software AG

Entire Net-Work Administration

Installation and Administration

Version 1.3.3

June 2014

Table of Contents

Preface

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

This document is organized as follows:

Entire Net-Work Client Installation	Describes the installation of Entire Net-Work Client in Windows and UNIX environments.
Required Post-Installation Updates for Simple Connection Line Driver Support	Describes the required post-installation updates you must make to support the Simple Connection Line Driver.
Starting and Stopping Entire Net-Work Client	Describes how to start and stop Entire Net-Work Client.
Entire Net-Work Client Administration	Describes management tasks for Entire Net-Work Client.
Using the Entire Net-Work User Exit Interface	Explains the Entire Net-Work user exit interface in open systems.
Software AG Directory Server Documentation	Describes how to use the Software AG Directory Server.

1   Conventions

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

2   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 Software AG Directory Server entries have been migrated for Entire Net-Work, your client should be immediately able to access the Adabas databases it needs.

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

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

- **The System Management Hub (SMH)**

- **The Software AG Directory Server**

- Entire Net-Work Client and the code necessary to maintain it in SMH

- A default client configuration.

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

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

Directory Server

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

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

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

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

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

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

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

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

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

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

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

System Management Hub (SMH)

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

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

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

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

SSL Support

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

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

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

3   Understanding Partitioning

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

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

Here are some of the advantages of partitioning:

- You can use partitioning to direct Entire Net-Work Clients and Kernels to specific databases.

- If you have created Adabas databases with identical database IDs, you can use partitioning to correctly identify which client calls get directed to which Adabas database.

- You can use partitioning to group client calls to an Adabas database, thus reducing the number of actual connections required for that database. This can be especially useful if you are using an Entire Net-Work mainframe product to access a specific Adabas database. It also provides you with some level of client control: if you want to remove access to a specific database for clients in a given partition, simply remove the access URL entry for that database (using the System Management Hub) or stop the Kernel in that partition.

- Using SSL, you can use impose real security requirements on calls made by clients in specific partitions.

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

4   Understanding Filtering

Entire Net-Work supports filtering of Entire Net-Work Client configurations and Entire Net-Work 7.3 Kernel definitions by Adabas database ID. In this way, individual Entire Net-Work Client configuration definitions and Entire Net-Work 7.3 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 be accessed by the client. If no databases are listed in the **ACCEPTED_DBIDS** field, all databases defined in the Software AG Directory Server can be accessed except those listed in the **REJECTED_DBIDS** field. Likewise, if no databases are listed in the **REJECTED_DBIDS** field, all databases in the Directory Server can be accessed, unless a specific list is provided in the **ACCEPTED_DBIDS** field.

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

Filtering in Kernel Definitions

You can filter Kernels by requests made:

■ made to specific Adabas database IDs

■ relayed to other Kernels

■ submitted from other Kernels, by Kernel name

This section covers the following topics:

- Filtering Requests to Adabas Databases
- Filtering Relay Requests to Other Kernels

- Filtering Requests from Other Kernels

Filtering Requests to Adabas Databases

For Entire Net-Work 7.3 Kernel definitions, database filtering is specified on the **Kernel Basic Parameters** panel and allows you to identify databases for which service requests should be processed by the Kernel. If no databases are listed in the **ACCEPTED_DBIDS** field, the Kernel will process all requests to all databases defined in the Software AG Directory Server, except those listed in the **REJECTED_DBIDS** field. Likewise, if no databases are listed in the **REJECTED_DBIDS** field, the Kernel will process all requests to all databases defined in the Software AG Directory Server, unless a specific list is provided in the **ACCEPTED_DBIDS** field.

For more information on setting these Kernel parameters, read *Setting Basic Parameters*, 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 the **RELAY_TRAFFIC** parameter, read *Setting Basic Parameters*, 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 described later in this section.

  For more information on setting the **UNSOLICITED** parameter, read *Setting Advanced Parameters*, in your Entire Net-Work Server documentation.

- You can use the 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 the Kernel Filter List*, in your Entire Net-Work Server documentation.

5   Entire Net-Work Client 1.3 Release Information

This chapter describes the changes, enhancements, migration considerations, and documentation for this release.

1.3.3 Enhancements

This version of the Entire Net-Work Client introduces support for Windows 7 and Windows Server 2008 platforms. Entire Net-Work Client can now be installed and managed in these environments.

1.3.1 Enhancements

Entire Net-Work Client 1.3.1 is a complete replacement for any prior version of Entire Net-Work Client.

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

The following enhancements have been made to this release of Entire Net-Work Client:

- This version of the Entire Net-Work Client introduces support for Windows Vista platforms. Entire Net-Work Client can now be installed and managed in Windows Vista environments.

- For consistency, the installation directories of this version of Entire Net-Work Client have been reorganized on any platform so that they mirror the organization required and established on Windows Vista platforms. In past releases, the code and data of an Entire Net-Work Client installation were intermixed in the installation directories. In parallel with the Windows Vista installation requirements, the code and data of an Entire Net-Work Client installation are now separated into separate subdirectories -- regardless of the platform on which you install Entire Net-Work Client.

  While this has no affect on the migration of your Entire Net-Work Client configuration to Entire Net-Work Client 1.3 (during installation the files are reorganized automatically), it does impact where you can find your configuration and log files. Entire Net-Work executable and library files (the code files) are still stored in the following locations:

  - In Windows environments: `Program Files\Software AG\Entire Net-Work Client`

  - In UNIX environments: `$SAG\wcl\v`*nn*, where *nn* is the release number.

  However, data files (including configuration and log files and user exit libraries) are stored in 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 Vista environments: `ProgramData\Software AG\Entire Net-Work Client\`

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

■ This version of Entire Net-Work Client supports Software AG Directory Server 5.3, which introduces the ability to set up a failover Directory Server. This is a useful new feature you can use to ensure that if one Directory Server goes down, a second Directory Server automatically runs in its place. Both Directory Servers use the same configuration file and share a network alias name. Directory Server clients (machines that will make use of the Directory Server, such as Entire Net-Work or Tamino) refer to the pair of Directory Servers via their shared network alias name.

For more information about the use and configuration of a failover Directory Server, read *Configuring a Failover Directory Server*, elsewhere in this guide.

■ This version of Entire Net-Work Client includes an External Security Interface (ESI) for ADASAF support that provides access to secured Adabas resources on a z/OS host node. For more information about ESI, read *Accessing Secured z/OS Host Resources*, elsewhere in this guide.

■ This version of Entire Net-Work Client now allows you to call user exits before and after ACB and ACBX direct calls, if the Adabas interface supports user exits. For more information about these user exits, read *Using ADALNK User Exits*, elsewhere in this guide.

■ A number of log file changes have been made in this release of Entire Net-Work Client:

1. The log file names have been changed for Entire Net-Work Clients. The new log file names are described in *Starting a New Entire Net-Work Client Log File* , in the *Entire Net-Work Client Installation and Administration Guide*.

2. You can now specify the directory location of your log files for Entire Net-Work Clients. For more information, read *Specifying the Client Log File Location*, in the *Entire Net-Work Client Installation and Administration Guide*

   If you want to store your log files on a shared server, read *Directing Log Files to a Shared Server*, in the *Entire Net-Work Client Installation and Administration Guide*.

Migration Considerations

If the Software AG Directory Server is installed and used by a prior version of Entire Net-Work Client, be sure to use the existing Software AG Directory Server port number setting for the Entire Net-Work Client 1.3 installation. You can change the port number after Entire Net-Work Client 1.3 is installed. For complete information on changing the Directory Server port number used, read *Changing the Software AG Directory Server Port Number*, elsewhere in this guide.

To migrate from an older version of Entire Net-Work Client to Entire Net-Work Client 1.3, you need only install 1.3. Your older Entire Net-Work Client configurations will automatically be migrated during the installation process.

> **Note:** When you install Entire Net-Work Client 1.3 on a Windows system running an older version of Entire Net-Work Client, the older Entire Net-Work Client installation is automatically uninstalled. However, on UNIX systems, the older Entire Net-Work Client installation must be removed manually. Entire Net-Work Client Installation and Administration Guide

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.

Dropped Features

Support for 32-bit Linux operating systems will be dropped in a *future* version.

Documentation

The documentation for this product is new with this release. If you have an Empower account, current, updated, and past versions of the documentation can be reviewed and downloaded by linking to the Software AG documentation, found on Software AG's **Empower** web site. 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).

The Entire Net-Work Client documentation includes:

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

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

The System Management Hub documentation can be found in the System Management Hub installation. For example, if SMH is installed in Windows at *C:\Program Files\Software AG\ System*

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

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

Viewing Software AG Product Documentation under Windows XP SP2

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

The active content for which Software AG is responsible, that is, the JavaScript code in our HTML documentation pages, will not harm your computers. The risk in using the navigation applets is negligible: Software AG has received no reports from users concerning any harm caused to a computer by the applets. We therefore suggest that when reading Software AG documentation in a local context, you should allow active content via the Security settings in the browser (with Internet Explorer, usually found under Tools > Internet Options > Advanced).

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

6 Platform Coverage, Prerequisites, and Restrictions

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

Supported Platforms

Entire Net-Work 7.3 and Entire Net-Work Client 1.3 support the following platforms:

- Windows 2000 Professional
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2003 Standard Server
- Windows 2003 Enterprise Server
- Windows XP Professional
- Windows Vista

> **Note:** Entire Net-Work does not support Windows NT or Windows 2000 Data Center.

Space and Memory Requirements

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

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

  On OpenVMS systems : 20MB disk space for the Software AG Directory Server, 33MB disk space for Entire Net-Work Client, and 30MB disk space for Entire Net-Work (with no log files)

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

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

Firewall Requirements

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

Prerequisite Software AG Products

Adabas 3.3.1 patch level 9 or later is a prerequisite for Entire Net-Work Server 7.3. Using older Adabas patch levels or versions may lead to hanging transactions.

Entire Net-Work uses the Software AG Directory Server as well as System Management Hub (SMH), which can be installed from the Entire Net-Work CD. In addition, Entire Net-Work Server is used to provide communications with Adabas databases and as a concentrator for non-Adabas servers (such as EntireX Communicator, Tamino, and Adabas SQL Gateway). For information regarding which releases of these Software AG products are currently supported, refer to the documentation for the appropriate product.

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

If the Software AG Directory Server is installed and used by a prior version of Entire Net-Work, be sure to use the existing Software AG Directory Server port number setting for the Entire Net-Work 7.3 installation. You can change the port number after Entire Net-Work 7.3 is installed. For complete information on changing the Directory Server port number used, read .

Restrictions

The following restrictions exist in Entire Net-Work 7:

- The MHDR protocol is not supported.

- RDA-based calls do not support two-byte database IDs; therefore access is limited to database IDs less than 256. If your application needs to access a mainframe database with an ID greater than 255, you must use Entire Net-Work e-business connections or the TCP/IP protocol with

the Entire Net-Work mainframe Simple Connection (TCPX) Line Driver. For more information, read your Entire Net-Work mainframe documentation.

7 Configuration Considerations

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

Category	Question	Considerations
System Management Hub (SMH)	Is SMH already installed in your enterprise?	If SMH is already installed in your enterprise, it should not be installed again. Only one SMH is required to manage all Software AG products that require it. If SMH is not installed in your enterprise, you must install it when you install Entire Net-Work. Read *Installing Management Components*, elsewhere in this guide, for more information.
System Management Hub and Software AG Directory Server	Should you install Entire Net-Work management components on the same machine as Entire Net-Work clients?	Although you are able to install management components on the same machines as Entire Net-Work clients, Software AG does not recommend it. There are two reasons for this recommendation: ■ Your system performance could be impacted. ■ In Windows environments, problems will arise if the Entire Net-Work client service is started before the Directory Server service. The Directory Server service must be started before any Entire Net-Work service. We recommend, therefore, that the Directory Server be installed on a stable machine, separate from Entire Net-Work clients, that is not frequently rebooted.
Software AG Directory Server	Is a Directory Server already installed in your enterprise?	If a Directory Server is already installed in your enterprise, you do not need to install another, although you may if you wish. Read *Installing Management Components*, elsewhere in this guide, for information on the pros and cons of installing more than one Directory Server.

