software AG

Entire Net-Work Administration

Entire Net-Work Client Installation and Administration

Version 1.8

March 2024

ADABAS & NATURAL

Table of Contents

1 About this Documentation

Document Conventions

Convention	Description
Bold	Identifies elements on a screen.
`Monospace font`	Identifies service names and locations in the format *`folder.subfolder.service`*, APIs, Java classes, methods, properties.
`Italic`	Identifies: Variables for which you must supply values specific to your own situation or environment. New terms the first time they occur in the text. References to other documentation sources.
`Monospace font`	Identifies: Text you must type in. Messages displayed by the system. Program code.
{ }	Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the { } symbols.
|	Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the | symbol.
[ ]	Indicates one or more options. Type only the information inside the square brackets. Do not type the [ ] symbols.
...	Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).

Online Information and Support

Product Documentation

You can find the product documentation on our documentation website at **https://documenta-tion.softwareag.com**.

In addition, you can also access the cloud product documentation via **https://www.software-ag.cloud**. Navigate to the desired product and then, depending on your solution, go to "Developer Center", "User Center" or "Documentation".

Product Training

You can find helpful product training material on our Learning Portal at **https://knowledge.soft-wareag.com**.

Tech Community

You can collaborate with Software AG experts on our Tech Community website at **https://tech-community.softwareag.com**. From here you can, for example:

- Browse through our vast knowledge base.

- Ask questions and find answers in our discussion forums.

- Get the latest Software AG news and announcements.

- Explore our communities.

- Go to our public GitHub and Docker repositories at **https://github.com/softwareag** and **https://hub.docker.com/publishers/softwareag** and discover additional Software AG resources.

Product Support

Support for Software AG products is provided to licensed customers via our Empower Portal at **https://empower.softwareag.com**. Many services on this portal require that you have an account. If you do not yet have one, you can request it at **https://empower.softwareag.com/register**. Once you have an account, you can, for example:

- Download products, updates and fixes.

- Search the Knowledge Center for technical information and tips.

- Subscribe to early warnings and critical alerts.

- Open and update support incidents.

- Add product feature requests.

Data Protection

Software AG products provide functionality with respect to processing of personal data according to the EU General Data Protection Regulation (GDPR). Where applicable, appropriate steps are documented in the respective administration documentation.

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 Adabas Manager.

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

Entire Net-Work Client

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

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

When you install Entire Net-Work Client, its Windows service or Linux daemon is installed. Using the Adabas Manager (AMN), 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 information about using partitioning and filtering, read *Understanding Partitioning* and *Understanding Filtering*, elsewhere in this guide.

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

> **Note:** If you attempt to install and use Entire Net-Work Client in a system with a firewall in place, be sure that your system administrator has set up the firewall so that the Entire Net-Work Client component applications can access the ports they need (including the Adabas Directory Server port and those Entire Net-Work dynamically assigns during its own processing). For more information about Entire Net-Work ports, read . For information about configuring Entire Net-Work components for Windows 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 Adabas Directory Server. For more information about target entries in the Directory Server, read *Directory Server Target Entries* in the *Software AG Directory Server Installation and Administration Guide*. In addition, an SSL Toolkit is provided that allows you to set up a certificate authority that you can use to create security certificates for test purposes only. For more information about the SSL Toolkit, read *Using the SSL Toolkit* in the *Encryption for Entire Net-Work User Guide*, available from your Software AG support representative.

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

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

At least one Adabas Directory Server should be installed in your enterprise; we recommend that you install only one Directory Server to ensure centralized administration. However, your enterprise network configuration may require more than one. For example, you may want to install more than one Directory Server to fully direct requests to specific databases. While partitioning can also be used to restrict database access, all entries (in all partitions) of a Directory Server can be main-

tained via the Adabas Manager, so restriction is not complete. If, however, you use multiple Adabas Managers, you can limit what entries are available for viewing in the Directory Server portion of the Adabas Manager.

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

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

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

Adabas Manager (AMN)

The Adabas Manager (AMN) provides centralized management of all Software AG products installed in the enterprise, using a Web-based graphical user interface. The use of Adabas Manager eliminates the need for a system administrator to visit individual machines or maintain multiple product windows on the desktop.

