Entire Net-Work Client Installation and Administration Guide

Entire Net-Work Client Installation and Administration

Version 1.6.1

November 2017

This document applies to Entire Net-Work Client Version 1.6.1 and all subsequent releases.

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

Document ID: WCL-OWCLDOC-161-20171110

Table of Contents

1 Concepts

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

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

Entire Net-Work Client

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

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

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

When you receive your Entire Net-Work Client package, it includes installation code for a default client configuration.

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

Directory Server

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

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

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

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

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

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

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

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

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

The port number used by the Directory Server can be changed, but must be changed with care. For complete information on changing the Directory Server port used by Entire Net-Work 7 components, read ***Changing the Adabas Directory Server Port Number***, elsewhere in this guide.

System Management Hub (SMH)

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

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

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

For more information about performing these tasks, read ***Entire Net-Work Client Administration*** in the Entire Net-Work LUW Administration Guide.

SSL Support

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

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

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

2 Understanding Partitioning

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

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

Here are some of the advantages of partitioning:

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

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

3 Understanding Filtering

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

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

Filtering in Client Configurations

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

For more information on setting these Entire Net-Work Client configuration parameters, read ***Maintaining Client Configuration Parameters***, elsewhere in this guide.

Filtering in Kernel Definitions

You can filter Kernels by requests:

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

This section covers the following topics:

- Filtering Requests to and from Specific Clients

Filtering Requests to Adabas Databases

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

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

Filtering Relay Requests to Other Kernels

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

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

Filtering Requests from Other Kernels

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

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

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

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

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

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

Filtering Requests to and from Specific Machines

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

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

Filtering Requests to and from Specific Clients

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

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

4 Release Notes

This chapter provides release notes for the Entire Net-Work Client 1.6 release. It is organized as follows:

Enhancements

The primary enhancement in the Service Pack 1 release of Entire Net-Work Client is a rollup of fixes to the base release of v1.6.

Last-minute information on this release is available in the *ReadMe* file.

After installation, please visit the Software AG Empower Product Support website at ***https://empower.softwareag.com/*** to check for and apply any available fixes to v1.6_SP1.

Migration Considerations

If the Adabas Directory Server is installed and used by a prior version this product, be sure to use the existing Adabas Directory Server port number setting for this installation. You can change the port number after this product is installed. For complete information on changing the Directory Server port number used, read ***Changing the Adabas Directory Server Port Number***, elsewhere in this guide.

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

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

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

Caution: Once a Kernel configuration has been migrated to 7.6, 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.

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.

5 Installing and Uninstalling Entire Net-Work Client

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

This chapter provides product-specific instructions for installing Entire Net-Work Client. 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/***).

You can create a silent installation of Entire Net-Work Client using Software AG Installer scripts. For complete information, read *Using the Software AG Installer*.

This chapter covers the following topics:

Installation Overview

This product is installed using the Software AG Installer, which you can download from the Software AG Empower website at ***https://empower.softwareag.com/***.

The Software AG Installer offers typical development installations of Software AG products. When you select a typical development installation, the installer automatically groups and selects the Software AG products and components that make up that installation. The following are some typical installation configuration groupings of Adabas LUW (Linux/UNIX/Windows) and Entire Net-Work LUW products available in the Software AG Installer:

- The Adabas Directory Server can be installed without installing any other Software AG products; it is not grouped with any other product. However, a Directory Server must already be installed before you attempt any other Adabas family product installations; the Directory Server installation location is requested during the installation of many Adabas family products.

  If you have a Directory Server already installed at your site from an earlier release of Software AG products, you do not need to install it again; you can use the existing installation instead.

  The Directory Server must be installed on a machine in your network that can be accessed by all machines where Entire Net-Work will be installed (both Entire Net-Work Server and Entire Net-Work Client). It should be installed on a dedicated system that is operational 24 hours a day, with a UPS.

  We recommend that you install one Directory Server for use with all the Software AG products that require it.

- Entire Net-Work Client requires the use of the Adabas Directory Server; so be sure to have already installed the Directory Server before attempting an Entire Net-Work Client installation or install the Directory Server at the same time as Entire Net-Work Client.

- The Entire Net-Work Administration LUW installation is grouped with the installation of the **Event-Driven Architecture** tree components as well as all components of the **Infrastructure** tree provided for Software AG products in the Software AG Installer.

  Entire Net-Work Administration LUW requires the use of the Adabas Directory Server; so be sure to have already installed the Directory Server before attempting an Entire Net-Work Administration LUW installation or install the Directory Server at the same time as Entire Net-Work Administration LUW.

The **Infrastructure** entry in the Software AG Installer includes the installation of the System Management Hub (SMH). SMH should be installed on a machine in your network that can be accessed by all machines where the Adabas Directory Server and Entire Net-Work (both Entire Net-Work Server and Entire Net-Work Client) will be installed. It should be installed on a dedicated system that is operational 24 hours a day, with a UPS.

You cannot ungroup installations that have been paired or grouped. However, you can select multiple installation configurations for installation at the same time. To configure your installation of these products and create effective production environments, work with your system administrators and Software AG Global Consulting Services.

System Requirements

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

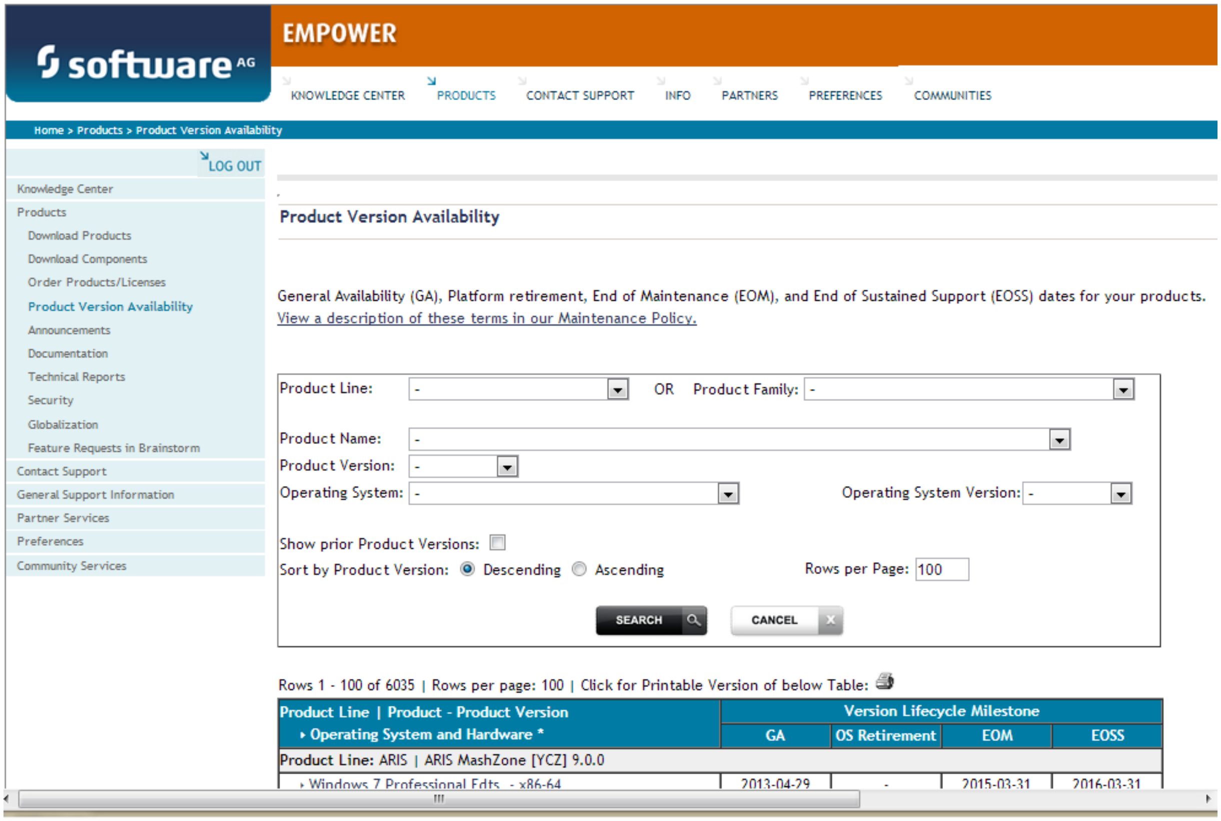
Supported Operating System Platforms

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** in the left menu of the web page and select **Product Version Availability** to access the Product Version Availability screen.



Product Version Availability

General Availability (GA), Platform retirement, End of Maintenance (EOM), and End of Sustained Support (EOSS) dates for your products.
View a description of these terms in our Maintenance Policy.

Product Line: - OR Product Family: -

Product Name: -
Product Version: -
Operating System: - Operating System Version: -

Show prior Product Versions: □
Sort by Product Version: ● Descending ○ Ascending Rows per Page: 100

Rows 1 - 100 of 6035 | Rows per page: 100 | Click for Printable Version of below Table:

Product Line | Product - Product Version ‣ Operating System and Hardware *	Version Lifecycle Milestone			
	GA	OS Retirement	EOM	EOSS
Product Line: ARIS | ARIS MashZone [YCZ] 9.0.0				
‣ Windows 7 Professional Edts. - x86-64	2013-04-29	-	2015-03-31	2016-03-31

3. Use the fields on this 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

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

Category	Question	Considerations
Adabas Directory Server and this product	Do you want to direct specific clients or Kernels to specific databases by department or other organizational grouping?	You can create multiple Kernels and use Directory Server partitioning and client and Kernel filtering in SMH to control which clients and Kernels have access to which databases.
Partitioning	Do you want to implement partitioning?	Partitioning allows you to direct specific clients or Kernels to specific databases. Partitions are defined for the clients and Kernels in the System Management Hub. For more information, read ***Understanding Partitioning***,elsewhere in this guide.
Entire Net-Work Clients	How many Entire Net-Work Clients will you need and on which machines will they be needed?	One Entire Net-Work Client must be installed on each machine that needs to communicate with an Adabas database or that needs to access other Software AG product servers (such as those for EntireX Communicator, Tamino, or Adabas SQL Gateway).
	If you are implementing partitioning, which clients will be part of which partition?	Partitioning allows you to direct specific clients to specific databases. For more information, read ***Understanding Partitioning***,elsewhere in this guide.
	Are you implementing filtering?	Filtering allows you to direct specific clients to specific databases. For more information, read ***Understanding Filtering***,elsewhere in this guide.
	Will any of the machines be used to run both databases and Entire Net-Work Clients?	At least one Entire Net-Work 7 Kernel must be defined and one Entire Net-Work 7 client must be installed on any machine on which a local database is installed and from which access to other databases is required.

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 Client 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 installation documentation provides a brief description on how to install the Entire Net-Work Client 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 Client, 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 Client, select (check) the Entire Net-Work Client entry from the **Adabas Family** product selection tree.

