.</li> <li>■ Optionally, specify any Adabas Directory Server additional parameters needed for this e-business Kernel access definition. Additional parameters you specify are described in <i>Parameters</i>, in the chapter entitled <i>Directory Server Target Entries</i> of the <i>Software AG Directory Server Installation and Administration Guide</i>. Separate parameters in this field with ampersand (&amp;) symbols. Note that not all Directory Server parameters apply to all access types.</li> </ul>	

- 8 Click **OK**.

The Kernel access definitions are added to the Kernel configuration file. These definitions only become available to the Kernel after it is restarted.

## Modifying Access Definitions

### ➤ To modify access definitions of a Kernel:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 Expand the name of the Kernel containing the access definition you want to modify by clicking on the plus sign (+) to the left of its label.

The access and connection definition categories are listed beneath the Kernel name in tree-view.

The access definitions are listed under the category names **E-Business Access**, **E-Business Client Access**, and **Classic Net-Work Access**.

- 7 Expand the category name containing the access definition you want to modify.

The access definitions in that category are listed in tree-view.

- 8 Right-click on the access definition you want to modify and select **Modify Entry** from the resulting drop-down menu.

A modification panel appears in detail-view, allowing you to modify the entry. For complete information about access definition parameters, read [Adding Access Definitions](#), elsewhere in this section

- 9 When all updates have been made, click **OK**.

The Kernel access definitions are modified to the Kernel configuration file. Updates to the definitions only become available to the Kernel after it is restarted.

## Deleting Access Definition

---

### ➤ To delete an access definition of a Kernel:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 Expand the name of the Kernel containing the access definition you want to delete by clicking on the plus sign (+) to the left of its label.

The access and connection definition categories are listed beneath the Kernel name in tree-view.

The access definitions are listed under the category names **E-Business Access**, **E-Business Client Access**, and **Classic Net-Work Access**.

- 7 Expand the category name containing the access definition you want to delete.

The access definitions in that category are listed in tree-view.

- 8 Right-click on the access definition you want to delete and select **Delete Entry** from the resulting drop-down menu.

A panel appears in detail-view verifying that you want to delete the access definition (entry) from the Kernel definition.

- 9 Click **OK** to confirm the deletion.

The Kernel access definition is deleted from the Kernel configuration file. Updates to the definitions only become available to the Kernel after it is restarted.



# 50

## Reviewing Kernel Access Status

---

➤ **To review the status of a Kernel's access definitions:**

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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





- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.

- 5 In tree-view, right-click on the name of the Kernel for which you want to review access definition status, and select **Access Status**.

The status of the Kernel's access definitions appears in detail-view. For example:

MYKERNEL on TEST-PC

	Name	Protocol	Port	Status
	Client Access	TCPIP	49162	Running
	E-Business Access	TCPIP	49161	Running
	SMH Server	TCPIP	49160	Running

The following information about each type of access definition is listed.

Field	Description
Name	The type of access definition.
Protocol	The protocol used for access attempts defined by the access definition.
Port	The port number used for the access definition.
Status	The status of the access definition.

# 51

## Maintaining Connection Definitions

---

■ Listing Connection Definitions .....	240
■ Adding Connection Definitions .....	241
■ Modifying Connection Entries .....	247
■ Deleting Connection Entries .....	248

Kernel connection definitions specify connection information for connections to other e-business Kernels or to classic Entire Net-Work installations. Classic connections are connections with an Entire Net-Work 2 for open systems node, an Entire Net-Work 3 for OpenVMS node or with an Entire Net-Work 6 (mainframe) node that does not have the Simple Connection Line Driver installed. You can only add e-business connection definitions for Entire Net-Work 7 Kernels or for Entire Net-Work 6 nodes with the Simple Connection Line Driver installed.

Each connection definition adds a connection entry to the Kernel configuration file. The Kernel configuration file is stored in the directory wherever you installed Entire Net-Work Server and has a name in the format *name.KERNEL*, where *name* is the name you assigned the Kernel definition when you added it.

This chapter describes how to maintain Kernel connection definitions.

## Listing Connection Definitions

---

### ➤ To review and list the connection definitions of a Kernel:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.



- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 In tree-view, expand the name of the Kernel for which you want to review connection definitions by clicking on the plus sign (+) to the left of its label.

The access and connection definition categories are listed beneath the Kernel name in tree-view.



- +  E-Business Access
- +  E-Business Client Access
- +  Classic Net-Work Access
- +  System Management Hub Access
- +  E-Business connections
- +  Classic Net-Work connections

The Kernel connection definitions are listed under the category names **E-Business connections** and **Classic Net-Work connections**.

Category	Description
E-Business connections	Lists the e-business (SSL and non-SSL) connection definitions specified for the Kernel.
Classic Net-Work connections	<p>Lists the classic connection definitions specified for the Kernel.</p> <p>Classic connections provides connection to an Entire Net-Work 2 for open systems node, an Entire Net-Work 3 for OpenVMS node or with an Entire Net-Work 6 (mainframe) node that does not have the Simple Connection Line Driver installed.</p>

## Adding Connection Definitions

You can add connection definitions dynamically (immediately and for only this execution of the Kernel) or permanently (for future executions of the Kernel). A dynamic connection occurs immediately, but if the Kernel is restarted, the connection is lost. A permanent connection occurs in the Kernel definition and takes effect only when the Kernel is restarted.

This section covers the following topics:

- [Permanently Adding a Connection Definition](#)
- [Dynamically Adding a Connection](#)

### Permanently Adding a Connection Definition

➤ To permanently add a connection definition for the Kernel:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 In tree-view, right-click on the name of the Kernel to which you want to add a connection and select the **Add Connection** command from the resulting drop-down menu.

The **Add Connection** panel appears in detail-view.

- 7 Fill in the fields on this panel, as described in the following table:

Field	Description	Required?
Entire Net-Work Kernel Name	The name of the Kernel to which you want to connect.	Yes
Protocol Type	<p>The type of connection you want to make</p> <p>■ E-Business: Select this protocol type if you want to make an e-business connection available to the Kernel. You can only add e-business</p>	Yes

Field	Description	Required?
	<p>connections for Entire Net-Work 7 Kernels or for Entire Net-Work 6 nodes with the Simple Connection Line Driver installed.</p> <ul style="list-style-type: none"> <li>■ E-Business SSL: Select this protocol type if you want to make an e-business connection available to the Kernel using Secure Sockets Layer (SSL). You can only add e-business connections of any kind for Entire Net-Work 7 Kernels or for Entire Net-Work 6 nodes with the Simple Connection Line Driver installed.</li> </ul> <p>For assistance in setting up SSL support in Entire Net-Work, read <i>Using the SSL Toolkit</i> in the <i>Encryption for Entire Net-Work User Guide</i>, available from your Software AG support representative.</p> <p><b>Note:</b> 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.</p> <ul style="list-style-type: none"> <li>■ Classic: Select this protocol type if you want to make a classic connection available to the Kernel for an Entire Net-Work 2 for open systems node, an Entire Net-Work 3 for OpenVMS node or with an Entire Net-Work 6 (mainframe) node that does not have the Simple Connection Line Driver installed.</li> </ul>	
Host Address	The name of the host machine on which the Kernel to which you are connecting is installed.	Yes
Port Value	The port number of the Kernel to which you are connecting.	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
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
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
Additional Parameters	Optionally, specify any Adabas Directory Server additional parameters needed for this e-business Kernel access definition. Additional parameters you specify are described in <i>Parameters</i> , in the chapter entitled <i>Directory Server Target Entries</i> of the <i>Software AG Directory Server Installation and Administration Guide</i> . Separate parameters in this field with ampersand (&) symbols. Note that not all Directory Server parameters apply to all access types.	No
Manual Connection	Select this checkbox if you always want to manually connect to this connection.	No

- 8 Click **OK**.

