IBM Security Identity Manager
Version 6.0

Active Directory Adapter with 64-bit Support Installation and Configuration Guide

IBM
IBM Security Identity Manager
Version 6.0

Active Directory Adapter with 64-bit Support Installation and Configuration Guide
Figures

1. One-way SSL authentication (server authentication) ........................................ 51
2. Two-way SSL authentication (client authentication) .......................................... 52
3. Adapter operating as an SSL server and an SSL client ........................................ 53
Tables

1. Preinstallation roadmap ................. 9
2. Installation roadmap .................. 9
3. Prerequisites to install the adapter ... 10
4. Default values ...................... 17
5. Installation options .................. 17
6. Options for the main configuration menu 20
7. Options for the DAML protocol menu ... 22
8. Options for the event notification menu 26
9. Registry keys and description .......... 30
10. Options for modify context .......... 31
11. DN elements and definitions .......... 33
12. Options for the activity logging menu 35
13. Attribute configuration option descriptions 37
14. Registry key descriptions .......... 38
15. Options for advanced settings menu ... 43
16. Arguments and descriptions for the agentCf
temp command ....................... 45
17. Profile files ....................... 70
18. Troubleshooting the Active Directory Adapter errors ............... 83
19. Data types and values for syntax tags 103
20. Attributes, descriptions, and corresponding data types .......... 105
21. Attributes, descriptions, and corresponding data types ......................... 114
22. Add request attributes ............. 115
23. Change request attributes ......... 116
24. Delete request attributes .......... 116
25. Suspend request attributes ........ 116
26. Restore request attributes .......... 116
27. Reconciliation attributes .......... 117
Preface

About this publication

The Active Directory Adapter with 64-bit Support Installation and Configuration Guide provides the basic information that you can use to install and configure the IBM® Security Identity Manager Active Directory Adapter. The Active Directory Adapter enables connectivity between the IBM Security Identity Manager server and a managed resource. The IBM Security Identity Manager server is the server for your IBM Security Identity Manager product.

Access to publications and terminology

This section provides:

- A list of publications in the IBM Security Identity Manager library.
- Links to Online publications.
- A link to the IBM Terminology website.

IBM Security Identity Manager library

For a complete listing of the IBM Security Identity Manager and IBM Security Identity Manager Adapter documentation, see the online library [http://www-01.ibm.com/support/knowledgecenter/SSRMWJ/welcome].

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security Identity Manager library


IBM Security Systems Documentation Central

[IBM Security Systems Documentation Central] provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

IBM Publications Center


IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at [http://www.ibm.com/software/globalization/terminology].
Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical training

For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

Appendix C, “Support information,” on page 119 provides details about:
   • What information to collect before contacting IBM Support.
   • The various methods for contacting IBM Support.
   • How to use IBM Support Assistant.
   • Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The Community and Support tab on the product information center can provide additional support resources.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.
Chapter 1. Overview of the Active Directory Adapter

An adapter provides an interface between a managed resource and the IBM Security Identity Manager server.

Adapters might reside on the managed resource. The IBM Security Identity Manager server manages access to the resource by using your security system. Adapters function as trusted virtual administrators on the target platform. They perform tasks, such as creating, suspending, and restoring user accounts, and other administrative functions that are performed manually. The adapter runs as a service, independently of whether you are logged on to the IBM Security Identity Manager server.

Features of the adapter

You can use the Active Directory Adapter to automate administrative tasks.

- **Active Directory**
  - Creating an Active Directory account
    Use the adapter to create an Active Directory account on Windows 2008 domain servers.
  - Managing an Active Directory account
    Use the adapter to manage an Active Directory account on Windows 2008 domain servers.
  - Managing an Exchange Mailbox
    The 64-bit version of the adapter supports Exchange 2010 and 2013 only. The 64-bit adapter has no backward support for Exchange 2000, 2003, or 2007.
  - Creating home directories
    Use the adapter to create home directories.
  - Move user in hierarchy
    A user can be moved in different containers managed by the Active Directory Adapter by changing the container of the user from IBM Security Identity Manager.
  - Managing an Active Directory group
    Use the adapter to add, modify, and delete an Active Directory group.

The Active Directory Adapter does not create or manage local system accounts. Use the Windows Local Account Adapter for this purpose.