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 When the **Configure** panel appears, specify 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 port used by the Directory Server, read ***Port Number Reference***, elsewhere in this guide.

In addition, select the radio button indicating whether Entire Net-Work Client should be installed as an application or a service. You can only select one. By default, it is installed as a service.

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.

After Entire Net-Work Client has been installed, it will start automatically if it has been started as a system service. You can start and stop it as you would any system service. If you have installed the Entire Net-Work Client as an application, you will need to manually start it.

Required Post-Installation Updates for Simple Connection Line Driver Support

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

You can do this in one of two ways:

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

be created in the Directory Server for each open systems Adabas database you want to access using the Simple Connection Line Driver. You can add these target entries using SMH.

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

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

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

Configure the Adabas Client Environment

To ensure that the Adabas Client environment is set correctly for use with Entire Net-Work Client, it must be configured.

The Adabas Client environment is only required by applications and services that access an Adabas database or use the database communication facilities. An Adabas Client environment is not automatically configured during installation. An Adabas Client environment enables you to configure the environment to fit the needs of your application or service.

The Adabas Client environment can either be set system-wide (global setting) or locally to the application (local setting). A global Adabas Client environment is required, when one or more of the following conditions apply:

- When the remote administration of the database is required;
- When the database is to be accessed via Entire Net-Work;
- When a service application requires access to the database;
- When multiple database versions are accessed concurrently.

Setting a global Adabas Client environment implies that only one Adabas Client version can be used. In such cases, the newest Adabas Client version installed on your machine should always be used.

Setting a local Adabas Client environment enables custom configuration of applications. This can be achieved in one of two ways:

1. By executing the application at a Local Client Environment command prompt; or
2. By executing the application with a local Adabas Client environment.

This section covers the following topics:

- Creating a Local Adabas Client Environment
- Setting up the Global Adabas Client Environment
- Modifying an Existing Global Adabas Client Environment

Creating a Local Adabas Client Environment

There are two ways to create a local Adabas Client environment:

1. Execute the application from a local Adabas Client command prompt via the Start menu: **All Programs > Software AG > Administration > Adabas Client** `v.r` **> Start Local Environment**.
2. Initialize the Adabas Client environment prior to executing the application by calling the script *aclenv.bat* located in the directory *<install_dir>\AdabasClient\INSTALL\*.

Setting up the Global Adabas Client Environment

There are two ways to set up a global Adabas Client environment:

1. Execute the application from a local Adabas Client command prompt via the Start menu: **All Programs > Software AG > Administration > Adabas Client** `v.r` **> Configure Global Environment**.
2. As a system administrator, open a command prompt and run the script *aclenvvar.bat* located in the directory *<install_dir>\AdabasClient\INSTALL\*.

Modifying an Existing Global Adabas Client Environment

When upgrading from a previous Adabas Client version, use one of the methods described in ***Setting up the Global Adabas Client Environment*** to set the global environment.

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	*<your-installation-location>\EntireNetWorkClient\bin\wclservice.exe*
Entire Net-Work Kernel program	*<your-installation-location>\EntireNetWorkServer\bin\wcpkernel.exe*
Entire Net-Work Server Service	*<your-installation-location>\EntireNetWorkServer\bin\wcpservice.exe*
Adabas Directory Server Service	*<your-installation-location>\SoftwareAG\SoftwareAgDirectoryServer\bin\xtsdssvcadi.exe*
System Management Hub (SMH) CSLayer Service	*<your-installation-location>\InstanceManager\bin\argsrv.exe*
System Management Hub (SMH) EventLayer Service	*<your-installation-location>\InstanceManager\bin\argevsrv.exe*

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.

6 Starting and Stopping Entire Net-Work Client

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 daemonshould 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.The UNIX Entire Net-Work Client daemon 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 daemon will be available in UNIX.

Once the Entire Net-Work Client service or daemon 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 daemonstarted 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 or daemon 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 daemonstarted 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.

To start the Entire Net-Work Client daemon in UNIX environments:

- Run the shell script *wclstart.sh*.

  The Entire Net-Work Client daemon 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. You can shut down (stop) the Entire Net-Work Client UNIX daemon using SMH or using a shell script. 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 daemon in UNIX environments:

- Run the shell script *wclstop.sh*.

  The Entire Net-Work Client daemon is stopped.

To stop the Entire Net-Work Client service or daemon 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 daemonis 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 daemonautomatically started when the machine is started.

7 About the System Management Hub

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.

Commands for Managing the System Management Hub Service in UNIX

After you set the environment for running Software AG products, as outlined in the previous section, you can issue the following commands to start, stop, restart, pause, and resume the System Management Hub on UNIX.

Note: Before issuing these commands, open a terminal window, and change to the *$SAG/InstanceManager* directory.

Command	Description
`argsrvs.bsh start`	Starts the System Management Hub.
`argsrvs.bsh stop`	Stops the System Management Hub.
`argsrvs.bsh restart`	Restarts the System Management Hub.
`argsrvs.bsh pause`	Pauses the System Management Hub.
`argsrvs.bsh resume`	Resumes 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.

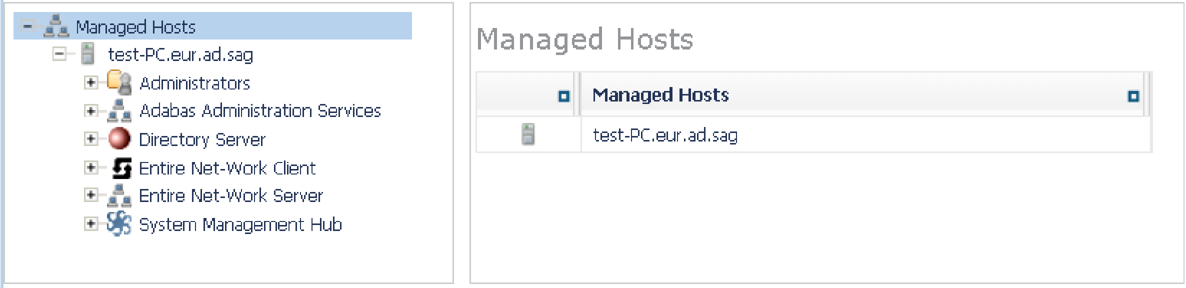
Or:

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.

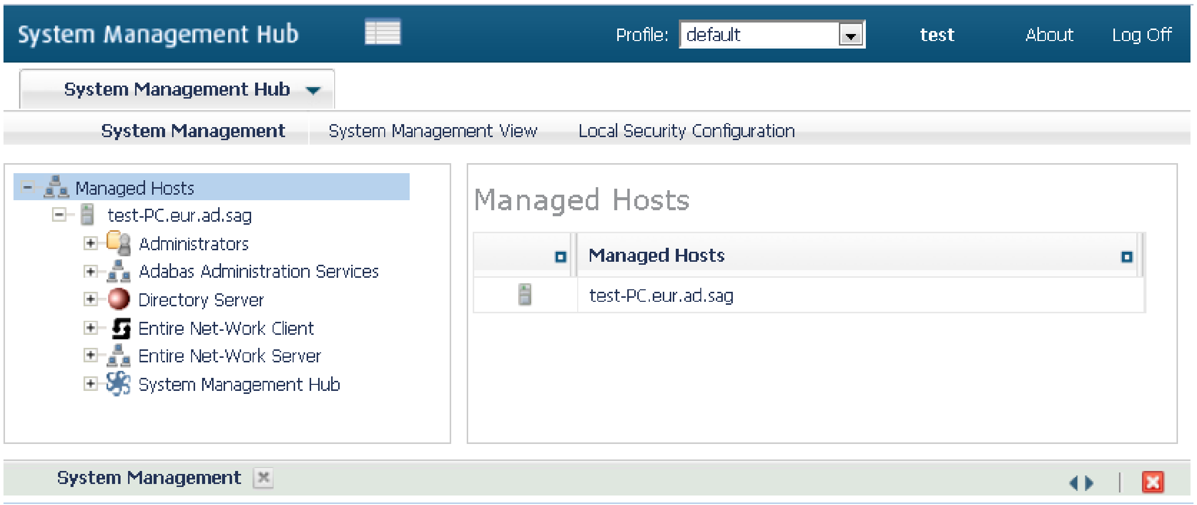


	Managed Hosts
	test-PC.eur.ad.sag

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.

8 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:

Changing the Adabas Directory Server	Provides instructions for changing the Adabas Directory Server for an Entire Net-Work Client service and for specific client configurations.
Tracing Entire Net-Work Client Processing	Describes Entire Net-Work Client trace processing.

9 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.

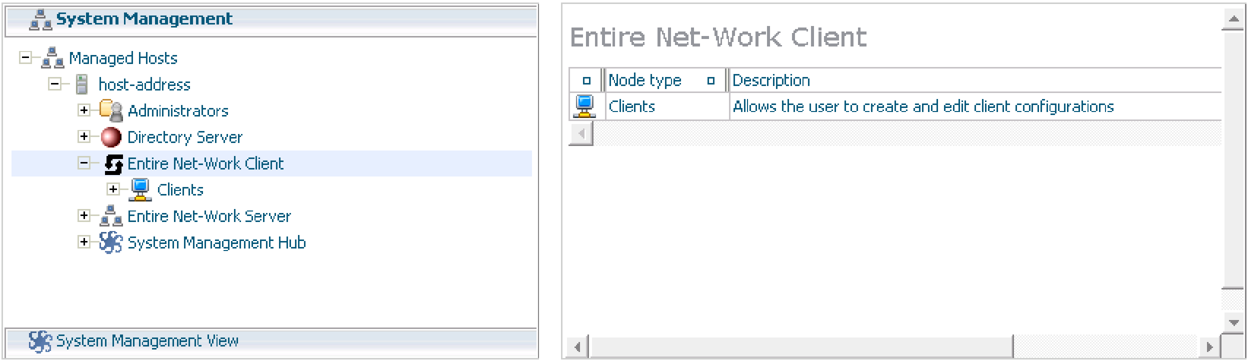
1 Select the name of the managed host on which Entire Net-Work Client is installed.

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.



Entire Net-Work Client

Node type	Description
Clients	Allows the user to create and edit client configurations

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.

10 About Client Configurations

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

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

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

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

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.

11 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:
Add to Browser Favorites	Add a node in tree-view to your browser favorites.
Add to View	Add a node in tree-view to System Management View. For more information about System Management View, read your System Management Hub documentation.
Help	Link to help for your use of SMH as it pertains to the Entire Net-Work Client administration area.
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.