The connection definition is added to the Adabas Directory Server for this Kernel. The connection definition is only available to the Kernel after the Kernel is restarted.

## Dynamically Adding a Connection

### ➤ To dynamically add a connection for the Kernel:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of Kernels that have been started appears.

- 5 In tree-view, right-click on the name of the Kernel to which you want to add a connection and select the **Add Connection Online** command from the resulting drop-down menu.

The **Add Connection Online** panel appears in detail-view.

### Add Connection Online

Enter Entire Net-Work Kernel Name:

Protocol Type

☒ E-Business  
☐ E-Business SSL  
☐ Classic

Enter Host Address:

Enter Port Value:

Reconnect ☐ Retry Count:  Retry Interval:

Enter Additional Parameters:

☐ Manual Connection

- 6 Fill in the fields on this panel, as described in the following table:

Field	Description	Required?
Entire Net-Work Kernel Name	The name of the Kernel to which you want to connect.	Yes
Protocol Type	<p>The type of connection you want to make</p> <ul style="list-style-type: none"> <li>■ E-Business: Select this protocol type if you want to make an e-business connection available to the Kernel. You can only add e-business connections for Entire Net-Work 7 Kernels or for Entire Net-Work 6 nodes with the Simple Connection Line Driver installed.</li> <li>■ E-Business SSL: Select this protocol type if you want to make an e-business connection available to the Kernel using Secure Sockets Layer (SSL). You can only add e-business connections of any kind for Entire Net-Work 7 Kernels or for Entire Net-Work 6 nodes with the Simple Connection Line Driver installed.</li> </ul> <p>For assistance in setting up SSL support in Entire Net-Work, read <i>Using the SSL Toolkit</i> in the <i>Encryption for Entire Net-Work User Guide</i>, available from your Software AG support representative.</p> <p><b>Note:</b> 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.</p>	Yes

Field	Description	Required?
	<ul style="list-style-type: none"> <li>Classic: Select this protocol type if you want to make a classic connection available to the Kernel for an Entire Net-Work 2 for open systems node, an Entire Net-Work 3 for OpenVMS node or with an Entire Net-Work 6 (mainframe) node that does not have the Simple Connection Line Driver installed.</li> </ul>	
Host Address	The name of the host machine on which the Kernel to which you are connecting is installed.	Yes
Port Value	The port number of the Kernel to which you are connecting.	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
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
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
Additional Parameters	Optionally, specify any Adabas Directory Server additional parameters needed for this e-business Kernel access definition. Additional parameters you specify are described in <i>Parameters</i> , in the chapter entitled <i>Directory Server Target Entries</i> of the <i>Software AG Directory Server Installation and Administration Guide</i> . Separate parameters in this field with ampersand (&) symbols. Note that not all Directory Server parameters apply to all access types.	No
Manual Connection	Select this checkbox if you always want to manually connect to this connection.	No

7 Click **OK**.

The connection definition is temporarily added for this Kernel. Once the Kernel definition is restarted, this temporary connection definition will no longer be available; you will have to define it again if you need it.

## Modifying Connection Entries

### ➤ To modify connection definitions of a Kernel:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 Expand the name of the Kernel containing the connection definition you want to modify by clicking on the plus sign (+) to the left of its label.

The access and connection definition categories are listed beneath the Kernel name in tree-view.

The Kernel connection definitions are listed under the category names **E-Business connections** and **Classic Net-Work connections**.

- 7 Expand the category name containing the connection definition you want to modify.

The connection definitions in that category are listed in tree-view.

- 8 Right-click on the connection definition you want to modify and select **Modify Entry** from the resulting drop-down menu.

A modification panel appears in detail-view, allowing you to modify the entry. For complete information about connection definition parameters, read [Adding Connection Definitions](#), elsewhere in this section

- 9 When all updates have been made, click **OK**.

The Kernel connection definitions are modified to the Kernel configuration file. Updates to the definitions only become available to the Kernel after it is restarted.

## Deleting Connection Entries

---

➤ **To delete a connection definition of a Kernel:**

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 Expand the name of the Kernel containing the connection definition you want to delete by clicking on the plus sign (+) to the left of its label.

The access and connection definition categories are listed beneath the Kernel name in tree-view.

The Kernel connection definitions are listed under the category names **E-Business connections** and **Classic Net-Work connections**.

- 7 Expand the category name containing the connection definition you want to delete.

The connection definitions in that category are listed in tree-view.

- 8 Right-click on the connection definition you want to delete and select **Delete Entry** from the resulting drop-down menu.

A panel appears in detail-view verifying that you want to delete the connection definition (entry) from the Kernel definition.

- 9 Click **OK** to confirm the deletion.

The Kernel connection definition is deleted from the Kernel configuration file. Updates to the definitions only become available to the Kernel after it is restarted.



## 52 Reviewing Kernel Outgoing Connection Status

---

➤ To review the status of a Kernel's outgoing connection definitions:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.

- 5 In tree-view, right-click on the name of the Kernel for which you want to review the outgoing connection status, and select **Outgoing Connections Status**.

The status of the Kernel's outgoing connection definitions appears in detail-view. For example:

Target	Type	Protocol	Port	A/M	Status
↓ MYKERN2	E-business	TCPIP	49158	Auto	Connection defined

The following information about each outgoing connection is listed.

Field	Description
Target	The name of the target Kernel definition.
Type	The type of connection definition.
Protocol	The protocol used for connection attempts defined by the connection definition.
Port	The port number used for the connection.
A/M	Whether the connection was automatic or manual.
Status	The status of the connect.

# 53

## Reviewing Kernel Statistics

---

### » To review the statistics for a Kernel:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.

- 5 In tree-view, right-click on the name of the Kernel for which you want to review statistics, and select **Statistics**.

Statistics for the Kernel appears in detail-view. For example:

**MYKERNEL on TEST-PC**

<b>Statistics for Kernel MIHAI75</b>	<b>Count</b>
Nodes	2
Connections	0
Clients	0
Relay Clients	0
Databases	1
Adabas Contexts	0
Adabas Calls	11101
RDA Messages	0
Ebz Messages	0
Total Requests	0
Total Replies	0
Bytes Received	0
Bytes Sent	0
Relayed Messages	0
Admin Messages	0
Errors	0

# 54

## Dynamically Collecting Detailed Statistics

---

Collecting detailed statistics for a Kernel can provide useful data in resolving problems. However, we do not recommend that you collect detailed statistics all the time as the performance of your system may be affected by their collection.