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

8 Installing Management Components

The management components used by Entire Net-Work 7 are the System Management Hub (SMH) and the Software AG Directory Server. These components:

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

◾ Can be installed together on the same machine or individually on separate machines. To reduce resource consumption, Software AG recommends that you install them on the same machine.

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

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

Installation Considerations for SMH

Only one System Management Hub (SMH) should be installed in your enterprise. It can be used to manage all Software AG products that use it. However, if you elect to install SMH while running a Entire Net-Work Client or Entire Net-Work Server installation, the installation automatically checks to see if SMH is already installed on the machine and will either update the installed version or perform a new installation of SMH. It will also install the SMH agents specific to Entire Net-Work (one agent is required for Entire Net-Work Client and one is required for Entire Net-Work Server).

If SMH has already been installed in your enterprise, you still need to run the SMH installations supplied with the Entire Net-Work Client and Entire Net-Work Server installations on the machine where SMH is installed to ensure that the Entire Net-Work Client or Entire Net-Work Server SMH agents get installed. Prompts to install the SMH agents are provided during the Entire Net-Work Client and Entire Net-Work Server installations.

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

📄   **Notes:**

1. SMH is not available in OpenVMS environments. Therefore, you must use SMH in Windows or UNIX to perform Entire Net-Work for OpenVMS administration tasks.

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

Installation Considerations for the Software AG Directory Server

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

▪ You will have to manage and administer multiple Directory Server configurations.

▪ You will need to be very careful about which Directory Server you select to use in your installations of Entire Net-Work Client and Entire Net-Work Server -- especially if other Directory Servers have been installed by other Software AG products.

▪ As you are restricted to a single pointer to a Directory Server in your DNS (via its SAGXTSDSHOST and SAGXTSDSPORT entries), all systems required to use a different Directory Server must be redirected using local, manual, administration. For more information on this manual administration, contact your Software AG technical support representative.

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

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

If you decide to install a Directory Server on the current machine during the installation of Entire Net-Work Client or Entire Net-Work Server, select the **Custom** installation type and then select **Directory Server** as one of the components to be installed.

In an OpenVMS installation, the installation of a Directory Server occurs as part of the polycenter installation if requested. You can also install a Directory Server later by running the *installadi.com* procedure. This procedure prompts you for the Directory Server port number and creates the *adienv.com* environment file and all of the other needed command procedures required to run Directory Server in OpenVMS. The *adienv.com* environment file contains the following environment settings:

Environment Setting Name	Default Setting
ADIDIR	SAG$ROOT:[ADI]
ADIVERS	V521

If SMH has already been installed in your enterprise, you still need to run the SMH installation supplied with the Software AG Directory Server installation code. This SMH installation for Directory Server should be run on the machine where SMH is installed. This will ensure that the Software AG Directory Server SMH agents get installed properly. Prompts to install the Directory Server SMH agents are provided during the Software AG Directory Server installation.

9 Entire Net-Work Client Installation

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

Entire Net-Work Client License Key	Describes the Entire Net-Work Client license key, where to find it, and how it gets implemented.
Installation Prerequisites	Describes the prerequisites you should meet before you install Entire Net-Work Client.
Entire Net-Work Client Installation Steps	Describes the steps necessary to install Entire Net-Work Client.
Uninstalling Entire Net-Work Client	Describes the steps necessary to uninstall the Entire Net-Work Client components in Windows and UNIX environments.

10   Entire Net-Work Client License Key

A permanent license is required in order to run the Entire Net-Work Client. Every time the Entire Net-Work Client software starts, the license key file is read and the validity of the license key is checked. So, you will be required to specify the location of a license key file that contains your Entire Net-Work Client license key during the installation procedure. The license key you specify for an Entire Net-Work Client installation is not the same license key you specify for an Entire Net-Work Server installation.

This chapter contains the information on license keys for Entire Net-Work Client.

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

License Key File Location and Use

The Entire Net-Work Client license key file is generally distributed on diskette, although, in special cases, it can be shipped via e-mail. The file name is in the following format, where *vr* is the version and release number of the product: *wclvrm.xml*.

Be sure that the file containing the license key is in a location that will be accessible during the Entire Net-Work Client installation, such as on the file system or in a disk drive. During the installation of Entire Net-Work Client with the InstallShield, you are asked to locate the license file. Once it is located, the license file will be copied into a Software AG common area.

If you are installing Entire Net-Work Client on a laptop and you have received your license file on a diskette, note that some laptop configurations do not allow you access to the CD-ROM drive and the diskette drive simultaneously. In such cases you must copy the license file to a location that is accessible while the CD-ROM drive is in use, such as your laptop's hard disk, before you start the installation procedure. In general, Software AG recommends that you place the license file on the file system before starting the installation procedure.

> 🗎 **Note:** The license file is sometimes transmitted via e-mail. If you received the file via e-mail, copy it to a directory on your hard drive. If you received the file on a floppy disk, you may leave it there.

The License Key File

The license key file is provided as an XML document. This document can be viewed, using a browsing tool or text editor. It contains text, which represents the licensing information and a digital signature. It displays Software AG legal notices, copyright information, etc., as well as the product license information.

Caution: Any modification of the license key file will invalidate the digital signature and the license key check will fail. If the check fails, you will not be able to install or run the product. In the event of a check failure, please contact your Software AG Support representative.

11 Installation Prerequisites

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

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

2. Disable any antivirus software.

3. Ensure the target computer is connected to the network.

4. Verify the license key files are copied somewhere in your environment or have the diskette available. Entire Net-Work Client will not run without valid license keys. For more information, read *Entire Net-Work Client License Key*, elsewhere in this guide.

5. Read the *Entire Net-Work Client Release Notes*, *Configuration Considerations*, and *Concepts* (earlier in this guide).

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

6. Determine whether or not the Entire Net-Work management components (Software AG Directory Server and System Management Hub) need to be installed as part of this Entire Net-Work Client installation.

   If SMH is already installed in your enterprise, you should run the Entire Net-Work Client installation on the machine on which SMH is installed to install the Entire Net-Work Client agent required to maintain Entire Net-Work Clients (for more details, read *Installation Considerations for the SMH*, elsewhere in this guide).

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

Server are allowed (for more details, read *Installation Considerations for the Software AG Directory Server*, elsewhere in this guide).

12 Entire Net-Work Client Installation Steps

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

> **Notes:**

1. We recommend that you use only one Directory Server for all Software AG products that require it.

2. Do not install both Entire Net-Work Client and Entire Net-Work 7.2 Client on the same machine.

3. Ideally, the installation of Entire Net-Work Client should be performed by a system administrator or someone with administrator privileges.

4. The steps provided in this chapter will install only an Entire Net-Work Client on the machine. Be aware that the sequence of steps will vary if you are installing one of the Entire Net-Work management components (SMH or the Software AG Directory Server) as well.

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

Installing Entire Net-Work Client on Windows Platforms

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

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

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

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

2   Locate and run the *setup.exe* file found in the root directory or in the *\windows\wcl* subdirectory on the CD-ROM.

   The Welcome panel appears.

3   Follow the prompts on the installation panels. The following panels should be noted:

   ▪ When you get to the **Setup Type** panel, select the type of installation you wish to perform.

      The following table summarizes the selections on the **Setup Type** panel.

Installation Type	Description
Client Mode	Installs an Entire Net-Work Client only.
Custom	Allows you to choose particular components to install, including the Entire Net-Work Client, the Software AG Directory Server, and the System Management Hub (SMH) and allows you to direct the installation to a specific directory and to specify a program folder name for the installation. If SMH is also installed on this machine, be sure to run the installation of SMH during this installation process to ensure that the appropriate Entire Net-Work Client SMH agents get installed. For more information, read *Installing Management Components*, elsewhere in this guide.

■ When the **License File** panel appears, type the fully qualified name of the **license file** in the **License File** text box, or click the **Browse** button to locate it. The same license file should be used for Entire Net-Work 7 Clients as are used for Entire Net-Work Kernels.

> **Note:** The **license file** is sometimes supplied on a floppy disk delivered with Entire Net-Work.

■ The **Directory Server Detection** panel may appear. If a Directory Server is already installed on this machine, the installation assumes that the local Directory Server will be used and the **Directory Server Detection** panel does not appear. If the **Directory Server Detection** panel appears, select one of the options on it to indicate whether or not you want to use the named Directory Server or whether you want to install one on this machine. For complete information on the port used by the Directory Server, read *The Directory Server Port Number*, in the *Software AG Directory Server Administration Guide*.

■ Software AG installs a Common Java Package (CJP) as part of the underlying infrastructure of its components. During the Entire Net-Work installation, the following message may appear as a result of this CJP installation:

```
You must restart your system for the configuration changes made to Software ↵
AG Common Java Package to take effect. Click Yes to restart now or No if you ↵
plan to restart later.
```

To address this situation, complete the following steps:

1. Select "Yes" when prompted to restart your system.

2. Close any open installation dialogs and reboot the machine.

3. Restart the Entire Net-Work installation, using the exact same settings as you used in your earlier installation attempt.

The installation should complete without problems.

If the installation is not successful, you will receive one of several possible error messages. Contact your local distributor for information about customer support services. If the installation fails, it

is likely that some parts of the product will have been installed. Therefore, before you attempt to install Entire Net-Work again, run the installation program to remove it. See *Uninstalling Entire Net-Work Client*, elsewhere in this guide, for instructions on removing the product.

13   Uninstalling Entire Net-Work Client

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

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

Uninstalling Entire Net-Work Client on Windows

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

📄 **Notes:**

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

2. Uninstalling will stop Entire Net-Work Client.

3. Uninstalling will remove the license file.

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

- Entire Net-Work Client-specific software

- Software AG Directory Server software

- Software AG's System Management Hub (SMH)

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

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

1 If you are running the Entire Net-Work Client as a Windows service, stop the service before you start these steps. This uninstallation procedure will uninstall the service, but it cannot do so if the service is running. If you do not uninstall the service (or if its uninstallation fails) and you try to reinstall Entire Net-Work Client later, errors will occur when you try to use your new Entire Net-Work installation.

2 Go to Start/Settings/Control Panel.

3 Select **Add/Remove Programs**.

4 Select **Software AG Entire Net-Work Client** *v.r.m* (where *v.r.m* are the version, release, and modification levels of the Entire Net-Work code) and click on the **Change/Remove** button.

The InstallShield Wizard is invoked.

5   Select **Remove** on the **Welcome** panel and click **Next**. Click **OK** for any verification messages.

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

6   You may be prompted for the uninstallation of the Software AG Directory Serverand SMH. In these cases, select the option appropriate for your site. If these components are needed by other Software AG products that are still installed, do not uninstall them.

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

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

14 Required Post-Installation Updates for Simple Connection Line Driver Support

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

You can do this in one of two ways:

- You can add them on your local machine by adding an Adabas access definition to a client configuration in SMH. Specifically, one Adabas access definition must be added for each open systems Adabas database you want to access using the Simple Connection Line Driver. For more information, read *Adding Adabas Access Definitions* , elsewhere in this guide.

- You can manually set up Directory Server target entries for the Adabas open systems databases in the Directory Server that the client uses. Specifically, one XTSaccess (access) target entry must be created in the Directory Server for each open systems Adabas database you want to access using the Simple Connection Line Driver. You can add these target entries using SMH.

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

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

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

15 Configuring Entire Net-Work Components for Windows XP Personal Firewall

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

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

Allow Ports for a Specific Executable Program

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

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

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

Component Name	Default Path and File Name
Entire Net-Work Kernel program	*C:\Program Files\Software AG\Entire Net-Work Server\v731\wcpkernel.exe*
Entire Net-Work Client Service	*C:\Program Files\Software AG\Entire Net-Work Client\wclservice.exe*
Entire Net-Work Server Service	*C:\Program Files\Software AG\Entire Net-Work Server\v731\wcpservice.exe*
Software AG Directory Server Service	*C:\Program Files\Software AG\Directory Server\xtsdssvcadi.exe*
System Management Hub (SMH) CSLayer Service	*C:\Program Files\Software AG\System Management Hub\bin\argsrv.exe*
System Management Hub (SMH) EventLayer Service	*C:\Program Files\Software AG\System Management Hub\bin\argevsrv.exe*
System Management Hub (SMH) MILayer Service	*C:\Program Files\Software AG\System Management Hub\bin\argmlsrv.exe*

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

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

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

Open a Specific Port

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

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

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

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

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

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

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

16 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.

