Entire Net-Work Administration

Software AG Directory Server Documentation

Version 5.9.1

September 2009

Entire Net-Work

This document applies to Entire Net-Work Administration Version 5.9.1 and to all subsequent releases.

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

Table of Contents

1 Software AG Directory Server Documentation

This document describes the Software AG Directory Server and explains how to use and maintain it.

It is intended for system administrators in your enterprise.

This document is organized as follows:

●	*Software AG Directory Server Concepts*	Introduces you to the Software AG Directory Server and explains how use partitioning in a Directory Server
●	*Performing Software AG Directory Server Administration*	Describes administrative tasks you can perform for the Software AG Directory Server.
●	*Advanced Directory Server Configuration*	Describes advanced configuration tasks you can perform for the Software AG Directory Server.
●	*Advanced Support Operations*	Describes advanced support tasks you can perform for the Software AG Directory Server with the assistance of Software AG Customer Support.

2 Software AG Directory Server Concepts

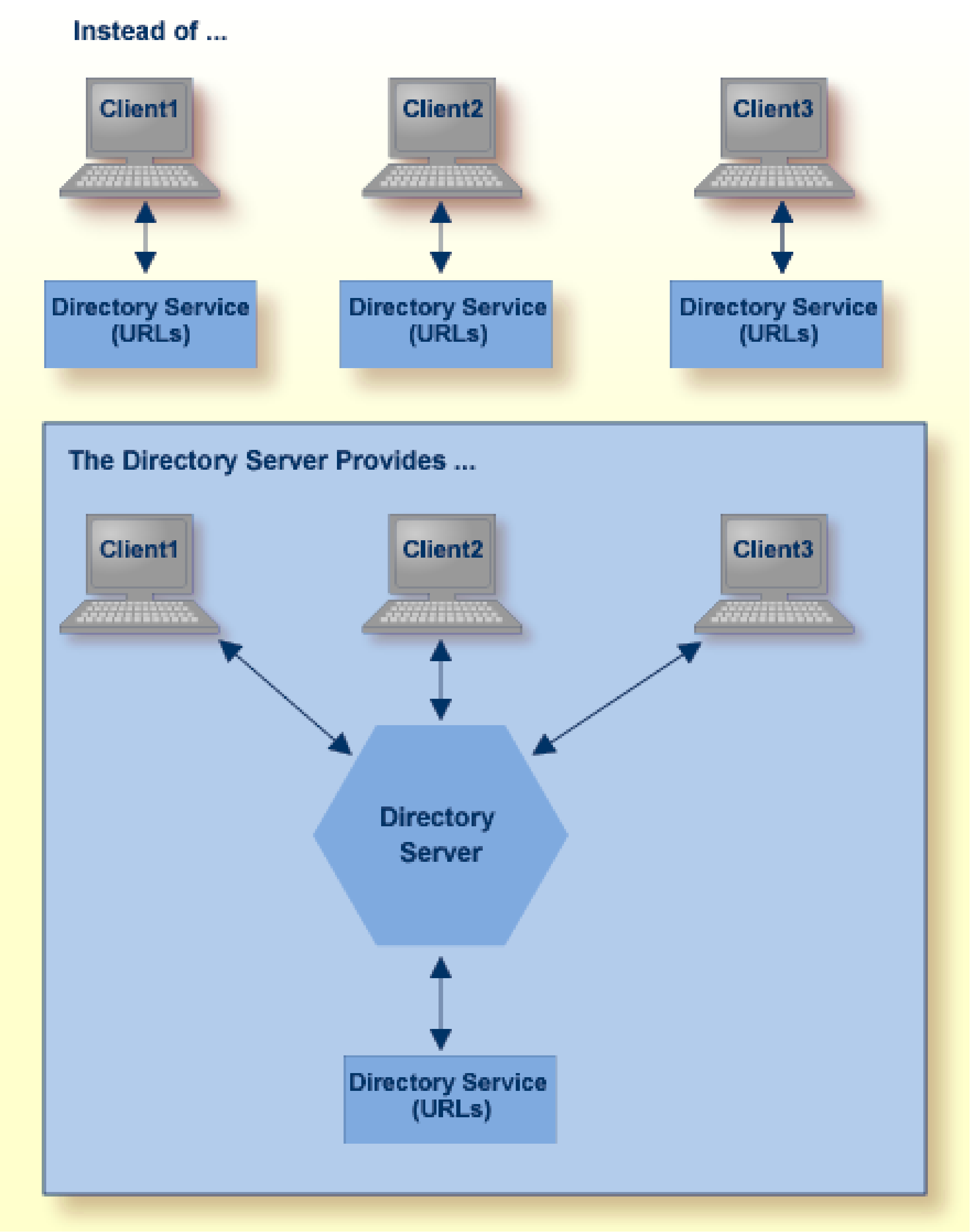
This chapter covers the following topics:

- *What is the Directory Server?*
- *Partitioning a Directory Server*
- *Identifying Which Directory Server To Use*
- *Starting and Stopping the Software AG Directory Server*
- *Directory Server Target Entries*

3 What is the Directory Server?

The Software AG Directory Server provides central management of directory services. It runs as either a Windows service or a UNIX daemon.

Instead of individual directory service configuration files for each application or machine, a centralized Directory Server enhances control and management of configuration, as shown in the figure below.

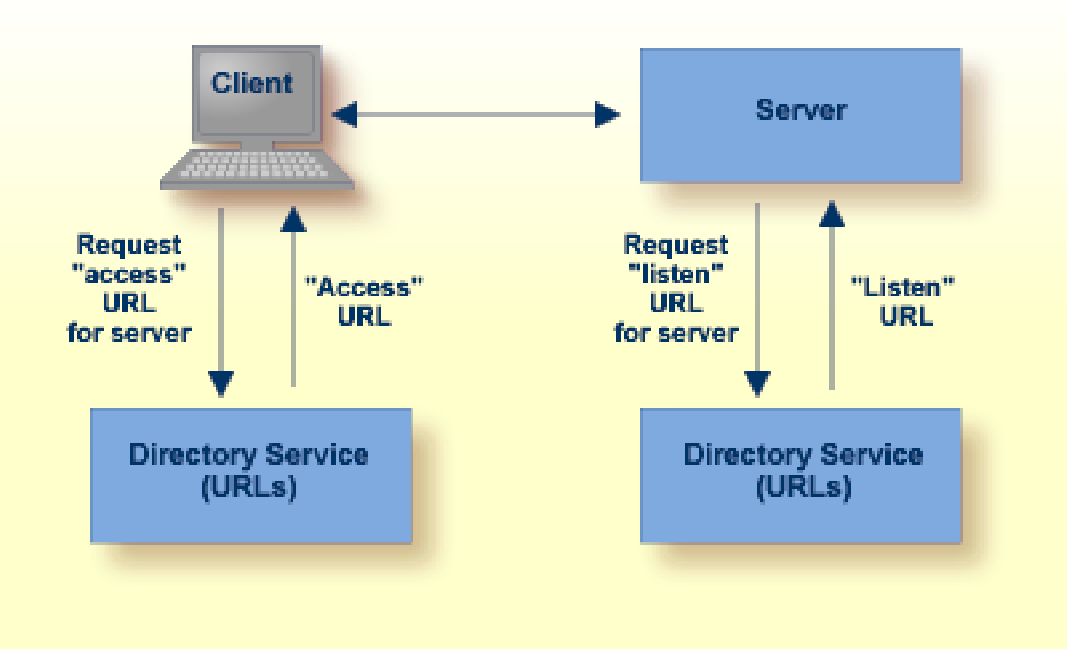


All directory information required to accomplish communication between clients and servers is obtained from the Directory Server. Only Directory Server address information, essentially the host and port of the Directory Server, is required for clients and servers to use the Directory Server.

Software AG recommends that you use only one Directory Server in your enterprise. However, if you install more than one, remember:

- You will have to manage and administer multiple Directory Server configurations.
- The more Directory Servers you use, the more physical resources on your system will be consumed.
- You will need to be very careful about which Directory Server you select to use in your installation of a Software AG product -- 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 *directory services* are Uniform Resource Locators (URLs) used to identify the locations of Adabas databases, Entire Net-Work Kernels, and other target servers. These URLs allow a client to access a target server and allow a target server to "listen" for clients, as shown in the figure below.



4 Partitioning a Directory Server

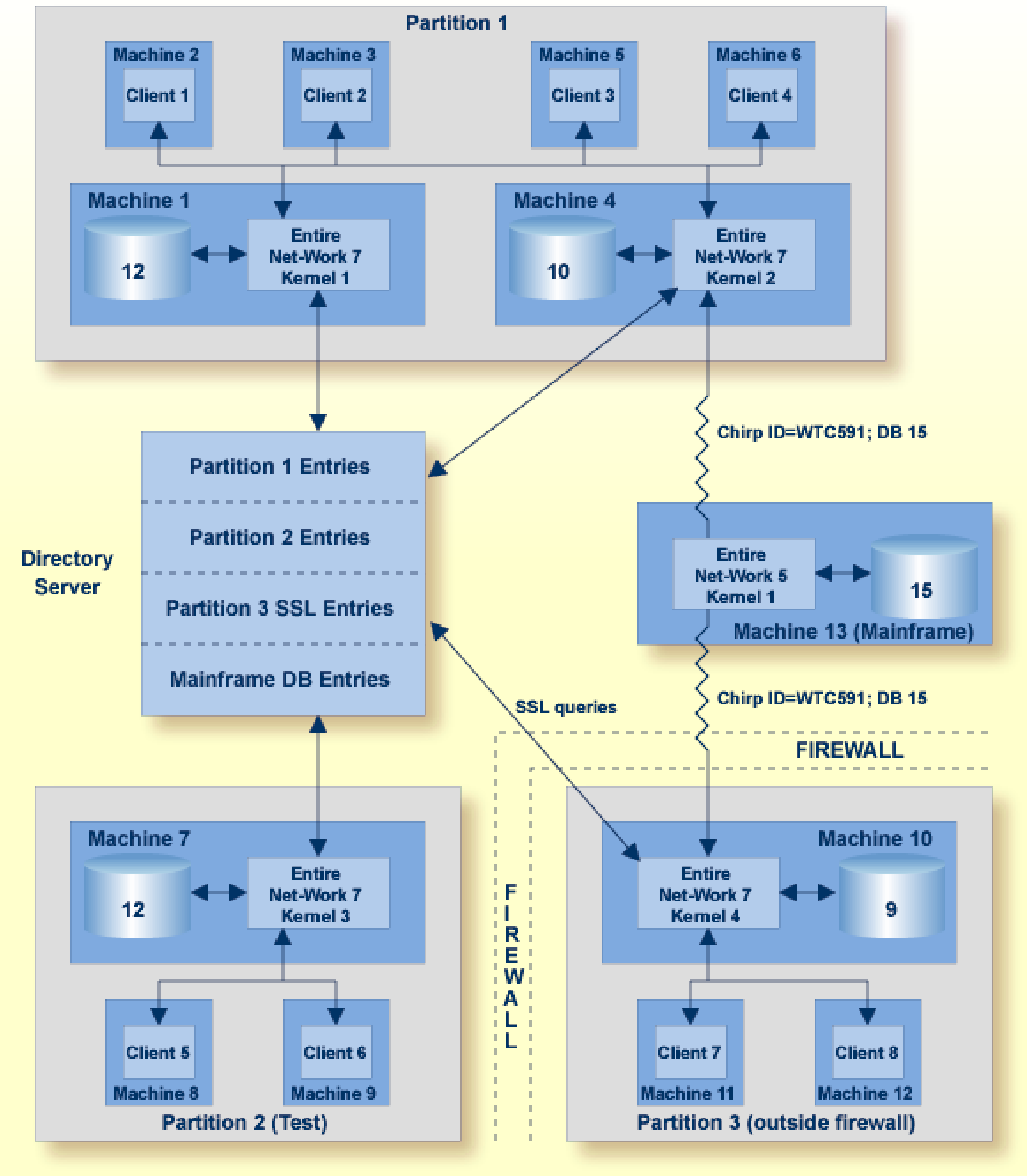
Partitioning enhances your ability to use one Directory Server for your whole enterprise, rather than separate Directory Servers for different departments within your enterprise. The partitions each need to be managed separately, but only one Directory Server needs to be installed.

Here are some of the advantages of partitioning:

- You can use partitioning to direct specific clients 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 Entire Net-Work on the mainframe to access a specific Adabas database. Simply remove the access URL entries for the databases from the appropriate partition.
- If your Software AG product supports the use of SSL, you can use impose real security requirements on calls made by clients in specific partitions.

Partitions can be defined for a Directory Server in the System Management Hub. For complete information on maintaining partitions and the targets in them, read ***Maintaining Partitions*** and ***Maintaining Targets***, elsewhere in this chapter.

Suppose you configure your network as depicted in the following diagram:



In this diagram, partitioning is used to:

- Restrict calls for Database 12 (on Machine 1) and Database 10 (on Machine 4) to Clients 1 through 4 in the Partition 1 partition.
- Restrict calls for Database 12 on Machine 7 to clients in the Partition 2 (Test) partition.

- Establish a test environment. The Partition 2 (Test) partition has been set up as a testing partition. Only Clients 5 and 6 are included in it and use Database 12 on Machine 7.
- Group calls to Database 15 on the mainframe. The calls to this database are grouped by the Kernel 2 in Partition 1 and Kernel 4 in Partition 3, thus reducing the number of connections necessary for the database.
- Impose security, via SSL, on the clients who are outside the firewall. Clients in Partition 3 are outside the company firewall. Security restrictions are also enforced when accessing Database 9, which is also outside the security firewall.

Partitions are assigned clients during client installation. If you need to change the partition assigned a client after installation, contact your Software AG technical representative for instructions.

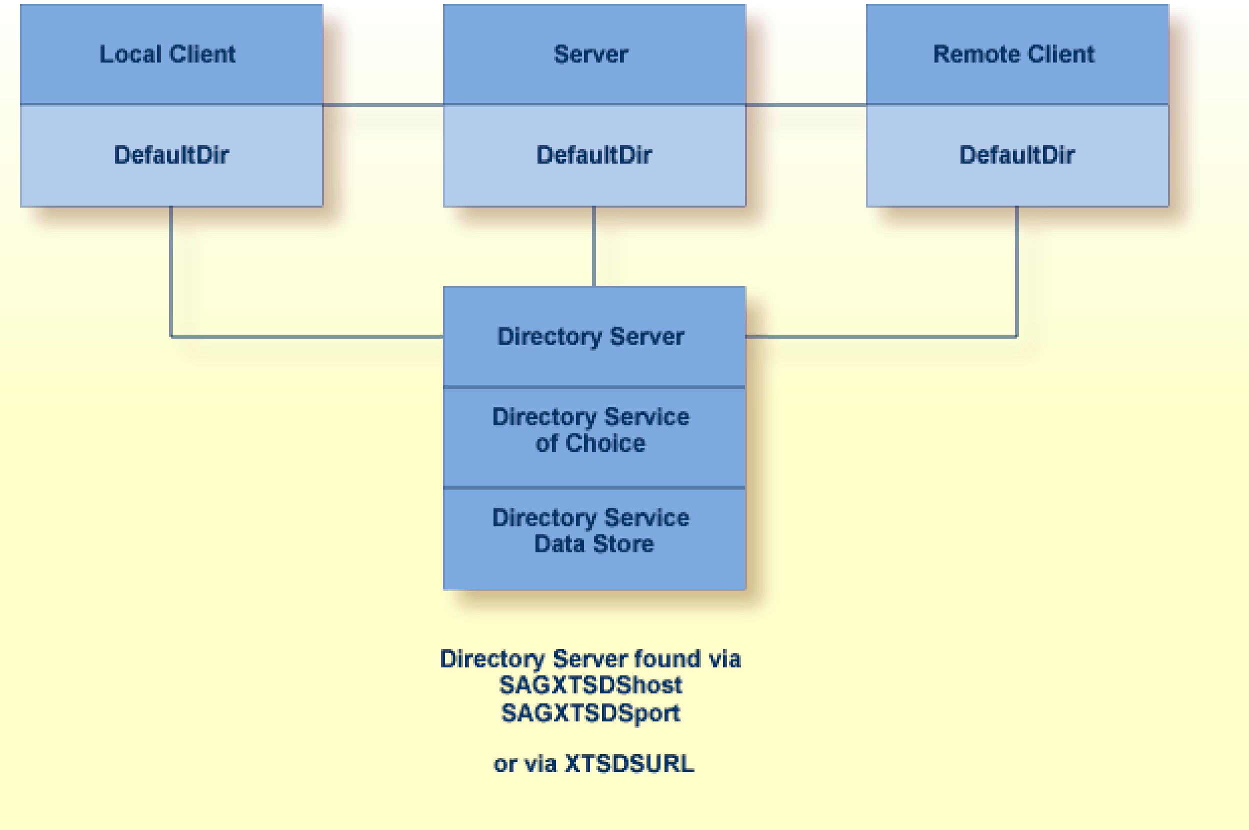
5 Starting and Stopping the Software AG Directory Server

The Directory Server runs as either a Windows service or a UNIX daemon. To start or stop it, simply start or stop the service or daemon -- as you would any other Windows service or UNIX daemon.