» **To dynamically turn on the collection of detailed statistics for a Kernel:**

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

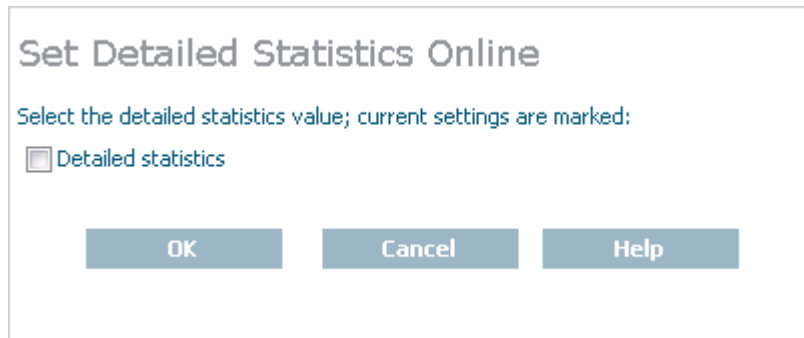
The Entire Net-Work Server administration area of the System Management Hub becomes available to you.

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.

- 5 In tree-view, right-click on the name of the Kernel for which you want to set detailed statistics, and select **Set Detailed Statistics On Line**.

The **Set Detailed Statistics Online** panel appears in detail-view. For example:



- 6 Click **OK** to turn on the collection of detailed statistics.

Detailed statistic collection for the Kernel is started.

# 55

## Generate a Kernel Configuration Dump

---

You can request that a Kernel configuration dump be written to the log file. This dump information includes the servers, database IDs, connections, clients, host machines, and Adabas contexts associated with the Kernel.

» **To generate a Kernel configuration dump in the log file:**

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

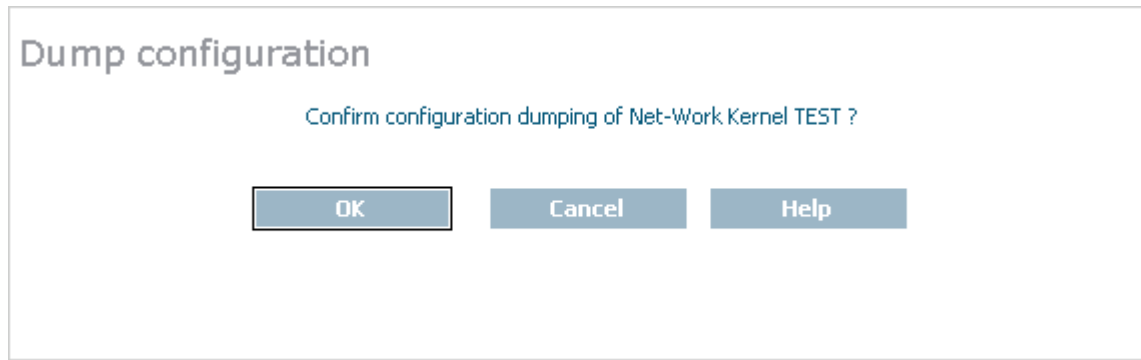
The Entire Net-Work Server administration area of the System Management Hub becomes available to you.

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.

- 5 In tree-view, right-click on the name of the Kernel for which you want to generate a kernel configuration dump, and select **Dump Configuration**.

The **Dump Configuration** panel appears in detail-view. For example:



- 6 Click **OK** to dump the kernel configuration.

The dump is generated



## 56 Checking Kernel Databases

---

You can check the databases managed by a Kernel. Checking the databases causes Entire Net-Work to search for any Adabas databases that were started recently and to refresh its internal table and corresponding SMH information. This is useful, for example, when you want to obtain the latest status of the databases that a specific Kernel manages.

### ➤ To check the databases managed by a Kernel:

Make sure you have accessed the System Management Hub and that the Kernel is started. For complete information about starting Kernels, read [Starting a Kernel](#), elsewhere in this guide.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.



**Note:** If the Kernel you need is not listed, it is not started. You must start the Kernel before you can proceed with these instructions. Read [Starting a Kernel](#), elsewhere in this guide, for more information.

- 5 Right-click on **Databases** in tree-view and select **Check Databases** from the resulting drop-down menu.

A **Check Databases** panel appears in detail-view.

### Check Databases

Confirm the checking of Net-Work Kernel MYKERNEL databases?

OK

Cancel

Help

- 6 Click **OK** to check the Kernel databases.

The databases are checked and the list and status of the databases is refreshed.

# 57

## Pinging Databases and Classic Nodes

---

■ Pinging Databases .....	260
■ Pinging Classic Nodes .....	261

You can ping the databases managed by a Kernel and any classic nodes specified in classic connection definitions for the Kernel. Pinging allows you to determine if the database or classic nodes are active.



**Note:** Classic connections are connections to an Entire Net-Work 2 for open systems node, an Entire Net-Work 3 for OpenVMS node or with an Entire Net-Work 6 (mainframe) node that does not have the Simple Connection Line Driver installed.

## Pinging Databases

---

### ➤ To ping a database managed by a Kernel:

Make sure you have accessed the System Management Hub and that the Kernel is started. For complete information about starting Kernels, read [Starting a Kernel](#), elsewhere in this guide.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.



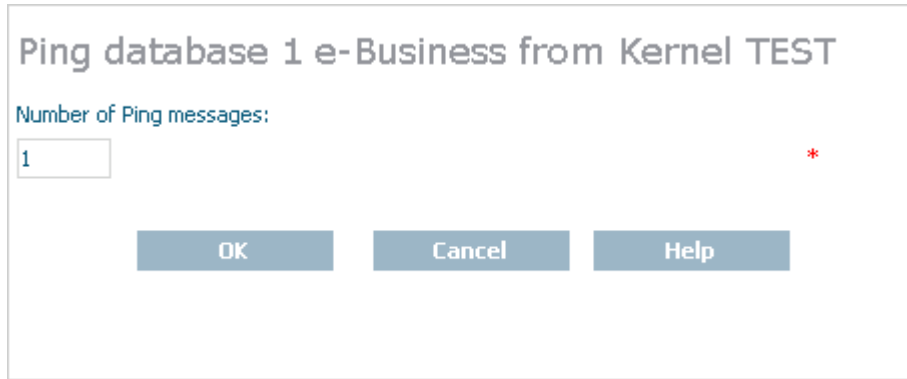
**Note:** If the Kernel you need is not listed, it is not started. You must start the Kernel before you can proceed with these instructions. Read [Starting a Kernel](#), elsewhere in this guide, for more information.

- 5 Expand **Databases** in tree-view, by clicking on the plus sign (+) to the left of its label.

The databases managed by the Kernel are listed in tree-view.

- 6 Right-click on the database you want to ping and select **Ping** from the resulting drop-down menu.

A Ping panel appears in detail-view.



Ping database 1 e-Business from Kernel TEST

Number of Ping messages:

1 \*

OK Cancel Help

- 7 Specify the number of ping messages that should be sent from the Kernel to the database in the **Number of Ping messages** box.
- 8 Click **OK** to start pinging.

The results of the ping attempts appears in detail-view, indicating whether or not the database is active.

## Pinging Classic Nodes

### ➤ To ping a classic node managed by a Kernel:

Make sure you have accessed the System Management Hub and that the Kernel is started. For complete information about starting Kernels, read [Starting a Kernel](#), elsewhere in this guide.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.