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

Automatically Starting Entire Net-Work Client

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

The OpenVMS Entire Net-Work Client service must be started manually.

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

Manually Starting Entire Net-Work Client

If, during installation of the Entire Net-Work Client on Windows systems, you elected not to have its service or 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.

Stopping Entire Net-Work Client

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

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

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

The Entire Net-Work Client service is stopped.

▶ **To stop the Entire Net-Work Client service in OpenVMS environments:**

■ Run the *wclstop.com* command procedure.

> **Note:** OpenVMS Entire Net-Work Client services can also be stopped using the System Management Hub in a Windows or UNIX environment.

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

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

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

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

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

Or:

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

The Entire Net-Work Client service or 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.

17 About the System Management Hub

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

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

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

Accessing the System Management Hub

▶ **To access the System Management Hub:**

1   Type the following URL into your Web browser:

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

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

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

Or:

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

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

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

The System Management Hub main panel appears.
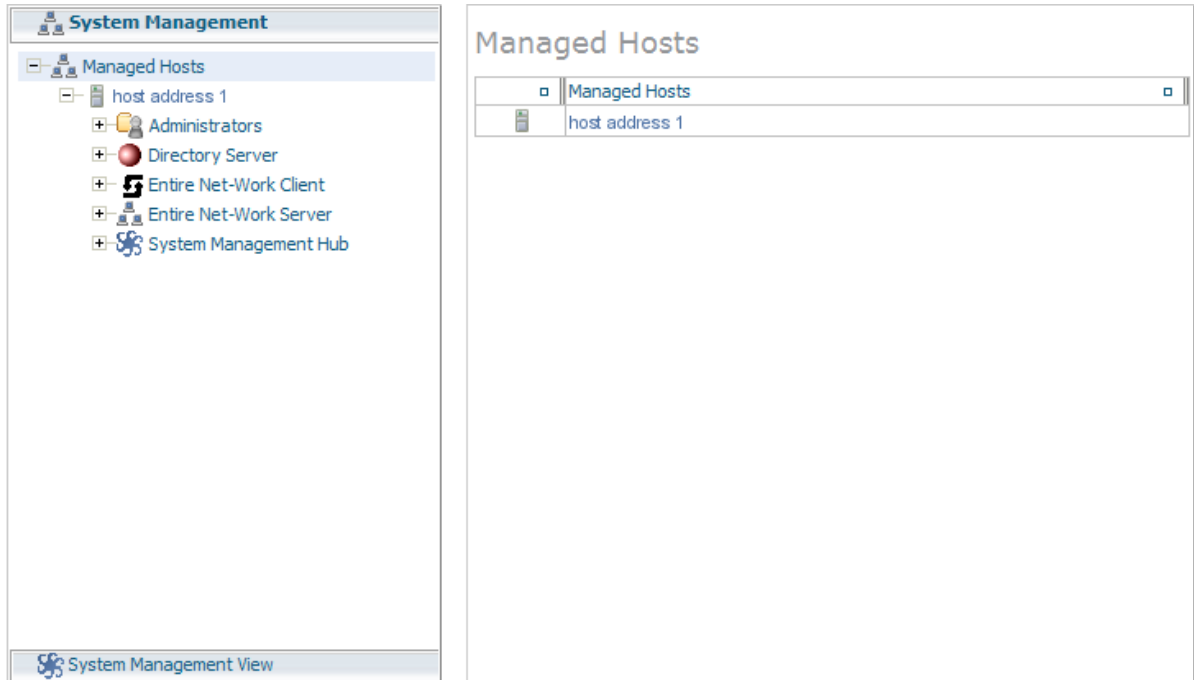
Leaving the System Management Hub

▶ **To leave the System Management Hub:**

■   Click the `Log Off` command at the top of the screen.
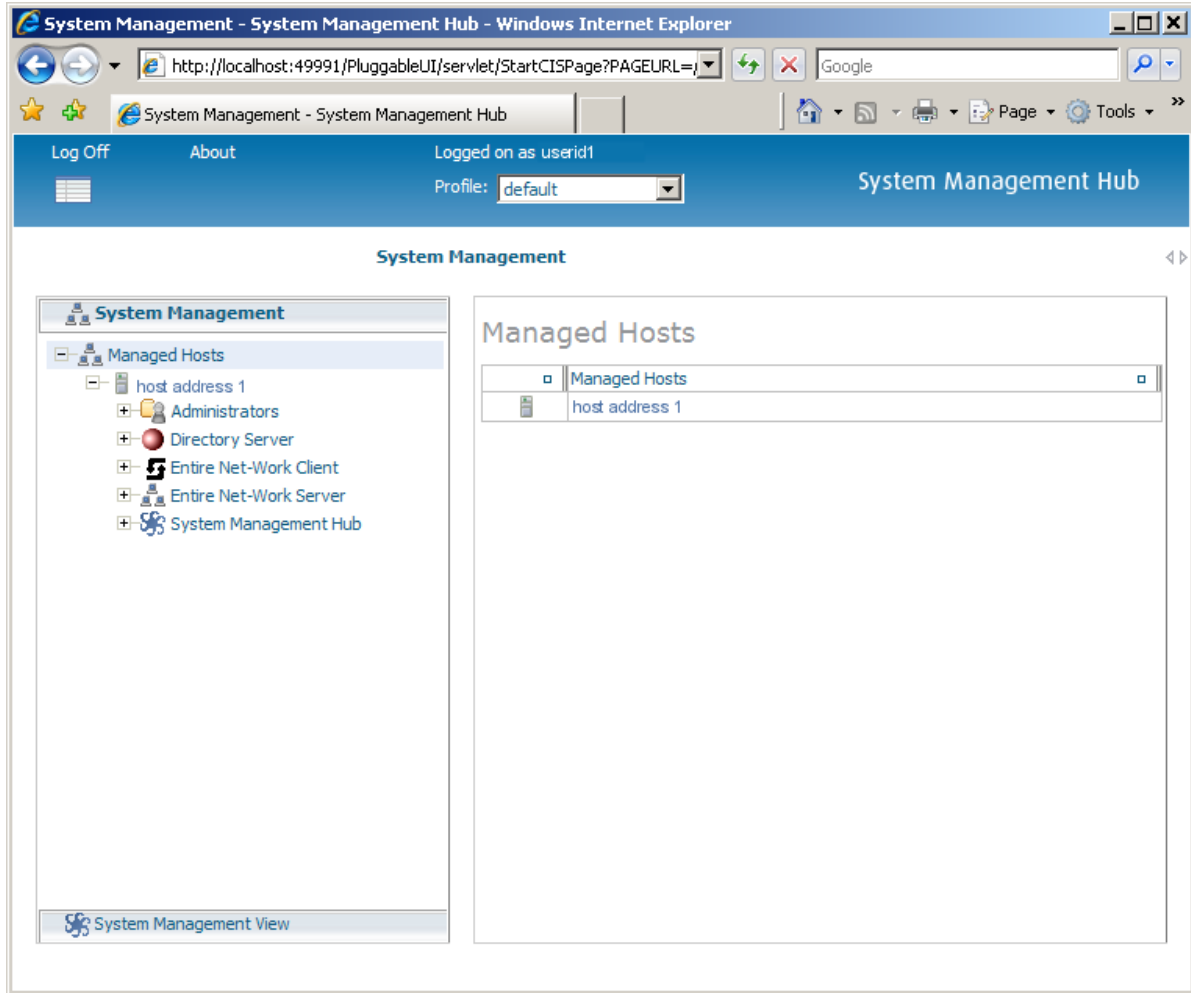
Or:

Close the Browser window.

The System Management Hub window is closed.

Using the Refresh Button in the System Management Hub

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

Getting Help

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

▶ **To get help on an area:**

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

The documentation pertaining to that System Management Hub area appears.

18 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:

Using the Entire Net-Work User Exit Interface

Explains the Entire Net-Work user exit interface in open systems.

19 The Entire Net-Work Client SMH Administration Area

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

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

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

2   Expand the tree-view frame for the managed host by clicking on the plus sign (+) to the left of its name.

3   Select "Entire Net-Work Client" in the tree-view under the managed host.

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

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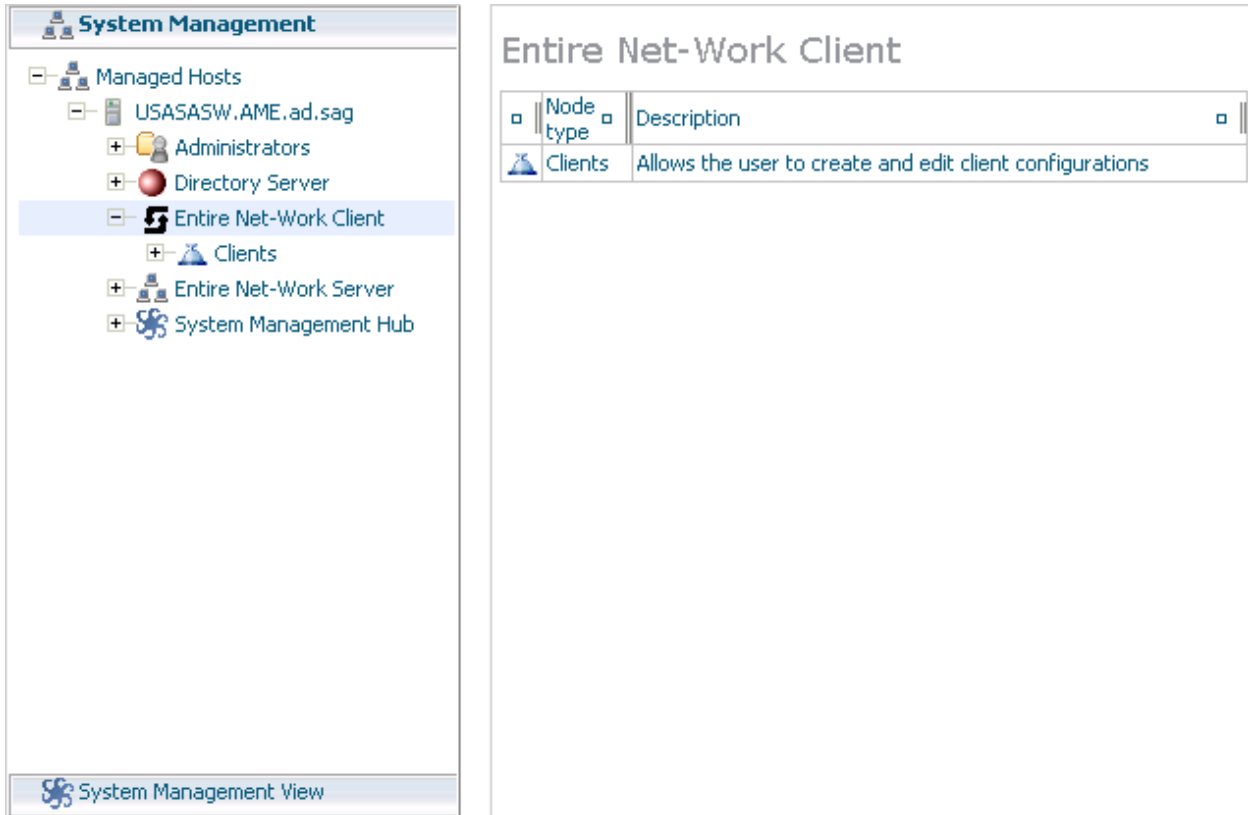
The following commands are available in the command menu of the Entire Net-Work Client administration area or by right-clicking on "Entire Net-Work Client" in tree-view:

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

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

20 About Client Configurations

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

- The Software AG Directory Server that should be used by the client in its attempts to work with Adabas databases.