6 Identifying Which Directory Server To Use

More than one Directory Server may be installed for your organization. This chapter describes how Software AG products determine which Directory Server to use.

The Directory Server implementation diagram is shown below.



Software AG products obtain the address of the Directory Server by searching the following sources in the specified order:

1. The environment variable `xtsdsurl`. For example,

   ```
   set xtsdsurl=tcpip://dshost:port
   ```

2. An `xtsdsurl` parameter passed by an application call.
3. The well-known names *SAGXTSDShost* and *SAGXTSDSport*.

   Port 12731 is used if the well-known name *SAGXTSDSport* is not defined.

   The well-known names can be defined to a DNS server or as an alternative they can be defined in a local "hosts" file. Use of the local "hosts" file implies manual reconfiguration should the Directory Server host change, but it has the advantage of supporting different Directory Servers per computer. Using `xtsdsurl` has the advantage of using different Directory Servers per process.

   The following table defines the well known names, their purpose, and encoding requirements.

Name	Purpose
SAGXTSDShost	Specifies the IP address of the Directory Server.
SAGXTSDSport	Specifies, through an encoded IP address, the listen port of the Directory Server. The encoded IP address is in the following format: `nnnn.mmmm.0.0` ""where: *nnnn* = port / 256 *mmmm* = port % 256 (256 modulus) The default port is "12731", therefore the encoded default port is "49.187.0.0" .

7 Directory Server Target Entries

Software AG communication information for your product is stored in one or more Software AG Directory Servers. The client's send message includes the target server name. Your Software AG product forwards the name and a use qualifier to the Directory Server, which returns an appropriate qualified URL (Universal Resource Locator) for the target back to your product.

Physical connection information (transport protocol , protocol specific parameters, timeout, and so on) must be entered in Directory Server target entries as qualified URLs before this communication can occur. The qualified URL contains the information required to direct the message to the correct target. The qualifier identifies which target URL is to be returned, based on the use implied by the qualifier. For example, a client *send* request returns an *access* target URL .

Directory Server target entries can be added manually using the System Management Hub. For more information, read ***Maintaining Targets***, elsewhere in this guide.

This chapter covers the following topics:

Qualified URL Structure

Physical connection information (transport protocol , protocol specific parameters, timeout, and so on) must be entered in the Directory Server target entries as qualified URLs before the Directory Server can be used for Software AG communication. Each qualified URL is specified in this format:

```
qualifier.protocol://host:port[?parm=value][&parm=value]...
```

For example:

```
access.tcpip://serverhost:3001?retry=3
```

Entry	Meaning
qualifier	The use of this target URL. Three types of qualifiers are supported: "access", "connect", and "listen". For more information, read ***Qualifiers***, elsewhere in this section.
protocol	The communication protocol that will be used to connect to the server. For more information, read ***Protocols***, elsewhere in this section.
host	The name of the host computer where the server runs.
port	The server's port. Port is a destination or a receiving port dependent upon URL usage. See next table.
parm	One of multiple optional parameters that can be used. The first parameter is preceded by a "?" and subsequent parameters, if any, are preceded by an "&". For more information, read ***Parameters***, elsewhere in this section.
value	The value of the parameter.

Qualifiers

URLs are qualified in the Directory Server target entries by their use. Qualifiers are used to specify this use. Three qualifiers (uses) of a URL are supported in the Software AG Directory Server, as described in the following table:

Qualifier (Use)	Description
access	Defines a communication path between the client and the server. The path provides the means for the client to communicate with the server either directly or through a proxy; this communication path tells the client where to find the server. Internally, a URL with this specification appears as an "XTSaccess" URL.
listen	Defines a listen port for the server or the proxy. Internally, a URL with this specification appears as an "XTSlisten" URL.
connect	Defines an active connection between a server and a proxy or between a proxy and an Entire Net-Work node. Internally, a URL with this specification appears as an "XTSconnect" URL.

Protocols

The following communication protocols can be used in Directory Server URLs.

Protocol	Description
HTTP11	Although this protocol is still listed on Directory Server administration screens in the System Management Hub, this protocol is no longer supported.
MHDR	Only Software AG products that require the proxy can use this protocol. The MHDR protocol allows the proxy to communicate with these Software AG products. The MHDR protocol supports two-byte database IDs; therefore, databases with database IDs greater than "255" can be accessed using this protocol.
RDA	Only Software AG products that require the proxy can use this protocol. The RDA protocol allows the proxy to communicate with these Software AG products. The RDA protocol does not support two-byte database IDs; therefore access is limited to database IDs less than "256".
SSL	The SSL (Secure Sockets Layer) protocol enables secure TCP/IP connections.
TCP/IP	The TCP/IP protocol is the standard communication protocol used. It provides the most basic and efficient service.

Parameters

The parameters you can specify in a qualified URL vary, depending on the protocol and qualifier selected. The following table describes the parameters available and indicates which protocols and qualifiers support them.

Parameter	Qualifier Support	Protocol Support	Description
`cafile`	access connect listen (Client authentication only)	SSL - C applications only	Identifies the file containing the trusted CA certificates. The CA's certificate that signed an inbound certificate must reside in this file. **Note:** The file name specified may include the path information, unless a value for parameter `capath` is specified. The `cafile` and `capath` parameters are required for client and server authentication.
`capath`	access connect listen (Client authentication only)	SSL - C applications only	Supplies a hash value generated by the OpenSSL tool that specifies the location of a `cafile` in a complex CA structure. This location is not a path. If parameter `cafile` includes location information, the value of `capath` should be ".", which is also the `capath` default. The `cafile` and `capath` parameters are required for client and server authentication.
`cert_file`	access (Client authentication only) connect listen	SSL - C applications only	Specifies the file containing the participant's certificate. The certificate file may contain the participant's private key. **Note:** The file name specified may include the path information. This is useful if the certificate is not in the current directory.
`cert_passwd`	access (Client authentication only) connect listen	SSL - C applications only	Specifies the password for extracting information from the certificate file. **Note:** You can specify a fully-qualified file name for this parameter. In this case, the file name you provide must contain the password.
`charset`	all	RDA	Identifies the character encoding of the classic Entire Net-Work node associated with the URL. The value "EBCDIC" must be specified when and only when

Parameter	Qualifier Support	Protocol Support	Description
			the URL is for a mainframe connection; no other value can be specified. The default value is "ASCII" which applies to non-mainframe connections.
chirpinterval	all	RDA SSL TCP/IP	Specifies the number of seconds to wait between chirp attempts for this connection. Chirping is the communication mechanism used to validate the availability of the connection specified by the URL. The valid range is "0" through the maximum integer that can be stored by your operating system. The default value is "300"seconds (5 minutes). A value of "0" implies the default, "300".
key_file	all	SSL - C applications only	Specifies the file containing the server's private key. Must be specified if the private key is kept separate from the certificate file. **Note:** The file name specified may include the path information. This is useful if the certificate is not in the current directory.
keystore	access (Client authentication only) connect listen	SSL - Java application only	Identifies the Java keystore containing the participant's certificate and private key.
keystore_passwd	access (Client authentication only) connect listen	SSL - Java application only	Specifies the password for extracting information from keystore.
node	all	RDA	Specifies the node ID by which this node will be known to a classic Entire Net-Work installation. The valid range is 1 through 65535. The default value is "7654". If more than one proxy is connected in the same Entire Net-Work domain, the node and nodename must be given to avoid conflicts.
nodename	all	RDA	Specifies the node name by which this node will be known to a classic Entire Net-Work installation. The default value is the name of the proxy. If more than one proxy is connected in the same Entire Net-Work domain, the node and nodename must be given to avoid conflicts.
priority	---	none	Reserved for future use.

Parameter	Qualifier Support	Protocol Support	Description
`random_file`	all	SSL - C applications only	Identifies a text file that contains at least 14 random characters. The random characters in this file are used by the encryption routines to ensure that encryption itself occurs in a random manner.
`raw`	all	RDA SSL TCP/IP	Indicates whether transport subsystem headers are sent. If present, then no transport subsystem headers are sent and no proxy is possible. Values are "on" and "off". The default value is "off". RDA target entries must specify `raw=on` or the connections will not work.
`reconnect`	all	RDA SSL TCP/IP	Indicates whether or not to reconnect if disconnected. Values are "on" or "off". The default value is "on".
`recvtimeout`	all	RDA SSL TCP/IP	Specifies a protocol timeout value in seconds. Valid values range from "0" through the maximum integer that can be stored by your operating system. The default is "60" seconds. A value of "0" implies the default, "60". This parameter is most useful for performance tuning. We do not recommend that you modify this parameter unless necessary. For assistance, contact Software AG Customer Support.
`retry`	all	RDA SSL TCP/IP	Specifies the number of times to retry a connection. The valid range is 0 through 2147483648. The default value is "0" (no retry).
`retryint`	all	RDA SSL TCP/IP	Specifies the interval in seconds between retries. The valid range is 0 through 2147483648. The default value is "60000" seconds.
`security`	all	RDA	Specifies the name of a security file containing a list of IP addresses authorized to access this protocol. There is no default value.
`sendtimeout`	all	RDA SSL TCP/IP	Specifies a protocol timeout value in seconds. Valid values range from "0" through the maximum integer that can be stored by your operating system. The default is "60" seconds. A value of "0" implies the default, "60".

Parameter	Qualifier Support	Protocol Support	Description
			This parameter is most useful for performance tuning. We do not recommend that you modify this parameter unless necessary. For assistance, contact Software AG Customer Support.
`trace`	all	RDA SSL TCP/IP	Indicates whether or not to trace this connection. Values are "on" or "off". The default value is "off".
`truststore`	access connect listen (Client authentication only)	SSL - Java application only	Identifies the Java truststore containing the trusted CA certificates. The CA's certificate that signed an inbound certificate must reside in this file.
`truststore_passwd`	access connect listen (Client authentication only)	SSL - Java application only	Specifies the password for extracting information from the truststore.
`ttl`	---	none	Reserved for future use.
`verify`	access connect listen (Client authentication only)	SSL - both C and Java applications	Identifies the certificate processing level. For C applications, valid values are: 0 (No peer verification occurs. This is the default value.) 1 (The application requests that the peer certificate be verified.) 2 (The application requests that the peer certificate be verified. A fatal condition occurs if there is no certificate.) 4 (The application requests that the peer certificate be verified only once.) 8 (The application requests that the issuer name is checked against the host name.) Values 1, 2, and 4 can be specified in combination. For example, if you want to specify both 1 and 2, you would add them and set the `verify` parameter to "3". **Note:** This parameter must be set to "3" if you are performing client authentication.

Parameter	Qualifier Support	Protocol Support	Description
			For Java applications, valid values are: 0 (No peer verification occurs. This is the default value.) 1 (The application requests that the peer certificate be verified.) 2 (The application requests that the peer certificate be verified. A fatal condition occurs if there is no certificate.) Values 4 and 8 are not valid for Java.
`version`	all	SSL - both C and Java applications	Indicates the SSL version: 1 (TLSv1) 2 (SSLv2). This value is required for Java applications. 3 (SSLv23). For C applications only, this indicates that Version 2 or 3 should be used. 4 (SSLv3)

8 Performing Software AG Directory Server Administration

This chapter describes the administration tasks you can perform for the Directory Server using the System Management Hub.

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

This chapter covers the following topics:

- *The Directory Server Administration Area*
- *Refreshing SMH Displays*
- *Maintaining Directory Server Links*
- *Maintaining Partitions*
- *Maintaining Targets*
- *Specifying Trace Settings*
- *Changing Hosts*

9 The Directory Server Administration Area

To access the Directory Server administration area of the System Management Hub (SMH):

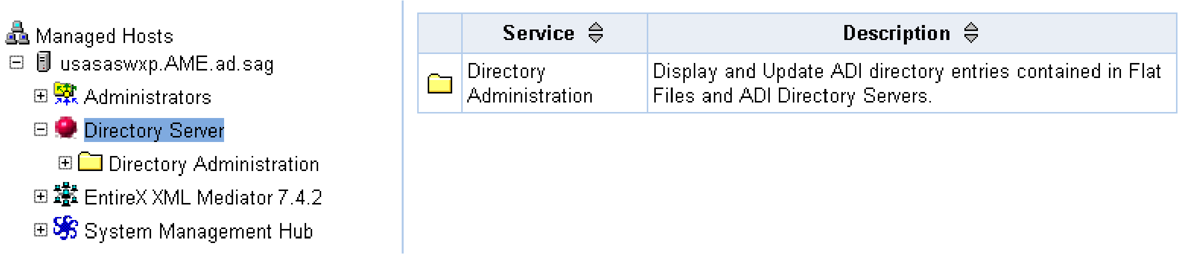
Make sure you have started and logged into the System Management Hub.

1 Select the name of the managed host on which the Directory Server is installed.

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

3 Select and expand "Directory Server" in the tree-view under the managed host.

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



	Service	Description
	Directory Administration	Display and Update ADI directory entries contained in Flat Files and ADI Directory Servers.

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

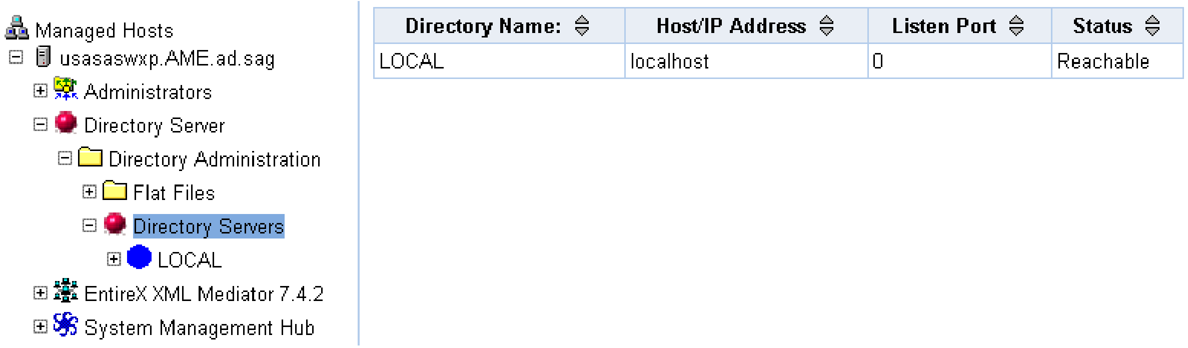
Two types of Software AG Directory Server administration are listed: **Flat Files** and **Directory Servers**.

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

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

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

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



Directory Name:	Host/IP Address	Listen Port	Status
LOCAL	localhost	0	Reachable

The following commands are available in the command menu of the Directory Server administration area or by right-clicking on **Directory Servers** in tree-view:

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

Button	Use this command to:
Add Directory Server	Add a new directory server, linked to this SMH.
Set Trace Options	Set trace options for the directory servers linked to this SMH.
Refresh	Refresh the screen.

10 Refreshing SMH Displays

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

11 Maintaining Directory Server Links

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

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

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

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

This chapter covers the following topics:

Listing Linked Directory Servers

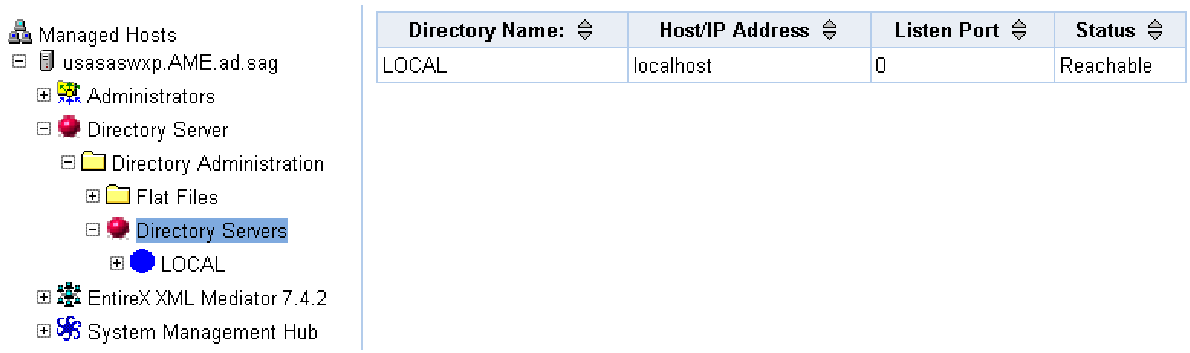
▶ To list the installed Directory Servers that are linked to SMH:

1 Access the Directory Server administration area, as described in ***The Directory Server Administration Area***, earlier in this section.