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

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

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

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

Command	Use this command to:
Add Client Configuration	Add a client to be maintained by SMH. For more information, read *Adding Client Configurations*, elsewhere in this chapter.
Add to Browser Favorites	Add a node in tree-view to your browser favorites.
Add to View	Add a node in tree-view to System Management View. For more information about System Management View, read your System Management Hub documentation.
Help	Link to help for your use of SMH as it pertains to the Entire Net-Work Client administration area.
Migrate WCL13 Client Configuration	Migrate the client configurations you set up in Entire Net-Work Client 1.3. This process converts them to Entire Net-Work Client 1.5 client configurations. For more information, read *Migrating Entire Net-Work Client Configurations*, elsewhere in this chapter.
Migrate WCL14 Client Configuration	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 *Migrating Entire Net-Work Client Configurations*, elsewhere in this chapter.
New Log File	Close the current Entire Net-Work Client log file and start a new one. For more information, read *Managing Entire Net-Work Client Log Files*, elsewhere in this chapter.
Refresh	Refresh the screen.
Remove from View	Remove a node in tree-view from System Management View. For more information about System Management View, read your System Management Hub documentation.
Set Service Parameters	Change the parameters used by the client machine, including the Directory Server used by the client machine. For more information, read *Setting Service Parameters*, elsewhere in this chapter.
Set Service Trace Granularity	Set the Entire Net-Work Client trace level for all clients. For more information, read *Tracing Entire Net-Work Client Processing*, elsewhere in this chapter.
Shutdown	Shut down the Entire Net-Work Client service. For more information, read *Stopping Entire Net-Work Client*, elsewhere in this chapter.
View Log File	View the current Entire Net-Work Client log file. For more information, read *Managing Entire Net-Work Client Log Files*, elsewhere in this chapter.

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

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

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

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

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

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

12 Identifying the Client Configuration to Your Application

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

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

Specifying the Configuration by Environment Variable

To specify the client configuration using an environment variable:

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

Specifying the Configuration in Your Application

To specify the client configuration in your application:

- Use the AdaSetParameter API function 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.

13 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.

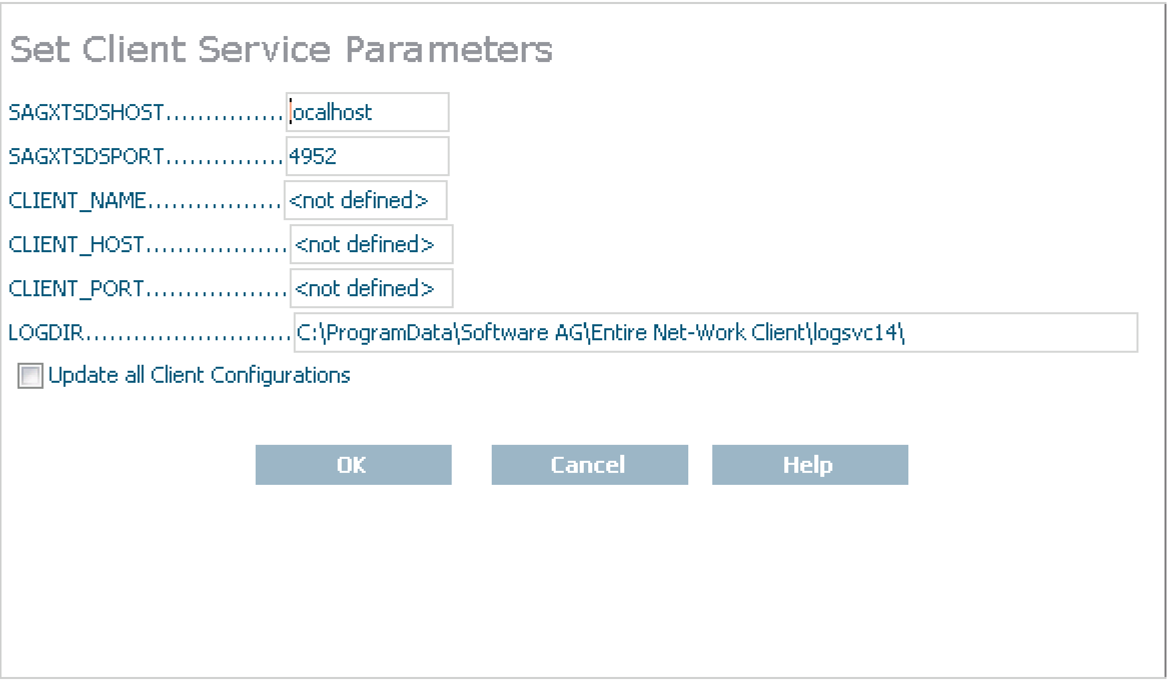
1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.

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

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	Normally, port numbers are dynamically assigned by Entire Net-Work when the 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.).

Parameter	Description
	■ Once an available port number is found, it is assigned to the client in its Adabas Directory Server entry. 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.
LOGDIR	Specify the fully-qualified path of the directory where Entire Net-Work Client log files should be written. For more information, read ***Specifying the Log File Location***, elsewhere in this chapter.

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

6 When all parameters are set as you want, click OK.

The client machine parameters are updated.

14 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.

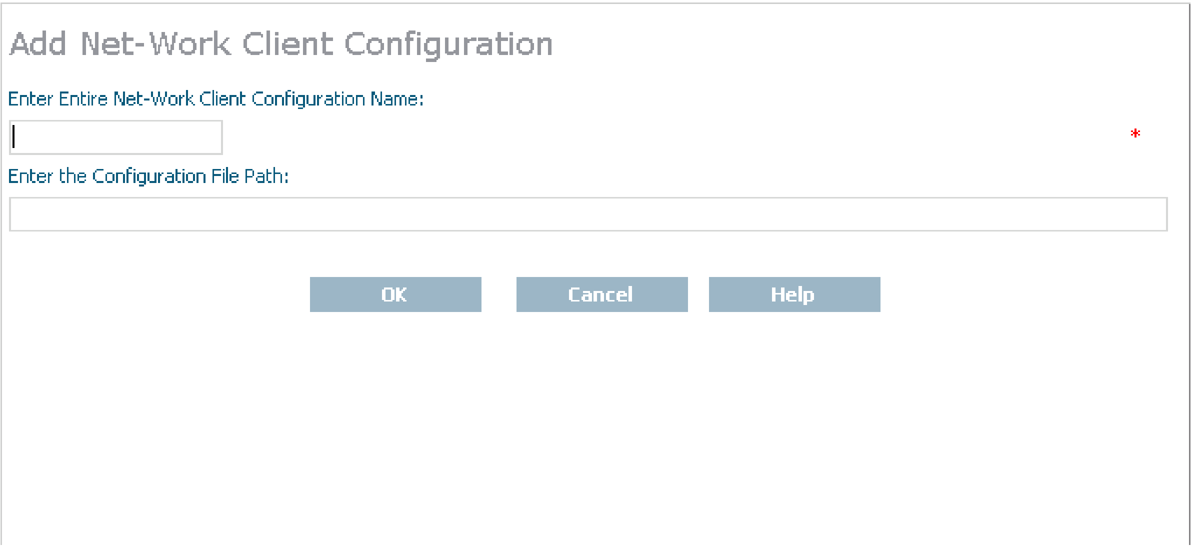
1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.

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:

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.

15 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.

16 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:

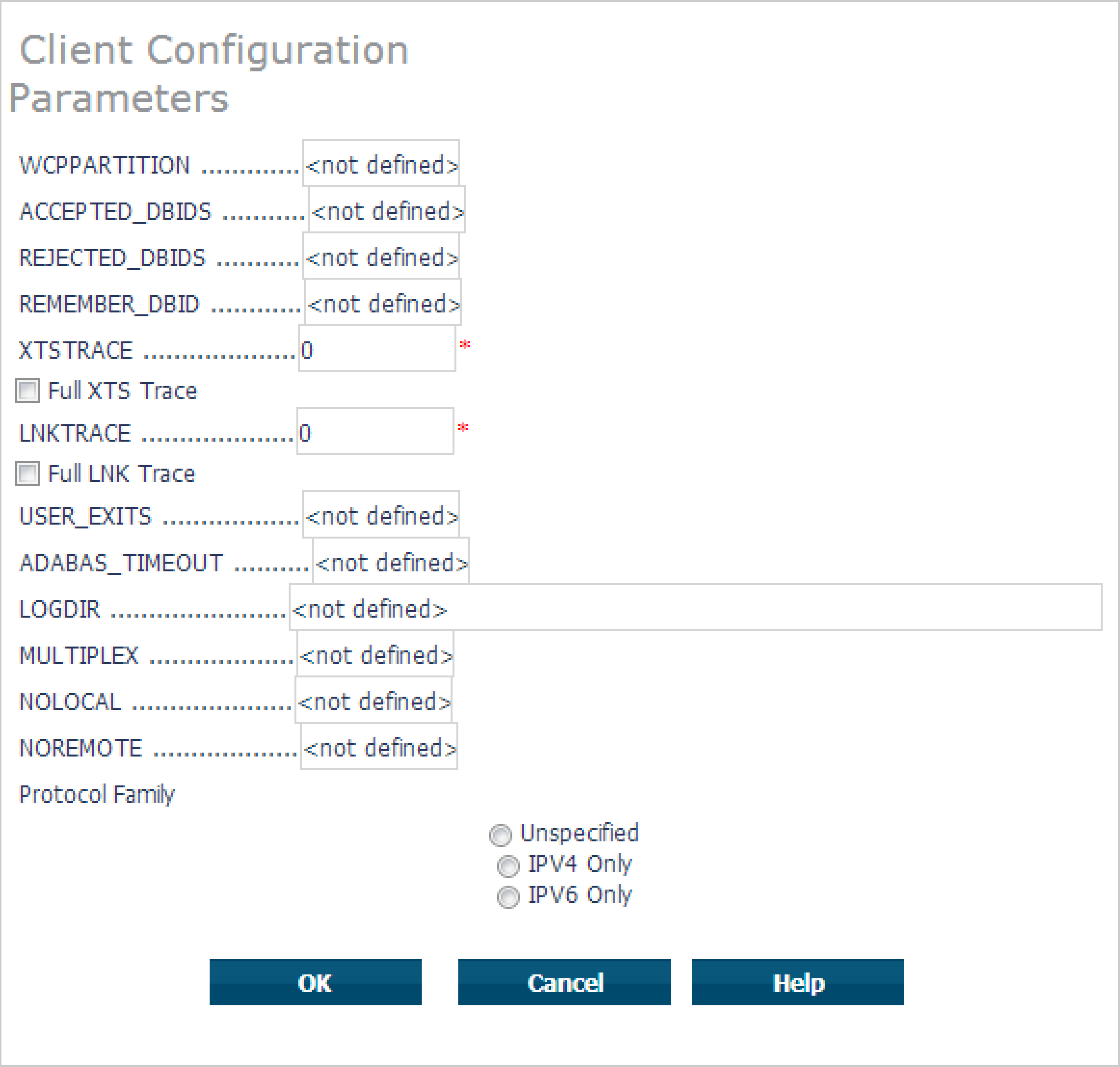
Make sure you have accessed the System Management Hub.