- The databases that should be included or excluded for use by the client.

- Specific database access definitions for the client, including any additional access parameters that should be used.

- XTS (communication service) and ADALNK trace levels used for the client.

- Any user exit used for the client.

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

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

- In Windows XP environments (up to XP Server 2003): `Documents and Settings\All Users\Application Data\Software AG\Entire Net-Work Client\`

- In Windows Vista 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.

21 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 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.

The following commands are available for this client list:

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

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

3   Select 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 commands are available for each client machine:

> **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.
Help	Link to help for your use of SMH as it pertains to the Entire Net-Work Client administration area.
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.
Set Client Parameters	Change the parameters used by the client machine, including the Directory Server used by the client machine. For more information, read *Setting Client Parameters*, elsewhere in this chapter.
Set Trace Level	Set the Entire Net-Work Client trace level. 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 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 commands are available for each 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 Parms	Add additional access parameters for an Adabas database to the client.
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.
Set ADASAF Parms	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.

Command	Use this command to:
Set Client Configuration Parameters	Maintain the parameters for the client configuration. For more information, read *Maintaining Client Configuration Parameters*, elsewhere in this chapter.
Set LNK User Exits Parms	Specify the user exit file and function names that should be called before and after ACB and ACBX direct calls, if the Adabas interface supports user exits. For more information, read *Using ADALNK User Exits*, elsewhere in this chapter.
Set Directory Server	Change the Software AG Directory Server used by the client. For more information, read *Changing the Software AG Directory Server for the Client*, elsewhere in this chapter.

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

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

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

23   Setting Client Parameters

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

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

Make sure you have accessed the System Management Hub.

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

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

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

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

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

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

Parameter	Description
SAGXTSDSHOST	Specify the Software AG Directory Server host name you want to use for this client machine.
SAGXTSDSPORT	Specify the port number of the Software AG Directory Server you specified in the SAGXTSDSHOST parameter.
CLIENT_NAME	Normally, the client machine name is the machine name. However, for cosmetic reasons only, you can change the client machine name. If a client name is specified in this parameter, the new client name is changed in the access entries in the local Entire Net-Work Client configuration file.
CLIENT_HOST	Normally, the host name for a client is the client machine name. However, you may want to select a different host name for the client machine. For example, you might want to specify the fully qualified host name (such as, "user.aaa.com") or physical address (such as, "10.124.221.36") of the machine instead. If a client host name is specified in this parameter, the new host name is changed in the access entries in the local Entire Net-Work Client configuration file.

Parameter	Description
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.). ■ Once an available port number is found, it is assigned to the client in its Software AG 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.

24 Adding Client Configurations

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

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

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

Make sure you have accessed the System Management Hub.

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

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

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

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

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

Add Net-Work Client Configuration

Enter Entire Net-Work Client Configuration Name:

                                            *

Enter the Configuration File Path:

| OK | Cancel | Help |

4   Enter the name of the client configuration in **Enter Entire Net-Work Client Configuration Name** the 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.

25 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.

26   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 Parameters** from the resulting drop-down list.

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

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

Parameter	Description
ACCEPTED_DBIDS	Specify the database IDs you want this client to be able to access. If more than one database ID is needed, separate them with commas. If a range of database numbers is needed, separate them with a dash. For example, "4,12-15,62" indicates that the client should have access to databases 4, 62, and any databases with numbers between 12 and 15 (inclusive). For more information, read *Understanding Filtering*, elsewhere in this guide.
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.
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.
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

Parameter	Description
	representative. If you do, your installation could be overrun with trace messages that would be meaningless to you and would likely affect system performance.
LOGDIR	Specify the fully-qualified path of the directory where Entire Net-Work Client log files should be written. For more information, read *Specifying the Log File Location*, elsewhere in this chapter.
LNKTRACE	Set the hexadecimal ADALNK trace level using this parameter. This is the trace level for Adabas calls. Valid values are hexadecimal values ranging from "00" (no tracing) through "f1 (full tracing).". Do not specify full tracing unless specifically instructed to do so by a Software AG Customer Support representative. If you do, your installation could be overrun with trace messages that would be meaningless to you and would likely affect system performance. For more information about Entire Net-Work Client tracing, read *Tracing Entire Net-Work Client Processing*, elsewhere in this guide.
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.
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. Valid values are "YES" and "NO". If you specify "YES", the access entry information is stored locally; if you specify "NO", the access entry information is available only in the Directory Server configuration file, wherever the Software AG Directory Server is installed.
USER_EXITS	Specify the name of the user exit DLL file that should be used with this client. For more information about Entire Net-Work Client user exits, read *Using the Entire Net-Work User Exit Interface*, elsewhere in this guide.
WCPPARTITION	Specify the partition in which the client is assigned, if any. For more information, read *Understanding Partitioning*, elsewhere in this guide.
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.

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

27 **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 Software AG Directory Server definitions. These definitions are stored in the Directory Server configuration file, wherever the Software AG Directory Server is installed, and are published and available for other clients using the same Directory Server.

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

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

▪ You can use filtering to identify databases that the client can and cannot access.

▪ You can define local Adabas access definitions for specific databases.

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

For complete information on filtering in the Entire Net-Work Client configuration, read *Understanding Filtering*, elsewhere in this guide.

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

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

Maintaining Adabas Access Definitions

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

This section covers the following topics:

- Adding Adabas Access Definitions
- Listing Adabas Access Definitions
- Modifying Adabas Access Definitions
- Deleting Adabas Access Definitions

Adding Adabas Access Definitions

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

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

Make sure you have accessed the System Management Hub.

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

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

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

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

    The list of clients defined on the client machine appears.

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

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

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
Adabas ID	Specify the ID of the Adabas database to which this definition applies.
Protocol Type	Select the communication protocol that will be used to connect to the database: TCP/IP or SSL
Host Address	Specify the name of the host computer where the database runs.
Port Value	The port number of the host computer for the database.
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.
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.
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.

Parameter	Description
Additional Parameters	Specify additional parameters as described in *Parameters*, in the chapter entitled *Directory Server Target Entries* of the *Software AG Directory Server Administration Guide*. Separate parameters in this field with ampersand (&) symbols.

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.

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
Port	The port number of the host computer for the database.
Host	The name of the host computer on which the database is installed.
Protocol Type	Select the communication protocol that will be used to connect to the database: TCP/IP or SSL
Additional Parameters	Specify additional parameters as described in *Parameters*, in the chapter entitled *Directory Server Target Entries* of the *Software AG Directory Server Administration Guide*. Separate parameters in this field with ampersand (&) symbols.

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 Access Parameter Definitions
- Listing Access Parameter Definitions
- Modifying Access Parameter Definitions
- Deleting Access Parameter Definitions

Adding 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 Parms** from the resulting drop-down menu.

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

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

Parameter	Description
Adabas ID	Specify the ID of the Adabas database to which this definition applies.
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.
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.
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.
Additional Parameters	Specify additional parameters as described in *Parameters*, in the chapter entitled *Directory Server Target Entries* of the *Software AG Directory Server Administration Guide*. Separate parameters in this field with ampersand (&) symbols.

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

Listing 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 Access Parameter Definitions

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

Make sure you have accessed the System Management Hub.

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

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

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

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

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

4   In tree-view, expand the client configuration containing the Adabas access parameter definitions you want to modify.
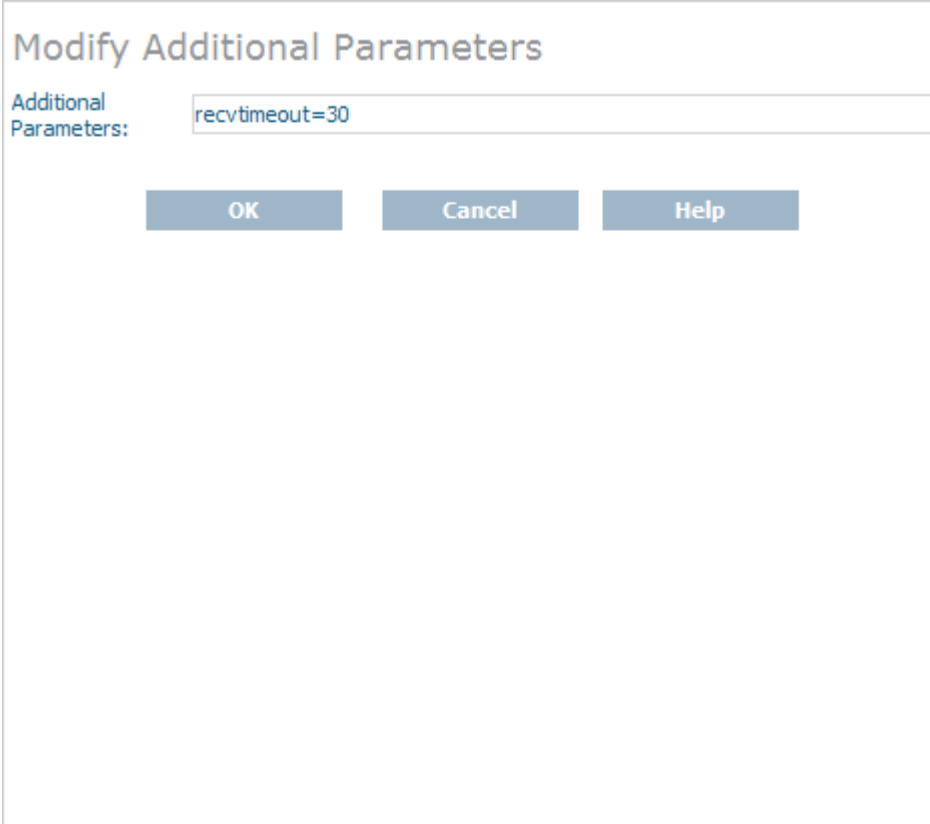
Options for the Adabas access and additional access parameter definitions appear in tree-view.

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

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

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

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

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

Parameter	Description
Additional Parameters	Specify additional parameters as described in *Parameters*, in the chapter entitled *Directory Server Target Entries* of the *Software AG Directory Server Administration Guide*. Separate parameters in this field with ampersand (&) symbols.

The access parameter definition is modified.

Deleting 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.

28 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 Vista environments: `ProgramData\Software AG\Entire Net-Work Client\`

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

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

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

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

Make sure you have accessed the System Management Hub.

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

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

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

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

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

4   Click **OK** at the prompt.

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

Specifying the Client Log File Location

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

◾ In Windows XP environments (up to XP Server 2003): `Documents and Settings\All Users\Application Data\Software AG\Entire Net-Work Client\`

◾ In Windows Vista environments: `ProgramData\Software AG\Entire Net-Work Client\`

◾ In UNIX environments: `$SAG\wcl\`.

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

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

Make sure you have accessed the System Management Hub.

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

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

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

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

     The client configuration section becomes available in tree-view.