2 Select **Directory Servers** in the tree-view frame.

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

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



Directory Name:	Host/IP Address	Listen Port	Status
LOCAL	localhost	0	Reachable

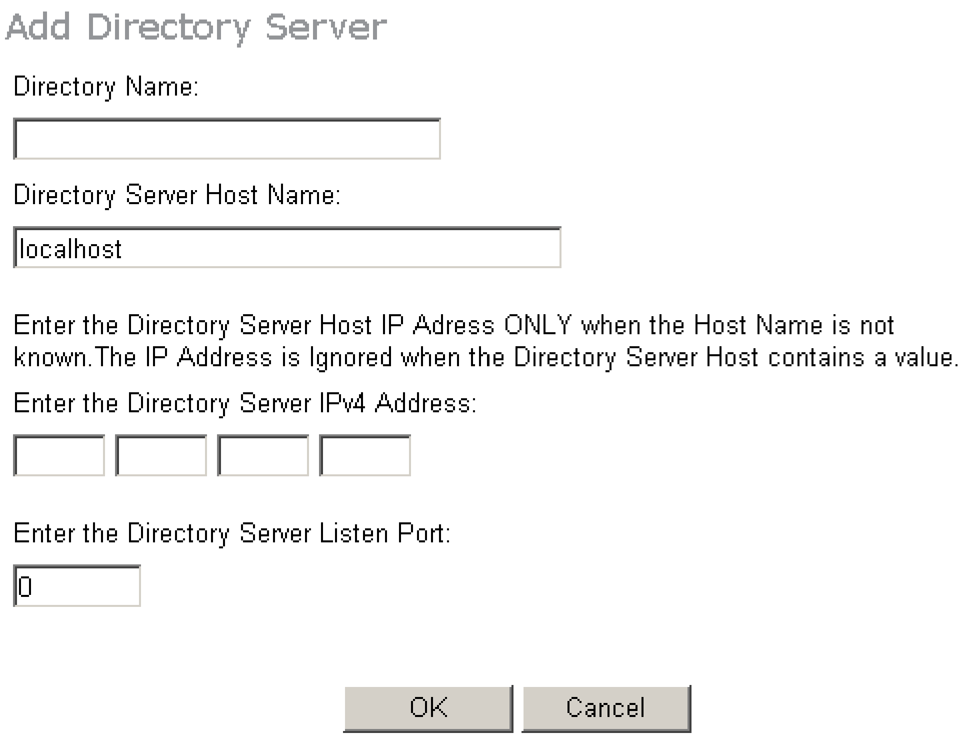
Adding a Link to a Directory Server

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

1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.

2 Run the `Add Directory Server` command in the command menu of SMH. Be sure you have **Directory Servers** selected in the tree-view frame to see this command.

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



Add Directory Server

Directory Name:

Directory Server Host Name:

localhost

Enter the Directory Server Host IP Adress ONLY when the Host Name is not known.The IP Address is Ignored when the Directory Server Host contains a value.

Enter the Directory Server IPv4 Address:

Enter the Directory Server Listen Port:

0

3 Specify a user-friendly name for the Directory Server in the **Directory Name** field.

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

Note: Host names are case-sensitive in SMH.

Or:

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

5 Generally it is best to leave the **Directory Server Listen Port** as "0". If set to "0", then the port used will be that defined by the well-known name *SAGXTSDSport* or "12731", if *SAGXTSDSport* is not defined. If you have problems accessing the Directory Server, contact your system administrator for the correct port setting to use.

6 Click OK.

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

Modifying a Directory Server Link Definition

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

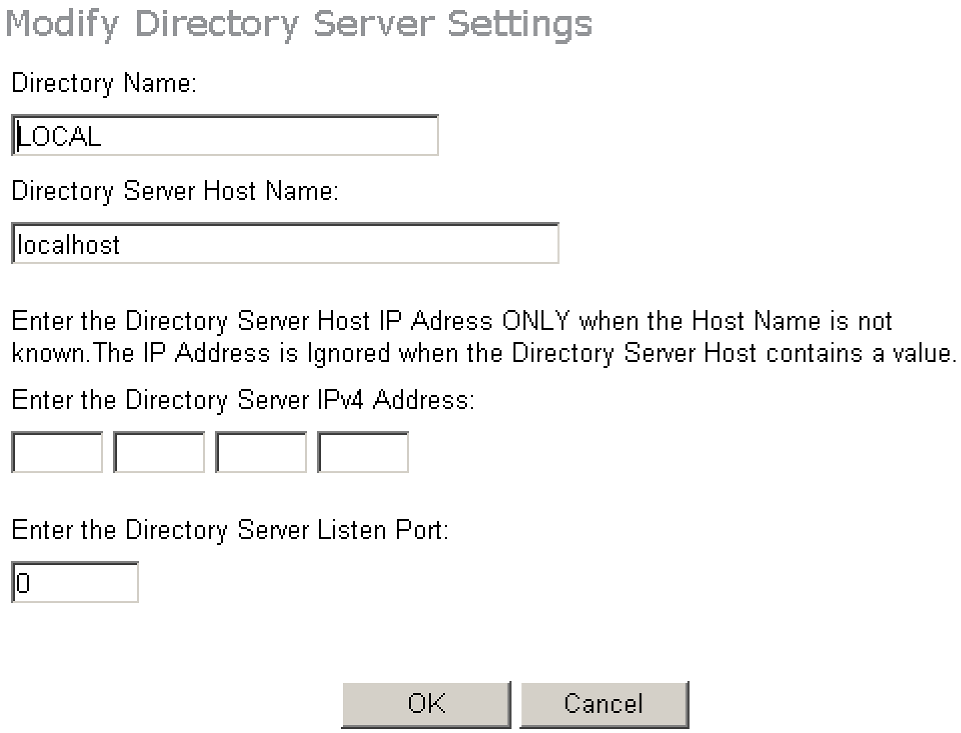
1 Access the Directory Server administration area, as described in ***The Directory Server Administration Area***, earlier in this section.

2 Click on the name of the Directory Server whose link definition you wish to modify in the tree-view frame of SMH.

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

3 Click on the `Modify Directory Server Settings` command in the command menu of SMH. You can also see this menu by right-clicking on the name of the Directory Server whose link definition you wish to modify.

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



Modify Directory Server Settings

Directory Name:

LOCAL

Directory Server Host Name:

localhost

Enter the Directory Server Host IP Adress ONLY when the Host Name is not known.The IP Address is Ignored when the Directory Server Host contains a value.

Enter the Directory Server IPv4 Address:

Enter the Directory Server Listen Port:

0

4 Change the name for the Directory Server in the **Directory Name** field.

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

Note: Host names are case-sensitive in SMH.

Or:

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

6 Change the **Directory Server Listen Port** as needed.

Generally it is best to leave the **Directory Server Listen Port** as "0". If set to "0", then the port used will be that defined by the well-known name *SAGXTSDSport* or "12731", if *SAGXTSDSport* is not defined. If you have problems accessing the Directory Server, contact your system administrator for the correct port setting to use.

7 Click OK.

The Directory Server link definition is modified.

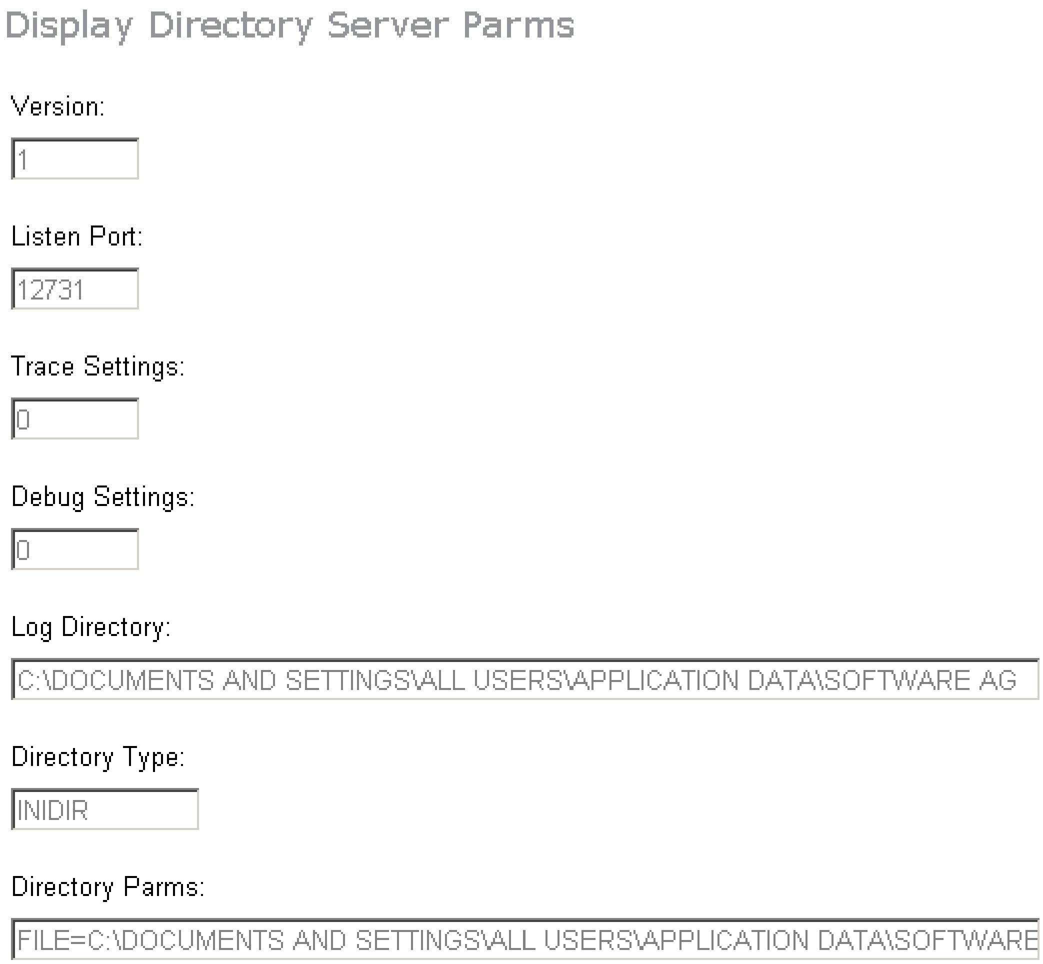
Listing Directory Server Parameters

▶ To display the parameters for a Directory Server:

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

   The targets for that Directory Server are listed in the detail-view frame.
3. Click on the `Display Directory Server Parms` command in the command menu of SMH. You can also see this menu by right-clicking on the name of the Directory Server whose parameters you wish to review.

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



Display Directory Server Parms

Version:

1

Listen Port:

12731

Trace Settings:

0

Debug Settings:

0

Log Directory:

C:\DOCUMENTS AND SETTINGS\ALL USERS\APPLICATION DATA\SOFTWARE AG

Directory Type:

INIDIR

Directory Parms:

FILE=C:\DOCUMENTS AND SETTINGS\ALL USERS\APPLICATION DATA\SOFTWARE

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

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

Deleting a Link to a Directory Server

▶ To delete the link to an Directory Server in SMH:

1 Access the Directory Server administration area, as described in ***The Directory Server Administration Area***, earlier in this section.

2 Click on the name of the Directory Server whose definition you wish to delete in the tree-view frame of SMH.

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

3 Click on the `Delete Directory Server Entry` command in the command menu of SMH. You can also see this menu by right-clicking on the name of the Directory Server whose definition you wish to delete.

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

4 Click OK.

The Directory Server definition is deleted.

12 Maintaining Partitions

This chapter covers the following topics:

Listing the Partitions

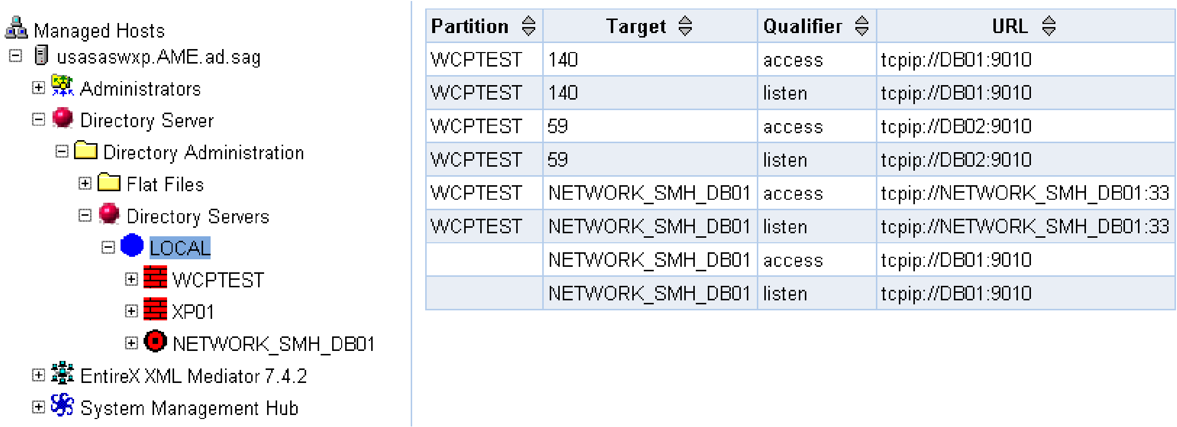
You can list the partitions defined for a Directory Server using the System Management Hub.

To list the partitions defined in a Directory Server:

1 Access the Directory Server administration area, as described in ***The Directory Server Administration Area***, earlier in this section.

2 Click and expand the name of the Directory Server whose partitions you wish to review in the tree-view frame of SMH.

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



Partition	Target	Qualifier	URL
WCPTEST	140	access	tcpip://DB01:9010
WCPTEST	140	listen	tcpip://DB01:9010
WCPTEST	59	access	tcpip://DB02:9010
WCPTEST	59	listen	tcpip://DB02:9010
WCPTEST	NETWORK_SMH_DB01	access	tcpip://NETWORK_SMH_DB01:33
WCPTEST	NETWORK_SMH_DB01	listen	tcpip://NETWORK_SMH_DB01:33
	NETWORK_SMH_DB01	access	tcpip://DB01:9010
	NETWORK_SMH_DB01	listen	tcpip://DB01:9010

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

Adding a Partition

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

▶ To add a partition in the Directory Server:

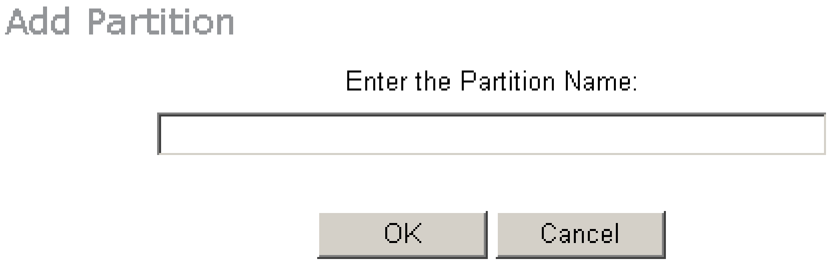
1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.

2 In the tree-view frame of SMH, click and expand the name of the Directory Server to which you want to define partitions.

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

3 Click on the `Add Partition` command in the command menu of SMH. You can also see this menu by right-clicking on the name of the Directory Server to which you want to add a partition.

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



4 Specify a name for the partition in the **Enter the Partition Name:** field.

5 Click OK.

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

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

Changing a Partition Name

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

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

To change the name of a partition:

1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.

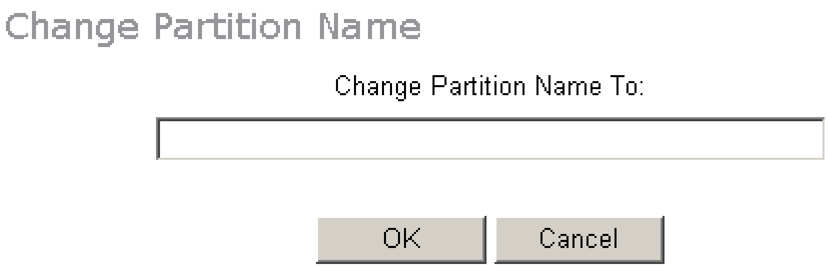
2 In the tree-view frame of SMH, click and expand the name of the Directory Server containing the partition you want to rename.