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

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

Parameter	Description	Required?	Default
ACCEPTED_DBIDS	Specify the database IDs you want this client to be able to access. If more than one database ID is needed, separate them with commas. If a range of database numbers is needed, separate them with a dash. For example, "4,12-15,62" indicates that the client should have access to databases 4, 62, and any databases with numbers between 12 and 15 (inclusive). For more	No	All defined databases can be accessed.

Parameter	Description	Required?	Default
	information, read *Understanding Filtering*, elsewhere in this guide.		
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 *Specifying the Client Log File Location*, elsewhere in this chapter.	No	■ 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\`.
LNKTRACE	Set the hexadecimal ADALNK trace level using this parameter. This is the trace level	No	00

Parameter	Description	Required?	Default
	for Adabas calls. Valid values are hexadecimal values ranging from "00" (no tracing) through "f1" (full tracing). Do not specify full tracing unless specifically instructed to do so by a Software AG Customer Support representative. If you do, your installation could be overrun with trace messages that would be meaningless to you and would likely affect system performance. For more information about Entire Net-Work Client tracing, read *Tracing Entire Net-Work Client Processing*, elsewhere in this guide.		
MULTIPLEX	Indicate whether a TCP/IP connection is shared by multiple Adabas open system clients connected to Entire Net-Work. Valid values are "YES" and "NO". If you specify "YES", the TCP/IP connection is shared; if you specify "NO", the TCP/IP connection is not shared. Sharing a TCP/IP connection can result in reduced speed across the network. However, it can be useful if the number of sockets available is limited (especially in UNIX environments).	No	For Adabas open systems versions 6.3 and earlier, the default is "YES". For all versions after 6.3, the default is "NO"
NOLOCAL	Indicate whether or not you want this client to use local databases. Valid values are "YES" and "NO". If you specify "YES", local databases are *not* 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 *not* used; if you specify "NO", they are used.	No	NO
Protocol Family	Select the TCP/IP protocol family used for this client. Click (check) **Unspecified**, **IPV4 Only**, or **IPV6 Only**. If you select **IPV4 Only** or **IPV6 Only**, only the selected protocol is used for communications with this client. If you select **Unspecified**, the domain name server (DNS) will determine which	No	Unspecified

Parameter	Description	Required?	Default
	protocol is used; **Unspecified** is the default. **Caution:** We recommend that you use the default value (**Unspecified**) 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 *not* 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 *not* have access to databases 4, 62, and any databases with numbers between 12 and 15 (inclusive). For more information, read ***Understanding Filtering***, elsewhere in this guide.	No	All defined databases can be accessed.
REMEMBER_DBID	Indicate whether the access entries for databases used by this client should be remembered and stored in local Entire Net-Work Client access entries in the Entire Net-Work Client configuration file as well as in the Directory Server. Valid values are "YES" and "NO". If you specify "YES", the access entry information is 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 theDirectory 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	No	No user exit is used with this client.

Parameter	Description	Required?	Default
	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. .		
WCPPARTITION	Specify the partition in which the client is assigned, if any. For more information, read *Understanding Partitioning*, elsewhere in this guide.	No	The client is not assigned a partition.
XTSTRACE	Set the hexadecimal XTS trace level using this parameter. This is the trace level for Software AG transport services. Valid values are hexadecimal values ranging from "0000" (no tracing) through "FFFE" (full tracing). Do not specify full tracing unless specifically instructed to do so by a Software AG Customer Support representative. If you do, your installation could be overrun with trace messages that would be meaningless to you and would likely affect system performance. For more information about Entire Net-Work Client tracing, read *Tracing Entire Net-Work Client Processing* , elsewhere in this guide.	No	0000

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

17 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.

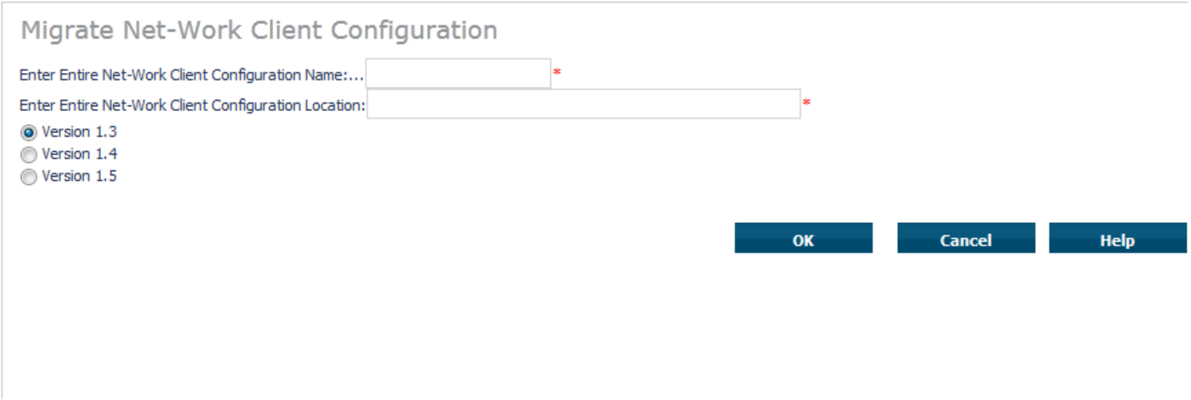
To convert an Entire Net-Work Client configuration to configuration used by the current version of Entire Net-Work Client:

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

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.

18 Controlling Client Access to Databases

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 ***Understanding Filtering***, elsewhere in this guide.

Globally, you can perform such filtering in the Directory Server configuration, using partitioning and target definitions. For more information about using the Directory Server, read 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

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

To add an Adabas access definition to a client configuration:

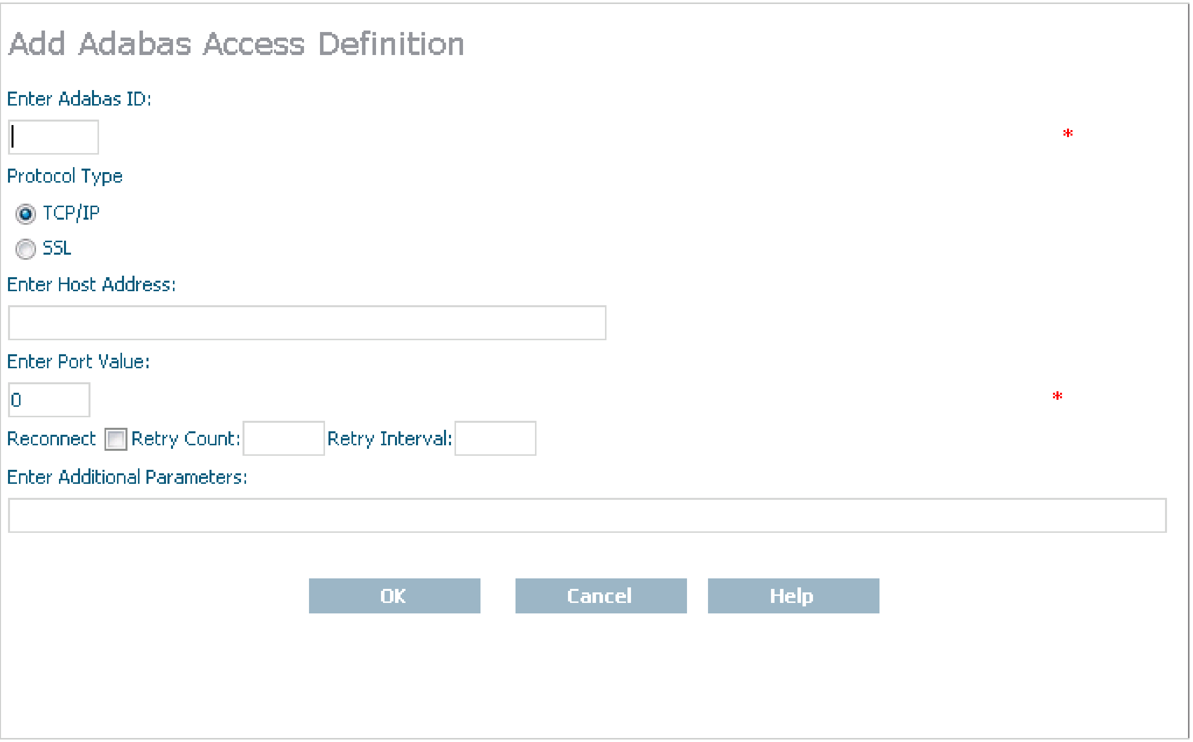
Make sure you have accessed the System Management Hub.

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

   A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.
3. Select and expand the client machine on which the client configuration is defined.

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

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



Add Adabas Access Definition

Enter Adabas ID: *

Protocol Type

● TCP/IP

○ SSL

Enter Host Address:

Enter Port Value: 0 *

Reconnect □ Retry Count: Retry Interval:

Enter Additional Parameters:

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

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

Parameter	Description	Required?	Default
	Reconnect parameter is turned on (checked). If no value is specified, reconnection attempts do not occur.		
Additional Parameters	Specify additional parameters as described in *Parameters*, in the chapter entitled *Directory Server Target Entries* of the *Software AG Directory Server Installation and Administration Guide*. 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.

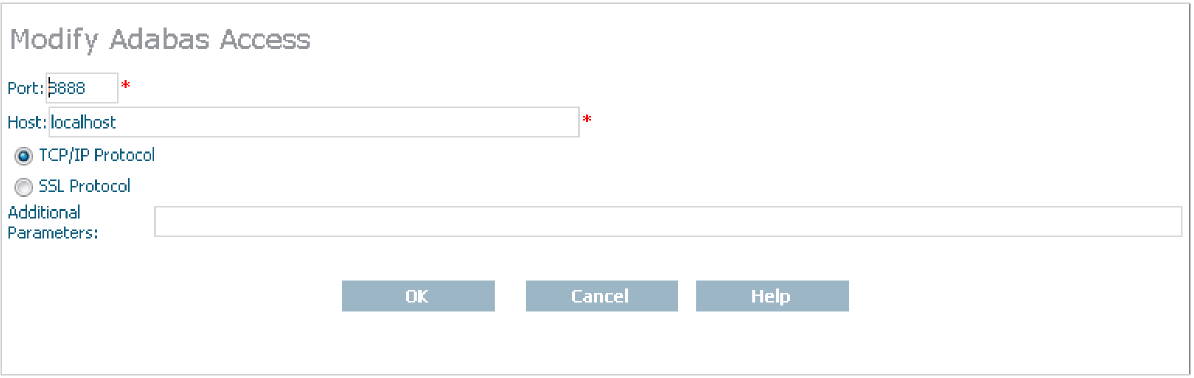
Options for the Adabas access and additional access parameter definitions appear in tree-view.

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: 3888 *

Host: localhost *

● TCP/IP Protocol

○ SSL Protocol

Additional Parameters:

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 *Parameters*, in the chapter entitled *Directory Server Target Entries* of the *Software AG Directory Server Installation and Administration Guide*. Separate parameters in this field with ampersand (&) symbols.	No	—

The Adabas access definition is modified.