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

Adabas Manager is used by Entire Net-Work 7 to manipulate configuration information. Using Adabas Manager, 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 AMN. The status of classic nodes and databases for which connections have been defined can be determined. Statistics can be examined and various control functions, such as node disconnection, Kernel shutdown, and trace settings can be performed.

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

SSL Support

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

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

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

3 Understanding Partitioning

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

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

Here are some of the advantages of partitioning:

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

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

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

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

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

4 Understanding Filtering

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

Filtering is set up in the Adabas Manager for both client configurations and for Kernels.

Filtering in Client Configurations

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

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

Filtering in Kernel Definitions

You can filter Kernels by requests:

- made to specific Adabas database IDs;

- relayed to other Kernels;

- submitted from other Kernels, by Kernel name;

- submitted to and from specific machines, by machine name; and

- submitted from other clients, by client name

This section covers the following topics:

- Filtering Requests to Adabas Databases
- Filtering Relay Requests to Other Kernels
- Filtering Requests from Other Kernels
- Filtering Requests to and from Specific Machines

- Filtering Requests to and from Specific Clients

Filtering Requests to Adabas Databases

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

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

Filtering Relay Requests to Other Kernels

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

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

Filtering Requests from Other Kernels

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

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

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

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

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

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

Filtering Requests to and from Specific Machines

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

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

Filtering Requests to and from Specific Clients

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

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

5 Release Notes

This chapter provides release notes for the Entire Net-Work Client 1.8 release. It is organized as follows:

Enhancements

The primary enhancement in this release of Entire Net-Work Client is a rollup of fixes to the last release.

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

After installation, please visit the Software AG Empower Product Support website at *https://empower.softwareag.com/* to check for and apply any available fixes to Entire Net-Work Client Version 1.8_SP1.

As Entire Net-Work Client has some dependencies on the product Adabas Client, you should also check for and apply any available fixes to Adabas Client for your platform.

Fixes to Entire Net-Work Client are delivered using the Software AG Update Manager. For more details, see section *Installing and Uninstalling Entire Net-Work Client* of this documentation.

Migration Considerations

Please note that you cannot use the System Management Hub (SMH) agents installed with an earlier version of Entire Net-Work Client or Entire Net-Work Server to manage this version of Entire Net-Work Client or Entire Net-Work Server. You must use the Adabas Manager (AMN).

The current version of Entire Net-Work Client and Entire Net-Work Server configuration files are compatible with Entire Net-Work Client Version 1.7 or Entire Net-Work Server Version 7.8.

Configuration files from previous versions can be copied into the new installation's */config* directory.

End of Maintenance

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

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

Documentation and Other Online Information

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

- Software AG Documentation Website
- Software AG TECHcommunity
- Software AG Empower Product Support Website

Software AG Documentation Website

You can find documentation for all Software AG products on the Software AG Documentation website at *https://documentation.softwareag.com*. This site requires Empower credentials. If you do not have an Empower user ID and password yet, you will find instructions for registering on this site (free for customers with maintenance contracts) or you can also use the TECHcommunity website to access the latest documentation.

Software AG TECHcommunity

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

- Access product documentation, if you have TECHcommunity credentials. If you do not, you will need to register and specify "Documentation" as an area of interest. If you already have TECHcommunity credentials, you can adjust your areas of interest on the TECHcommunity website by editing your TECHcommunity profile. To access documentation in the TECHcommunity once you are logged in, select **Documentation** from the **Communities** menu.

- Access articles, demos, and tutorials.

- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.

- Link to external websites that discuss open standards and web technology.

Software AG Empower Product Support Website

You can find product information on the Software AG Empower Product Support website at *https://empower.softwareag.com*. This site requires Empower credentials. If you do not have an Empower user ID and password yet, you will find instructions for registering on this site (free for customers with maintenance contracts).