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

3 Click on the name of the partition you want to rename.

4 Click on the `Change Partition Name` command in the command menu of SMH. You can also see this menu by right-clicking on the name of the partition.

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



5 Specify a new name for the partition in the **Change Partition Name To** field.

6 Click OK.

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

Deleting a Partition

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

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

To delete a partition in a Directory Server:

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

   The partitions and targets for that Directory Server are listed in the detail-view frame.
3. Click on the partition you wish to delete.
4. Click on the `Delete Partition` command in the command menu of SMH. You can also see this menu by right-clicking on the name of the partition.

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

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

13 Maintaining Targets

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

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

This chapter covers the following topics:

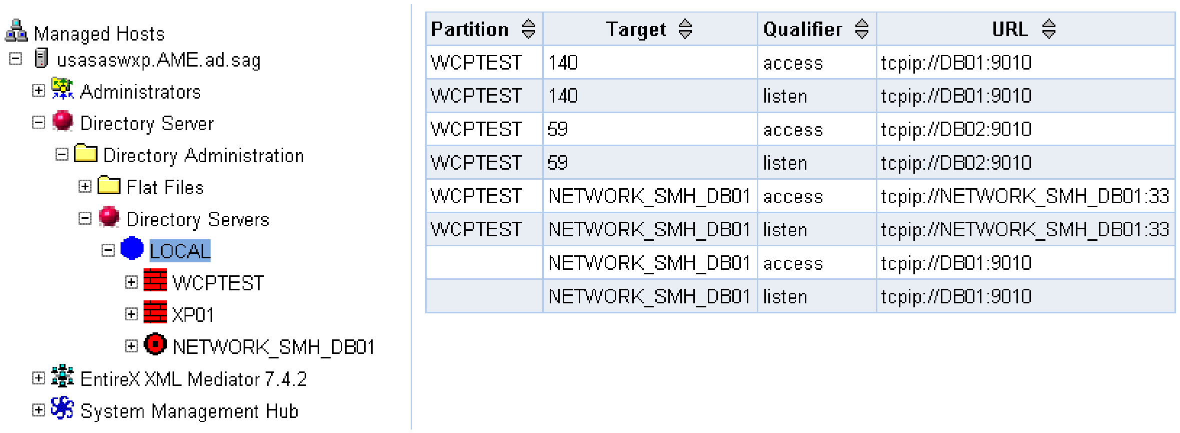
Listing the Targets

To list the targets defined in a Directory Server:

1 Access the Directory Server administration area, as described in ***The Directory Server Administration Area***, earlier in this section.

2 Click and expand the name of the Directory Server or the partition within a Directory Server whose targets you wish to review in the tree-view frame of SMH.

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



Partition	Target	Qualifier	URL
WCPTEST	140	access	tcpip://DB01:9010
WCPTEST	140	listen	tcpip://DB01:9010
WCPTEST	59	access	tcpip://DB02:9010
WCPTEST	59	listen	tcpip://DB02:9010
WCPTEST	NETWORK_SMH_DB01	access	tcpip://NETWORK_SMH_DB01:33
WCPTEST	NETWORK_SMH_DB01	listen	tcpip://NETWORK_SMH_DB01:33
	NETWORK_SMH_DB01	access	tcpip://DB01:9010
	NETWORK_SMH_DB01	listen	tcpip://DB01:9010

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

Adding Targets

You can add targets to the Directory Server directly, within a partition of the Directory Server, or both. For information on the use of partitions in a Directory Server, read ***Partitioning a Directory Server***, elsewhere in this guide.

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

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

▶ **To add a target definition:**

1 Access the Directory Server administration area, as described in ***The Directory Server Administration Area***, earlier in this section.

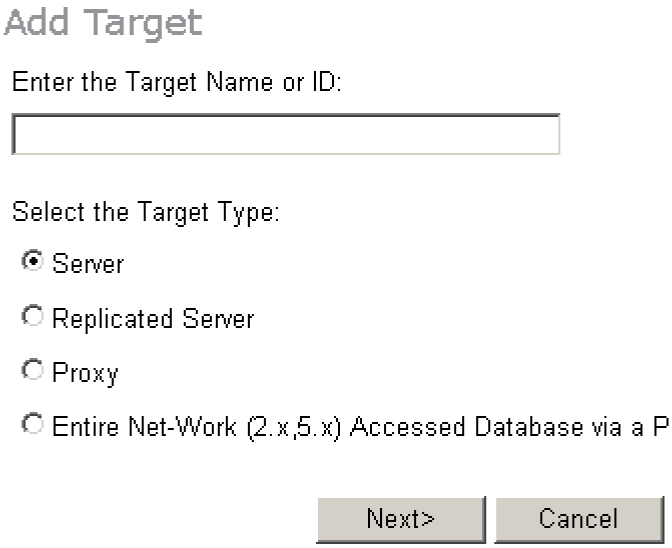
2 In the tree-view frame of SMH, click and expand the name of the Directory Server to which you want to define the target.

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

3 Optionally, if you want to define the target to a specific partition, click and expand the a name of the partition in the tree-view frame of SMH.

4 Click on the `Add Target` command in the command menu of SMH. You can also see this menu by right-clicking on the name of the Directory Server or partition to which you wish to add the target..

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



Add Target

Enter the Target Name or ID:

Select the Target Type:

● Server

○ Replicated Server

○ Proxy

○ Entire Net-Work (2.x,5.x) Accessed Database via a Proxy

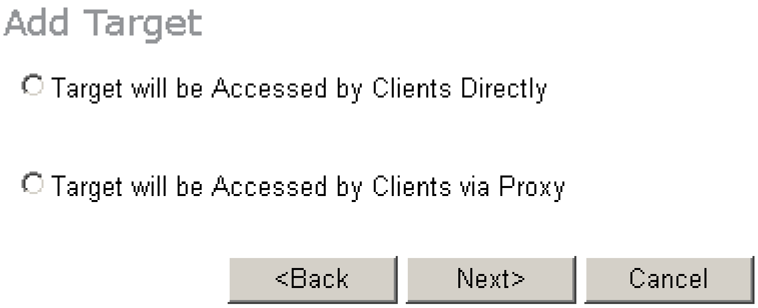
5 Enter the database ID (DBID) into the **Target Name or ID** field.

6 Ensure that the **Server** option is selected.

- The **Server** option is usually the option you should select.
- The **Replicated Server** option is reserved for future use by Software AG.
- The **Proxy** option is only applicable to configurations requiring a proxy. It is provided for compatibility with Software AG products that still require a proxy. If your Software AG product requires a proxy, refer to the documentation for your Software AG product for information about proxies and how to configure them in SMH.

7 Click **Next**.

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



Add Target

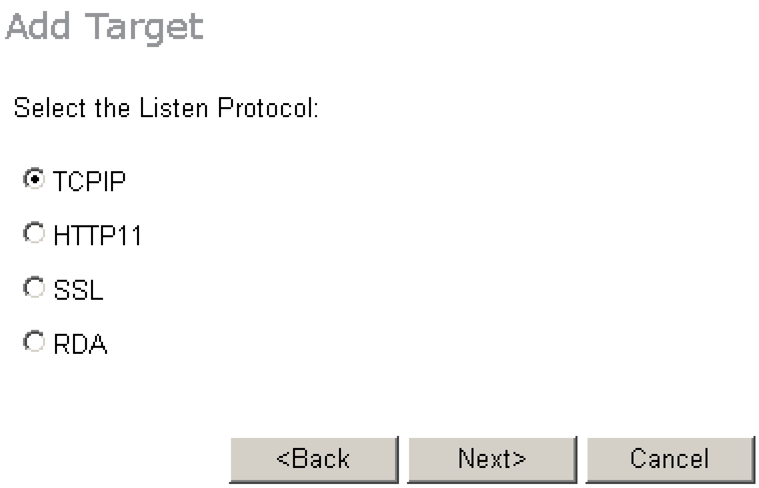
○ Target will be Accessed by Clients Directly

○ Target will be Accessed by Clients via Proxy

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

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

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



Add Target

Select the Listen Protocol:

● TCPIP

○ HTTP11

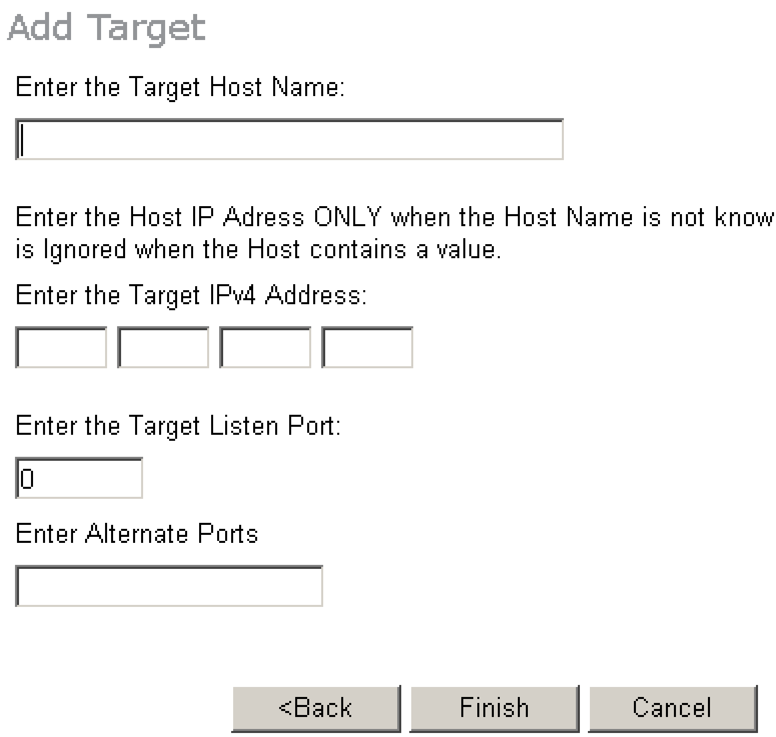
○ SSL

○ RDA

9 Select the listen protocol, then click **Next**. In most cases, the listen protocol will be **TCPIP**. For a complete description of these protocols, read ***Protocols***, elsewhere in this guide.

> **Note:** Although the HTTP11 protocol is still listed on Directory Server administration screens in the System Management Hub, it is no longer supported.

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



Add Target

Enter the Target Host Name:

Enter the Host IP Adress ONLY when the Host Name is not known.The IP Address is Ignored when the Host contains a value.

Enter the Target IPv4 Address:

Enter the Target Listen Port:

0

Enter Alternate Ports

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

Note: Host names are case-sensitive in SMH.

Or:

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

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

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

12 Click **Finish**.

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

Maintaining Qualified URLs

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

Using SMH, you can add and delete qualified URLs for a target. For more information about qualified URLs, read *Qualified URL Structure*, elsewhere in this guide.

This section covers the following topics:

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

Listing Qualified URLs

To list the qualified URLs of a target:

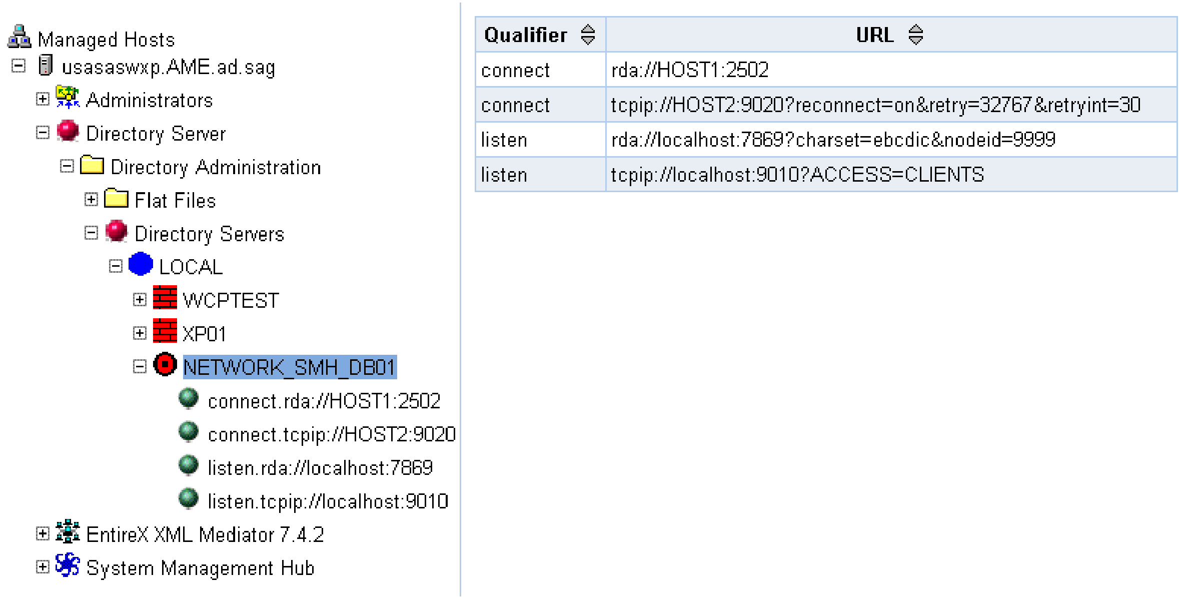
1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.

2 In the tree-view frame of SMH, click and expand the name of the Directory Server containing the qualified URLs you wish to list.

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

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

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



- Managed Hosts
  - usasaswxp.AME.ad.sag
    - Administrators
    - Directory Server
      - Directory Administration
        - Flat Files
        - Directory Servers
          - LOCAL
            - WCPTEST
            - XP01
            - NETWORK_SMH_DB01
              - connect.rda://HOST1:2502
              - connect.tcpip://HOST2:9020
              - listen.rda://localhost:7869
              - listen.tcpip://localhost:9010
    - EntireX XML Mediator 7.4.2
    - System Management Hub

Qualifier	URL
connect	rda://HOST1:2502
connect	tcpip://HOST2:9020?reconnect=on&retry=32767&retryint=30
listen	rda://localhost:7869?charset=ebcdic&nodeid=9999
listen	tcpip://localhost:9010?ACCESS=CLIENTS

Adding Qualified URLs for the Target

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

To add a qualified URL for a target:

1 Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this section.

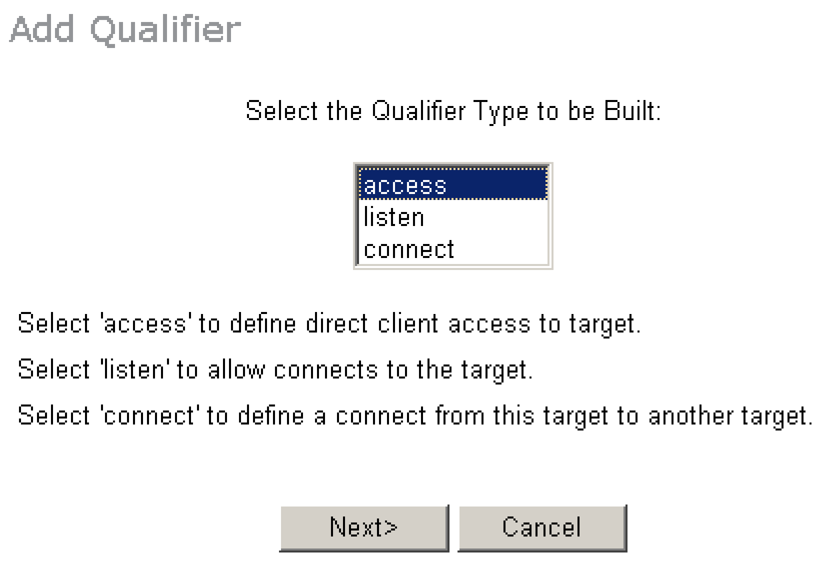
2 In the tree-view frame of SMH, click and expand the name of the Directory Server in which you want to add a qualifier.

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

3 Click and expand the target in which you want to add a qualifier. If the target is in a partition, you must first select the partition and then click on the target.

4 Click on the `Add Qualifier` command in the command menu of SMH. You can also see this menu by right-clicking on the name of the target to which you want to add a qualifier.

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



Add Qualifier

Select the Qualifier Type to be Built:

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

Select 'listen' to allow connects to the target.