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

     The **Client Configuration Parameters** panel appears in detail-view.
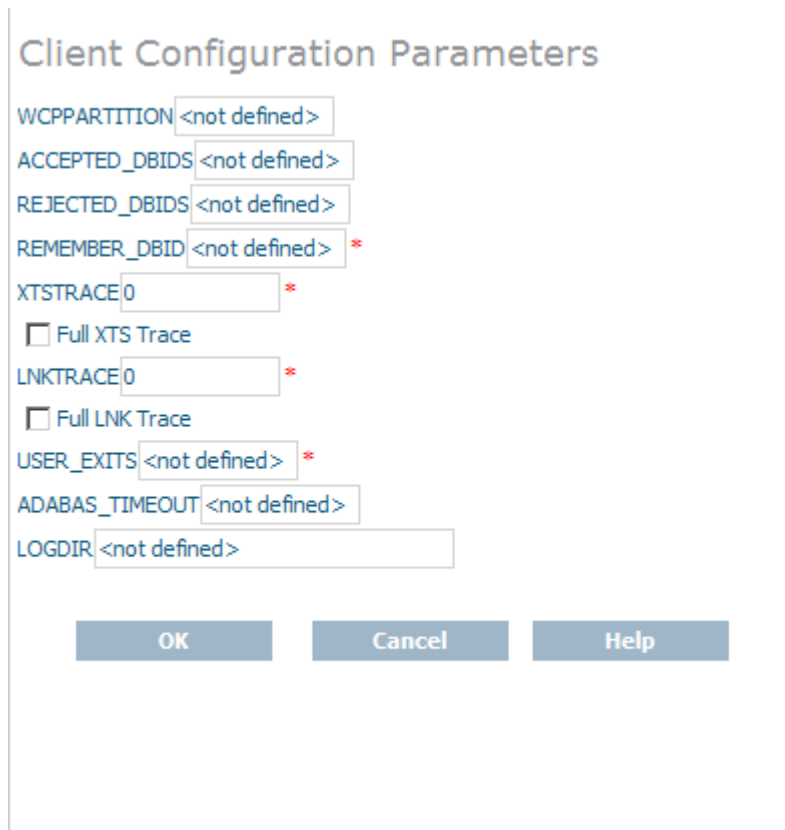
5   Specify the fully-qualified path of the directory in which you want log files stored in the LOGDIR parameter. When all changes are made, click **OK** to save the setting.

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

29 Accessing Secured z/OS Host Resources

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

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

- In Windows environments only, you can use an online application to log onto ESI.

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

Specifying the ESI Method and Appropriate Adabas SAF Security Kernel Parameters

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

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

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

Make sure you have accessed the System Management Hub.

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

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

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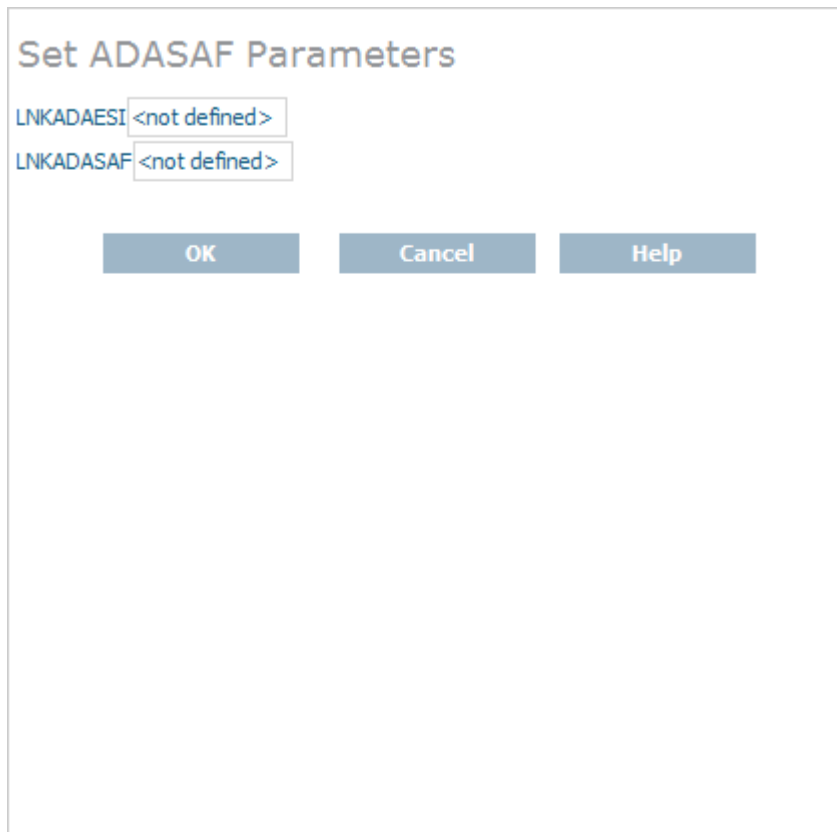
3   Select and expand the client machine on which the client is defined.

The client configuration section becomes available in tree-view.

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

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

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

Parameter	Description
LNKADAESI	This parameter is available for Windows systems only.
	Indicate whether the ESI online application should be used instead of a user exit. Valid values are "YES" (use the online application) or "NO" (use a user exit). The default is "NO". If LNKADAESI is set to "YES" and a value is given in LNKADASAF, the online application is used (LNKADAESI settings override LNKADASAF).
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:

Parameter	Description
| | ```
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*). |

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

Accessing z/OS Resources Using the ESI Online Application

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

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

This section covers the following topics:

- Accessing the ESI Logon Dialog
- Automatic Logoff
- Encryption Method Modifications

Accessing the ESI Logon Dialog

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

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

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

■ If the security check is passed, the application is allowed to access those resources that are permitted according to your Adabas security user profile.

■ If the security check is not passed, an Adabas security response code is returned to the application.

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

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

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

    The ESI logon dialog appears, as shown below.

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

    Your ESI access information is encrypted and stored.

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

Automatic Logoff

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

- If the Auto Logoff value is "60", you are logged off of Adabas security after 60 minutes of Adabas
  inactivity. When you log on again, the security check is performed as if you were logging on
  for the first time.

- If the Auto Logoff value is "0", the automatic no automatic logoff occurs.

Encryption Method Modifications

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

> **Notes:**

1. Software AG strongly recommends that you modify the encryption/decryption code. The en-
   cryption/decryption algorithm you use must match the ones used on the mainframe.

2. In past versions of ESI, an *ADAESI.INI* file and ADAESIX parameter were used to modify the
   encryption/decryption algorithms. This file and parameter are no longer supported. Instead,
   you must use the procedure described in this section. In addition, Entire Net-Work Client no
   longer supports changing the *adacrypt.dll* library name.

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

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

2   Modify the encryption and decryption code as required and then compile and link it using
     the files in the *\examples\adaesi_uexit* directory.

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

Accessing z/OS Resources Using the ESI Security Exit

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

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

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

2   Modify the user exit as required and then compile and link it using the files in the *\examples\adasaf_uexit* directory.

30   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

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

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

▶ **To specify the user exit file and function names:**

Make sure you have accessed the System Management Hub.

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

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

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

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

The client configuration section becomes available in tree-view.

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

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

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

> **Note:** Values should be specified for these parameters using the following format:
>
> `file_name;function_name`

Parameter	Description
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.
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.
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.
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.

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

Modifying the User Exit Code

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

▶ **To modify and use the sample ADALNK user exits:**

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

Directory	Contains	Sample User Exit File Name
\examples\acb_uexit	The sample user exit and files required to compile and link the ADALNK ACB before and after user exits.	*lnkuex.c*
\examples\acbx_uexit	The sample user exit and files required to compile and link the ADALNK ACBX before and after user exits.	*lnkuexacbx.c*

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

31 Changing the Software AG Directory Server

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

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

Changing the Software AG Directory Server for the Client Machine

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

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

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

Make sure you have accessed the System Management Hub.

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

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

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

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

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

4   In the SAGXTSDSHOST parameter, specify the Software AG Directory Server host name you want to use for this client machine.

5   In the SAGXTSDSPORT parameter, specify the port number of the Software AG Directory Server you specified in the SAGXTSDSHOST parameter.

6   When all parameters are specified, click **OK**. For more information about the other client parameters, read *Setting Client Parameters*, elsewhere in this guide.

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

Changing the Software AG Directory Server for a Specific Client

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

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

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

Make sure you have accessed the System Management Hub.

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

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

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

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

     The list of clients defined on the client machine appears.

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

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

5   In the SAGXTSDSHOST parameter, specify the Software AG Directory Server host name you want to use for this client.

6   In the SAGXTSDSPORT parameter, specify the port number of the Software AG Directory Server you specified in the SAGXTSDSHOST parameter.

7   When all parameters are specified, click **OK**.

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

32 Tracing Entire Net-Work Client Processing

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

- 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 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 machine you want from the list and select **Set Trace Level** from the resulting drop-down menu.

   The **Set Trace Level** panel appears in detail-view.

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

    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.

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
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.
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.

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.

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
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.
LNKTRACE	Set the hexadecimal ADALNK trace level using this parameter. This is the trace level for Adabas calls. Valid values are hexadecimal values ranging from "00" (no tracing) through "f1 (full tracing).". Do not specify full tracing unless specifically instructed to do so by a Software AG Customer Support representative. If you do, your installation could be overrun with trace messages that would be meaningless to you and would likely affect system performance.

The communications trace levels are set and activated.

33 Using the Entire Net-Work User Exit Interface

The Entire Net-Work user exit interface supports the implementation of user-written programs that perform the following types of functions:

- Compression and decompression of message data to optimize line transmission.
- Tailored statistical information gathering.
- Encryption and decryption of message data using an independent hardware or software formula.
- Control over the connection process, both inbound and outbound, based on local security requirements.
- Detection of node disconnections so that site-specific actions can be performed; for example, activation of a watchdog security function.

Entire Net-Work user exits can be implemented on all open systems platforms where Entire Net-Work is supported. Compiled user exit code is placed in a library where it can be accessed by Entire Net-Work when required.

Writing User Exits

User exits must be written in C and must use C calling conventions. If you wish, you can use the files from the supplied user exit examples as a basis.

Note the following additional restrictions, when writing your own user exit:

1. The destination buffer cannot be larger than the source buffer. Therefore, a message that is compressed or encrypted by a user exit must not exceed the size of the original message.

2. Data that has been modified by a user exit must be restored to its original form before being processed again by another Entire Net-Work Client node. For example, if you use a user exit to encrypt a message sent from an Entire Net-Work Client, you must use a corresponding user exit to decrypt the message before it can be processed by another server.

Once your user exit has been written, it and any files it requires must be built and compiled into a user exit library (a DLL file) on Windows systems or a shared library on UNIX systems before Entire Net-Work Client can use it. Entire Net-Work Kernel and Entire Net-Work Client configurations reference user exit DLL file or shared library names in their definitions.

Storing User Exit Library Files

Windows compiled user exit libraries (DLL files) or UNIX user exit shared libraries should be stored in the installation directory wherever the other executable and library files for Entire Net-Work Server or Entire Net-Work Client are installed (as appropriate for the user exit). By default, Entire Net-Work Server and Entire Net-Work Client user exit files should be stored in one of the following locations:

- In Windows environments for Entire Net-Work Server: `Program Files\Software AG\Entire Net-Work Server\v`*nn*, where *nn* is the release number

  In Windows environments for Entire Net-Work Client: `Program Files\Software AG\Entire Net-Work Client`

- In UNIX environments: `$SAG\`*ppp*`\v`*nn*, where *nn* is the release number of Entire Net-Work Client or Entire Net-Work Server and *ppp* is either "wcl" (for Entire Net-Work Client) or "wcp" (for Entire Net-Work Server).

In addition, user exit libraries should be stored in the root directory; they should not be stored in the *examples* subdirectory of the Entire Net-Work Client installation.

> ⚠ **Important:** It is a good idea to keep copies of your user exit libraries in a separate location from your Entire Net-Work installations.

User Exit Processing and Functions in Windows Environments

Entire Net-Work provides a user exit entry point (UE_Y) for every Entire Net-Work Kernel definition and every Entire Net-Work Client configuration. This user exit entry point is called from the transport layer protocol. At various times during processing, Entire Net-Work calls the user exit, passing it a structure that contains a function code and various optional data elements. The user exit program performs the desired function and returns a success or error indicator to Entire Net-Work.

> 📄 **Note:** Modification of data traffic (compression or encryption) requires processor cycles on both sending and receiving nodes. The User Exit Facility may be unsuitable in situations where processor performance is critical. Its use on relay nodes is not recommended.