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

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

6 Installing and Uninstalling Entire Net-Work Client

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

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

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

This chapter covers the following topics:

Installation Overview

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

System Requirements

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

- Supported Operating System Platforms
- Supported Hardware
- Supported Browsers
- Space Requirements
- Firewall Requirements

Supported Operating System Platforms

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

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

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

1. Access Software AG's Empower web site at *https://empower.softwareag.com*.

2. Log into Empower. Once you have logged in, you can expand **Products & Documentation** in the left menu of the web page and select **Product Version Availability** to access the Product Version Availability screen.

3. Use the fields on the top of this screen to filter its results for your Software AG product. When you click the **Search** button, the supported Software AG products that meet the filter criteria are listed in the table below the filter criteria.

    This list provides, by supported operating system platform:

    ▪ the Software AG general availability (GA) date of the Software AG product;

    ▪ the date the operating system platform is scheduled for retirement (OS Retirement);

    ▪ the Software AG end-of-maintenance (EOM) date for the product; and

    ▪ the Software AG end-of-sustained-support (EOSS) date for the product.

    Note: Although it may be technically possible to run a new version of your Software AG product on an older operating system, Software AG cannot continue to support operating system versions that are no longer supported by the system's provider. If you have questions about support, or if you plan to install this product on a release, version, or type of operating system other than one listed on the Product Version Availability screen described above, consult Software AG technical support to determine whether support is possible, and under what circumstances.

Supported Hardware

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

Supported Browsers

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

Space Requirements

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

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

Firewall Requirements

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

Configuration Considerations

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

Category	Question	Considerations
Adabas Directory Server and this product	Do you want to direct specific clients or Kernels to specific databases by department or other organizational grouping?	You can create multiple Kernels and use Directory Server partitioning and client and Kernel filtering in SMH to control which clients and Kernels have access to which databases.
Partitioning	Do you want to implement partitioning?	Partitioning allows you to direct specific clients or Kernels to specific databases. Partitions are defined for the clients and Kernels in the Adabas Manager. For more information, read *Understanding Partitioning,*elsewhere in this guide.

Before You Begin

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

1. Software AG strongly recommends that you create an installation image of your existing Software products and store the image on your internal network. You should create an image for each operating system on which you plan to run the installation (for example, 32-bit, 64-bit, or both). This will help you reduce WAN traffic and speed up installation and will ensure consistency across installations over time, since the Software AG Installer provides only the latest release of each product.

2. Close (stop) all open applications, especially those applications interacting with or depending on your Adabas databases. This includes Natural, Adabas Manager, the Adabas DBA Workbench, and prior releases of any other Adabas products. To be on the safe side, also shut down all Software AG services.

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

3. Disable any antivirus software.

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

5. If this product requires a license key file, verify the license key file is copied somewhere in your environment . Products requiring license key files will not run without valid license keys. For more information, read *The License Key*, elsewhere in this section.

6. Verify your environment supports the system requirements for this product, as described in *System Requirements*, elsewhere in this section.

Installation Steps

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

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

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

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

> **To install Entire Net-Work Client, complete the following steps:**

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

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

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

    > **Note:** The Infrastructure tree and required components therein is automatically selected for all Software AG product installations.

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

    > **Note:** You can opt to install other Software AG products from this list at the same time. This section just describes the installation of Entire Net-Work Client.

4   On the License panel, read the license agreement and select the check box to agree to the terms of the license agreement and then click **Next** to continue. If you do not accept the license agreement, the installation will stop.

5   When the **Configure** panel appears, specify the URL and port number for the Directory Server that should be used for this installation. The default is *tcpip://localhost:4952*. For complete information on the port used by the Directory Server, read *Port Number Reference*, elsewhere in this guide.

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

    Click **Next** to continue.

6   On the last panel, review the items you have selected for installation. If the list is correct, choose the **Next** button to start the installation process.

After Entire Net-Work Client has been installed, it will start automatically on Windows, and on Linux only, if it has been installed as a Daemon.

Required Post-Installation Updates for Simple Connection Line Driver Support

> **Note:** The most recent deliveries of Entire Net-Work and Adabas with ADATCP on the mainframe are compatible with a Directory server. If these products are configured to register their targets with the Directory Server, the steps outlined below are *not*not necessary. These steps only apply if you need to manually configure connections to your mainframe Adabas targets.