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

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

6 Click **Next**.

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

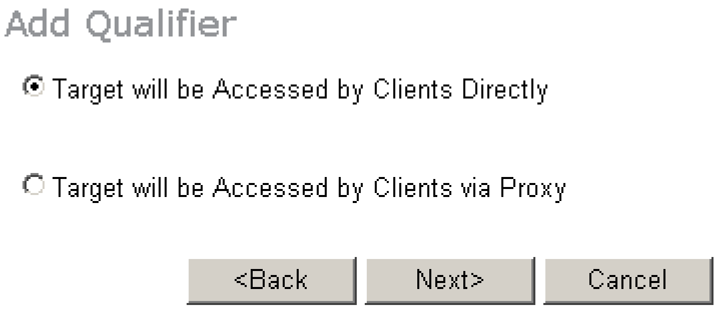
- Creating an access URL
- Creating a connect URL
- Creating a listen URL

Creating an access URL

▶ To create an access URL for a target:

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

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



Add Qualifier

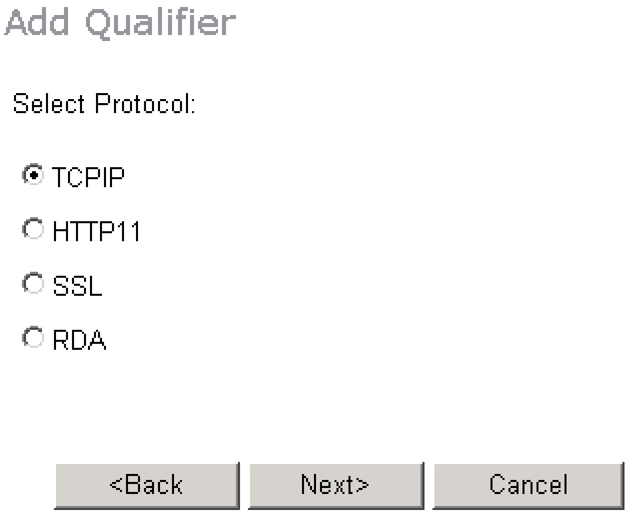
● Target will be Accessed by Clients Directly

○ Target will be Accessed by Clients via Proxy

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

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

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



Add Qualifier

Select Protocol:

● TCPIP

○ HTTP11

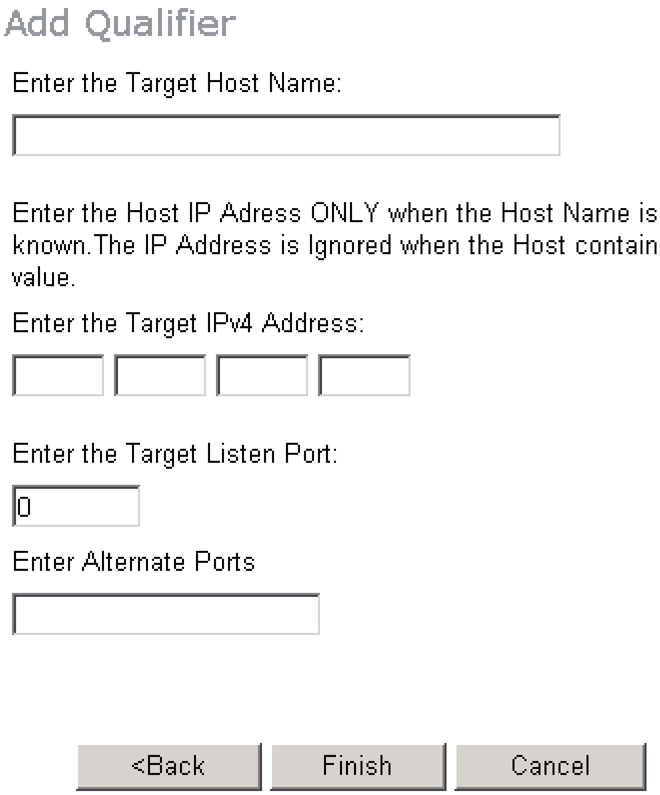
○ SSL

○ RDA

3 Select the protocol for the qualified URL and click **Next**. In most cases, the protocol will be **TCPIP**. For more information on the supported protocols, read ***Protocols***, elsewhere in this guide.

Note: Although the HTTP11 protocol is still listed on Directory Server administration screens in the System Management Hub, it is no longer supported.

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



Add Qualifier

Enter the Target Host Name:

Enter the Host IP Adress ONLY when the Host Name is not known.The IP Address is Ignored when the Host contains a value.

Enter the Target IPv4 Address:

Enter the Target Listen Port: 0

Enter Alternate Ports

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

Note: Host names are case-sensitive in SMH.

Or:

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

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

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

6 Click **Finish**.

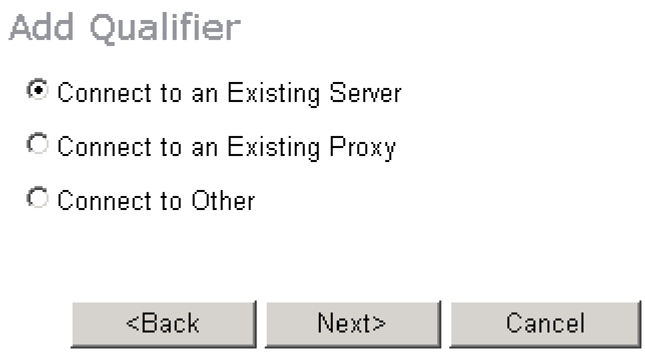
A message displays indicating that the new qualified access URL was added, and the added URL appears in the tree-view frame.

Creating a connect URL

To create a connect URL for a target:

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

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



Add Qualifier

● Connect to an Existing Server

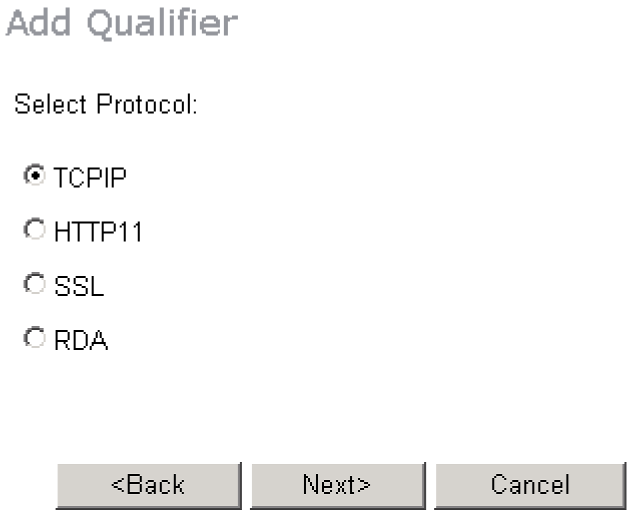
○ Connect to an Existing Proxy

○ Connect to Other

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

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

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



Add Qualifier

Select Protocol:

● TCPIP

○ HTTP11

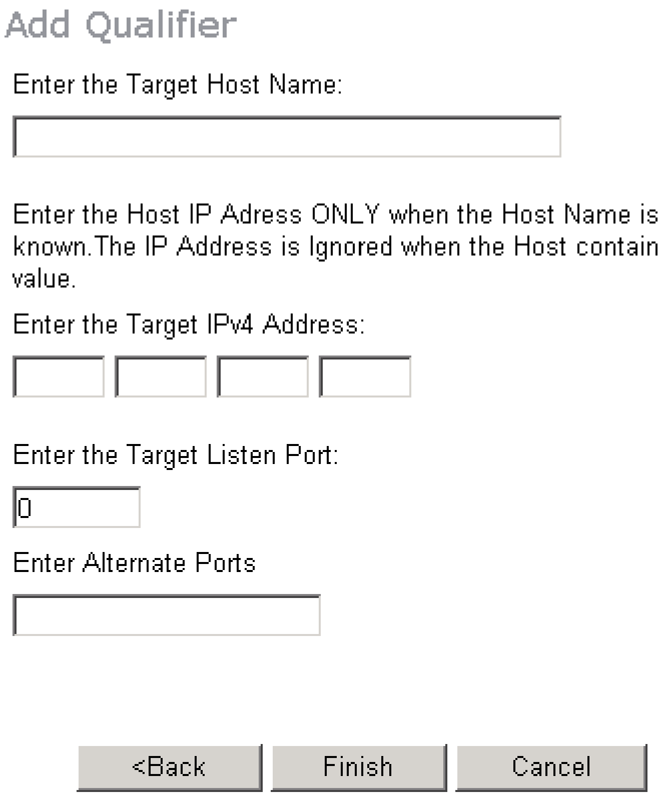
○ SSL

○ RDA

3 Select the protocol for the qualified URL and click **Next**. In most cases, the protocol will be **TCPIP**. For more information on the supported protocols, read ***Protocols***, elsewhere in this guide.

Note: Although the HTTP11 protocol is still listed on Directory Server administration screens in the System Management Hub, it is no longer supported.

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



Add Qualifier

Enter the Target Host Name:

Enter the Host IP Adress ONLY when the Host Name is not known.The IP Address is Ignored when the Host contains a value.

Enter the Target IPv4 Address:

Enter the Target Listen Port:

0

Enter Alternate Ports

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

Note: Host names are case-sensitive in SMH.

Or:

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

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

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

6 Click **Finish**.

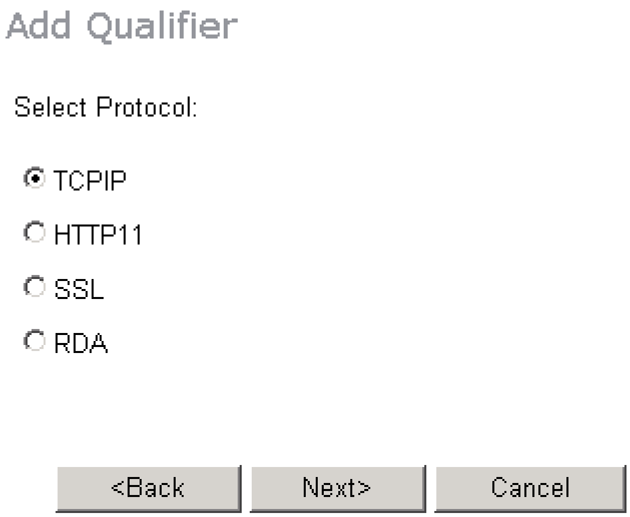
A message displays indicating that the new qualified connect URL was added, and the added URL appears in the tree-view frame.

Creating a listen URL

To create a listen URL for a target:

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

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



Add Qualifier

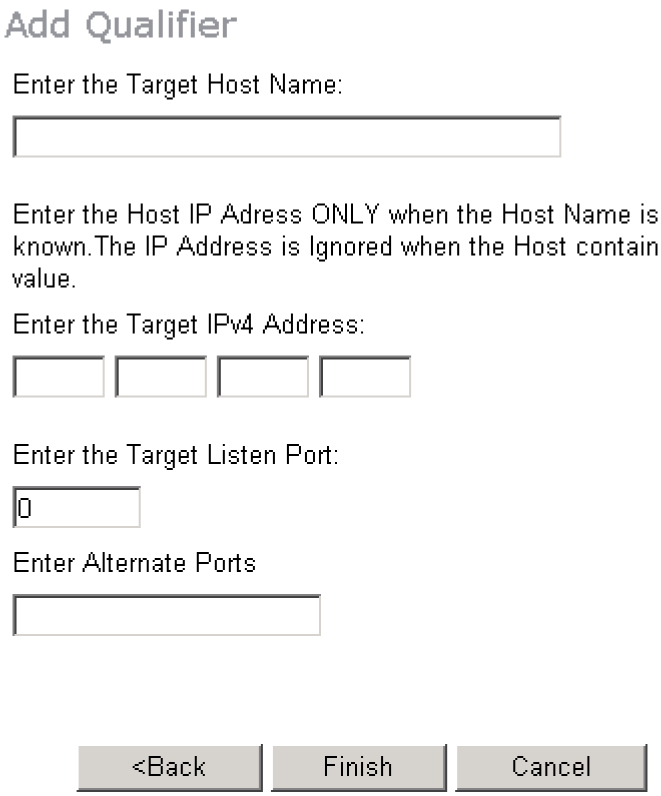
Select Protocol:

● TCPIP
○ HTTP11
○ SSL
○ RDA

2 Select the protocol for the qualified URL and click **Next**. In most cases, the protocol will be **TCPIP**. For more information on the supported protocols, read *Protocols*, elsewhere in this guide.

Note: Although the HTTP11 protocol is still listed on Directory Server administration screens in the System Management Hub, it is no longer supported.

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



Add Qualifier

Enter the Target Host Name:

Enter the Host IP Adress ONLY when the Host Name is not known.The IP Address is Ignored when the Host contains a value.

Enter the Target IPv4 Address:

Enter the Target Listen Port:

0

Enter Alternate Ports

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

Note: Host names are case-sensitive in SMH.

Or:

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

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

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

5 Click **Finish**.

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

Deleting Qualified URLs

To delete a qualifier from a target:

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

   The partitions and targets for that Directory Server are listed in the detail-view frame.
3. Click and expand the target containing the qualifier you wish to delete. If the target is in a partition, you must first select the partition and then click on the target.
4. Click on the qualifier you wish to delete.
5. Click on the `Delete Qualifier` command in the command menu of SMH. You can also see this menu by right-clicking on the name of the qualifier you wish to delete.

   The Delete Qualifier panel appears in the detail-view frame.
6. Click OK.

   The qualifier definition is deleted.

Maintaining Qualified URL Parameters

This section covers the following topics:

- Setting Reconnect Parameters
- Setting Basic Parameters
- Setting Advanced Parameters
- Setting JSSE Parameters
- Setting OpenSSL Parameters
- Setting RDA-MHDR Parameters

Setting Reconnect Parameters

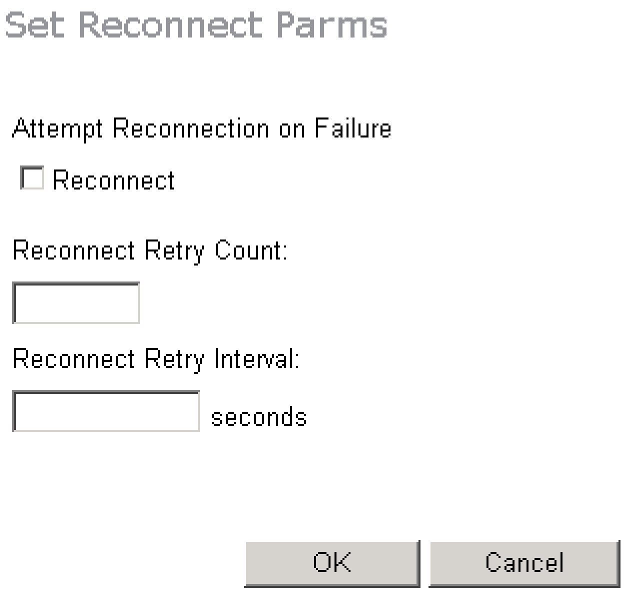
Using SMH, you can set or alter the values of the `reconnect`, `retry`, and `retryint` **parameters** for a qualified URL. These parameters control:

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

To set the reconnect parameters for a qualified URL:

1. Locate and list the qualified URL you want to change as described in ***Listing Qualified URLs***, elsewhere in this guide.
2. Click on the qualified URL whose reconnect parameters you want to change.
3. Select the **Set Reconnect Parms** command in the command menu of SMH. You can also see this menu by right-clicking on the name of the qualifier.

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



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

   When this check box is checked, the `reconnect` **parameter** appears in the qualified URL.
5. Specify the number of times reconnection should be attempted in the **Reconnect Retry Count** field. The valid range is "0" through "2147483648". The default value is "0" (no reconnection attempts).

   When a value other than "0" is specified, the `retry` **parameter** appears in the qualified URL.
6. Specify the number of seconds to wait between reconnection attempts. The valid range is "0" through "2147483648". The default value is "60000" seconds.

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

7 Click OK.

The reconnection parameters for the qualified URL are set.

Setting Basic Parameters

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

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

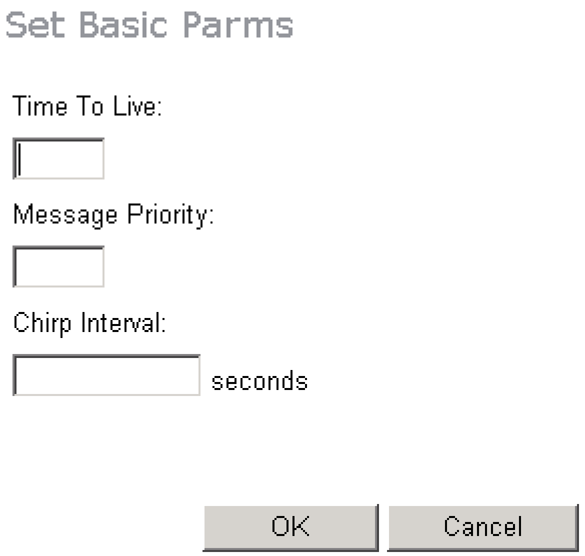
To set the basic parameters for a qualified URL:

1 Locate and list the qualified URL you want to change as described in ***Listing Qualified URLs***, elsewhere in this guide.