This section covers the following topics:

- Calling the User Exit
- User Exit Control Block Structure
- Windows User Exit Responses
- Windows Tracing, Debugging. or Dumping User Exit Processing

- User Exit Windows Functions
- Windows User Exit Examples

Calling the User Exit

The syntax of a user exit call in Windows environments is:

```
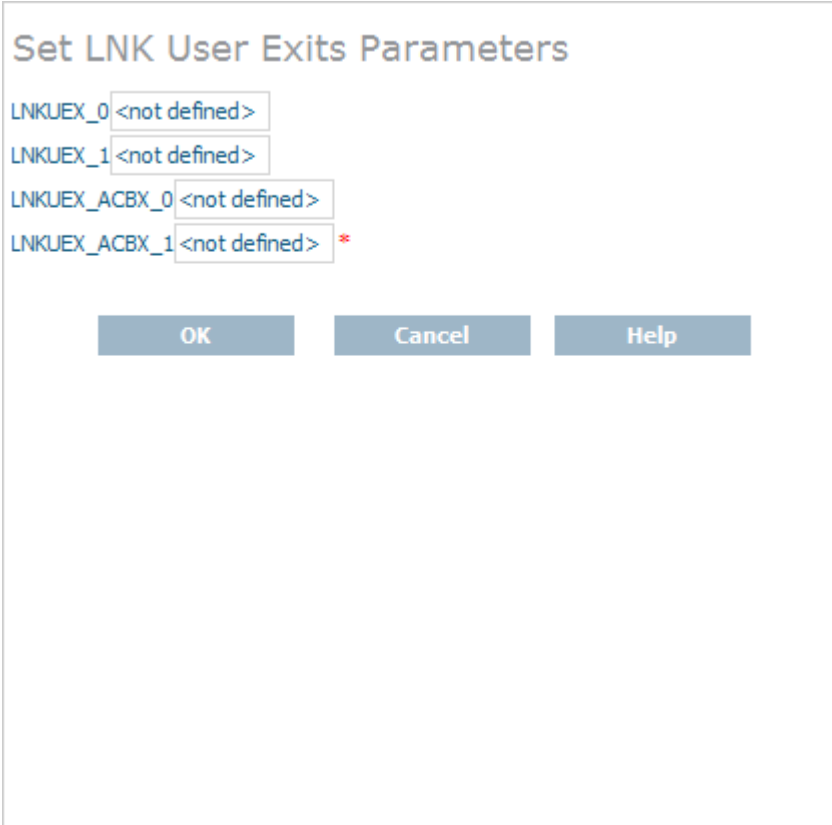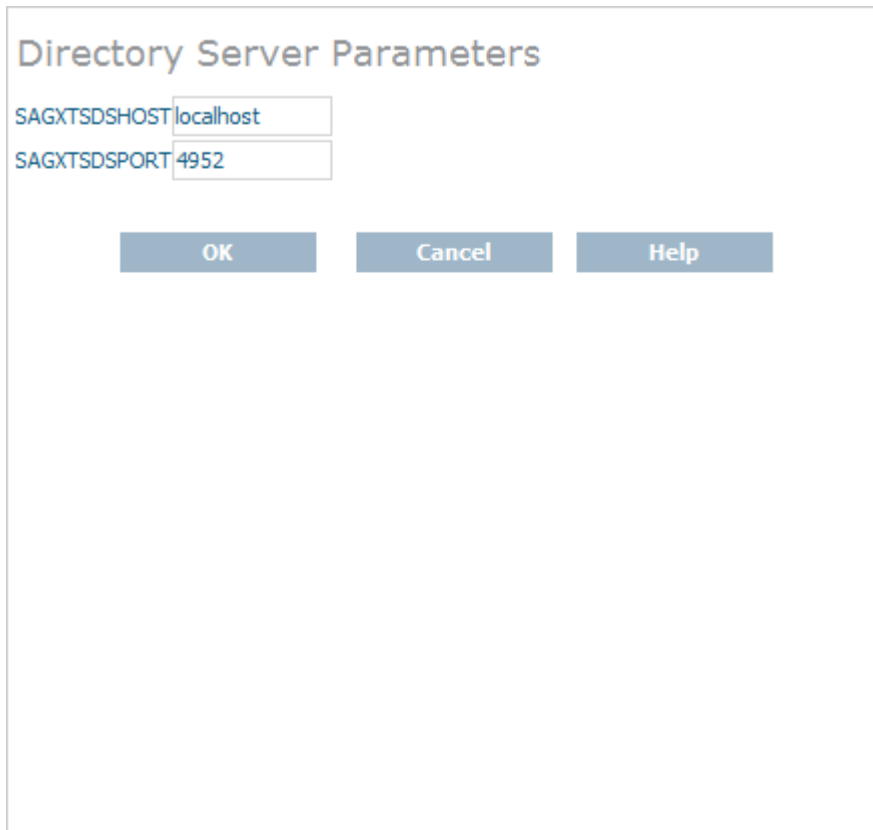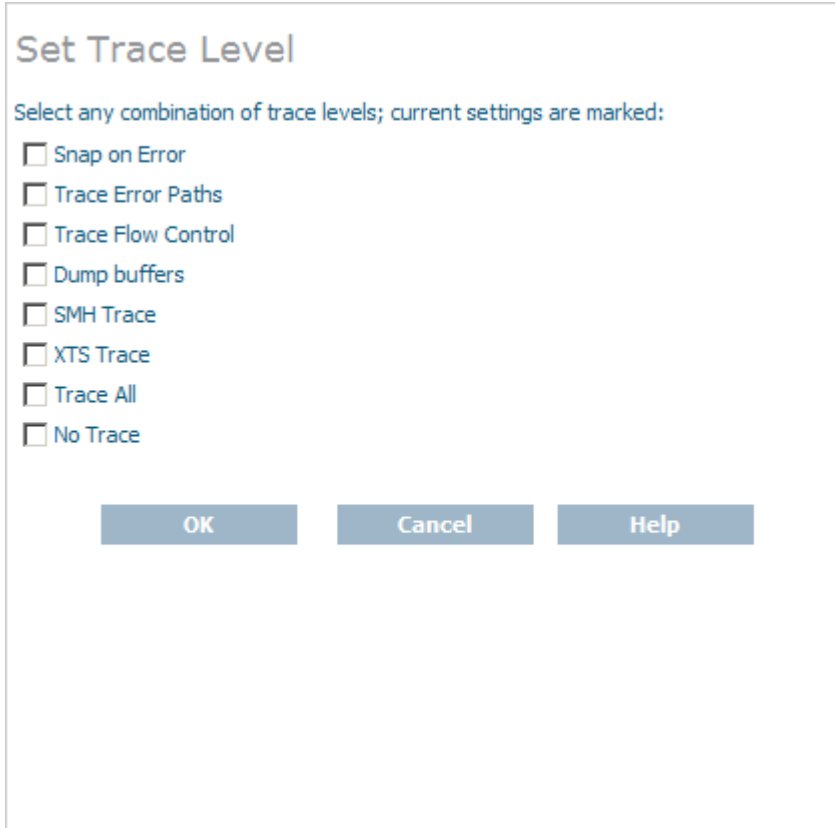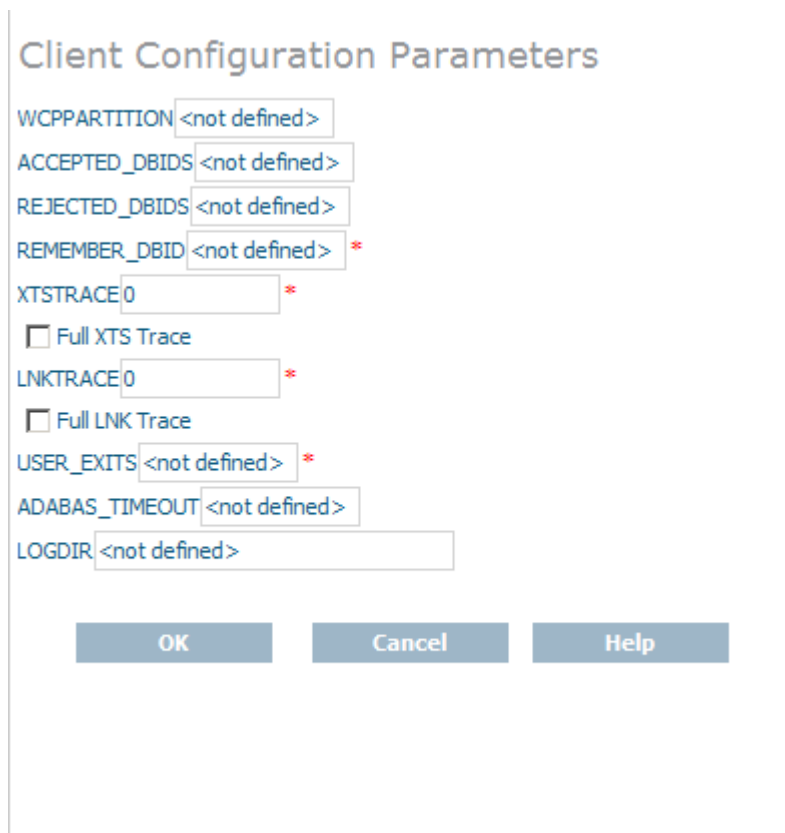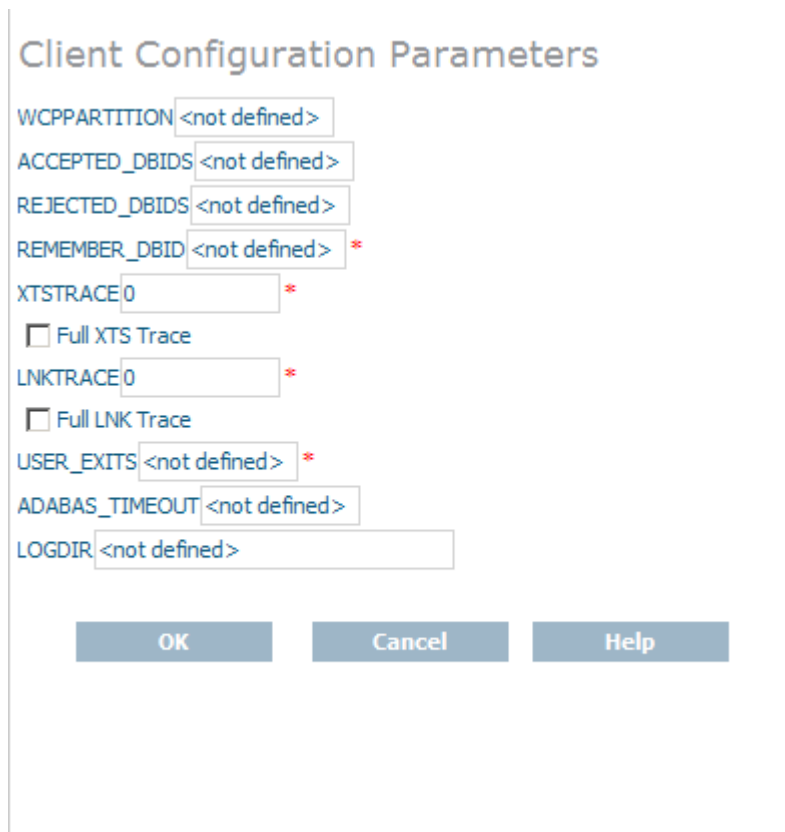LONG UE_Y(pUEYCB_control)
```

where `pUEYCB_control` is a pointer to the user exit control block (UEYCB).

User Exit Control Block Structure

The following table describes the user exit control block (UEYCB). For a full description of UEYCB, review the example user exit file *user_exit.h*, as described in *Windows User Exit Examples*, elsewhere in this section. Each user exit function must comply with this control block structure.

Element	Type	Description
Function	byte	The name of user exit function being processed by the call. Valid values include "UE_INIT", "UE_CON_OUT", "UE_CON_IN", "UE_SEND", "UE_RECV", "UE_DISCON", and "UE_TERM". For more information about each of these functions, read *User Exit Functions*, elsewhere in this section.
LineDriver	byte	The name of the transport protocol used by the call. At this time, the only valid value is "UE_D_TCP", indicating that TCP/IP is used.
Source	pvoid	The pointer to the source buffer; that is, the buffer used to contain the data to be processed by the user exit.
Slen	long	The size of the source buffer, which equals the length of the source data.
Dest	pvoid	The pointer to the destination buffer; that is, the buffer used to return data that has been modified by the user exit. Entire Net-Work is responsible for allocation and management of this buffer. The user exit should not attempt to free it.
Context	dword	A unique identifier supplied by Entire Net-Work for each connection.
Length	long	The length of the modified data message in the destination buffer.
MaxLength	long	The maximum size of the destination buffer. The destination buffer cannot be larger than the size of the source buffer.
Domain[6+1]	char	Not used.
Host[8+1]	char	Not used.
Argument	pvoid	Not used.
LD_Data	pvoid	Not used.
Model	pvoid	Not used.