Deleting Adabas Access Definitions

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

Make sure you have accessed the System Management Hub.

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

   A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.
3. Select and expand the client machine on which the client configuration is defined.

   The list of client configurations defined on the client machine appears.
4. In tree-view, expand the client configuration containing the Adabas access definitions you want to delete.

   Options for the Adabas access and additional access parameter definitions appear in tree-view.
5. Select and expand **Adabas Access Definitions** in the tree-view list for the client configuration.

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

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

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

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

The definition is deleted from the configuration.

Maintaining Additional Database Access Parameters

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

This section covers the following topics:

- Adding Additional Access Parameter Definitions
- Listing Additional Access Parameter Definitions
- Modifying Additional Access Parameter Definitions
- Deleting Additional Access Parameter Definitions

Adding Additional Access Parameter Definitions

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

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

Make sure you have accessed the System Management Hub.

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

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

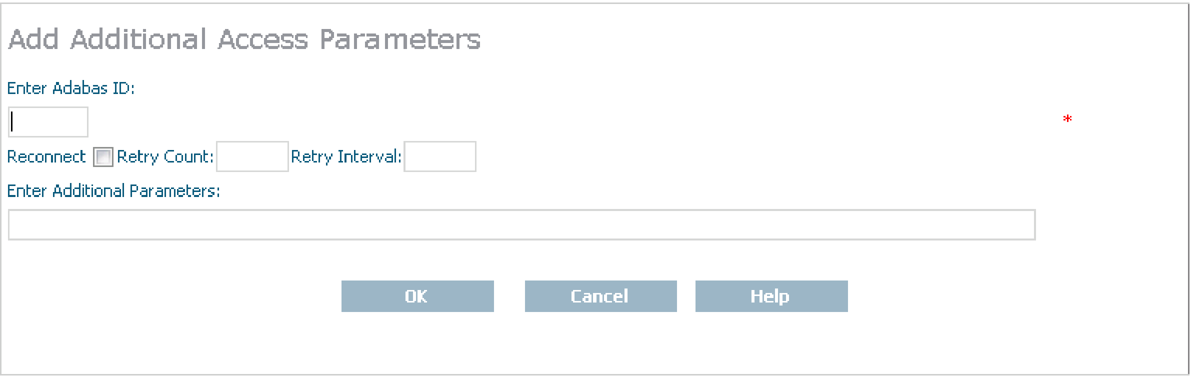
A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

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

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

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

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



Add Additional Access Parameters

Enter Adabas ID:

Reconnect □ Retry Count: Retry Interval:

Enter Additional Parameters:

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

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

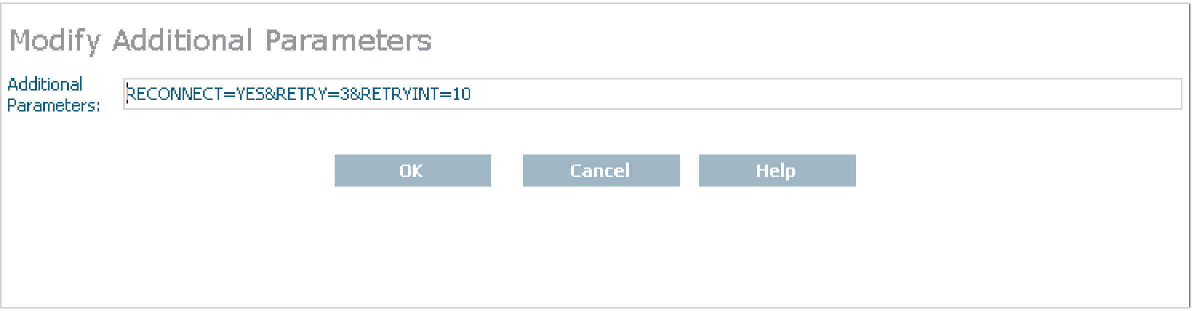
Options for the Adabas access and additional access parameter definitions appear in tree-view.

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.



Modify Additional Parameters

Additional Parameters: RECONNECT=YES&RETRY=3&RETRYINT=10

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 *Parameters*, in the chapter entitled *Directory Server Target Entries* of the *Software AG Directory Server Installation and Administration Guide*. 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.

19 Managing Entire Net-Work Client Log Files

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 `xxxxx` 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 ***Directing Log Files to a Shared Server***, elsewhere in this section. However, please be sure that the directory name you specify for the log files for each client is unique.

To specify the log file location:

Make sure you have accessed the System Management Hub.

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

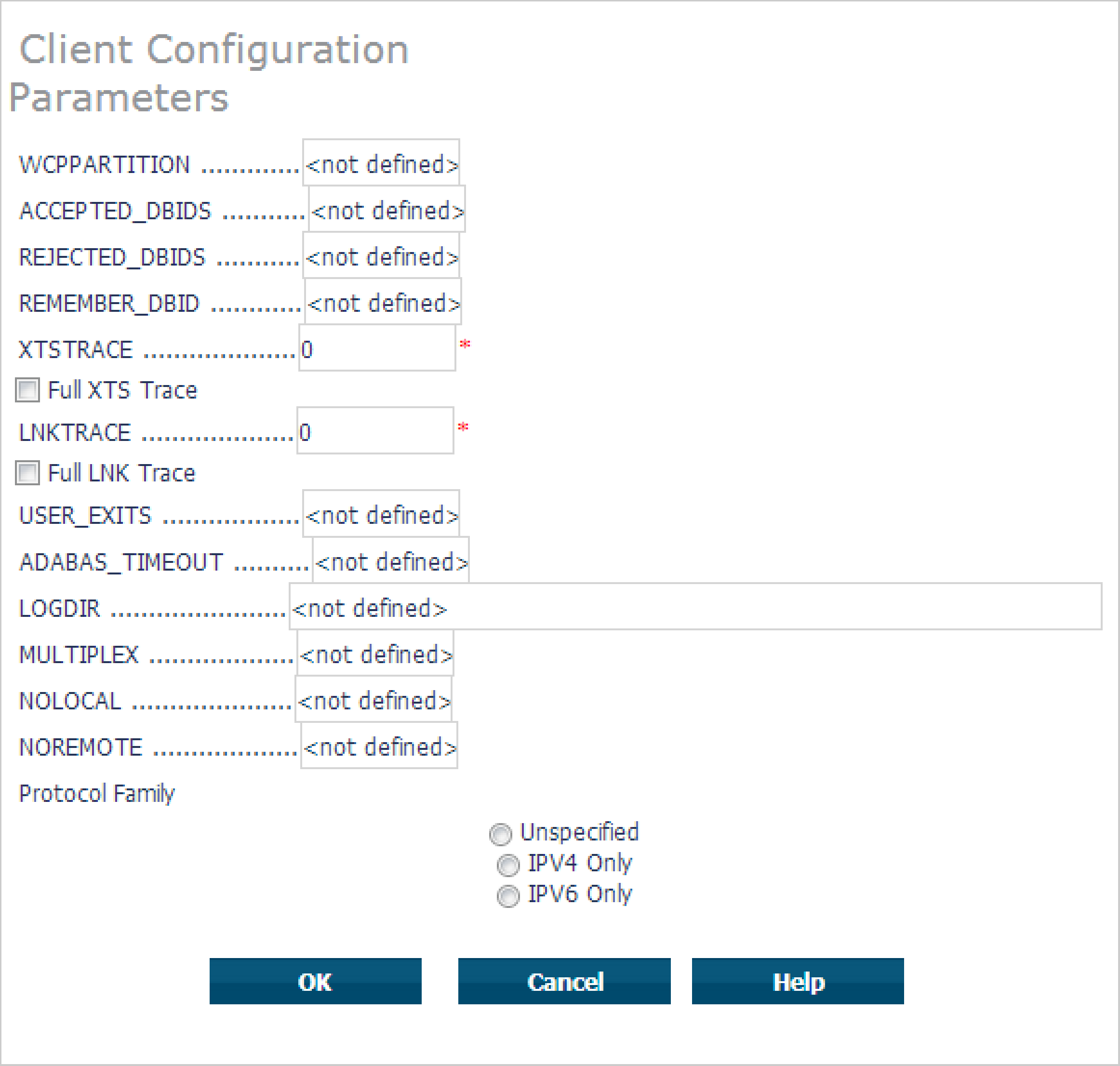
A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

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

The client configuration section becomes available in tree-view.

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

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



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 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.

20 Accessing Secured z/OS Host Resources

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.

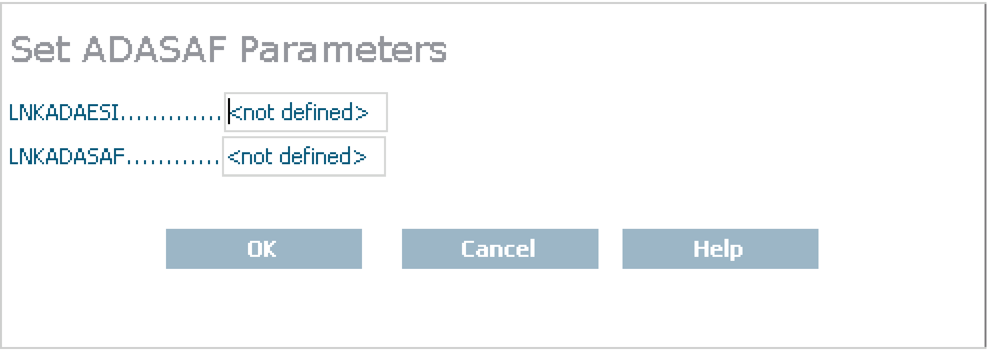
A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

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.



Set ADASAF Parameters

LNKADAESI............ <not defined>

LNKADASAF........... <not defined>

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

Parameter	Description	Required?	Default
LNKADAESI	This parameter is available for Windows systems only. Indicate whether the 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).	No	No
LNKADASAF	Specify the library and function names of the user exit that will provide access to the secured Adabas resource via the Adabas SAF Security Kernel (ADASAF). The library and function names should be specified with a space between them, using the following format: `library function` If no names are specified, ("<not defined>" is listed) and the value "lnkxsaf lnkxsaf" is used. (The lnkxsaf library is either *lnkxsaf.dll* or *lnkxsaf.so*).	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.

Note: 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.

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.