2 Click on the qualified URL whose reconnect parameters you want to change.

3 Select the **Set Basic Parms** command in the command menu of SMH. You can also see this menu by right-clicking on the name of the qualifier.

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



Set Basic Parms

Time To Live:

Message Priority:

Chirp Interval: seconds

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

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

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

5. Click OK.

   The basic parameters for the qualified URL are set.

Setting Advanced Parameters

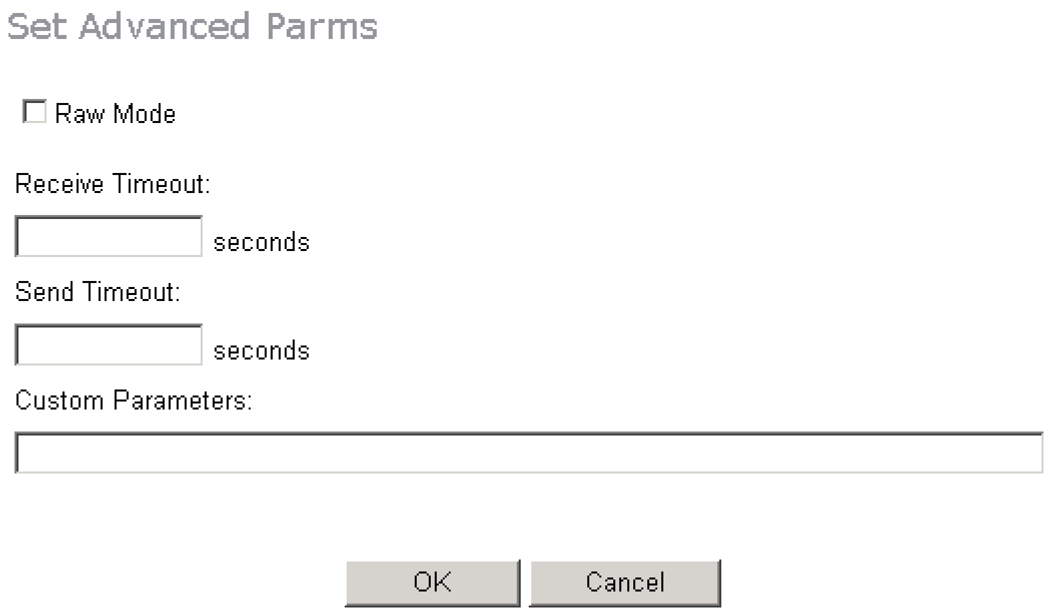
Using SMH, you can set or alter the values of advanced parameters `raw`, `recvtimeout`, `sendtimeout`, and various custom **parameters** for a qualified URL. These parameters control:

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

▶ To set the advanced parameters for a qualified URL:

1. Locate and list the qualified URL you want to change as described in ***Listing Qualified URLs***, elsewhere in this guide.
2. Click on the qualified URL whose reconnect parameters you want to change.
3. Select the **Set Advanced Parms** command in the command menu of SMH. You can also see this menu by right-clicking on the name of the qualifier.

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



Set Advanced Parms

□ Raw Mode

Receive Timeout:

seconds

Send Timeout:

seconds

Custom Parameters:

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

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

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

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

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

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

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

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

These custom parameters appear in the qualified URL.

8 Click OK.

The advanced parameters for the qualified URL are set.

Setting JSSE Parameters

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

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

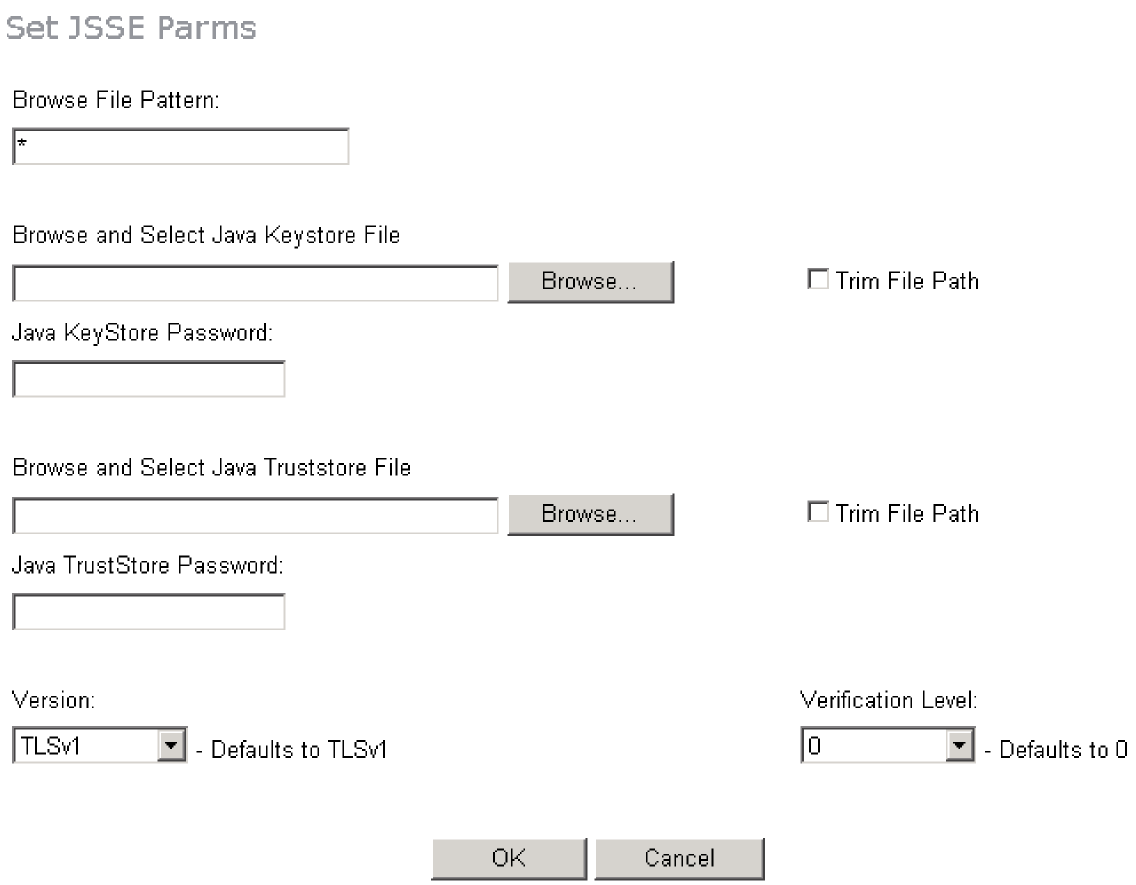
▶ To set the JSSE parameters for a qualified URL:

1 Locate and list the qualified URL you want to change as described in ***Listing Qualified URLs***, elsewhere in this guide.

2 Click on the qualified URL whose reconnect parameters you want to change.

3 Select the **Set JSSE Parms** command in the command menu of SMH. You can also see this menu by right-clicking on the name of the qualifier.

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



Set JSSE Parms

Browse File Pattern: *

Browse and Select Java Keystore File

Java KeyStore Password:

Browse and Select Java Truststore File

Java TrustStore Password:

Version: TLSv1 - Defaults to TLSv1

Verification Level: 0 - Defaults to 0

4 Optionally specify a browse file pattern in the **Browse File Pattern** field. This pattern is used to initially list files in the specified pattern when you click on any of the **Browse** buttons on this panel. However, once you get to the **Choose a File** panel produced by clicking on a **Browse** button, you can change the pattern if you choose.

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

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

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

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

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

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

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

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

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

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

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

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

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

For Java applications, valid values are:

0 (No peer verification occurs. This is the default value.)
1 (The application requests that the peer certificate be verified.)
2 (The application requests that the peer certificate be verified. A fatal condition occurs if there is no certificate.)
Values 4 and 8 are not valid for Java.

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

11 Click OK.

The JSSE parameters for the qualified URL are set.

Setting OpenSSL Parameters

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

- The SSL version that should be used for the SSL connection
- The verification processing level for the SSL connection
- The random file to use for the SSL connection
- The path for the Certificate Authority file that stores the trusted CA certificates
- The name of the Certificate Authority file that stores the trusted CA certificates
- The name of the file containing the participant's certificate
- The name of the file containing the server's private key

- The password for extracting information from the participant's certificate.

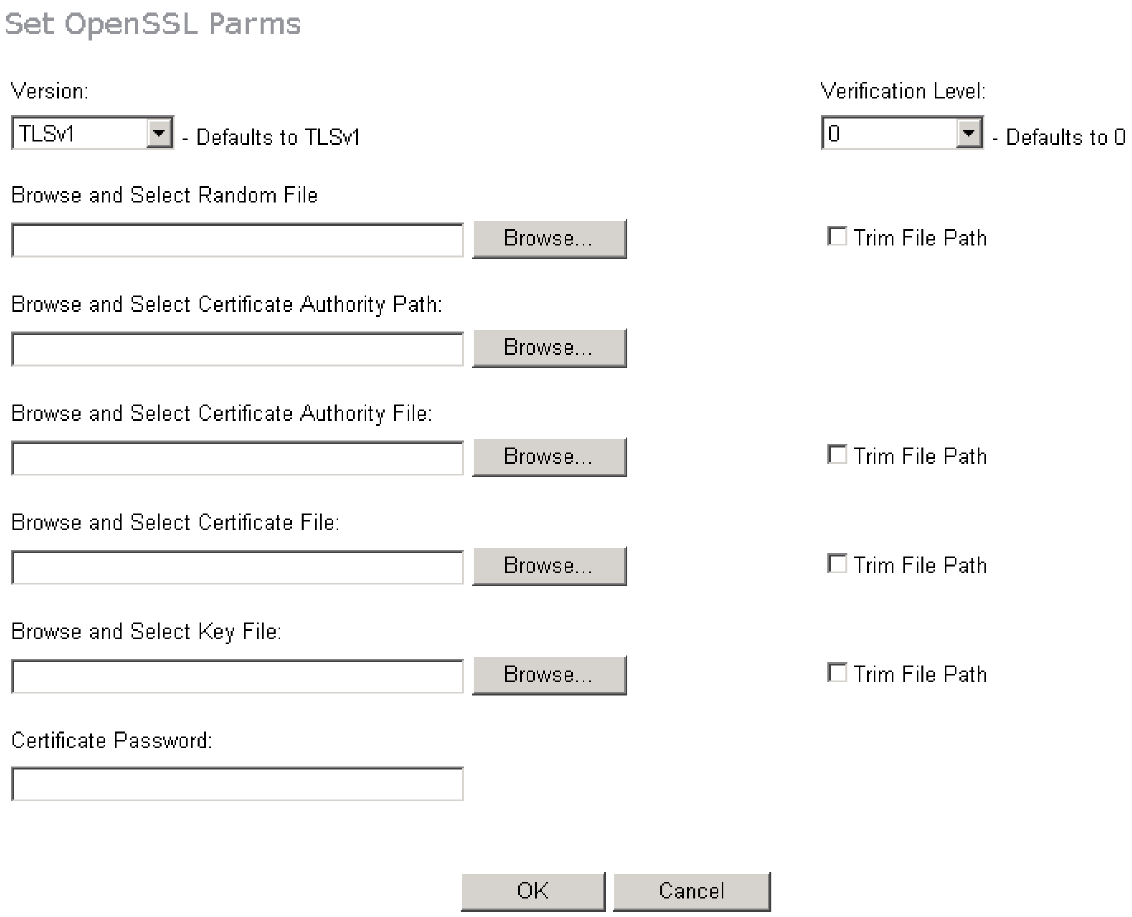
To set the OpenSSL parameters for a qualified URL:

1 Locate and list the qualified URL you want to change as described in ***Listing Qualified URLs***, elsewhere in this guide.

2 Click on the qualified URL whose reconnect parameters you want to change.

3 Select the **Set OpenSSL Parms** command in the command menu of SMH. You can also see this menu by right-clicking on the name of the qualifier.

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



Set OpenSSL Parms

Version: TLSv1 - Defaults to TLSv1

Verification Level: 0 - Defaults to 0

Browse and Select Random File

Browse and Select Certificate Authority Path:

Browse and Select Certificate Authority File:

Browse and Select Certificate File:

Browse and Select Key File:

Certificate Password:

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

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

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

   For C applications, valid values are:

   0 (No peer verification occurs. This is the default value.)
   1 (The application requests that the peer certificate be verified.)
   2 (The application requests that the peer certificate be verified. A fatal condition occurs if there is no certificate.)
   4 (The application requests that the peer certificate be verified only once.)
   8 (The application requests that the issuer name is checked against the host name.)

   Values "1", "2", and "4" can be specified simultaneously, but only if you use the **Custom Parameter** field on the **Set Advanced Parms** panel.

   If no client certificate is available, certification fails.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

12 Click OK.

The OpenSSL parameters for the qualified URL are set.

Setting RDA-MHDR Parameters

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

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

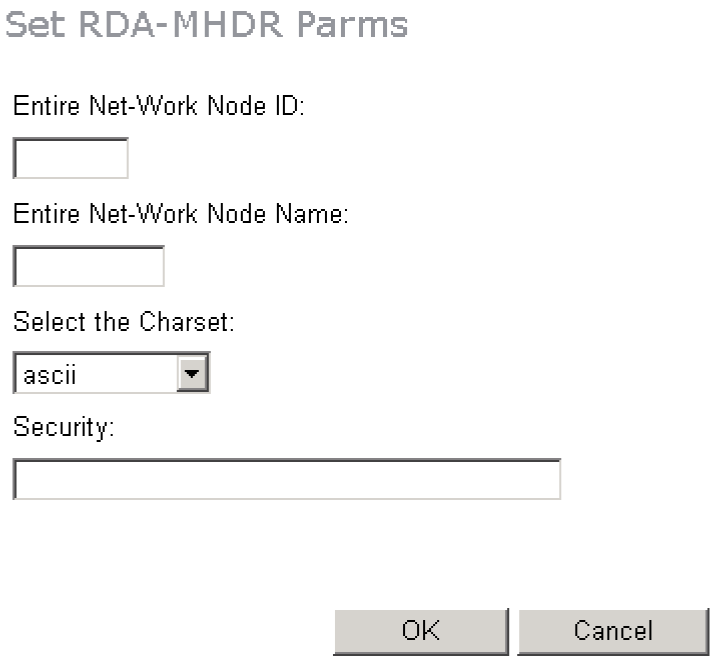
To set the RDA parameters for a qualified URL:

1 Locate and list the qualified URL you want to change as described in ***Listing Qualified URLs***, elsewhere in this guide.

2 Click on the qualified URL whose reconnect parameters you want to change.

3 Select the **Set RDA-MHDR Parms** command in the command menu of SMH. You can also see this menu by right-clicking on the name of the qualifier.