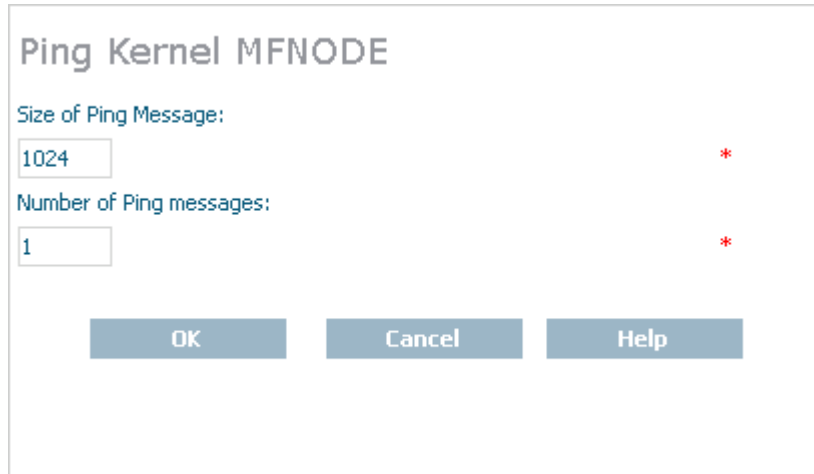
**Note:** If the Kernel you need is not listed, it is not started. You must start the Kernel before you can proceed with these instructions. Read [Starting a Kernel](#), elsewhere in this guide, for more information.

- 5 Expand **Connections** in tree-view, by clicking on the plus sign (+) to the left of its label.

The connection definitions for the Kernel are listed in **Outgoing** and **Incoming** categories in tree-view.

- 6 Expand the **Outgoing** category to see the list of outgoing connection definitions. Connections to classic nodes are always outgoing from Entire Net-Work Server nodes.
- 7 Right-click the classic connection for the classic node you want to ping and select **Ping** from the resulting drop-down menu.

A Ping panel appears in detail-view.



Ping Kernel MFNODE

Size of Ping Message:  
1024 \*

Number of Ping messages:  
1 \*

OK Cancel Help

- 8 Specify the size and number of ping messages that should be sent from the Kernel to the classic node in the **Size of Ping Message** and **Number of Ping messages** boxes.
- 9 Click **OK** to start pinging.

The results of the ping attempts appears in detail-view, indicating whether or not the classic node is active.

# 58

## Dynamically Connecting and Disconnecting a Connection

---

■ Dynamically Connecting .....	264
■ Dynamically Disconnecting .....	265

You can dynamically connect to or disconnect from any node for which a Kernel connection definition has been specified.

## Dynamically Connecting

---

### » To dynamically connect to a node specified in a connection definition of a Kernel:

Make sure you have accessed the System Management Hub and that the Kernel is started. For complete information about starting Kernels, read [Starting a Kernel](#), elsewhere in this guide.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.



**Note:** If the Kernel you need is not listed, it is not started. You must start the Kernel before you can proceed with these instructions. Read [Starting a Kernel](#), elsewhere in this guide, for more information.

- 5 Expand **Connections** in tree-view, by clicking on the plus sign (+) to the left of its label.

The connection definitions for the Kernel are listed in **Outgoing** and **Incoming** categories in tree-view.

- 6 Locate the connection to which you wish to connect in either category.
- 7 Right-click the connection and select **Connect** from the resulting drop-down menu.

A panel appears in detail-view verifying that you want to make the connection.

- 8 Click **OK** to make the connection.

The results of the connection attempt appear in detail-view, indicating whether or not the connection was successful.



## Dynamically Disconnecting

### ➤ To dynamically disconnect to a node specified in a connection definition of a Kernel:

Make sure you have accessed the System Management Hub and that the Kernel is started. For complete information about starting Kernels, read [Starting a Kernel](#), elsewhere in this guide.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.



**Note:** If the Kernel you need is not listed, it is not started. You must start the Kernel before you can proceed with these instructions. Read [Starting a Kernel](#), elsewhere in this guide, for more information.

- 5 Expand **Connections** in tree-view, by clicking on the plus sign (+) to the left of its label.

The connection definitions for the Kernel are listed in **Outgoing** and **Incoming** categories in tree-view.

- 6 Locate the connection to which you wish to disconnect in either category.
- 7 Right-click the connection and select **Disconnect** from the resulting drop-down menu.

A panel appears in detail-view verifying that you want to disconnect from the node.

- 8 Click **OK** to process the disconnection request.

The results of the disconnection attempt appear in detail-view, indicating whether or not the disconnection was successful.



# 59      Dynamically Managing Kernel Clients and Adabas

## Contexts

---

▪ Listing Kernel Clients and Adabas Contexts .....	268
▪ Viewing Kernel Client and Adabas Context Statistics .....	269
▪ Dynamically Disconnecting Kernel Clients .....	270
▪ Dynamically Deleting Adabas Contexts .....	271

Direct clients are clients that process Adabas calls on the current Kernel. Relay clients are clients that relay to other Kernels to process Adabas calls on those Kernels. Using Entire Net-Work you can dynamically manage the direct and relay clients of a Kernel. You can also view statistical information about clients and contexts.

Adabas contexts are memory tokens that associate clients and Adabas databases and are used for Adabas session identification and statistics purposes.

This chapter covers the following topics:

## Listing Kernel Clients and Adabas Contexts

---

### ➤ To dynamically list the clients and Adabas contexts of a Kernel:

Make sure you have accessed the System Management Hub and that the Kernel is started. For complete information about starting Kernels, read [Starting a Kernel](#), elsewhere in this guide.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.



**Note:** If the Kernel you need is not listed, it is not started. You must start the Kernel before you can proceed with these instructions. Read [Starting a Kernel](#), elsewhere in this guide, for more information.

- 5 Expand **Clients** in tree-view, by clicking on the plus sign (+) to the left of its label.

The client and Adabas context definitions for the Kernel are listed in categories in tree-view. Three categories are listed: **Direct Clients**, **Adabas Contexts**, and **Relay Clients**.

- 6 Expand the appropriate category (**Direct Clients**, **Adabas Contexts**, or **Relay Clients**) in tree-view, by clicking on the plus sign (+) to the left of its label.

The client or Adabas context definitions for the category you selected are listed in tree-view.

## Viewing Kernel Client and Adabas Context Statistics

To activate this feature, set the `STATISTICS_DETAILS` parameter to "YES" on the [Kernel Advanced Parameters](#) screen.

### » To dynamically view statistics for a Kernel client or Adabas context:

Make sure you have accessed the System Management Hub and that the Kernel is started. For complete information about starting Kernels, read [Starting a Kernel](#), elsewhere in this guide.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.



**Note:** If the Kernel you need is not listed, it is not started. You must start the Kernel before you can proceed with these instructions. Read [Starting a Kernel](#), elsewhere in this guide, for more information.

- 5 Expand **Clients** in tree-view, by clicking on the plus sign (+) to the left of its label.

The client and Adabas context definitions for the Kernel are listed in categories in tree-view. Three categories are listed: **Direct Clients**, **Adabas Contexts**, and **Relay Clients**.

- **Direct Clients:** Direct clients are clients directly connected to this node. These clients are included in Entire Net-Work counts for currently active clients and are the clients covered by the license agreement (so they *are* counted against the maximum number of clients that can be used by this Kernel).
- **Adabas Contexts:** Adabas contexts are memory tokens that associate clients and Adabas databases and are used for Adabas session identification and statistics purposes.
- **Relay Clients:** Relay clients are clients connected through another node. These clients are included in Entire Net-Work counts for currently active clients, but are *not* counted against the maximum number of clients that can be used by this Kernel.

- 6 Expand the appropriate category (**Direct Clients**, **Adabas Contexts**, or **Relay Clients**) in tree-view, by clicking on the plus sign (+) to the left of its label.

The client or Adabas context definitions for the category you selected are listed in tree-view.