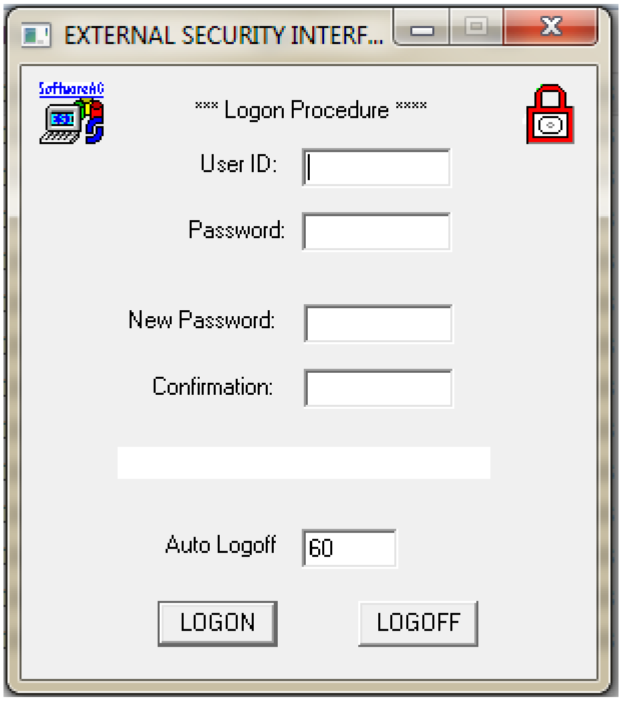
- If the security check is passed, the application is allowed to access those resources that are permitted according to your Adabas security user profile.
- If the security check is not passed, an Adabas security response code is returned to the application.

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.



EXTERNAL SECURITY INTERF...

*** Logon Procedure ****

User ID:

Password:

New Password:

Confirmation:

Auto Logoff 60

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.

21 Using ADALNK User Exits

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.

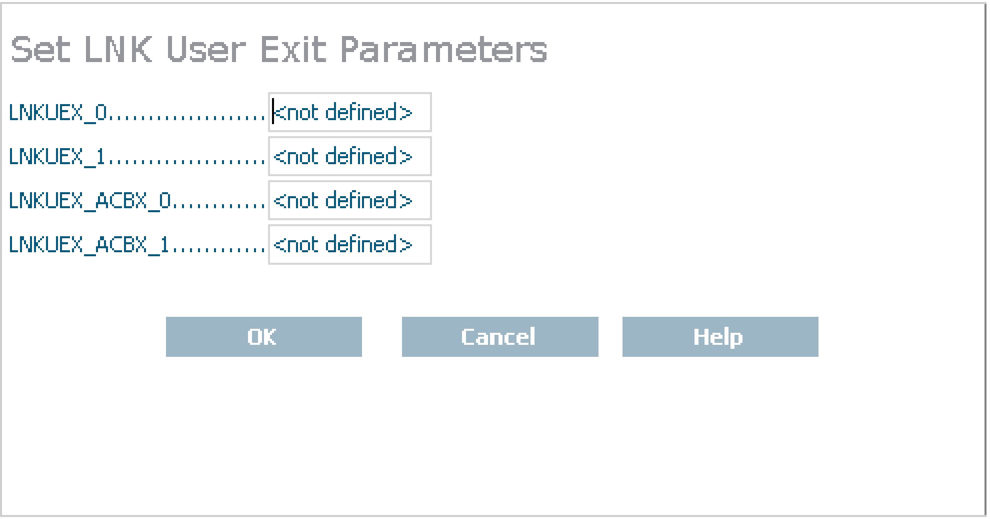
   A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

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>

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 *before* 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 *before* 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 *after* 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 *after* 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 *before* 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 *before* 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 *after* 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 *after* 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
lnkuex.c	The sample user exit and files required to compile and link the ADALNK ACB before and after user exits.
lnkuexacbx.c	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.

22 Changing the Adabas Directory Server

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.

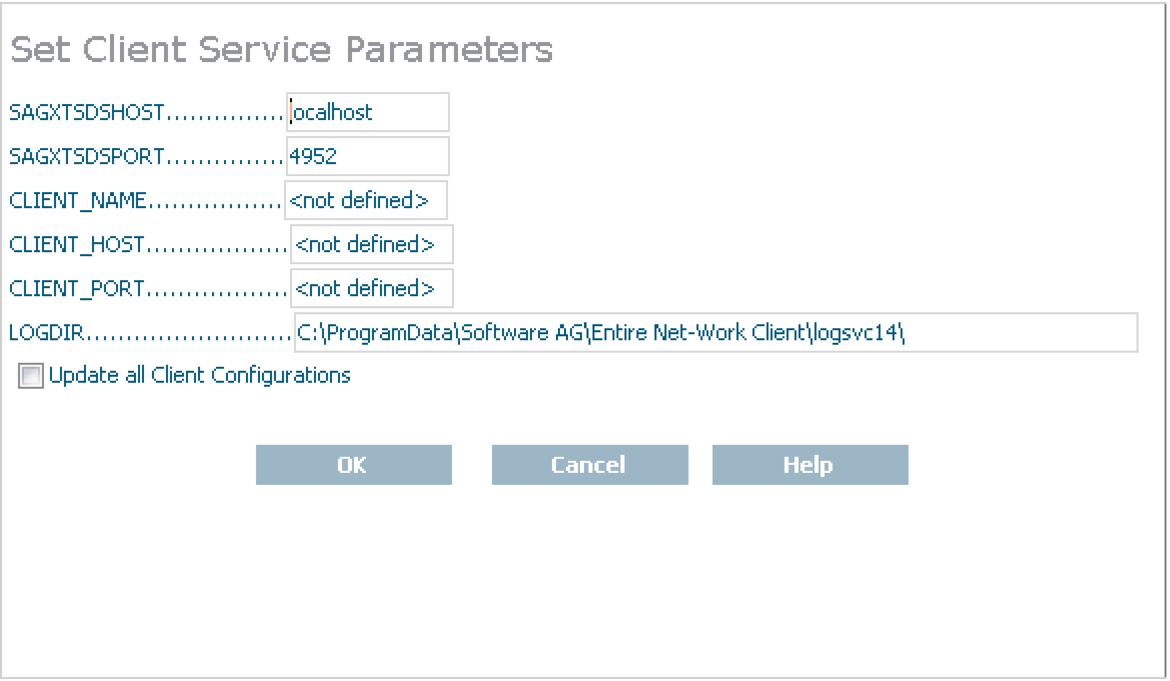
To change the Adabas Directory Server for a client machine:

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

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.

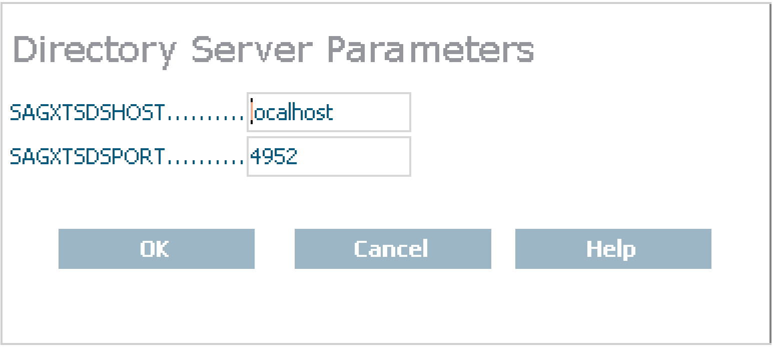
A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

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.



Directory Server Parameters

SAGXTSDSHOST.......... localhost

SAGXTSDSPORT.......... 4952

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.

23 Tracing Entire Net-Work Client Processing

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.

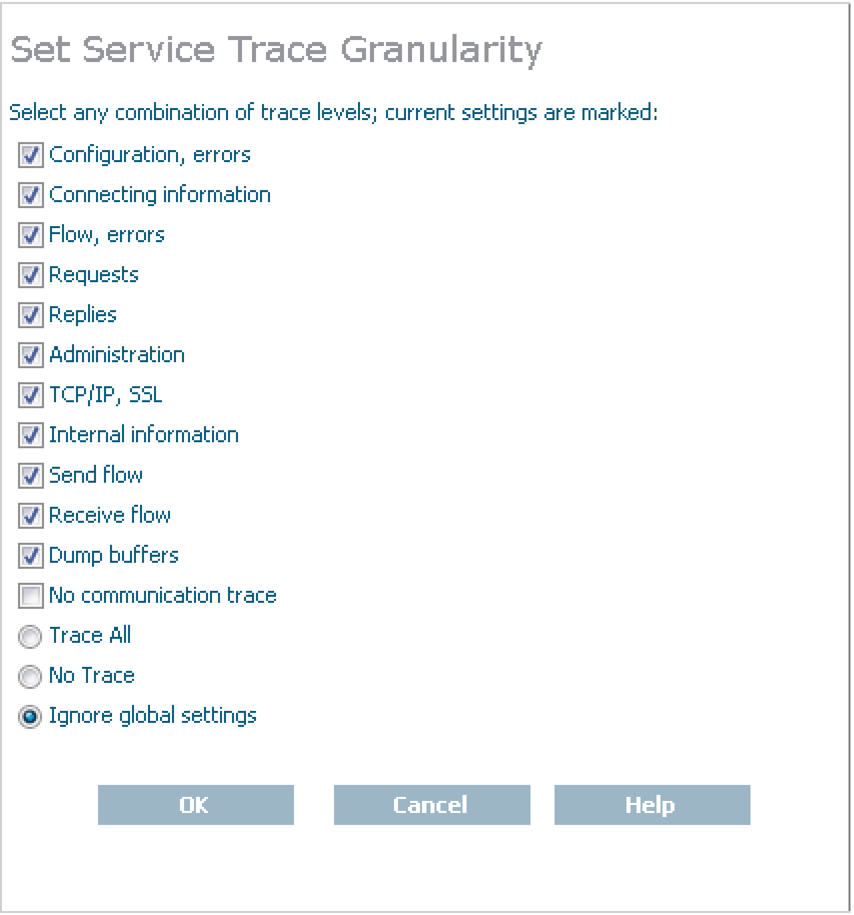
1 Select and expand Entire Net-Work Client from the list in tree-view to access the Entire Net-Work Client administration area.

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

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

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

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

The client service trace levels are set and activated.

Managing Client Tracing

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

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

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

To set the client trace level and activate client tracing:

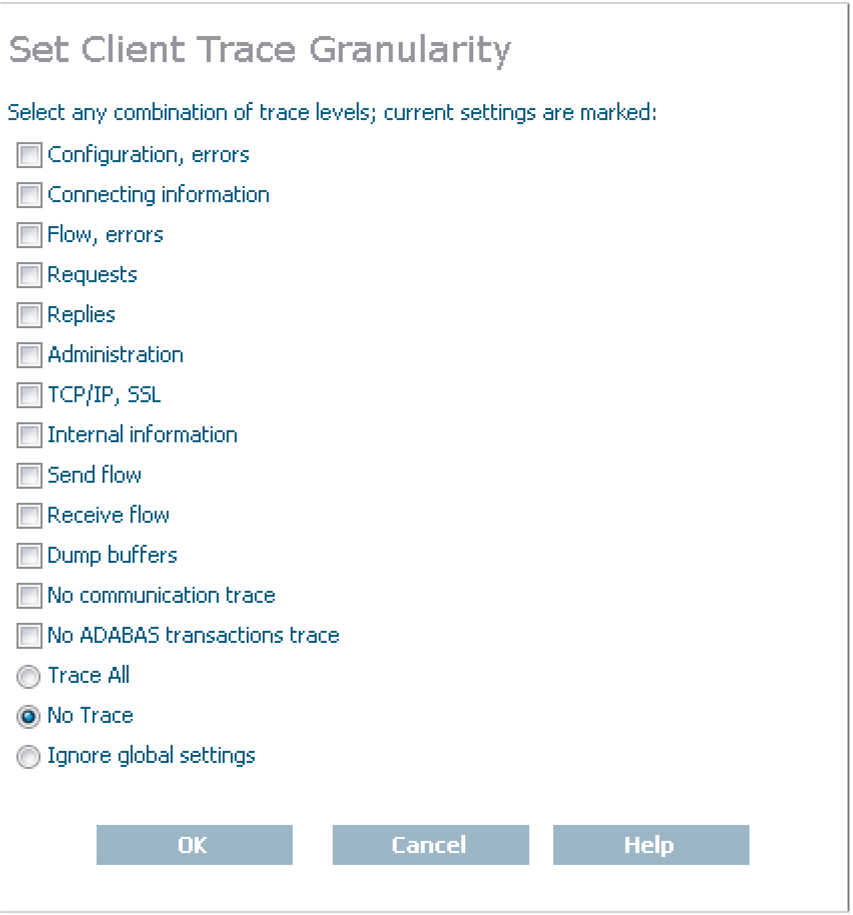
Make sure you have accessed the System Management Hub.