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



Set RDA-MHDR Parms

Entire Net-Work Node ID:

Entire Net-Work Node Name:

Select the Charset: ascii

Security:

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

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

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

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

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

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

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

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

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

8 Click OK.

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

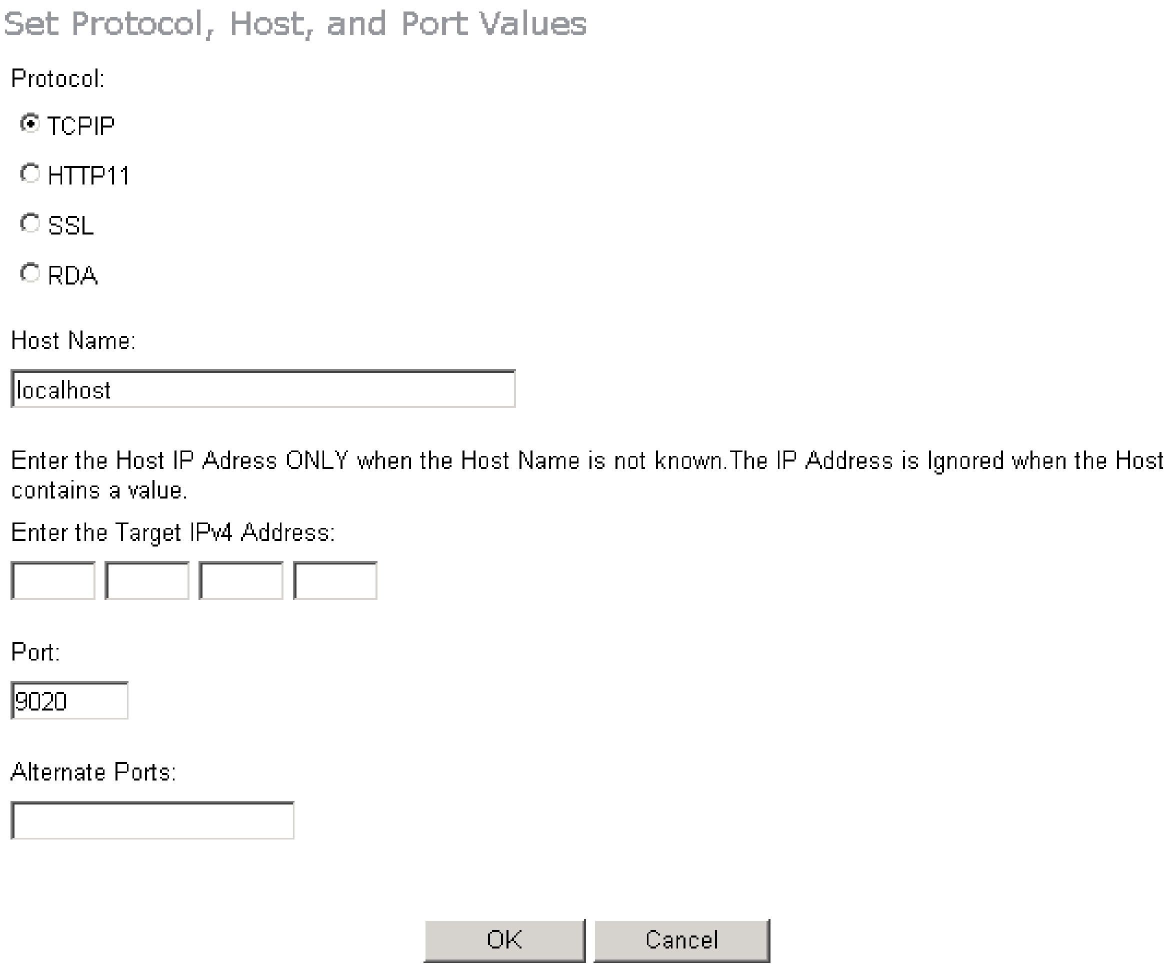
Changing Protocol, Host, and Port Values of the Qualified URL

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

To change these values for a qualified URL:

1. Locate and list the qualified URL you want to change as described in ***Listing Qualified URLs***, elsewhere in this guide.
2. Click on the qualified URL whose reconnect parameters you want to change.
3. Select the **Set Protocol, Host, and Port Values** command in the command menu of SMH. You can also see this menu by right-clicking on the name of the qualifier.

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



Set Protocol, Host, and Port Values

Protocol:

● TCPIP

○ HTTP11

○ SSL

○ RDA

Host Name:

localhost

Enter the Host IP Adress ONLY when the Host Name is not known.The IP Address is Ignored when the Host contains a value.

Enter the Target IPv4 Address:

Port:

9020

Alternate Ports:

4 Click on the appropriate protocol checkbox in the **Protocol** field. In most cases, the protocol will be **TCPIP**. For a complete description of these protocols, read ***Protocols***, elsewhere in this guide.

Note: Although the HTTP11 protocol is still listed on Directory Server administration screens in the System Management Hub, it is no longer supported.

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

Note: Host names are case-sensitive in SMH.

Or:

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

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

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

7 Click OK.

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

Setting the Target Type

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

▶ **To change the target type of a target definition:**

1 Access the Directory Server administration area, as described in ***The Directory Server Administration Area***, earlier in this section.

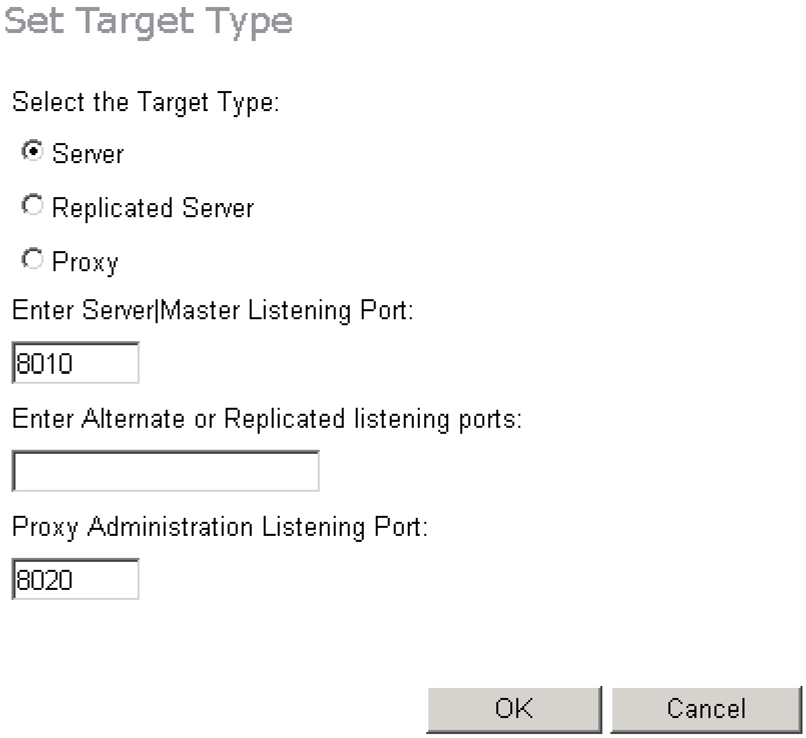
2 In the tree-view frame of SMH, click and expand the name of the Directory Server containing the target definition you want to modify.

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

3 Click on the target you want to modify. If the target is in a partition, you must first select the partition and then click on the target.

4 Click on the `Set Target Type` command in the command menu of SMH. You can also see this menu by right-clicking on the name of the target.

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



Set Target Type

Select the Target Type:

● Server

○ Replicated Server

○ Proxy

Enter Server|Master Listening Port: 8010

Enter Alternate or Replicated listening ports:

Proxy Administration Listening Port: 8020

5 Select the appropriate option in the **Select the Target Type** area for the target type you want used for the target definition.

- The **Server** option is usually the option you should select.
- The **Replicated Server** option is reserved for future use by Software AG.
- The **Proxy** option is only applicable to configurations requiring a proxy. It is provided for compatibility with Software AG products that still require a proxy. If your Software AG product requires a proxy, refer to the documentation for your Software AG product for information about proxies and how to configure them in SMH.

6 Optionally, change the listening ports used by the target in the **Enter Server/Master Listening Port**, **Enter Alternate or Replicated listening ports**, or **Proxy Administration Listening Port** fields.

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

7 Click **OK**.

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

Changing the Target Name

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

To change the name of a target:

1 Access the Directory Server administration area, as described in ***The Directory Server Administration Area***, earlier in this section.

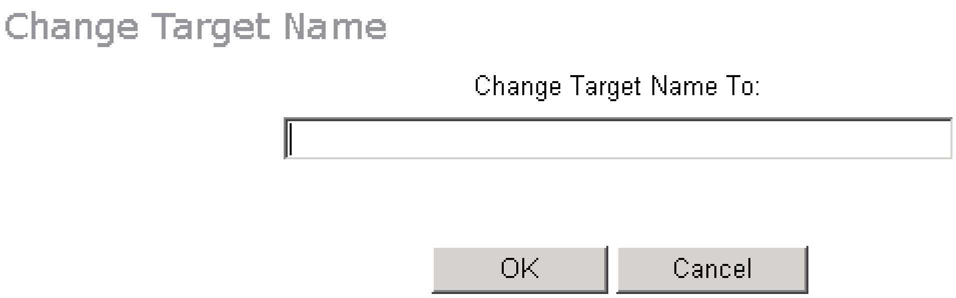
2 In the tree-view frame of SMH, click and expand the name of the Directory Server containing the target definition you want to modify.

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

3 Click on the target you want to modify. If the target is in a partition, you must first select the partition and then click on the target.

4 Click on the `Change Target Name` command in the command menu of SMH. You can also see this menu by right-clicking on the name of the target.

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



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

Note: Target names are case-sensitive.

6 Click **OK**.

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

Changing the Host

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

Changing the Protocol

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

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

1 Access the Directory Server administration area, as described in ***The Directory Server Administration Area***, earlier in this section.

2 In the tree-view frame of SMH, click and expand the name of the Directory Server containing the target definition you want to modify.

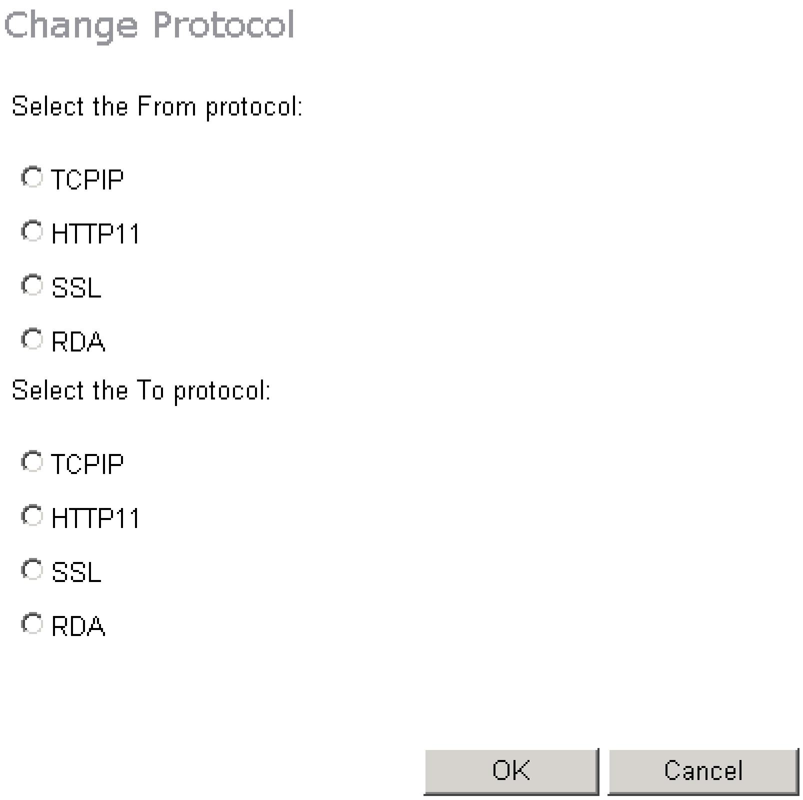
The partitions and targets already defined for that Directory Server are listed in the detail-view frame and under the Directory Server name in the tree-view frame.

3 Click on the target you want to modify. If the target is in a partition, you must first select the partition and then click on the target.

4 Click on the `Change Protocol` command in the command menu of SMH. You can also see this menu by right-clicking on the name of the target.

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

Note: Although the HTTP11 protocol is still listed on Directory Server administration screens in the System Management Hub, it is no longer supported.



Change Protocol

Select the From protocol:

○ TCPIP

○ HTTP11

○ SSL

○ RDA

Select the To protocol:

○ TCPIP

○ HTTP11

○ SSL

○ RDA

5 Click on the checkbox in the **Select the From protocol** area for the protocol you want to change. All URLs for the target definition using this protocol will be changed when these steps are completed.

6 Click on the checkbox in the **Select the To protocol** area for the protocol you want to use instead. The URLs using the protocol you specified in the previous step will be changed to use the protocol you select in this step.

7 Click **OK**.

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

Deleting a Target

To delete a target definition:

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

   The partitions and targets for that Directory Server are listed in the detail-view frame.
3. Click on the target you wish to delete. If the target is in a partition, you must first select the partition and then click on the target.
4. Click on the `Delete Target` command in the command menu of SMH. You can also see this menu by right-clicking on the name of the target.

   The Delete Target panel appears in the detail-view frame.
5. Click OK.

   The target definition is deleted.

14 Specifying Trace Settings

You can specify trace settings for:

- all Directory Servers linked to this SMH
- individual Directory Servers
- individual partitions within a Directory Server
- individual targets
- individual qualifiers of a target.

The trace settings for individual Directory Servers override the general trace settings for all Directory Servers. Likewise, the trace settings for an individual qualifier override the trace settings for its target, the trace settings for a target override the trace settings for its partition or Directory Server, and the trace settings for a partition override the trace settings for its Directory Server.

▶ To specify trace settings:

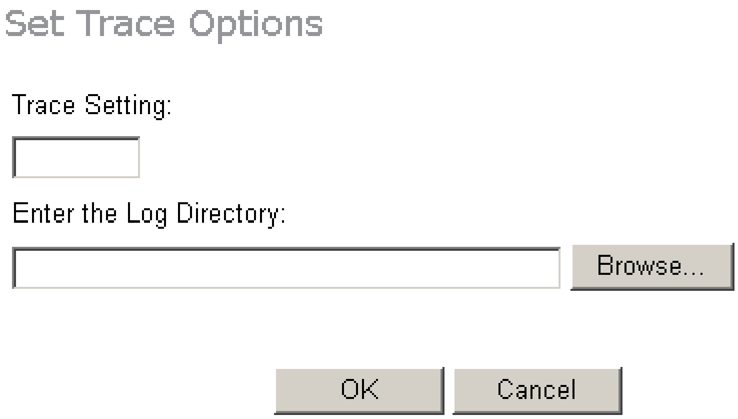
1 Access the Directory Server administration area, as described in ***The Directory Server Administration Area***, earlier in this chapter.

2 Navigate to the administration area for the particular Directory Server, partition, target, or qualifier for which you want to specify trace settings. For example, if you want to specify trace settings for a particular qualifier of a target, navigate through the SMH screens until you have selected that qualifier in the tree-view frame.

If you want to specify general trace settings for all Directory Servers linked to this SMH, remain on the first panel of the Directory Server administration area (with **Directory Servers** selected in the tree-view frame).

3 Click on the `Set Trace Options` command in the command menu of SMH. You can also see this menu by right-clicking on the name of the Directory Server, partition, target, or qualifier.

The **Set Trace Options** panel appears in the detail-view frame.



Set Trace Options

Trace Setting:

Enter the Log Directory:

4 Specify a numeric value to indicate the trace level to be used by the Directory Server, partition, target, or qualifier in the **Trace Setting** field. The default value is "0". Specify "65534" to obtain full tracing.

If you specify "65535", an internal buffer trace only occurs. Do not specify "65535", unless specifically instructed to do so by a Software AG Customer Support representative.

The Software AG Directory Server Windows service or UNIX daemon must be stopped and restarted before the new trace settings will be used.

5 In the **Enter the Log Directory** field, specify the full path name of the directory in which the Directory Server, partition, target, or qualifier trace log should be stored. Enclose the value in double quotes if the directory name contains spaces.

The default value set by the installation is "C:\Documents and Settings\All Users\Application Data\Software AG\".

The log filename is *xtsnnnnn.log*, where *nnnnn* is a sequential number

6 Click OK.

The general trace settings are defined.

15 Changing Hosts

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

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

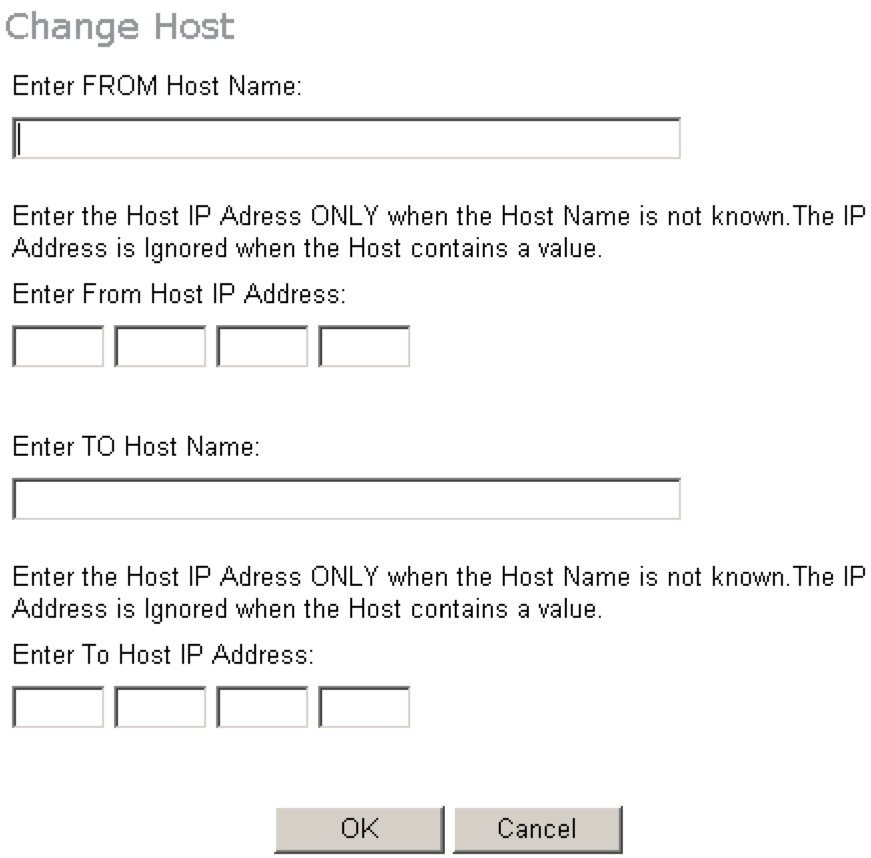
- Directory Server
- partition within a Directory Server
- target

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

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

1. Access the Directory Server administration area, as described in *The Directory Server Administration Area*, earlier in this chapter.
2. Navigate to the administration area for the particular Directory Server, partition, or target containing the URLs you want to change. For example, if you want to change the host name for the URLs in a particular target, navigate through the SMH screens until you have selected that target in the tree-view frame.
3. Click on the `Change Host` command in the command menu of SMH. You can also see this menu by right-clicking on the name of the Directory Server, partition, or target.