The Active Directory Adapter requires administrator authority. IBM Security Identity Manager requests might fail if the adapter is not given sufficient authority to perform the requested task.

The Active Directory Adapter can be installed within the managed domain or in a different domain. If the adapter is installed in a different domain, trusts must be configured on both the domain that is managed and the domain where the adapter is installed. For more information about configuring trusts for domains, see the Microsoft documentation that corresponds to your operating system.

Configure the Active Directory Adapter to support both subdomains and multiple domains through the Base Point feature on the adapter service form. The best deployment for your environment is based on the topology of your Windows domain and Active Directory structure. However, the primary factor is the planned design of your IBM Security Identity Manager provisioning policies.
and approval workflow process. For more information about provisioning policies and approval workflow, see the IBM Security Identity Manager product documentation.

- Windows Lync Server
  Running under an account with sufficient authority, the adapter supports Lync. Lync is communications software for instant messaging, conferencing, and telephony solutions.
  The adapter uses a remote PowerShell to interface with the Lync Server and set the Lync attributes.
  It is not necessary to install the Lync management tools on the machine that runs the adapter. However, it does require that the machine running the adapter has PowerShell 2.0 and that the Execution Policy allows local scripts to be run (RemoteSigned or Unrestricted).

**Limitations of the adapter**

Running under an account with sufficient authority, the adapter is able to manage user accounts and Exchange mailboxes for all domains within a single forest. Some limitations and configuration issues exist.

- The Exchange 2010 interface now uses a remote PowerShell session with the Exchange server to manage Exchange attributes. This means that it is no longer necessary to install the Exchange management tools on the machine that is running the adapter. However, it does require that the machine running the adapter has PowerShell version 2.0. The Execution Policy must also allow local scripts to be run (RemoteSigned or Unrestricted).
- The adapter cannot manage domains or Exchange servers that are in a different forest.
- The supporting data returned from a reconciliation only includes groups from the domain being reconciled. Local groups from other domains are not returned. Although you can join local groups in other domains, you cannot specify groups in other domains when sending requests to the adapter.

In this illustration, the user account in Domain 2 is joined directly to a group in Domain 1. While this is possible to do in Active Directory, the adapter does not support it.

You can use Active Directory to create a universal group and make it a member of the group you wish to join. Do not add users directly to the universal group. Instead create a group in the local domain and add it to the universal group. You can then add users to the group in the local domain. See your Microsoft Active Directory documentation for more information. This configuration is supported by the adapter.

With this configuration, you join Domain 2 users to the local group in Domain 2 and by association they are members of the cross domain group in Domain 1.
Because you can create multiple service instances on the IBM Security Identity Manager server that point to the same adapter, ensure that you do not specify base points that overlap. If you use a base point for one service instance that contains the base point of another service instance, only the users in the contained base point are returned as duplicates of the parent base point.

**Account limitations for Lync**

Running under an account with sufficient authority, the adapter is able to manage Lync accounts. Some limitations exist.

- To enable a user to use Lync, you must provide a Session Initiation Protocol (SIP) address and a Registrar Pool.
- A SIP address specified on account form must be in Session Initiation Protocol format. For example: sip:abc@test.com
- When the Telephony field of the user is set to Remote call control or Remote call control only on the account, then both Line URI and Line server URI fields must also be set.
  The URI values must conform to RFC 3966. For example, a telephone number must start with tel: such as tel:+91222222.
- Moving a user to another registrar pool changes the Lync Server account location of the user. It does not move the Active Directory account or the user to a new organizational unit (OU) or location.
Chapter 2. Communication between the Active Directory Adapter and the IBM Security Identity Manager server

The adapter communicates with the IBM Security Identity Manager server with the Directory Access Markup Language (DAML) protocol. You can configure SSL authentication for the adapter.

Data transfer from IBM Security Identity Manager to the adapter

The Active Directory Adapter is an individual IBM Security Identity Manager software program on a domain controller or a non-domain controller workstation.

Data is transferred between the Active Directory Adapter and the IBM Security Identity Manager server using the Directory Access Markup Language (DAML) protocol. DAML uses Secure Sockets Layer (SSL) to send XML-formatted messages between the adapter and IBM Security Identity Manager.