- 7 Click on the client or Adabas context name whose statistics you wish to view.

A panel appears in detail-view listing statistics about the client or Adabas context.

## Dynamically Disconnecting Kernel Clients

---

### ➤ To dynamically disconnect a direct or relay client of a Kernel:

Make sure you have accessed the System Management Hub and that the Kernel is started. For complete information about starting Kernels, read [Starting a Kernel](#), elsewhere in this guide.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.



**Note:** If the Kernel you need is not listed, it is not started. You must start the Kernel before you can proceed with these instructions. Read [Starting a Kernel](#), elsewhere in this guide, for more information.

- 5 Expand **Clients** in tree-view, by clicking on the plus sign (+) to the left of its label.

The client and Adabas context definitions for the Kernel are listed in categories in tree-view. Three categories are listed: **Direct Clients**, **Adabas Contexts**, and **Relay Clients**.

- 6 Expand either the **Direct Clients** or **Relay Clients** category in tree-view, by clicking on the plus sign (+) to the left of its label.

The client definitions for the category you selected are listed in tree-view.

- 7 Right-click on the name of the client you wish to disconnect and select **Disconnect** from the resulting drop-down menu.

A panel appears in detail-view requesting confirmation of the disconnect request.

- 8 Click **OK** to disconnect the selected client.

The client is disconnected.

## Dynamically Deleting Adabas Contexts

### ➤ To dynamically delete an Adabas context of a Kernel:

Make sure you have accessed the System Management Hub and that the Kernel is started. For complete information about starting Kernels, read [Starting a Kernel](#), elsewhere in this guide.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.



**Note:** If the Kernel you need is not listed, it is not started. You must start the Kernel before you can proceed with these instructions. Read [Starting a Kernel](#), elsewhere in this guide, for more information.

- 5 Expand **Clients** in tree-view, by clicking on the plus sign (+) to the left of its label.

The client and Adabas context definitions for the Kernel are listed in categories in tree-view. Three categories are listed: **Direct Clients**, **Adabas Contexts**, and **Relay Clients**.

- 6 Expand **Adabas Contexts** category in tree-view, by clicking on the plus sign (+) to the left of its label.

The Adabas context definitions for the Kernel are listed in tree-view.

- 7 Right-click on the name of the Adabas context you wish to delete and select **Delete** from the resulting drop-down menu.

A panel appears in detail-view requesting confirmation of the deletion request.

- 8 Click **OK** to delete the selected Adabas context.

The Adabas context is deleted.





# 60

## Dynamically Managing Kernel Client Hosts

---

■ Listing Client Hosts .....	274
■ Viewing Client Host Statistics .....	274
■ Dynamically Disconnecting All Clients and Contexts of a Client Host .....	275

Client hosts are the host machines from which client requests are sent to the Kernel. Entire Net-Work lets you dynamically manage your Kernel's interaction with client hosts.

This chapter covers the following topics:

## Listing Client Hosts

---

### ➤ To dynamically list the client hosts of a Kernel:

Make sure you have accessed the System Management Hub and that the Kernel is started. For complete information about starting Kernels, read [Starting a Kernel](#), elsewhere in this guide.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.



**Note:** If the Kernel you need is not listed, it is not started. You must start the Kernel before you can proceed with these instructions. Read [Starting a Kernel](#), elsewhere in this guide, for more information.

- 5 Expand **Client Hosts** in tree-view, by clicking on the plus sign (+) to the left of its label.

The client host definitions for the Kernel are listed in tree-view.

## Viewing Client Host Statistics

---

### ➤ To dynamically view statistics for a Kernel client host:

Make sure you have accessed the System Management Hub and that the Kernel is started. For complete information about starting Kernels, read [Starting a Kernel](#), elsewhere in this guide.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.



**Note:** If the Kernel you need is not listed, it is not started. You must start the Kernel before you can proceed with these instructions. Read [Starting a Kernel](#), elsewhere in this guide, for more information.

- 5 Expand **Client Hosts** in tree-view, by clicking on the plus sign (+) to the left of its label.

The client host definitions for the Kernel are listed in tree-view.

- 6 Click on the client host name whose statistics you wish to view.

A panel appears in detail-view listing statistics about the client host.

## Dynamically Disconnecting All Clients and Contexts of a Client Host

### » To dynamically disconnect all the clients and context of a Kernel client host:

Make sure you have accessed the System Management Hub and that the Kernel is started. For complete information about starting Kernels, read [Starting a Kernel](#), elsewhere in this guide.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.



**Note:** If the Kernel you need is not listed, it is not started. You must start the Kernel before you can proceed with these instructions. Read [Starting a Kernel](#), elsewhere in this guide, for more information.

- 5 Expand **Client Hosts** in tree-view, by clicking on the plus sign (+) to the left of its label.

The client host definitions for the Kernel are listed in tree-view.

- 6 Right-click on the name of the client host whose clients and Adabas contexts you wish to disconnect and select **Disconnect all clients** from the resulting drop-down menu.

A panel appears in detail-view requesting confirmation of the disconnect request.

- 7 Click **OK** to disconnect all of the clients on the selected client host.

The clients and Adabas contexts are disconnected.

# 61

## Reviewing Kernel Status

---

You can review the status of a Kernel service and of a Kernel. This chapter describes both methods.

### ➤ To view the status of a Kernel service:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Expand **Entire Net-Work Server** in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of servers that have been defined appears.

- 5 Expand an Entire Net-Work name in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of Kernels that have been defined for that server appears.

- 6 In tree-view, right-click on the name of the Kernel whose status you want to view and select the **Status** command from the resulting drop-down menu.

The status of the Kernel service appears in detail-view.

### ➤ To view the status of a Kernel:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server is installed.

- Expand the tree-view frame for the managed host by clicking on the plus sign (+) to the left of its name.
- Expand **Entire Net-Work Server** in the tree-view under the managed host.

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

- Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of started Kernels appears.



**Note:** If the Kernel you need is not listed, it is not started. You must start the Kernel before you can proceed with these instructions. Read [Starting a Kernel](#), elsewhere in this guide, for more information.

- In tree-view, click on the name of the Kernel whose status you want to view.

The status of the Kernel appears in detail-view.

MYKERNEL on TEST-PC										
Kernel	NodeId	Version	Tcpip	Active Clients	Max Clients	Age	Total CPU	CPU Share	Current CPU	
MIHA175	3399	7.5.0	Undefined	0	1000	42h:32m:15s	0h:0m:19s	0.1%	0.0%	

This status also provides the following statistical information:

- The number of clients currently using the Kernel (**Active Clients**) includes direct clients, relay clients, and Adabas context clients.
- The maximum number of clients allowed to use the Kernel (**Max Clients**) is based on the license provided by Software AG when Entire Net-Work was purchased. This count includes direct clients only; relay clients and Adabas context clients are not included in this count.
- The length of time the Kernel has been running (**Age**) is shown.
- The total CPU used (Total CPU) is provided.
- The percentage of CPU (**CPU Share**) the Kernel has used since it started is listed.
- The Kernel's current CPU consumption (**Current CPU**) is shown.

# 62

## Managing Kernel Log Files

---

■ Viewing the Kernel Log File .....	280
■ Starting a New Kernel Log File .....	280
■ Specifying the Kernel Log File Location .....	282

You can view the current Kernel log file or start a new one.

## Viewing the Kernel Log File

---

➤ To view the log file for a Kernel:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of Kernels that have been started appears.