Once you have installed the Entire Net-Work Client components, you must add target entries in the Adabas Manager (AMN) 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 Adabas Manager. 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 Adabas Manager.

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

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

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

Configure the Adabas Client Environment

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

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

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

- When the remote administration of the database is required;

- When the database is to be accessed via Entire Net-Work;

- When a service application requires access to the database;

- When multiple database versions are accessed concurrently.

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

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

1. By executing the application at a Local Client Environment command prompt; or

2. By executing the application with a local Adabas Client environment.

This section covers the following topics:

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

Creating a Local Adabas Client Environment

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

1. Execute the application from a local Adabas Client command prompt via the Start menu: **All Programs > Software AG > Administration > Adabas Client *v.r* > Start Local Environment**.

2. Initialize the Adabas Client environment prior to executing the application by calling the script *aclenv.bat* located in the directory *<install_dir>\AdabasClient\INSTALL*.

Setting up the Global Adabas Client Environment

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

1. Execute the application from a local Adabas Client command prompt via the Start menu: **All Programs > Software AG > Administration > Adabas Client *v.r* > Configure Global Environment**.

2. As a system administrator, open a command prompt and run the script *aclenvvar.bat* located in the directory *<install_dir>\AdabasClient\INSTALL*.

Modifying an Existing Global Adabas Client Environment

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

Configuring Product Components for Windows Personal Firewall

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

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

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

Allow Ports for a Specific Executable Program

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

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

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

Component Name	Path and File Name
Entire Net-Work Client Service	*<your-installation-location>\EntireNetWorkClient\bin\wclservice.exe*
Entire Net-Work Kernel program	*<your-installation-location>\EntireNetWorkServer\bin\wcpkernel.exe*
Entire Net-Work Server Service	*<your-installation-location>\EntireNetWorkServer\bin\wcpservice.exe*
Adabas Directory Server Service	*<your-installation-location>\SoftwareAG\SoftwareAgDirectoryServer\bin\xtsdssvcadi.ex*

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

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

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

Open a Specific Port

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

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

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

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

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

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

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

Uninstallation Steps

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

Installing Fixes Using Software AG Update Manager

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

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

This SUM installation documentation on Empower provides a brief description on how to update Software AG products directly on the target machine using the Update Manager wizard. The SUM documentation also includes instructions on how to apply updates in console mode or using scripts.

≫ **To update Entire Net-Work Client, complete the following steps:**

1   Download and install Software AG Update Manager for your platform from Empower.

2   Shut down any running instances of the product. Updates cannot successfully apply if the application is active.

3   From a console prompt in the SUM */bin* directory, enter `UpdateManagerGUI.bat` (`UpdateManagerGUI.sh` on Linux).

4   On the opening page of the SUM tool, select **Install Fixes from Empower**, enter your SAG product directory root location and provide your Empower User ID and password. Click **Next**.

5   Expand through the **Adabas Family** product selection tree to find the entry for this product.

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

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

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

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

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

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

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

Uninstalling Fixes Using Software AG Update Manager

≫ **To remove an installed update, complete the following steps:**

1   Shut down any running instances of the product.

2   Start Software AG Update Manager.

3   On the opening page, select **Uninstall Fixes** from the selection panel. Click **Next**.

4   If any product selected for uninstall requires manual steps, you will be directed to review the update readme and confirm you have performed any pre-uninstallation steps. Click **Next**.

5   The fix(es) you selected for uninstall will be removed and the product(s) returned to their previous state. Click **Close** to exit SUM or **Home** to return to the tool's starting panel.

7 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 Adabas Manager (AMN) to configure the client.

Automatically Starting Entire Net-Work Client

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

> **Note:** You must manually stop the Entire Net-Work Client service 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 AMN or using the Windows Services window. This section describes all methods.

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

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

   The Entire Net-Work Client service is stopped.