Note: The user exit must not modify the contents of the Context element in the control block. It will be required for later use in send/receive calls. For an example of a user exit source

code file, review the supplied example file *user_exit.c*, described in *Windows User Exit Examples*, elsewhere in this section.

Windows User Exit Responses

The response from the user exit may include one of the return codes described in the table below. The specific meaning of these return codes varies, based on the user exit function you are trying to perform. To interpret these return codes, read about the user exit function you are using in *User Exit Functions*, elsewhere in this section.

Response	Description
UE_DATAOUT	The user exit function processes a modified data message in an intermediate buffer. The control block's Length element contains the length of this message.
UE_FAILURE	The user exit function fails and a message is written to the log file.
UE_RESTRICT	The user exit connection is allowed to continue to function on a restricted basis (only the `UE_DISCON` function is enabled for the exit).
UE_SUCCESS	The requested user exit function is successful.

Windows Tracing, Debugging. or Dumping User Exit Processing

You can include any trace, debug, or dump information pertaining to your user exit in the Entire Net-Work log file. To do this, use one of the following Software AG Transport Subsystem trace functions listed in the user exit file *user_exit.h*, as described in *Windows User Exit Examples*, elsewhere in this section. Each user exit function must comply with this control block structure.

- `XtsDump`
- `XtsDump_ex`
- `XtsTrace`
- `XtsDebug`

In addition to using any of these functions in your user exit, you should be sure to include the *xts2.lib* file in your user exit library. If you do not, the trace, debug, or dump processing will not occur. The *xts2.lib* file is supplied in the sample user exit supplied with Entire Net-Work. For more information, read *Windows User Exit Examples*, elsewhere in this section

If you need additional assistance with tracing, debugging, or dumping your user exit processing, contact your Software AG technical support representative.

User Exit Windows Functions

This section describes the available user exit functions, in order of normal use.

- UE_INIT Function
- UE_CON_OUT Function
- UE_CON_IN Function
- UE_SEND Function
- UE_RECV Function
- UE_DISCON Function
- UE_TERM Function

UE_INIT Function

The `UE_INIT` function is called once during Entire Net-Work startup (before remote connections are enabled) to allow the user exit to allocate resources for this session of Entire Net-Work and to describe its capabilities to Entire Net-Work. Software AG strongly recommends that a reason message be written to the log file if an initialization attempt fails.

Prior to user exit processing, the contents of the UEYCB elements should be:

pUEYCB	Contents
Function	UE_INIT
LineDriver	Zero
Source	NULL
Slen	Zero
Dest	NULL
Context	Zero
Length	Zero
MaxLength	Zero
Domain	not applicable
Host	not applicable
Argument	not applicable
LD Data	not applicable
Model	not applicable

The user exit should supply one of the following return codes to indicate processing results:

Response	Description
UE_FAILURE	Enable all future user exit calls.
UE_SUCCESS	Disable all future user exit calls (including UE_TERM) and write a message to the log file.

UE_CON_OUT Function

The UE_CON_OUT function is called once for each outbound connection attempt. The user exit can accept the connection attempt, accept the connection but restrict user exit functions, or reject the connection and terminate the connection process.

Software AG strongly recommends that a reason message be written to the log file if a connection attempt is rejected. Because rejection of an outbound connection attempt is unlikely, this function is normally used to allocate statistical recording memory and other resources. It is also the point at which DES encryption hardware is allocated, if it is being used.

Prior to user exit processing, the contents of the UEYCB elements should be:

pUEYCB	Contents
Function	UE_CON_OUT
LineDriver	Protocol type
Source	NULL
Slen	Zero
Dest	NULL
Context	Non-zero
Length	Zero
MaxLength	Zero
Domain	not applicable
Host	not applicable
Argument	not applicable
LD Data	not applicable
Model	not applicable

The user exit should supply one of the following return codes to indicate processing results:

Response	Description
UE_FAILURE	Terminate the connection process and a write a message to the log file.
UE_RESTRICT	Continue the connection process on a restricted basis and enable the exit for UE_DISCON functions, but not for the UE_SEND or UE_RECV functions.
UE_SUCCESS	Continue the connection process and enable this exit for UE_SEND, UE_RECV, and UE_DISCON functions for this node.

UE_CON_IN Function

The `UE_CON_IN` function is called during inbound connection processing. The user exit can accept the connection, accept the connection but restrict user exit functions, or reject the connection for security reasons.

Software AG strongly recommends that a reason message be written to the log file if a connection attempt is rejected. If the connection is accepted, the user exit should allocate the resources and memory required for the connection.

Prior to user exit processing, the contents of the UEYCB elements should be:

pUEYCB	Contents
Function	UE_CON_IN
LineDriver	Protocol type
Source	NULL
Slen	Zero
Dest	NULL
Context	Non-zero
Length	Zero
MaxLength	Zero
Domain	not applicable
Host	not applicable
Argument	not applicable
LD Data	not applicable
Model	not applicable

The user exit should supply one of the following return codes to indicate processing results:

Response	Description
UE_FAILURE	Reject the connection and write a message to the log file.
UE_RESTRICT	Accept the connection on a restricted basis and enable the user exit for `UE_DISCON` functions, but not for `UE_SEND` or `UE_RECV` functions.
UE_SUCCESS	Accept the connection and enable the user exit for `UE_SEND`, `UE_RECV`, and `UE_DISCON` functions.

UE_SEND Function

The `UE_SEND` function is called before a data message is transmitted to a remote node. The user exit can send the message, modify the message before sending it, or reject the message and force disconnection of the node. Software AG strongly recommends that a reason message be written to the log file if the message is rejected.

`UE_INIT` and either `UE_CON_IN` or `UE_CON_OUT` must have been successful (returned response "UE_SUCCESS") for this node before the `UE_SEND` function can be run.

Prior to user exit processing, the contents of the UEYCB elements should be:

pUEYCB	Contents
Function	UE_SEND
LineDriver	Protocol type.
Source	Pointer to the source buffer containing the data message to be transmitted.
Slen	Length of the source data.
Dest	Pointer to the destination buffer.
Context	Unique connection ID supplied by Entire Net-Work during the connection.
Length	Zero (see the "UE_DATAOUT" return code)
MaxLength	Maximum size of the user exit buffer.
Domain	not applicable
Host	not applicable
Argument	not applicable
LD Data	not applicable
Model	not applicable

The user exit should supply one of the following return codes to indicate processing results:

Response	Description
UE_DATAOUT	Send the modified data message in the destination buffer. The Length element contains the length of the message.
UE_FAILURE	Reject the message, force a disconnection of the node, and write a message to the log file.
UE_SUCCESS	Send the unmodified source data.

UE_RECV Function

The UE_RECV function is called when a data message that was modified before transmission arrives from a remote node. The user exit can accept the message for processing, modify the message, or discard the message and force disconnection of the node. Software AG strongly recommends that a reason message be written to the log file if the message is discarded.

Prior to user exit processing, the contents of the UEYCB elements should be:

pUEYCB	Contents
Function	UE_RECV
LineDriver	Protocol type
Source	Pointer to the buffer containing the data message received.
Slen	Length of the data received.
Dest	Pointer to the user exit buffer, which contains the data message when and if it is modified by the user exit.
Context	Unique connection ID supplied by Entire Net-Work during the connection.
Length	The original message length (see the UE_DATAOUT return code).
MaxLength	The maximum size of the user exit buffer.
Domain	not applicable
Host	not applicable
Argument	not applicable
LD Data	not applicable
Model	not applicable

The user exit should supply one of the following return codes to indicate processing results:

Response	Description
UE_DATAOUT	Process the modified message contained in the user exit buffer. The Length element contains the length of the message.
UE_FAILURE	Discard the message, force the disconnection of the node, and write a message to the log file.
UE_SUCCESS	Continue processing the source data.

UE_DISCON Function

The `UE_DISCON` function is called once immediately after a node is disconnected for any reason. The user exit can release resources allocated during a connection call, log statistical information, and initiate actions to reestablish the connection (activate a watchdog security function).

Prior to user exit processing, the contents of the UEYCB elements should be:

pUEYCB	Contents
Function	UE_DISCON
LineDriver	Protocol type
Source	NULL
Slen	Zero
Dest	NULL
Context	Unique connection ID supplied by Entire Net-Work during the connection.
Length	Zero
MaxLength	Zero
Domain	not applicable
Host	not applicable
Argument	not applicable
LD Data	not applicable
Model	not applicable

Return codes for the `UE_DISCON` function are ignored.

UE_TERM Function

The `UE_TERM` function is called once during Entire Net-Work shutdown processing. It allows the user exit to release resources allocated during `UE_INIT` function processing and to log statistical data prior to shutdown.

Prior to user exit processing, the contents of the UEYCB elements should be:

pUEYCB	Contents
Function	UE_TERM
LineDriver	Zero
Source	NULL
Slen	Zero
Dest	NULL
Context	Zero
Length	Zero

pUEYCB	Contents
MaxLength	Zero
Domain	not applicable
Host	not applicable
Argument	not applicable
LD Data	not applicable
Model	not applicable

Return codes for the UE_TERM function are ignored.

Windows User Exit Examples

The Entire Net-Work Client installation kit includes several example user exits in a series of sub-directories in the *examples* subdirectory:

Subdirectory	Contains
acb_uexit	An ADALNK user exit. This user exit is called before an Adabas call is processed (ADALNK interface) and it rejects all Adabas operator calls whose user is not SAG. In addition, it blocks N1/N2 and A1 commands for the user SAG. Response code 22 is set when any of these call restrictions in encountered.
acbx_uexit	An ADALNKX user exit. This user exit is called before an Adabas call is processed (ADALNKX interface) and it rejects all Adabas operator calls whose user is not SAGPC. In addition, it blocks N1/N2 and A1 commands for the user SAGPC. A return value of ADA_UEXREJ is set when any of these call restrictions in encountered.
adaesi_uexit	An External Security Interface (ESI) user exit you can use to modify the method used to encrypt and decrypt the ESI logon dialog information, read .
adasaf_uexit	An External Security Interface (ESI) user exit you can use to access secured Adabas resources on a z/OS host node. For more information, read .
wcl_uexit	An example user exit and a shared library stub. These are provided to assist you in creating and implementing your user exit program.

The remainder of this section describes the files and compilation method you can use to create and compile your own user exit, based on the files in the *wcl_uexit* subdirectory.

- acb_uexit Example User Exit Files
- acbx_uexit Example User Exit Files
- wcl_uexit Example User Exit Files

- Compiling the Example User Exit Files

acb_uexit Example User Exit Files

The *examples/acb_uexit* subdirectory contains all of the necessary source code files to make a working example of an ADALNK user exit program, as described in the following table:

File Name	Description
adabas.h	Adabas call resource file. This file lists resources files that should be included when the user exit is compiled.
adabasx.h	Adabas call control block file.
lnkuex.c	ADALNK user exit source code file.
lnkuex.h	ADALNK user exit control block layout file.
makefile	C program to be run in Windows and used to create the user exit library from the files in the user exit source code library.
makefile.ux	C program to be run in UNIX and used to create the user exit library from the files in the user exit source code library.
mk.bat	A batch file that runs nmake on the *makefile* file.