- 5 In tree-view, right-click on the name of the Kernel whose log file you want to view and select **View Log File** command from the resulting drop-down menu.

The console log for the Kernel appears in detail-view.

## Starting a New Kernel Log File

---

You can close the current log file for an Entire Net-Work Kernel and start a new one at any time. When you do this, the current log file (with a name in the format *kernel-name.log*) is saved under a new name and is cleared of all log entries. The name of the renamed log file is assigned in the format *kkknnnnn.log*, where *kkk* is the first three characters of the Kernel name and *nnnnn* is an incremental number determined by the number of the most recent log file that was renamed and saved. The log file with the name that includes the highest number is the most recently saved log file.

By default, Kernel log 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 Server\
- In Windows 7 environments: ProgramData\Software AG\Entire Net-Work Server\logsvc75
- In UNIX environments: \$SAG\wcp\.



If you would like to specify the location in which Kernel log files should be stored, read [Specifying the Kernel Log File Location](#), elsewhere in this section.



**Note:** The LOGSIZE parameter for the Kernel defines the number of megabytes (MB) to which a Kernel log file can grow before it is automatically closed and a new log file is started. For more information on setting this parameter, read [Setting Advanced Parameters](#), elsewhere in this guide.

» **To start a new log file for the Kernel:**

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

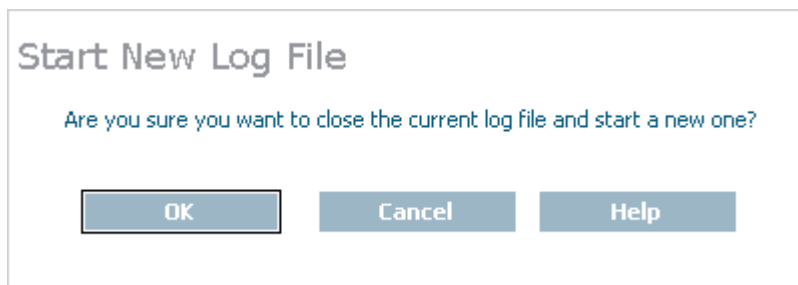
The Entire Net-Work Server administration area of the System Management Hub becomes available to you.

- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of Kernels that have been started appears.

- 5 In tree-view, right-click on the name of the Kernel for which you want to start a new log file and select **New Log File** command from the resulting drop-down menu.

The **Start New Log File** panel appears in detail-view.



- 6 Click **OK**.

A new log file is started for the Kernel and the old one is closed.

## Specifying the Kernel Log File Location

---

You can specify the fully-qualified path of the directory in which log files should be stored. If you do not specify a log file location, the default location for Kernel log files (the subdirectory named for the Kernel) will be used. By default, the Kernel log file directories 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 Server\`
- In Windows 7 environments: `ProgramData\Software AG\Entire Net-Work Server\logsvc75`
- In UNIX environments: `$SAG\wcp\`.



**Note:** If you want to put your Entire Net-Work log files on a shared server, read . However, please be sure that the directory name you specify for the log files for each Kernel is unique.

### ➤ To specify the log file location:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 In tree-view, right-click on the name of the Kernel for which you want to set advanced parameters and select the **Set Basic Parameters** command from the resulting drop-down menu.

The **Kernel Basic Parameters** panel appears in detail-view.

**Kernel Basic Parameters**

WCPARTITION..... <not defined>

NODEID..... 1234 \*

AUTOSTART..... <not defined>

AUTOSTOP..... <not defined>

WCPTRACE..... 0 \*

☐ Full WCP Trace

XTSTRACE..... 0 \*

☐ Full XTS Trace

LNKTRACE..... 0 \*

☐ Full LNK Trace

LOGDIR..... C:\ProgramData\Software AG\Entire Net-Work Server\MYKERNEL\

LOGSIZE..... 100

DATE\_STAMP..... <not defined>

OK Cancel Help

- 7 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 Kernel parameters are updated in the appropriate Kernel definition file. You must restart the Kernel in order for these parameter changes to take effect.



# 63

## Tracing Kernel Processing

---

■ Managing Kernel Tracing .....	286
■ Managing Software AG Transport Services Tracing .....	290
■ Managing Software AG Communications Tracing .....	292

There are three kinds of trace processing that can occur when using Kernels:

- Traces can be performed for individual Kernel 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 Kernel 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:** While you can set the trace level for a Kernel using SMH, we recommend that you perform this function only under the advisement of your Software AG support representative.

You can set the trace level for a Kernel dynamically (immediately and for only this execution of the Kernel) or permanently (for future executions of the Kernel). The dynamic trace level setting occurs immediately, but if the Kernel is restarted, it is reset to the trace level specified in the Kernel definition. The permanent trace level setting occurs in the Kernel definition and takes effect only when the Kernel is restarted.

This section covers the following topics:

- [Permanently Setting the Trace Level](#)
- [Dynamically Setting the Trace Level](#)

### Permanently Setting the Trace Level

➤ **To set the trace level offline in SMH for the Kernel:**

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 In tree-view, right-click on the name of the Kernel for which you want to set the trace level and select **Set Kernel Trace Granularity** command from the resulting drop-down menu.

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

**Set Kernel 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

OK Cancel Help

- 7 Select appropriate trace levels as requested by your Software AG support representative.

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.

8 Click **OK**.

The trace level is set. You must restart the Kernel in order for these trace level changes to take effect.

### Dynamically Setting the Trace Level

➤ To set the trace level offline in SMH for the Kernel:

Make sure you have accessed the System Management Hub.

- 1 Select the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

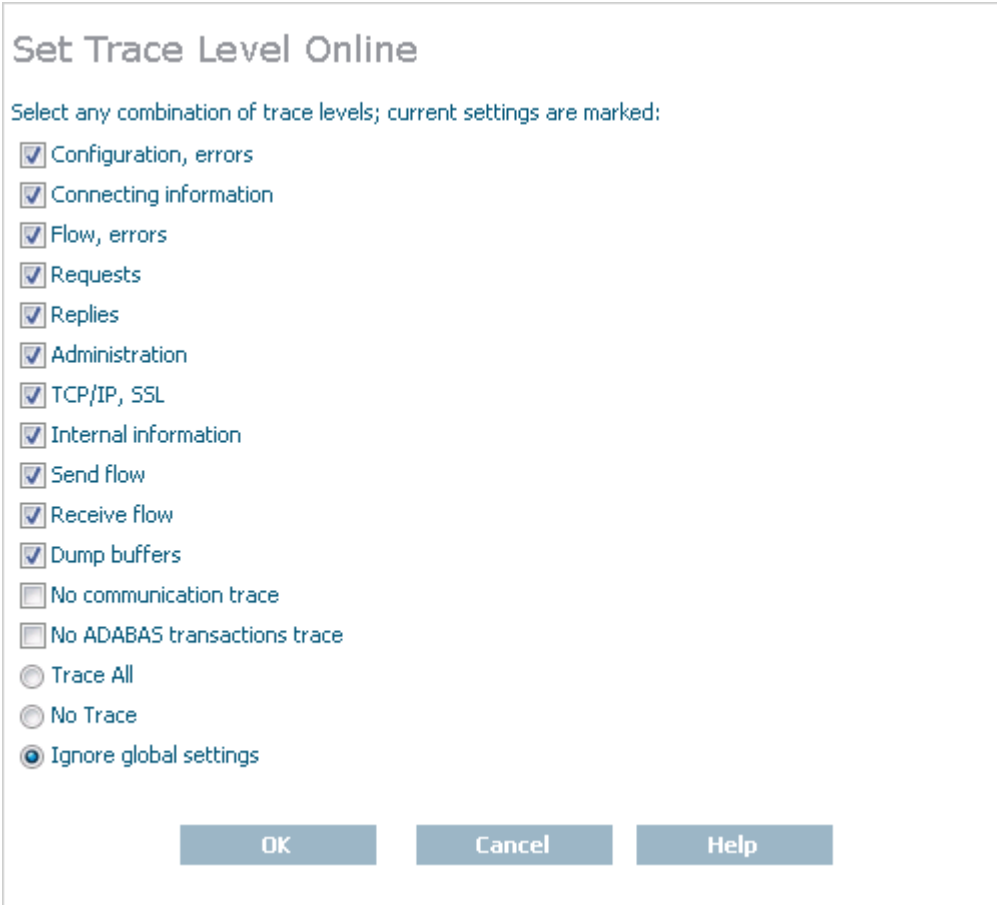
- 4 Expand **Kernels** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of Kernels that have been started appears.