> **To stop the Entire Net-Work Client service from the Adabas Manager (AMN):**

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 Adabas Manager 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 AMN.

   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.

8 Entire Net-Work Client Administration

Entire Net-Work Client administration tasks are largely performed using the Adabas Manager (AMN). Please refer to the section *Entire Net-Work Administration* in the *Adabas Manager* documentation for further details.

9 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 Adabas Manager (AMN), 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.

10 Port Number Reference

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

Port Overview and General Assignments

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

Software AG Product Component	Ports Needed	Default Port Number
Adabas Manager Communicator	One port is needed.	4980
Adabas Directory Server	One port is needed for Entire Net-Work requests to the Directory Server	4952 (IANA port) **Note:** If older versions of Entire Net-Work (older than 7.3) are in use, this port number may need to be changed to 12731.
Adabas Manager	One port is needed for Adabas Manager administration tasks	dynamically assigned
Entire Net-Work Kernel	A port is needed for Kernel access by clients	dynamically assigned
	A port is needed for Kernel access via connections (Entire Net-Work 7 or later)	dynamically assigned
	A port is needed for Kernel access via RDA connections (Entire Net-Work 2)	7869
	A port is needed for Adabas Manager administration of Kernels	dynamically assigned

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

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

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

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

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

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

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

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

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

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

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

For more information about adding Kernels, read *Adding Kernel Configuration Definitions* in the *Entire Net-Work Server LUW Installation and Administration Guide*.

Changing the Adabas Directory Server Port Number

≫ **If you need to change the Directory Server port number for your installation, follow these steps:**

1   Within the settings for Entire Net-Work Client and any client configurations definitions, change all specifications for the Directory Server port number to the new port number you want to use. Directory Server port numbers can be changed for Entire Net-Work Client and the client configurations using the Adabas Manager by changing the SAGXTSDSPORT parameter. See the *Adabas Manager* documentation for details.

2   Within the settings for Entire Net-Work Server and any Kernels definitions, change all specifications for the Directory Server port number to the new port number you want to use.

These port numbers can be changed using the Adabas Manager by changing the SAGXTSDSPORT parameter. See the *Adabas Manager* documentation for details.

3 Shut down the Entire Net-Work Client service or daemon and the Entire Net-Work Server service or daemon, as appropriate. Be sure to shut down every Kernel associated with the server as well.

For information on shutting down the Entire Net-Work Client service or daemon, read *Stopping Entire Net-Work Client* in the *Entire Net-Work Client Installation and Administration Guide*. For information on shutting down the Entire Net-Work Server service or daemon, read *Stopping Entire Net-Work Server* in the *Entire Net-Work Server LUW Installation and Administration Guide*.

4 Shut down the Directory Server service or daemon.

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

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

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

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

7 Start up the Entire Net-Work Client service or daemon and the Entire Net-Work Server service or daemon.

For information on starting up the Entire Net-Work Client service or daemon, read *Manually Starting Entire Net-Work Client* in the *Entire Net-Work Client Installation and Administration Guide*. For information on starting up the Entire Net-Work Server service or daemon, read *Manually Starting Entire Net-Work Server* in the *Entire Net-Work Server LUW Installation and Administration Guide*.

11 Entire Net-Work Configuration Parameters

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

- Entire Net-Work Adabas Manager (AMN) functions. For more information on this, refer to the section *Entire Net-Work Administration* in the *Adabas Manager* documentation.

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

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

- Use the checkadi utility function to check for a Directory Server.

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

This chapter describes both of these utilities.

The checkadi Utility

Use the checkadi utility to check for the existence of a Directory Server. The syntax of the checkadi function is:

```
checkadi [host=host-name] [[port=]port-value]
```

Use the host or port arguments to check for the existence of a Directory Server on a specific host or port number. You can use both the host and port arguments to more specifically check for a Directory Server on a specific host and port.