IBM Security Identity Manager communicates with the Active Directory Adapter in order to administer user accounts. When the IBM Security Identity Manager server issues a request to the Active Directory Adapter, the server opens a TCP/IP connection. This connection stays open until the agent completes the request and responds back to the server with an acknowledgement message. After the IBM Security Identity Manager server receives the anticipated response, it drops the connection to the adapter.

Basic configuration for server-to-adapter SSL communication

The following information pertains to IBM Security Identity Manager deployment on either the WebSphere or the WebLogic application server.

In this configuration, the IBM Security Identity Manager server initiates communication with the adapter (server-to-adapter) by using one-way authentication over SSL. The version of the SSL protocol that is used is either RSA or Open SSL.

Note: From IBM Security Identity Manager 4.6 and onward only the Open SSL protocol is used. For more information about SSL, see Chapter 7, “SSL authentication configuration,” on page 47.

Basic configuration for adapter-to-Active Directory SSL communication

The Active Directory Adapter can be on a domain controller or non-domain controller workstation.

Communication between Active Directory Adapter and Active Directory is not secure. Data sent over the network is in plain text. The Active Directory Adapter uses secure authentication method (no SSL) to identify itself to the active directory. For this, provision is made on the Active Directory service form to accept a user ID and password to authenticate to the Active Directory.
Active Directory uses Kerberos, and possibly NTLM, to authenticate the Active Directory Adapter. When the user name and password are NULL, ADSI binds to the object using the security context of the calling thread, which is either the security context of the user account under which the application is running or the context of the client user account that the calling thread represents.

When SSL communication is set up between the adapter and Active Directory, it allows data transfer over the network in encrypted form.

### SSL communication between the adapter and Active Directory

To use SSL-based encryption while communicating with Active Directory:
- Active Directory must have enabled Public Key Infrastructure (PKI). PKI requires that enterprise certificate authority (CA) is installed on one of the domain controller workstations in the domain. Setting up an enterprise certificate authority causes an Active Directory server to get a server certificate that can then be used to do SSL-based encryption.
- The certificate must be installed on the workstation on which Active Directory Adapter is running.

### Installing Enterprise CA in one of the domain controllers in a domain

To install Enterprise CA in one of the domain controllers in a domain, take these steps:

**About this task**

*Note: Internet Information Services must be stopped before installing the certificate.*

**Procedure**

1. Go to Control Panel > Add Remove Programs > Windows Components. Click Components.
2. Select Certificate Services and click Next.
3. A dialog box is displayed. Click Yes to continue.
4. Select Remote Administration mode. Click Next.
5. Select Enterprise root CA. Click Next.
6. Specify the information to identify this CA. Click Next.
7. Accept the default location or specify a different location to store data related to the certificate server. Click Next.
8. If Internet Information Services is running, a dialog box is displayed. Click OK to stop the service and continue with the certificate installation.
9. Click Finish to complete the installation.

*Note: A restart of the server is not required for SSL communication.*

### Installing the certificate on the workstation where Active Directory Adapter is running

To install the certificate on the workstation where Active Directory Adapter is running, perform these steps:
Procedure
1. Get the trusted root certificate from certificate server. Usually the certificate is present in the c:\winnt\system32\certsrv\certEnroll folder. For example, a certificate name might be ps0721.agents2.com_PS0721CA(1).crt
2. Copy the certificate on the workstation where Active Directory Adapter is installed.
3. Double click the certificate.
4. Click Install Certificate.
5. Click Next.
6. Select Place all certificates in the following store and click Browse.
7. Select Show Physical stores and from the tree view select the folder Local Computer.
8. Click OK.
9. Click Next.
10. Click Finish to complete the installation of the certificate.
Chapter 3. Installation planning for the Active Directory Adapter

Installing and configuring the adapter involves several steps that you must complete in the appropriate sequence. Review the roadmaps before you begin the installation process.

Preinstallation roadmap

To install the adapter, you must complete several tasks.

Table 1. Preinstallation roadmap

<table>
<thead>
<tr>
<th>What to do</th>
<th>Where to find more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain the installation software.</td>
<td>Download the software from Passport Advantage. See “Software download” on page 10.</td>
</tr>
<tr>
<td>Verify that the software and hardware requirements have been met for the adapter that you want to install.</td>
<td>See “Prerequisites” on page 10.</td>
</tr>
</tbody>
</table>

Installation roadmap

To install the adapter, you must complete a task sequence.