- 5 In tree-view, right-click on the name of the Kernel for which you want to set the trace level and select **Set Trace Level Online** command from the resulting drop-down menu.

The **Set Trace Level Online** panel appears in detail-view.





**Set Trace Level Online**

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

OK Cancel Help

- 6 Select appropriate trace levels as requested by your Software AG support representative.

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.

- 7 Click **OK**.

The trace level is temporarily set. Once the Kernel is restarted, it will revert to using its original trace settings.

## 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 Kernel 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 the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 In tree-view, right-click on the name of the Kernel for which you want to set the trace level and select **Set Basic Parameters** command from the resulting drop-down menu.

The **Kernel Basic Parameters** panel appears in detail-view.

**Kernel Basic Parameters**

WCPARTITION..... <not defined>

NODEID..... 1234 \*

AUTOSTART..... <not defined>

AUTOSTOP..... <not defined>

WCPTRACE..... 0 \*

☐ Full WCP Trace

XTSTRACE..... 0 \*

☐ Full XTS Trace

LNKTRACE..... 0 \*

☐ Full LNK Trace

LOGDIR..... C:\ProgramData\Software AG\Entire Net-Work Server\MYKERNEL\

LOGSIZE..... 100

DATE\_STAMP..... <not defined>

OK Cancel Help

- 7 Modify the **XTSTRACE** parameter and **Full XTS Trace** checkbox on the **Kernel Basic 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
XTSTRACE	Set the XTS trace level using this parameter.
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.

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 Kernel 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 the name of the managed host on which Entire Net-Work Server 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 Server" in the tree-view under the managed host.

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

- 4 Expand **Servers** in tree-view, by clicking on the plus sign (+) to the left of its label.

The list of installed servers appears.

- 5 Expand the name of the server in the server list in tree-view, by clicking on the plus sign (+) to the left of its label.

A list of Kernels defined to the server appears.

- 6 In tree-view, right-click on the name of the Kernel for which you want to set the trace level and select **Set Basic Parameters** command from the resulting drop-down menu.

The **Kernel Basic Parameters** panel appears in detail-view.

**Kernel Basic Parameters**

WCPARTITION.....<not defined>

NODEID.....1234 \*

AUTOSTART.....<not defined>

AUTOSTOP.....<not defined>

WCPTRACE.....0 \*

☐ Full WCP Trace

XTSTRACE.....0 \*

☐ Full XTS Trace

LNKTRACE.....0 \*

☐ Full LNK Trace

LOGDIR.....C:\ProgramData\Software AG\Entire Net-Work Server\MYKERNEL\

LOGSIZE.....100

DATE\_STAMP.....<not defined>

OK Cancel Help

- 7 Modify the **LNKTRACE** parameter and **Full LNK Trace** checkbox on the **Kernel Basic 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
LNKTRACE	Set the ADALNK trace level using this parameter.
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.

The communications trace levels are set and activated.