You can use these files as a model for writing your own ADALNK user exit programs. The supplied ADALNK user exit program is called before an Adabas call is processed (ADALNK interface) and it rejects all Adabas operator calls whose user is not SAG. In addition, it blocks N1/N2 and A1 commands for the user SAG. Response code 22 is set when any of these call restrictions in encountered.

acbx_uexit Example User Exit Files

The *examples/acbx_uexit* subdirectory contains all of the necessary source code files to make a working example of an ADALNKX user exit program, as described in the following table:

File Name	Description
adabas.h	Adabas call resource file. This file lists resources files that should be included when the user exit is compiled.
adabasx.h	Adabas call control block file.
lnkuexacbx.c	ADALNKX user exit source code file.
lnkuexacbx.h	ADALNKX user exit control block layout file.
makefile	C program to be run in Windows and used to create the user exit library from the files in the user exit source code library.
makefile.ux	C program to be run in UNIX and used to create the user exit library from the files in the user exit source code library.
mk.bat	A batch file that runs nmake/make on the *makefile* file.

You can use these files as a model for writing your own ADALNKX user exit programs. The supplied ADALNKX user exit is called before an Adabas call is processed (ADALNKX interface) and it rejects all Adabas operator calls whose user is not SAGPC. In addition, it blocks N1/N2 and A1 commands for the user SAGPC. A return value of ADA_UEXREJ is set when any of these call restrictions in encountered.

wcl_uexit Example User Exit Files

The *examples/wcl_uexit* subdirectory contains all of the necessary source code files to make a working example of a user exit program, as described in the following table:

File Name	Description
user_exit.c	User exit source code file.
user_exit.rc	User exit stub resource file. This file lists resource files that should be included when the user exit is compiled.
user_exit.def	User exit module definition file.
user_exit.h	User exit control block layout file.
makefile	C program used to create the user exit library from the files in the user exit source code library.
xts2.lib	If you need to make use of the Software AG transport subsystems's dump, trace and debug facilities in your code, include this file in your user exit library.

You can use these files as a model for writing your own user exit programs.

Compiling the Example User Exit Files

▶ **To compile a user exit into a user exit library in Windows environments:**

■ Navigate to the appropriate installation directory and enter the following command:

```
nmake -f makefile
```

The appropriate user exit library (**.dll* file) is generated.

User Exit Processing and Functions in UNIX Environments

The UNIX user exit shared library must contain an entry point, "ph_uexit", that will be called by the protocol handler processes.

This section covers the following topics:

- Calling the User Exit
- UNIX User Exit Return Codes
- Processing

Calling the User Exit

The syntax of a user exit call in UNIX environments is:

```
int ph_uexit (int fct_id, char *source, int slen, char *dest, int dlen);
```

📄 **Note:** The shared library's entry point function *must* be "ph_uexit".

This syntax uses the following call parameters and return codes:

Parameter	Description
int *fct_id*	The number of the user exit function to be run. Current valid values for *fct_id* are: ■ 0: The user exit is called by the send process before sending a buffer. ■ 1: The user exit is called by the receive process after receiving a buffer. .
char *source*	The pointer to the source buffer. The source buffer contains either original data to be sent or data just received.
int *slen*	The number of bytes in the source buffer.
char *dest*	The pointer to a free (destination) buffer to be used by the requested user exit function to store the manipulated data from the source buffer.
int *dlen*	The size of the destination buffer (which must equal the length of the original message).

UNIX User Exit Return Codes

The response from the user exit may include one of the return codes described in the table below.

Value	Description
-1	An error occurred. The user exit call failed.
Anything greater than 0 (>0)	The user exit call was successful. The return value is the length of the data in the destination buffer.

Processing

If user exit usage is enabled, the *ph_uexit* function is called by the protocol handler processes either just before starting to send a data buffer to a remote node or just after receiving a data buffer from a remote node. The protocol handler provides the data to be manipulated by the user exit in the buffer referenced by the source pointer, and expects the user exit's output to be in the buffer referenced by the destination pointer. The sizes of these buffers is passed to the user exit in the `slen` or `dlen` parameters, as appropriate. The user exit routines must ensure that there is no address violation when accessing these buffers.

On successful completion of the user exit call, the *ph_uexit* routine must return the length of data put into the destination buffer. If an error occurs, *ph_uexit* must return -1 to indicate the failure to the calling protocol handler processes.

When the *ph_uexit* routine is called during send processing, and a value greater than zero (0) is returned, the information from the destination buffer with the length returned by the *ph_uexit* is sent instead of the information in the source buffer. At the remote (destination) node, the user exit will be called for this buffer.

UNIX User Exit Examples

The Entire Net-Work Client installation kit includes several example user exits in a series of subdirectories in the *examples* subdirectory:

Subdirectory	Contains
acb_uexit	An ADALNK user exit. This user exit is called before an Adabas call is processed (ADALNK interface) and it rejects all Adabas operator calls whose user is not SAG. In addition, it blocks N1/N2 and A1 commands for the user SAG. Response code 22 is set when any of these call restrictions in encountered.
acbx_uexit	An ADALNKX user exit. This user exit is called before an Adabas call is processed (ADALNKX interface) and it rejects all Adabas operator calls whose user is not SAGPC. In addition, it blocks N1/N2 and A1 commands for the user SAGPC. A return value of ADA_UEXREJ is set when any of these call restrictions in encountered.
adasaf_uexit	An External Security Interface (ESI) user exit you can use to access secured Adabas resources on a z/OS host node. For more information, read .
wcl_uexit	An example user exit and a shared library stub. These are provided to assist you in creating and implementing your user exit program.

The remainder of this section describes the files and compilation method you can use to create and compile your own user exit, based on the files in the *wcl_uexit* subdirectory.

- acb_uexit Example User Exit Files
- acbx_uexit Example User Exit Files
- wcl_uexit Example User Exit Files

- Compiling the Example User Exit Files

acb_uexit Example User Exit Files

The *examples/acb_uexit* subdirectory contains all of the necessary source code files to make a working example of an ADALNK user exit program, as described in the following table:

File Name	Description
adabas.h	Adabas call resource file. This file lists resources files that should be included when the user exit is compiled.
adabasx.h	Adabas call control block file.
lnkuex.c	ADALNK user exit source code file.
lnkuex.h	ADALNK user exit control block layout file.
makefile	C program to be run in Windows and used to create the user exit library from the files in the user exit source code library.
makefile.ux	C program to be run in UNIX and used to create the user exit library from the files in the user exit source code library.
mk.bat	A batch file that runs nmake on the *makefile* file.

You can use these files as a model for writing your own ADALNK user exit programs. The supplied ADALNK user exit program is called before an Adabas call is processed (ADALNK interface) and it rejects all Adabas operator calls whose user is not SAG. In addition, it blocks N1/N2 and A1 commands for the user SAG. Response code 22 is set when any of these call restrictions in encountered.

acbx_uexit Example User Exit Files

The *examples/acbx_uexit* subdirectory contains all of the necessary source code files to make a working example of an ADALNKX user exit program, as described in the following table:

File Name	Description
adabas.h	Adabas call resource file. This file lists resources files that should be included when the user exit is compiled.
adabasx.h	Adabas call control block file.
lnkuexacbx.c	ADALNKX user exit source code file.
lnkuexacbx.h	ADALNKX user exit control block layout file.
makefile	C program to be run in Windows and used to create the user exit library from the files in the user exit source code library.
makefile.ux	C program to be run in UNIX and used to create the user exit library from the files in the user exit source code library.

You can use these files as a model for writing your own ADALNKX user exit programs. The supplied ADALNKX user exit is called before an Adabas call is processed (ADALNKX interface)

and it rejects all Adabas operator calls whose user is not SAGPC. In addition, it blocks N1/N2 and A1 commands for the user SAGPC. A return value of ADA_UEXREJ is set when any of these call restrictions in encountered.

wcl_uexit Example User Exit Files

The *examples/wcl_uexit* subdirectory contains all of the necessary source code files to make a working example of a user exit program, as described in the following table:

File Name	Description
user_exit.c	User exit source code file
user_exit.h	User exit control block layout file
makefile.ux	C program used to create the user exit library from the files in the user exit source code library.

You can use these files as a model for writing your own user exit programs.

Compiling the Example User Exit Files

▶ **To compile a user exit into a user exit library in UNIX environments:**

■ Navigate to the appropriate installation directory and enter the following command:

```
make -f makefile.ux
```

The appropriate user exit library (**.dll* file) is generated.

34   Port Number Reference

This chapter describes the ports that are needed by Entire Net-Work to perform its processing and how they can be assigned.

Port Overview and General Assignments

The following table describes the ports that are needed by Entire Net-Work to perform its processing and any default ports assumed by Entire Net-Work. You should consider avoiding the use of these default port numbers for other applications.

Software AG Product Component	Ports Needed	Default Port Number
Software AG Directory Server	One port is needed for Entire Net-Work requests to the Directory Server	4952 (IANA port) **Note:** If older versions of Entire Net-Work (older than 7.3) are in use, this port number may need to be changed to 12731.
Entire Net-Work Server	One port is needed for System Management Hub (SMH) administration of Entire Net-Work Server	dynamically assigned
Entire Net-Work Kernel	A port is needed for Kernel access by clients	dynamically assigned
	A port is needed for Kernel access via e-business connections (Entire Net-Work 7 or later)	dynamically assigned
	A port is needed for Kernel access via classic RDA connections (Entire Net-Work 2)	7869
	A port is needed for System Management Hub (SMH) administration of Kernels	dynamically assigned

Note that Software AG has registered port number 4952 with the Internet Assigned Numbers Authority (IANA) for use by the Software AG Directory Server. For more information about Directory Server port number specifications, read *The Directory Server Port Number*, in the *Software AG Directory Server Administration Guide*. For information on changing the Directory Server port number for an Entire Net-Work installation, read *Changing the Software AG Directory Server Port Number*.

In general, there are no default port numbers assigned to Entire Net-Work 7.3 Kernels or clients. These are dynamically assigned by Entire Net-Work when the Kernel or client is started, unless you specify a specific port or range of ports to use when you define the Kernel or client. If you set the port number to "0", the Entire Net-Work will dynamically assign a port.

Port numbers are dynamically assigned by Entire Net-Work when the Kernel or client is started, as follows:

■ Entire Net-Work searches for the first available port starting from port 49152 through 65535. (The starting search port number, 49152, is the IANA-recommended value from which to start.).

■ Once an available port number is found, it is assigned to the Kernel or client in its Software AG Directory Server entry.

While defining Entire Net-Work 7.3 Kernels, you can also select a specific port or specify a range or list of port numbers that Entire Net-Work should search during the process in which it dynamically assigns a port to the Kernel:

■ To specify a specific port number, enter the number in the port number field when you define the Kernel.

■ To specify a range of port numbers that Entire Net-Work should search to dynamically assign a port, list the starting and ending ports in the port number field when you define the Kernel, separated by a dash (-). For example, a specification of "9010-9019" would cause Entire Net-Work to search for the first available port between and including port numbers 9010 and 9019.

■ To specify a list of port numbers that Entire Net-Work should search to dynamically assign a port, list the port numbers in the port number field when you define the Kernel, separated by commas (,). For example, a specification of "9010,9013,9015,9017,9019" would cause Entire Net-Work to search for the first available port from this list of ports, starting with port 9010 and working from left to right through the list.

■ You can, of course, combine search ranges and lists in a port number field. For example, a specification of "9010-9019,10020,10050-10059" would cause Entire Net-Work to search for the first available port first in the 9010-9019 range (inclusive), then port 10020, and finally in the 10050-10059 range (inclusive). The first available port that Entire Net-Work encounters would be used for the Kernel.

If no available port is found in a specified range or list, an error occurs.

For more information about adding Kernels, read *Adding Kernels*, in your Entire Net-Work Server documentation.

Changing the Software AG Directory Server Port Number

▶ **If you need to change the Directory Server port number for your Entire Net-Work installation, follow these steps:**

1   Shut down the Directory Server service or daemon.

For information on shutting down the Directory Server service or daemon, read *Starting and Stopping the Software AG Directory Server*, in the *Software AG Directory Server Administration Guide*.

2   Modify the Directory Server installation, as appropriate for the operating system. When prompted, change the Directory Server port number to the new port number you want to use.

3   Start up the Directory Server service or daemon, if it is not automatically started after its installation was modified.

For information on starting up the Directory Server service or daemon, read *Starting and Stopping the Software AG Directory Server*, in the *Software AG Directory Server Administration Guide*.

35 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.

Index