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

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

   The client configuration section becomes available in tree-view.
4. Right-click the client configuration you want from the list and select **Set Client Trace Granularity** from the resulting drop-down menu.

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



Set Client Trace Granularity

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

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

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

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

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

The client trace levels are set and activated.

Managing Software AG Transport Services Tracing

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

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

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

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

Make sure you have accessed the System Management Hub.

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

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

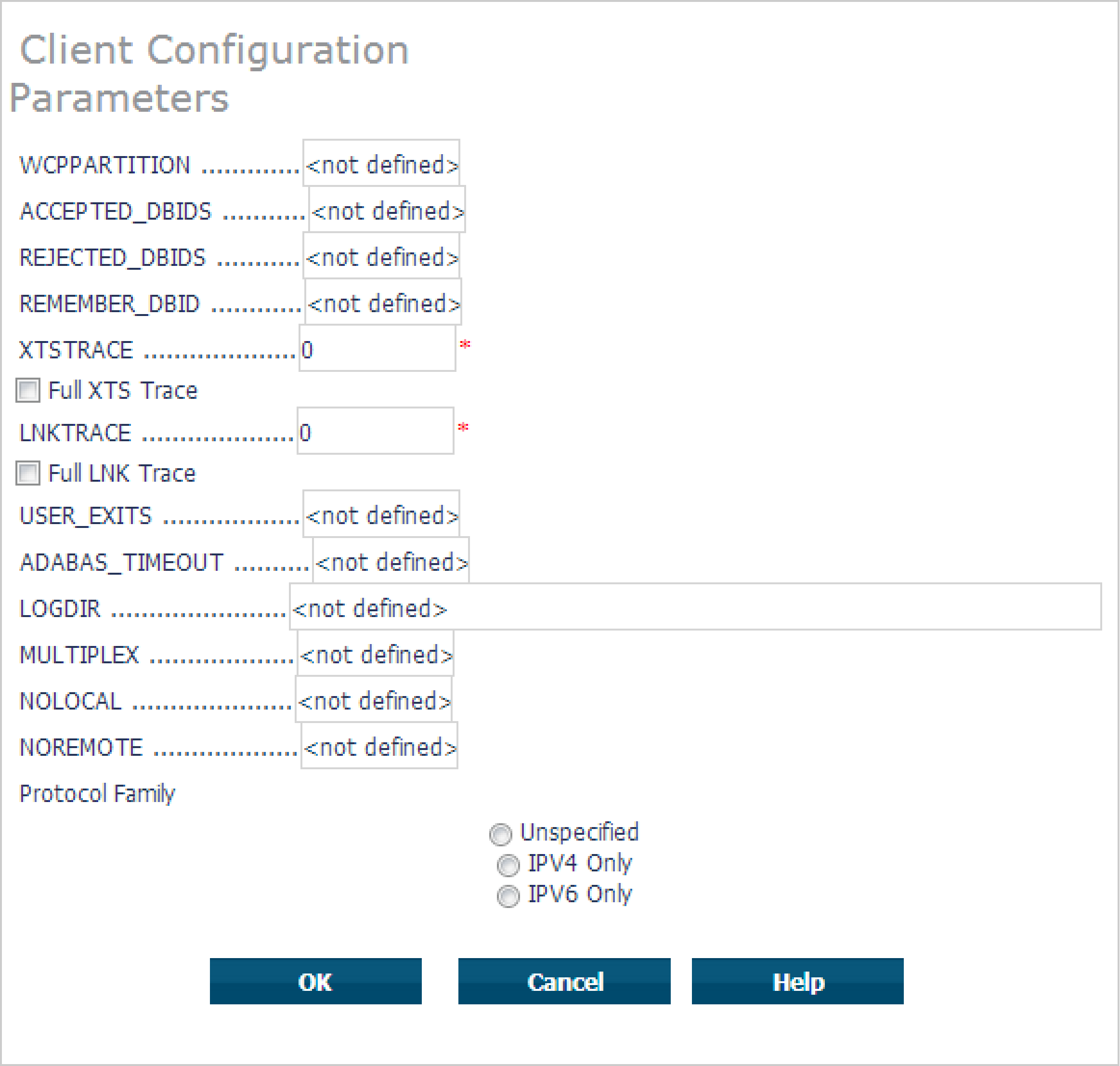
A list of machine names appears. The machines listed are computers on which clients managed by this installation of the System Management Hub are defined.

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

The client configuration section becomes available in tree-view.

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

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



Client Configuration Parameters

WCPPARTITION .... <not defined>

ACCEPTED_DBIDS .... <not defined>

REJECTED_DBIDS .... <not defined>

REMEMBER_DBID .... <not defined>

XTSTRACE .... 0 *

□ Full XTS Trace

LNKTRACE .... 0 *

□ Full LNK Trace

USER_EXITS .... <not defined>

ADABAS_TIMEOUT .... <not defined>

LOGDIR .... <not defined>

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 "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.		

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:

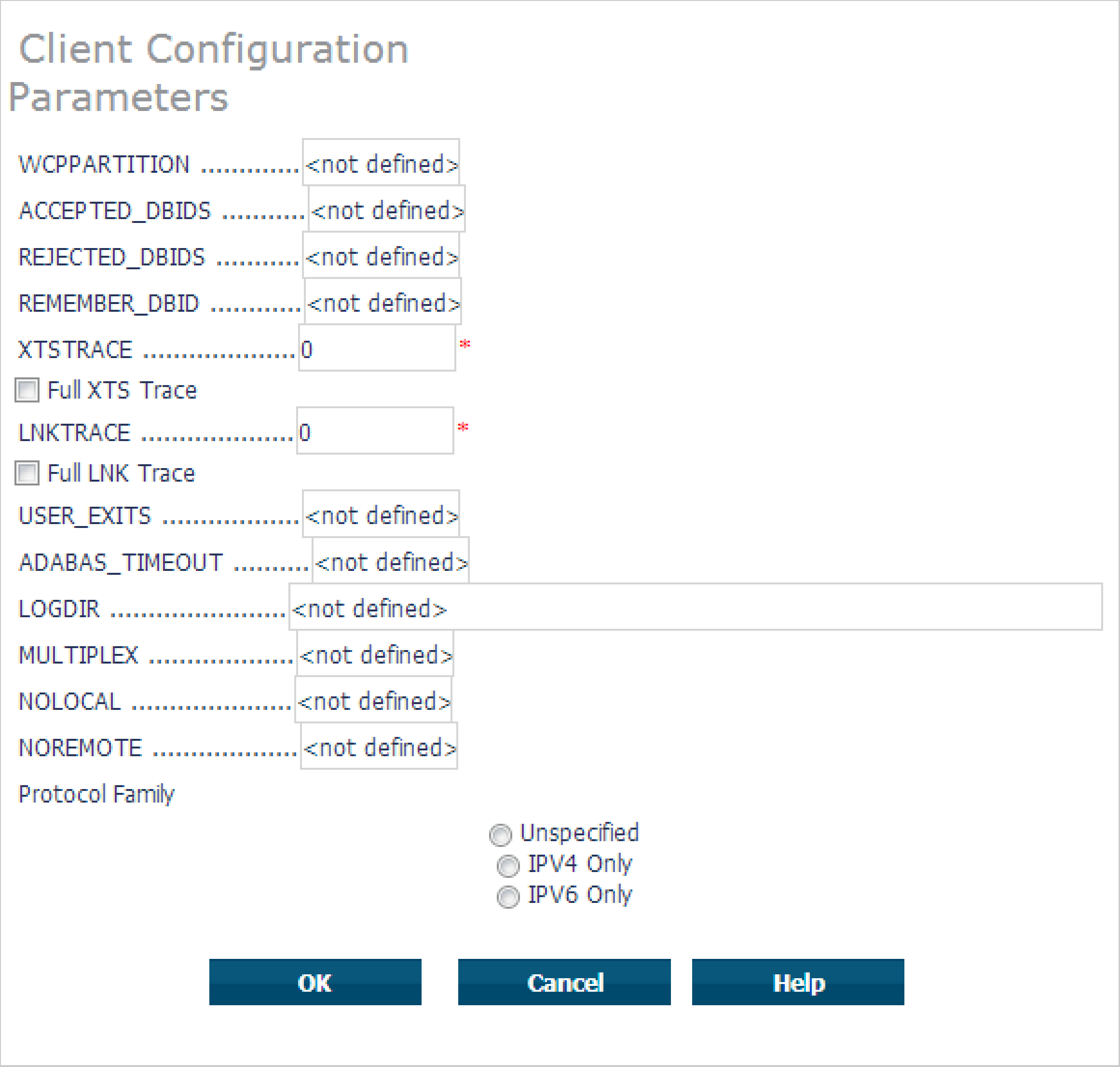
Make sure you have accessed the System Management Hub.

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

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.

24 Directing Log Files to a Shared Server

If you are using Entire Net-Work 7.3.3 or Entire Net-Work Client 1.3 or later, you can direct your Entire Net-Work log files to a shared server.

Caution: To avoid overwriting log files with the same name, log files for individual servers, Kernels, and clients should be stored in directories with unique names.

The process of directing log files to a shared server involves the steps (note that the second step is only required on Windows) described in this chapter.

Step 1. Specify the Log File Locations

Using the System Management Hub (SMH), specify the fully-qualified path of the directory in which you want to store the log files.

Caution: To avoid overwriting log files with the same name, log files for individual servers, Kernels, and clients should be stored in directories with unique names.

- For information on redirecting Entire Net-Work Client log files, read ***Specifying the Client Log File Location***, elsewhere in this guide.