# 64

## Entire Net-Work Utility Functions for the Directory Server (checkadi and setadi)

---

■ The checkadi Utility .....	296
■ The setadi Utility .....	297

Two Entire Net-Work utility functions with focus on the Adabas 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 ...
```

# 65

## Port Number Reference

---

■ Port Overview and General Assignments .....	300
■ Changing the Adabas Directory Server Port Number .....	301
■ About System Management Hub Ports .....	303

This chapter describes the ports that are needed by Adabas LUW and Entire Net-Work LUW products 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
Adabas Manager Communication Client	One port is needed.	4980
Adabas Directory Server	One port is needed for Entire Net-Work requests to the Directory Server	4952 (IANA port)  <b>Note:</b> 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 Administration LUW	One port is needed for System Management Hub (SMH) administration tasks	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

Software AG has registered port number 4952 with the Internet Assigned Numbers Authority (IANA) for use by the Adabas Directory Server. For more information about Directory Server port number specifications, read *The Directory Server Port Number* in the *Software AG Directory Server Installation and Administration Guide*. For information on changing the Directory Server port number for an Entire Net-Work installation, read [Changing the Adabas 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 Adabas 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 Kernel Configuration Definitions* in the *Entire Net-Work Server LUW Installation and Administration Guide*.

## Changing the Adabas Directory Server Port Number

➤ If you need to change the Directory Server port number for your installation, follow these steps:

- 1 Within the settings for Entire Net-Work Client and any client configurations definitions, change all specifications for the Directory Server port number to the new port number you want to use. Directory Server port numbers can be changed for Entire Net-Work Client and the client configurations using the System Management Hub (SMH), as follows:
  1. Start up SMH and access the Entire Net-Work Client SMH administration area. For more information about the Entire Net-Work Client SMH administration area, read *The Entire*

*Net-Work Client SMH Administration Area*, in the *Entire Net-Work Client Installation and Administration Guide*.

2. Right-click on the name of a client machine listed under **Clients** in the Entire Net-Work Client SMH administration area.
3. Select the **Set Parameters** command from the drop-down menu that appears.

The **Set Client Parameters** panel appears in detail-view. For complete information about this screen, read *Setting Client Parameters*, in the *Entire Net-Work Client Installation and Administration Guide*.

4. On the **Set Client Parameters** panel, change the Directory Server port number to the new port number you want to use in the SAGXTSDSPORT field.
5. On the **Set Client Parameters** panel, click on **Update all Client Configurations**. A check mark should appear for this option.
6. Click **OK** to save the settings for the client machine and all of the client configurations associated with it.

- 2 Within the settings for Entire Net-Work Server and any Kernels definitions, change all specifications for the Directory Server port number to the new port number you want to use. These port numbers can be changed using the System Management Hub (SMH), as follows:

1. Start up SMH and access the Entire Net-Work Server SMH administration area. For more information about the Entire Net-Work Server SMH administration area, read *The Entire Net-Work Server SMH Administration Area*, in the *Entire Net-Work Server LUW Installation and Administration Guide*.
2. Right-click on the name of an Entire Net-Work Server listed under **Servers** in the Entire Net-Work Server SMH administration area.
3. Select the **Set Server Parameters** command from the drop-down menu that appears.

The **Server Parameters** panel appears in detail-view. For complete information about this screen, read *Setting Server Parameters*, in the *Entire Net-Work Server LUW Installation and Administration Guide*.

4. On the **Server Parameters** panel, change the Directory Server port number to the new port number you want to use in the SAGXTSDSPORT field.
5. On the **Server Parameters** panel, click on **Update all Kernels**. A check mark should appear for this option.
6. Click **OK** to save the settings for the server and all of the Kernels associated with it.

- 3 Shut down the Entire Net-Work Client service or daemon and the Entire Net-Work Server service or daemon, as appropriate. Be sure to shut down every Kernel associated with the server as well.

For information on shutting down the Entire Net-Work Client service or daemon, read *Stopping Entire Net-Work Client* in the *Entire Net-Work Client Installation and Administration Guide*. For information on shutting down the Entire Net-Work Server service or daemon, read *Stopping Entire Net-Work Server* in the *Entire Net-Work Server LUW Installation and Administration Guide*.

- 4 Shut down the Directory Server service or daemon.

For information on shutting down the Directory Server service or daemon, read *Starting and Stopping the Adabas Directory Server*, in the *Software AG Directory Server Installation and Administration Guide*.

- 5 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.
- 6 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 Adabas Directory Server*, in the *Software AG Directory Server Installation and Administration Guide*.

- 7 Start up the Entire Net-Work Client service or daemon and the Entire Net-Work Server service or daemon.

For information on starting up the Entire Net-Work Client service or daemon, read *Manually Starting Entire Net-Work Client* in the *Entire Net-Work Client Installation and Administration Guide*. For information on starting up the Entire Net-Work Server service or daemon, read *Manually Starting Entire Net-Work Server* in the *Entire Net-Work Server LUW Installation and Administration Guide*.

## About System Management Hub Ports

---

For information about any System Management Hub installation issues, including port number settings, read *Installing webMethods Products* in Empower.

---



# Index

---

## A

- accessing
  - System Management Hub, 20
- accessing secured host resources, 125
- Adabas
  - configuring components for Windows Personal Firewall, 14
- Adabas Directory Server
  - changing, 137
- ADALNK user exits, 133
- adding
  - a link to a Directory Server, 29
  - client configurations, 95
  - Kernel configurations, 167
  - partitions, 37
  - targets, 43
- administration area, 23
- applications
  - identifying client configurations, 89

## B

- browsers, 10

## C

- changing
  - host, 73
  - protocol, 73
  - target name, 72
- changing hosts, 77
- checkadi utility, 296
- client configurations
  - about, 83
  - adding, 95
  - controlling client access to databases, 107
  - deleting, 97
  - identifying in your applications, 89
  - listing, 85
  - maintaining, 99
  - migrating, 105
  - reviewing, 85
  - selecting, 85
  - setting service parameters, 91
  - used for testing, 84
- configurations (see Kernel configurations and client configurations)
- configuring

- Windows personal firewall, 14

## D

- databases
  - controlling client access to, 107
- dates, end-of-maintenance, 4
- deleting
  - client configurations, 97
  - Directory Server links, 33
  - partitions, 38
  - targets, 75
- Directory Server
  - administration tasks, 23
  - utility functions for, 295
- Directory Server links
  - maintaining, 27
- Directory Servers
  - adding a link to, 29
  - administration area, 23
  - changing hosts, 77
  - deleting the link, 33
  - displaying parameters, 32
  - listing linked, 28
  - listing parameters, 32
  - maintaining partitions, 35
  - maintaining targets, 41
  - modifying link definition of, 30
- displaying
  - Directory Server definition, 32
- documentation
  - in TECHcommunity website, 5
  - obtaining updates, 4
  - on Documentation website, 5
- Documentation website
  - documentation, 5

## E

- Empower
  - platform support, 9
- Empower website
  - product support, 5
- end-of-maintenance dates, 4
- Entire Net-Work
  - configuring components for Windows Personal Firewall, 14
  - starting and stopping Entire Net-Work Client, 151
  - System Management Hub, 19
- Entire Net-Work Client
  - accessing secured z/OS host resources, 125

- changing the Adabas Directory Server, 137
- managing client service tracing, 142
- managing client tracing, 144
- managing log files, 119
- managing Software AG communications tracing, 148
- managing Software AG transport services tracing, 146
- specifying log file location, 121
- starting a new log file, 120
- tracing processing, 141
- viewing log files, 120

## F

- firewall requirements, 10

## H

- hardware support, 10
- help
  - System Management Hub, 22
- host
  - changing, 73
- hosts
  - changing, 77

## I

- installation
  - preinstallation steps, 12

## K

- Kernel configurations
  - adding, 167
  - migrating, 173

## L

- listing
  - client configurations, 85
  - Directory Server definition, 32
  - linked Directory Servers, 28
  - partitions definition, 36
  - targets definition, 42
- log files
  - managing Entire Net-Work Client, 119
  - specifying Entire Net-Work Client log file location, 121
  - starting a new Entire Net-Work Client log file, 120
  - viewing Entire Net-Work Client, 120
- logging in
  - SMH, 20

## M

- maintaining
  - client configurations, 99
  - Directory Server links, 27
  - partitions, 35
  - targets, 41
- Microsoft Windows support, 9
- migrating
  - client configurations, 105
  - Kernel configurations, 173

- older client configurations, 105
- older Kernel configurations, 173
- modifying
  - Directory Server link definition, 30
  - partition name, 37

## O

- operating system coverage, 9

## P

- partitions
  - adding, 37
  - changing the name, 37
  - deleting, 38
  - listing, 36
  - maintaining, 35
- platform support, 9
- port numbers, 299
- preinstallation steps, 12
- product support
  - obtaining in Empower, 5
  - obtaining updated documentation, 4
  - supported platforms, 9
- protocol
  - changing, 73

## R

- Refresh button
  - System Management Hub, 22
- requirements
  - browsers, 10
  - firewall, 10
  - operating system coverage, 9
  - space, 10
  - system, 8
  - Windows, 10
- reviewing
  - client configurations, 85

## S

- security
  - accessing secured host resources, 125
- selecting
  - client configurations, 85
- service parameters
  - client configurations, 91
- setadi utility, 297
- setting
  - target type, 70
- shutting down
  - System Management Hub, 21
- SMH (see System Management Hub)
- space requirements, 10
- starting
  - Entire Net-Work Client, 151
- stopping
  - Entire Net-Work Client, 151
- support
  - obtaining updated documentation, 4
  - platforms supported, 9

- support for prior versions, 4
- supported browsers, 10
- supported hardware, 10
- supported operating systems, 9
- supported platforms, 9
- system administration
  - System Management Hub, 19
- System Management Hub
  - about, 19
  - accessing, 20
  - Directory Server administration area, 23
  - getting help, 22
  - logging in, 20
  - Refresh button, 22
  - shutting down, 21
- system requirements, 8

## T

- target name
  - changing, 72
- target type
  - setting, 70
- targets
  - adding, 43
  - deleting, 75
  - listing, 42
  - maintaining, 41
- TECHcommunity website, 5
- testing network configurations, 84
- tracing
  - Entire Net-Work Client, 141
  - managing client, 144
  - managing client service, 142
  - managing Software AG communications, 148
  - managing Software AG transport services, 146

## U

- UNIX
  - supported platforms, 9
- utility functions
  - checkadi, 296
  - for the Directory Server, 295
  - setadi, 297

## W

- Windows Personal Firewall, 14
- Windows requirements, 10

## Z

- z/OS host resources
  - accessing secured, 125