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



Change Host

Enter FROM Host Name:

Enter the Host IP Adress ONLY when the Host Name is not known.The IP Address is Ignored when the Host contains a value.

Enter From Host IP Address:

Enter TO Host Name:

Enter the Host IP Adress ONLY when the Host Name is not known.The IP Address is Ignored when the Host contains a value.

Enter To Host IP Address:

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

Note: Host names are case-sensitive in SMH.

Or:

Specify the original IP address in the **Enter From Host IP Address** field. We do not recommend using IP addresses instead of host names because the IP address may change.

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

Note: Host names are case-sensitive in SMH.

Or:

Specify the new IP address in the **Enter To Host IP Address** field. We do not recommend using IP addresses instead of host names because the IP address may change.

6 Click OK.

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

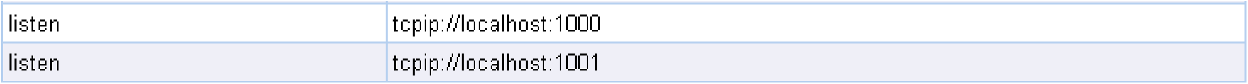
16 Advanced Directory Server Configuration

This chapter describes some advanced configuration techniques you can perform for the Directory Server.

17 Listening on Multiple Ports

Ordinarily, the Directory Server listens on only one port for a specific qualified URL. If, however, you want different services of that qualified URL to listen on different ports, you must set up a listen URL for each port of the target. This is also useful if you want to use multiple protocols for the same target. Software AG Directory Server allows you to set up eight listen URLs for the same target.

For example, you might create two listen URLs for a target that look like this in SMH:



listen	tcpip://localhost:1000
listen	tcpip://localhost:1001

When these two URLs are specified, Software AG Directory Server listens on ports 1000 and 1001 using the TCP/IP protocol.

And, if your Directory Server is named XTSDS, these listen entries would look like this internally:

```
XTSlisten.XTSDS[0]=TCPIP://localhost:1000
XTSlisten.XTSDS[0]=TCPIP://localhost:1001
```

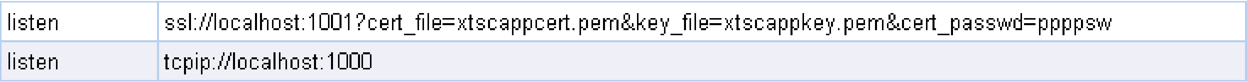
To create these entries:

- In SMH, create two identical qualified URLs for the same target, but specify different ports for each URL. For information on creating qualified URLs for a target, read ***Adding Qualified URLs for the Target***, elsewhere in this guide.

18 Listening Using Multiple Protocols

Ordinarily, the Directory Server listens on only one port using only one protocol. If, however, you want different services of that qualified URL to use different protocols, you must set up a listen URL for each protocol of the target, specifying a different port number for each listen URL. Software AG Directory Server allows you to set up eight listen URLs for the same target.

For example, you might create two listen URLs for a target that looks like this in SMH:



listen	ssl://localhost:1001?cert_file=xtscappcert.pem&key_file=xtscappkey.pem&cert_passwd=ppppsw
listen	tcpip://localhost:1000

When these two URLs are specified, Software AG Directory Server listens on ports 1000 using the TCP/IP protocol and on port 1001 using the SSL protocol.

And, if your Directory Server is named XTSDS, these listen entries would look like this internally:

```
XTSlisten.XTSDS[0]=tcpip://localhost:1000
XTSlisten.XTSDS[0]=ssl://localhost:1001?cert_file=xtscappcert.pem&key_file=xtscappkey.pem&cert_passwd=ppppsw
```

To create these entries:

- In SMH, create two identical qualified URLs for the same target, but specify different ports and protocols for each URL. For information on creating qualified URLs for a target, read *Adding Qualified URLs for the Target*, elsewhere in this guide.

19 Advanced Support Operations

Ordinarily, when the Directory Server is installed, it is automatically defined as a Windows service on Windows systems and a UNIX daemon on UNIX systems. In addition, the predefined Directory Server parameters set when you install Directory Server are usually sufficient for the needs of most products and environments. If you find that you have a specific need or are having a specific problem with your Directory Server installation, you should contact Software AG Customer Support. They will assist you in resolving the problem.

This chapter describes Directory Server operations you might be asked to perform under the guidance of Software AG Customer Support. It covers the following topics:

- Windows NT-Based Directory Server Operations
- UNIX Directory Server Operations
- Manually Configuring the Directory Server

Caution: We recommend that you perform the operations described in this chapter with the supervision of a Software AG Customer Support representative.

20 Windows NT-Based Directory Server Operations

The Directory Server for Windows runs as an Windows service. If used, the Windows Directory Server will start at boot time by default. However configuration and operational control is available via the Windows Directory Server command line program `xtsdssvc`.

The `xtsdssvc` program can be used to perform the following tasks:

- Register the Directory Server as a Windows service.
- Unregister the Directory Server service and remove the recorded startup parameters.
- Start the service.
- Stop the service.
- Obtain a status of the service.
- Set the Directory Server parameters.

Note the Windows **Services** control panel applet can be used to start and stop the service as well. The Directory Server Windows service name is "Software AG Directory Server".

This chapter covers the following topics:

xtsdssvc Parameters

The following parameters can be passed to `xtsdssvc`:

Parameter	Description
`-help`	Prints the help message.
`-register`	Registers the Software AG Directory Server service. It will be started at the next system boot.
`-unregister`	Removes the Software AG Directory Server service from the database of all registered services. Also removes all registry entries belonging to the Software AG Directory Server service.
`-start`	Starts the Software AG Directory Server service.
`-stop`	Stops the Software AG Directory Server service.
`-status`	Prints the status of the Software AG Directory Server service and displays the current configuration parameters.

Parameter	Description
`-name STRING`	Sets the serverDirectory Server name, where `STRING` is the name. This is not the same as the Software AG Directory Server Windows service name. The default value is "XTSDIR".
`-port NUMBER`	Sets the Directory Server listen port, where `NUMBER` is the port number. A value of "0" (zero) means that the value assigned to the well-known name *SAGXTSDSport* will be used. If *SAGXTSDSport* is not defined, port number "12731" will be used. The default value is "0".
`-directory STRING`	Sets the type of Directory Server to be used, where `STRING` is the Directory Server type. The default value is "INIDIR".
`-dirparms STRING`	Sets the parameters required by the selected Directory Server, where `STRING` indicates the Directory Server parameters applicable to the type of Directory Server defined in the `-directory` parameter. The default value is "file=C:\Documents and Settings\All Users\Application Data\Software AG\xtsurl.cfg".
`-logdir STRING`	Specifies the directory to contain the Directory Server trace log controlled by the `-trace` parameter (described below). Enclose value in double quotes if the directory name contains spaces. The default value set by the installation is "C:\Documents and Settings\All Users\Application Data\Software AG\". If null, the log will be written to "%SystemRoot%\system32". The log filename is *xts*`nnnnn`*.log*, where `nnnnn` is a sequential number
`-trace NUMBER`	Sets the trace level to be used by the Directory Server, where NUMBER indicates the trace level. The default value is "0". Specify "65534" to obtain full tracing. Specifying "65535" results in an internal buffer trace only, do not specify "65535",unless specifically instructed to do so. The Software AG Directory Server Windows service should be stopped and restarted when changing the trace value.
`-debug NUMBER`	Indicates whether service control manager related debugging output should be produced. The default value is "0". `NUMBER` should be set to "0" (output not produced) or "1" (output produced). The output is written to the Windows System Event Log.

xtsdssvc Sample Commands

The following examples illustrate how to perform various tasks using the `xtsdssvc` command:

Task	Sample Command
Register Directory Server	`xtsdssvc -register` Parameters should be set before registering the server.
Unregister Directory Server	`xtsdssvc -unregister`
Query status of Directory Server	`xtsdssvc -status`
Start Directory Server	`xtsdssvc -start`
Stop Directory Server	`xtsdssvc -stop`
Set Directory Server parameters	`xtsdssvc -name xtsdir -port 0 -directory INIDIR -dirparms "file=C:\Documents and Settings\All Users\Application Data\Software AG\xtsurl.cfg" -trace0 -debug0`

Note: You can also use a Windows program item to check the status of the Directory Server. Select the following items from the Windows Start Menu: **Programs>Software AG Directory Server>Directory Server Status.**

21 UNIX Directory Server Operations

The Directory Server for UNIX is run as a UNIX daemon.

This chapter covers the following topics:

Running Directory Server as a UNIX Daemon

After Software AG Directory Server is installed, it can be run as a UNIX daemon. Modify the shell script *$SAG/common/bin/xtsdsdmn.sh*, if desired (no modifications are required), and then invoke it.

The xtsdsdmn Program

The `xtsdsdmn` program, located in the *$SAG/common/bin* subdirectory, is used to start and stop the Directory Server.

To stop the Directory Server daemon, first obtain the `xtsdsdmn` process ID, as follows:

```
ps -ef | grep xtsdsdmn
```

Then enter the UNIX kill command and the process ID (*nnnnn*), as follows:

```
kill -9 nnnnn
```

The parameters described in the following table can be passed to `xtsdsdmn` at start time.

Parameter	Value
`-name STRING`	Indicates the Software AG Directory Server name. The default value is "XTSDIR".
`-port NUMBER`	Indicates the listen port for the server. A "0" value indicates that either the value defined by *SAGXTSDSport* or "12731" will be used. If *SAGXTSDSport* is not defined then "12731" is used. The default value is "0".
`-directory STRING`	Indicates the type of Directory Server to be employed. The default value is "INIDIR".
`-dirparms STRING`	Sets directory parameters appropriate for the Directory Server identified by the `-directory` parameter. If the `-directory` parameter is set to "INIDIR", then this parameter is set to the full path name of the Software AG Directory Server URL configuration file. The installation procedure sets this parameter to reference the file: *$SAG/common/xts/com/softwareag/XTS/xtsurl.cfg*.

Parameter	Value
`-logdir STRING`	Specifies the directory to contain the Directory Server process log controlled by the `-trace` parameter. (Refer to the documentation for `-trace` below. The installation default value is null, which results writing to the root directory by default.
`-trace NUMBER`	Turns on Directory Server process logging. The log is written to the root directory or the directory set by `-logdir` parameter. The default value is "0". Specify "65534" to obtain full tracing. Specifying "65535" results in an internal buffer trace only, do not specify "65535", unless specifically instructed to do so. The Directory Server should be stopped and restarted when changing the trace value.
`-pid`	This parameter is optional. Indicates the file where the Directory Server daemon process identifier will be recorded. When the daemon is terminated, an attempt will be made to delete the file identified in this parameter.
`-help`	Prints the help message.

22 Manually Configuring the Directory Server

Most configuration specifications for Directory Server can be made using SMH. Manual configuration of the Directory Server might be required is a configuration is lost or corrupted. Under normal circumstances, manual configuration is not required.

If you need to perform manual configuration of the Directory Server, please contact Software AG Customer Support for assistance.

This chapter covers the following topics:

Windows Manual Configuration

To manually configure the Directory Server:

1. Position to the Software AG Directory Server installation directory.
2. Set the Directory Server parameters.
3. Register the Directory Server service.
4. Start the Directory Server service.
5. Confirm the configuration.

Refer to the following sections (Example Commands (Windows) and Example Commands (UNIX) for examples of each of these steps.

- Example Commands (Windows)
- Special Considerations

Example Commands (Windows)

Note in the following commands "x:" is used to indicate the drive where the Software AG Directory Server has been installed. This would normally be the "C" drive. Substitute the installation's actual value before issuing the commands. From a Windows command prompt window, issue the following commands:

Activity	Example Command
Position to the Software AG Directory Server installation directory.	`cd x:\Program Files\Software AG\Directory Server`
Set the Directory Server parameters.	`xtsdssvc -name XTSDIR -port 0 -directory INIDIR -dirparms "file=c:\Documents and Settings\All Users\Application Data\Software AG\xtsurl.cfg" -logdir "c:\Document and Settings\All Users\Application Data\Software AG" -trace 0 -debug 0`

Activity	Example Command
Register the Directory Server service.	`xtsdssvc -register`
Start the Directory Server service.	`xtsdssvc -start`
Confirm the configuration.	`xtsdssvc -status`

Once the Directory Server is registered it will be automatically started at boot time. The Windows **Services** control panel application can be used to confirm the automatic start setting. Navigate the following program items to get to the services control panel applet: **Start>Settings>Control Panel>Administrative Tools>Services (Windows 2000)** . The Software AG Directory Server service is listed as **Software AG Directory Server**.

Special Considerations

This section covers the following topics:

- The -port 0 Setting
- The -dirparms Setting
- SAGXTSDShost Needs to be Set
- The xtsdssvc -help Command

The -port 0 Setting

Setting the `port` parameter to "0" indicates that the actual port to be used is determined by the DNS resolution of *SAGXTSDSport*. If *SAGXTSDSport* is not resolved, then port "12731" is used. The port number is encoded as an IP address, explained below. One should determine the setting or non-setting of *SAGXTSDSport*. If set, then confirm that the desired port is encoded correctly. To confirm, issue the following ping command:

```
PING SAGXTSDSport
```

Text similar to the following should appear if SAGXTSDSport is defined:

```
Pinging SAGXTSDSport [49.187.0.0] with 32 bytes of data:
```

```
Reply from 206.24.181.1: Destination host unreachable.
```

```
Reply from 206.24.181.1: Destination host unreachable.
Reply from 206.24.181.1: Destination host unreachable.
```

```
Reply from 206.24.181.1: Destination host unreachable.
```

```

Ping statistics for 49.187.0.0:
Packets:
```

```
Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum =0ms, Maximum = 0ms, Average = 0ms
```

The "Destination host unreachable" is expected as the *SAGXTSDSport* is the port number encoded as an IP address and as such is not a real IP address.

The port as an IP address encoding is done as follows:" port/256.port%256.0.0"

In above case, "49.187.0.0" equates to "12731" (i.e., "256*49+187").

If *SAGXTSDSport* is set but is not encoded to the the desired port value then one of the following should be done:

1. Correct DNS entry.
2. Define *SAGXTSDSport* in the local "hosts" file.
   - Under windows the local hosts file can be found at *%systemroot%\system32\drivers\etc*
   - Example entry for using port 12731: "49.187.0.0 SAGXTSDSport ".

The -dirparms Setting

The `-dirparms` parameter specifies the fully qualified name of the flat file repository to be used by the Directory Server. There should be an *xtsurl.cfg* file in the standard Windows application data subdirectory:

c:\Documents and Settings\All Users\Application Data\Software AG.

SAGXTSDShost Needs to be Set

In order for applications to access the Directory Server, *SAGXTSDShost* must be set and point to the Directory Server host. If *SAGXTSDShost* is not set, confirm with a `PING SAGXTSDShost` command , then set *SAGXTSDShost* in one of the following ways:

- Define to a DNS server.
- Define in the local *hosts* file for each computer needing access to the Directory Server.
- Set an XTSDSURL environmental variable for any process that needs access to the Directory Server.

For example: `set xtsdsurl=tcpip://dirserverhost:port`.

The xtsdssvc -help Command

The command `xtsdssvc -help` will display help on other `xtsdssvc` commands.

UNIX Manual Configuration

Under UNIX, manual configuration is possible by modifying the *$SAG/common/bin/xtsdsdmn.sh* script.

The *SAGXTSDSport* and *SAGXTSDShost* settings should be confirmed as in the Windows case.

The *xtsurl.cfg* file is located at *$SAG/common/xts/com/softwareag/XTS*. If *xtsurl.cfg* does not exist at the location there should be an *xtsurl.ghost* file at that location. If no *xtsurl.cfg* exists at *$SAG/common/xts/com/softwareag/XTS* the *xtsurl.ghost* file can be renamed to *xtsurl.cfg*.

Index