Make sure that your network administrator has allowed your local machine access to the directory and server to which you are redirecting the log files. On Windows systems, you must also complete the next step to do this.

Step 2. Configure the Entire Net-Work and Entire Net-Work Client Windows Services

On Windows systems only, you must configure the Entire Net-Work and Entire Net-Work Client services so that the local host can write to the log files on the shared server.

To update the Entire Net-Work and Entire Net-Work Client Windows services appropriately, follow these steps:

1 Edit the Windows service definition for the Directory Server and select the **Log On** tab.

2 On the **Log On** tab, select the **This account** radio button.

3 Enter a user account name that is known to both this host and the file server where the log files are located. This can be a domain account or a local account that is configured on both machines with the same password. The account should have full control access rights to the log file location.

4 Click the **OK** button.

5 Restart the service.

25 Port Number Reference

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) **Note:** If older versions of Entire Net-Work (older than 7.3) are in use, this port number may need to be changed to 12731.
Entire Net-Work 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.

26 Entire Net-Work Configuration Parameters

Entire Net-Work configuration settings are stored in a series of parameters. Some of these you can change; some you cannot or should not. You can change these configuration settings using:

- Entire Net-Work System Management Hub (SMH) functions. For more information on this, read *Entire Net-Work Client Administration* (in the *Entire Net-Work Client Installation and Administration Guide*) and *Entire Net-Work Server Administration* (in the *Entire Net-Work Server LUW Installation and Administration Guide*).
- Environment variables with the same names as the configuration parameter.

  Caution: Future releases of Entire Net-Work will not support configuration parameter settings in environment variables. For this reason, we recommend that you do not use this method.

- API functions supplied with Entire Net-Work that can also be used in your application programs. Additional information on these functions is provided elsewhere in this chapter.

Configuration Parameter List

The following table describes each of the Entire Net-Work configuration parameters, indicating whether or not you can or should modify its setting, the platforms on which it is available, the default (if any), the name of the SMH parameter that can be used to change it, and the name of the tool that can be used to change it.

Parameter	Description	Can you change it?	Platform Availability	Default	SMH Parameter	Batch Tool
LNKADAESI	whether the external security interface online application should be used instead of a user exit.	yes	Windows	NO	LNKADAESI	AdaSetParameter (set for the LNKADAESI parameter)
LNKADASAF	the library and function names of the user exit that will provide access to the secured Adabas resource via the Adabas SAF Security Kernel (ADASAF).	yes	UNIX and Windows	"lnkxsaf lnkxsaf"	LNKADASAF	AdaSetParameter (set for the LNKADASAF parameter)
LNKTIMEOUT	Global timeout for a response from a remote Adabas call.	yes	UNIX and Windows	1 minute	ADABAS_TIMEOUT	AdaSetTimeout
LNKTRACE	ADALNK and Software AG transport services trace levels.	yes	UNIX and Windows	0 (zero)	LNKTRACE and XTSTRACE	AdaSetTrace

Parameter	Description	Can you change it?	Platform Availability	Default	SMH Parameter	Batch Tool
LNKUEX_0	the file and function names of the user exit that should be called before an Adabas ACB command is sent to the database. **Note:** LNKUEX_0 handling triggers an undocumented Natural feature; if the user exit is called and returns a non-zero response code, but the Adabas command is an RC command, the RC command is suppressed and a successful return is indicated to the calling program.	yes	UNIX and Windows	—	LNKUEX_0	none
LNKUEX_1	the file and function names of the user exit that should be called after an Adabas ACB command is sent to the database.	yes	UNIX and Windows	—	LNKUEX_1	none
LNKUEX_ACBX_0	the file and function names of the user exit that should be called before an Adabas ACBX command is sent to the database. **Note:** LNKUEX_ACBX_0 handling triggers an undocumented Natural feature; if the user exit is called and returns a non-zero response code, but the Adabas command is an RC command, the RC command is suppressed and a successful return is indicated to the calling program.	yes	UNIX and Windows	—	LNKUEX_ACBX_0	none
LNKUEX_ACBX_1	the file and function names of the user exit that should be called after an	yes	UNIX and Windows	—	LNKUEX_ACBX_1	none

Parameter	Description	Can you change it?	Platform Availability	Default	SMH Parameter	Batch Tool
	Adabas ACBX command is sent to the database.					
WCLCODEDIR	the directory where the Entire Net-Work Client code is stored If you want to change the value of this configuration parameter, contact your Software AG support representative.	yes, with assistance	UNIX	local directory	none	none
WCLDATADIR	the directory where the Entire Net-Work Client data is stored If you want to change the value of this configuration parameter, contact your Software AG support representative.	yes, with assistance	UNIX	local directory	none	none
WCPCONFIG	Entire Net-Work configuration file name	yes	UNIX and Windows	local *xts.config*	none	AdaSetParameter (set for the WCPCONFIG parameter)
WCPDIR	the directory where the Entire Net-Work code is stored If you want to change the value of this configuration parameter, contact your Software AG support representative.	yes, with assistance	UNIX and Windows	local directory	none	none
WCPVERS	the Entire Net-Work version If you want to change the value of this configuration parameter, contact your Software AG support representative.	yes, with assistance	UNIX and Windows	—	none	none

Configuration API Functions

This section describes the API functions you can use to set some of the Entire Net-Work configuration parameters.

AdaSetParameter API Function

You can use the AdaSetParameter API function to set values for the following parameters:

- LNKADAESI: Valid values are "YES" (use the external security interface online application) or "NO" (use a user exit). The default is "NO". If LNKADAESI is set to "YES" and a value is given in LNKADASAF, the online application is used (LNKADAESI settings override LNKADASAF).
- LNKADASAF: Specify the library and function names of the user exit that will provide access to the secured Adabas resource via the Adabas SAF Security Kernel (ADASAF). The library and function names should be specified with a space between them, using the following format:

  ```
  library function
  ```

  If no names are specified, the value "lnkxsaf lnkxsaf" is used. (The lnkxsaf library is either *lnkxsaf.dll* or *lnkxsaf.so*).
- WCPCONFIG: Valid values for WCPCONFIG can be any valid file name.

The syntax of the AdaSetParameter API function is:

```
AdaSetParameter("parameter=value")
```

Replace *parameter* with one of the parameter names listed above and *value* with an appropriate value for that parameter.

In the following example, the name of the Entire Net-Work configuration file to be used is set to TEST.CFG:

```
AdaSetParameter("WCPCONFIG=TEST.CFG")
```

AdaSetTimeout API Function

Use the AdaSetTimeout API function to set a global time limit for a response from a remote Adabas call. The syntax of the AdaSetTimeout API function is:

```
AdaSetTimeout(dbid,seconds)
```

Replace `dbid` with a valid Adabas database ID and `seconds` with the number of seconds to use for the global time limit for the specified database.

In the following example, a 60-second timeout period is defined for database 12:

```
AdaSetTimeout(12,60)
```

AdaSetTrace API Function

Use the AdaSetTrace API function to set trace levels for ADALNK and Software AG transport services. The syntax of the AdaSetTrace API function is:

```
AdaSetTrace(level,{TRUE | FALSE})
```

Replace `level` with a valid trace level. Trace levels must be specified in hexadecimal and in the following format:

```
0xllxxxx
```

In the trace level syntax, substitute a hexadecimal value from "00" through "f1" for `ll` to represent the ADALNK trace level. Then substitute a hexadecimal value from "0000" through "FFFE" for `xxxx` to represent the Software AG transport services trace level.

Then specify TRUE or FALSE. If you specify TRUE, the trace level is set globally for all calls; if you specify FALSE, the trace level is set only for the thread in which the call is made.

In the following example, the maximum trace level is specified for both ADALNK and Software AG transport services, but only for the thread in which the call is made:

```
AdaSetTrace(0xf1FFFE,FALSE)
```

In the following example, the maximum trace level is specified for ADALNK calls and no tracing is performed for Software AG transport services. These settings are made globally for all calls:

```
AdaSetTrace(0xf10000,TRUE)
```

AdaSetSaf API Function

Use the AdaSetSaf API function to specify external security interface access information to the user exit that will provide access to the secured Adabas resource via the Adabas SAF Security Kernel (ADASAF). This is the same information you supply using the external security interface online application (read *Accessing z/OS Resources Using the Online Security Application* , in *Entire Net-Work Client Installation and Administration Guide* for more information).

The syntax of the AdaSetSaf API function is:

```
AdaSetSaf(PADASAF_INFO adasaf_info")
```

Replace `adasaf_info` with the name of a data structure that provides information in the following format:

```
  CE_CHAR  cUserID[8];         /* UserID                              */
  CE_CHAR  cPassword[8];       /* Password                            */
  CE_CHAR  cNewPassword[8];    /* NewPassword                         */
```

In the following example, the data structure "mysaf" is used to provide appropriate external security interface access information to secured Adabas resources via ADASAF:

```
AdaSetSaf(PADASAF_INFO mysaf
```

27 Entire Net-Work Utility Functions for the Directory Server (checkadi and setadi)

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 forEntire Net-Work Client). You should also specify the host name and port number parameters. The XTSTRACE parameter is optional; if you do not specify it, a default value of "65534" is used.

Note: While you can use setadi to change the Directory Server used, the changes only affect the configuration of the services and agents. It will not change the Directory Server assigned to any existing Kernels.

Example 1

In the following example, help for setadi is displayed, but no access parameters are set.

```
setadi
```

The following sample output from such a setadi request might appear:

```
Software AG Entire Net-Work, Copyright ©) 1997-2011 by Software AG
Usage: setadi <options...>
The following options are supported:
WCP|WCL
HOST=host name
PORT=port value
XTSTRACE=value (65534)

WCP|WCL -  the user selects which product to set, WCP or WCL
```

Example 2

In the following example, an Entire Net-Work entry for host "localhost" at port "12731" is defined. The default XTSTRACE value of "65534" is used.

```
setadi WCP host=localhost port=12731
```

The following sample output from such a setadi request might appear:

```
Software AG Entire Net-Work, Copyright ©) 1997-2010 by Software AG
argv[2] host=localhost
argv[3] port=12731
Check Host=localhost
Check Port=12731
Server is Active; check if this is a Directory Server
Select Data from Directory Server successful
Bytes ready to read=309
Response=0x010x33  0x760x310x090x720x650x730x700x6f0x6e0x730x650x090x09
Expected=                0x760x310x090x720x650x730x700x6f0x6e0x730x650x090x09
Directory Server is Active
CODEPATH=C:\Program Files\Software AG\Entire Net-Work Server\v74\
DATAPATH=C:\Documents and Settings\All Users\Application Data\Software AG\Entire ↩
Net-Work Server\
Changing C:\Documents and Settings\All Users\Application Data\Software AG\Entire ↩
Net-Work Server\service74.config
Changing C:\Documents and Settings\All Users\Application Data\Software AG\Entire ↩
Net-Work Server\agents\xts.config
Configuration file change successful
Setadi exiting ...
```

Index