Table 2. Installation roadmap

<table>
<thead>
<tr>
<th>What to do</th>
<th>Where to find more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the adapter.</td>
<td>See Chapter 4, “Adapter installation,” on page 11.</td>
</tr>
<tr>
<td>Verify the installation.</td>
<td>See “Installation verification” on page 12.</td>
</tr>
<tr>
<td>Create an adapter user account.</td>
<td>See “Adapter user account creation” on page 13.</td>
</tr>
<tr>
<td>Install the Lync Server CA certificate if the adapter manages Lync Server.</td>
<td>See “Installing the CA certificate of the Lync Server” on page 13.</td>
</tr>
<tr>
<td>Import the adapter profile.</td>
<td>See “Importing the adapter profile into the IBM Security Identity Manager server” on page 13.</td>
</tr>
<tr>
<td>Verify the profile.</td>
<td>See “Verifying the Active Directory Adapter profile installation” on page 14.</td>
</tr>
<tr>
<td>Create a service.</td>
<td>See “Creating an adapter service” on page 14.</td>
</tr>
<tr>
<td>Configure the adapter.</td>
<td>See Chapter 6, “Configuring the adapter for IBM Security Identity Manager,” on page 19.</td>
</tr>
<tr>
<td>Customize the adapter.</td>
<td>See Chapter 8, “Customizing the Active Directory Adapter,” on page 61.</td>
</tr>
</tbody>
</table>
Prerequisites

Verify that all hardware, software, and authorization prerequisites are met before installing the Active Directory Adapter.

Table 3 describes the prerequisites.

Table 3. Prerequisites to install the adapter

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>• A 64-bit x86-based microprocessor.</td>
</tr>
<tr>
<td></td>
<td>• A minimum of 256 MB of memory.</td>
</tr>
<tr>
<td></td>
<td>• At least 300 MB of free disk space.</td>
</tr>
<tr>
<td></td>
<td>• If you plan to manage Exchange or Lync servers, the workstation must have PowerShell 2.0 or later and must be configured to allow local scripts to run.</td>
</tr>
<tr>
<td>Operating system</td>
<td>• Windows 2008 Server Standard Edition 64-bit and Enterprise Edition 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows 2008 R2 Enterprise Edition 64-bit and Core Enterprise 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows 2012 Server</td>
</tr>
<tr>
<td></td>
<td>A Windows Server running Active Directory must be operational in the domain of the system where the adapter is installed.</td>
</tr>
<tr>
<td>Network connectivity</td>
<td>• Internet Protocol network</td>
</tr>
<tr>
<td></td>
<td>• For security purposes, the adapter must be installed on a Windows NT File System (NTFS).</td>
</tr>
<tr>
<td>System administrator authority</td>
<td>The person that performs the Active Directory Adapter installation procedure must have system administrator authority to complete the steps in this chapter.</td>
</tr>
<tr>
<td>IBM Security Identity Manager server</td>
<td>Version 6.0</td>
</tr>
<tr>
<td>Optionally, Exchange Server</td>
<td>Exchange Server 2010 and 2013</td>
</tr>
</tbody>
</table>

Software download

After you have purchased IBM Security Identity Manager, you can download the adapter software from your account in IBM Passport Advantage Online.

Go to IBM Passport Advantage

See the IBM Security Identity Manager Download Document for instructions.

Note:

You can also obtain additional adapter information from IBM Support.
Chapter 4. Adapter installation

You can install the Active Directory Adapter with the following information.

Installing the adapter

Use the Active Directory Adapter installer to manually install the adapter.

About this task

The Active Directory Adapter for IBM Security Identity Manager installation program is available for download from the IBM Web site. Contact your IBM account representative for the Web address and download instructions.

To manually install the adapter, complete these steps.

Note: All directory paths apply to Windows operating systems. Change the directory paths as needed for UNIX operating systems.

Make sure you do the following:

- Verify that your site meets all the prerequisite requirements. See "Prerequisites" on page 10.
- Obtain a copy of the installation software. See "Software download" on page 10.
- Obtain system administrator authority.
- If you are updating a previous installation, the adapter you want to update must already exist. If it does not exist, the software generates the following message:

Adapter is not found at specified location.
Can not perform Update Installation. Please correct the path of installed adapter or select Full Installation.