Example 1

In the following example, a check is run for a Directory Server on the usaxxx2 host at port 12731:

```
checkadi host=usaxxx2 port=12731
```

The following sample output from such a check might appear:

```
Software AG Entire Net-Work, Copyright ©) 1997-2019 by Software AG
USAGE: checkadi [host=hostname] [port]=portvalue]
argv[1] host=usaxxx2
Check host=usaxxx2
argv[2] port=12731
Check port=12731
Port was set to 12731
Check Host=usaxxx2
Check Port=12731
Server is Active; check if this is a Directory Server
Select Data from Directory Server successful
Bytes ready to read=309
Response=0x010x33  0x760x310x090x720x650x730x700x6f0x6e0x730x650x090x09
Expected=             0x760x310x090x720x650x730x700x6f0x6e0x730x650x090x09
Directory Server is Active
Checkadi ending ...
```

Example 2

In the following example, a check is run to determine where a Directory Server exists:

```
checkadi
```

The following sample output from such a check might appear:

```
Software AG Entire Net-Work, Copyright ©) 1997-2019 by Software AG
USAGE: checkadi [host=hostname] [port]=portvalue]
Resolve SAGXTSDSHOST
Failure Resolve Host Name; use localhost
Port was not set, so we will use the default port=12731
Check Host=usaxxx2.YYY.ww.zzz
Check Port=12731
Server is Active; check if this is a Directory Server
Select Data from Directory Server successful
Bytes ready to read=309
Response=0x010x33  0x760x310x090x720x650x730x700x6f0x6e0x730x650x090x09
Expected=         0x760x310x090x720x650x730x700x6f0x6e0x730x650x090x09
Directory Server is Active
Checkadi ending ...
```

The setadi Utility

Use the setadi utility to set Directory Server access parameters for Entire Net-Work and Entire Net-Work Client. The syntax of the setadi function is:

```
setadi {WCP|WCL} host=host-name port=port-value [XTSTRACE={value|65534}]
```

You must specify either "WCP" (to set the access parameters for Entire Net-Work) or "WCL" (to set access parameters forEntire Net-Work Client). You should also specify the host name and port number parameters. The XTSTRACE parameter is optional; if you do not specify it, a default value of "65534" is used.

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

Example 1

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

```
setadi
```

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

```
Software AG Entire Net-Work, Copyright ©) 1997-2019 by Software AG
Usage: setadi <options...>
The following options are supported:
WCP|WCL
HOST=host name
PORT=port value
XTSTRACE=value (65534)

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

Example 2

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

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

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

```
Software AG Entire Net-Work, Copyright ©) 1997-2019 by Software AG
argv[2] host=localhost
argv[3] port=12731
Check Host=localhost
Check Port=12731
Server is Active; check if this is a Directory Server
Select Data from Directory Server successful
Bytes ready to read=309
Response=0x010x33   0x760x310x090x720x650x730x700x6f0x6e0x730x650x090x09
Expected=                0x760x310x090x720x650x730x700x6f0x6e0x730x650x090x09
Directory Server is Active
CODEPATH=C:\Program Files\Software AG\Entire Net-Work Server\v74\
DATAPATH=C:\Documents and Settings\All Users\Application Data\Software AG\Entire ↵
Net-Work Server\
Changing C:\Documents and Settings\All Users\Application Data\Software AG\Entire ↵
Net-Work Server\service74.config
Changing C:\Documents and Settings\All Users\Application Data\Software AG\Entire ↵
Net-Work Server\agents\xts.config
Configuration file change successful
Setadi exiting ...
```

Index

R

release notes, 18
requirements
  browsers, 23
  firewall, 24
  operating system coverage, 22
  space, 24
  system, 22

S

setadi utility, 51
Simple Connection Line Driver
  Entire Net-Work Client post-installation updates to support,
  27
space requirements, 24
SSL support, 9
starting
  Entire Net-Work Client, 33
stopping
  Entire Net-Work Client, 33
support
  obtaining updated documentation, 19
  platforms supported, 22
support for prior versions, 18
supported browsers, 23
supported hardware, 23
supported operating systems, 22
supported platforms, 22
system requirements, 22

T

TECHcommunity website, 19

U

utility functions
  checkadi, 50
  for the Directory Server, 49
  setadi, 51

W

Windows Personal Firewall, 29