Procedure

1. If you downloaded the installation software from Passport Advantage, perform the following steps:
   a. Create a temporary directory on the computer on which you want to install the software.
   b. Extract the contents of the compressed file into the temporary directory.
2. Start the installation program with the SetupAD64.exe file in the temporary directory.
3. Select the language and click OK to display the Introduction window.
4. On the Introduction window, click Next.
5. Select either Typical installation or Update installation and click Next to display the Choose Install Folder window. Remember that the adapter must already exist if you want to perform an updated installation.
6. Specify where you want to install the adapter in the Directory Name field. Do one of the following.
   a. Click Next to accept the default location.
   b. Click Browse and navigate to a different directory and click Next.
7. Do the following at the Software License Agreement window:
   a. Review the license agreement and select Accept.
8. Review the installation settings at the Pre-Installation Summary window and do one of the following:
   - Click **Previous** and return to a previous window to change any of these settings.
   - Click **Install** when you are ready to begin the installation.
9. Click **Done** on the Install Complete window.
10. After you finish the installation, create a user account for the adapter and import the adapter profile. See "Adapter user account creation" on page 13 and "Importing the adapter profile into the IBM Security Identity Manager server" on page 13.

### Installation verification

To determine whether the adapter is installed correctly, verify that required components exist.

**bin**  
The following components exist in the `bin` directory:
- ADAgent.exe
- agentCfg.exe
- CertTool.exe
- Exchg2010.dll
- IsamTool.exe
- regis.exe

**data**  
Initially, the `data` directory is empty.

**license**  
The `license` directory contains files that provide license information in supported languages.

**log**  
The `log` directory contains the adapter log files. After the adapter installation is complete, the adapter creates `WinADAgent.log` file.

**Uninstall IBM Windows AD Adapter for ITIM (64 Bit)**  
The directory contains the `Uninstall IBM Windows AD Adapter for ITIM (64 Bit).exe` file. You can uninstall the adapter from agent server workstation by using the `uninstaller.exe` file.

After the adapter installation completes, ensure that windows service for Tivoli Active Directory Agent is created and its status is **Started**. To view the windows service status:

1. Click **Start > Programs > Administrative Tools > Services** to display the Services page.
2. Search for the service that is named ISIM Active Directory Adapter.

The adapter copies the following files to the `system32` directory:
- AdkApi.dll
- ErmApi.dll
- ErmApiDaml.dll
- icudt36.dll
- icuuc36.dll
- libeay32.dll
Review the installer log file IBM_Windows_AD_Adapter_for_ITIM_(64_Bit)_InstallLog.log located in the installation directory for any errors.

Adapter user account creation

You must create a user account for the Active Directory Adapter on the managed resource. Account information is provided when you create a service.

The accounts must be able to remotely connect to the Active Directory server and must have sufficient privileges to administer Active Directory end users. The adapter account, used by the adapters to manage Active Directory, Exchange, and Lync, must be supplied on the logon tab of the Windows Adapter service that is named ISIM Active Directory Adapter.

Installing the CA certificate of the Lync Server

If the adapter manages Lync Server, install the CA certificate of the Lync Server on the computer where the adapter is running.

About this task

After you install the adapter, you must to install the CA certificate of the Lync Server in the truststore for the adapter service account.

Procedure

1. Run the \texttt{mmc.exe} command from the Start menu or a command prompt.
2. Add the certificate snap-in.
3. Select Service Account and click Next.
4. Select Local computer and click Next.
5. Select ISIM Active Directory Adapter and click Next.
6. Right-click Trusted Root Certification Authorities and select All Tasks\Import...
7. Select the CA certificate file and import the file to the truststore.
8. Restart the adapter service.

Importing the adapter profile into the IBM Security Identity Manager server

You must import the adapter profile into the IBM Security Identity Manager server before you use the adapter.

About this task

An adapter profile defines the types of resources that the IBM Security Identity Manager server can manage. The profile is used to create a service on the IBM Security Identity Manager server and to communicate with the adapter.

Before you import the adapter profile, verify that the following conditions are met:

- The IBM Security Identity Manager server must be installed and running.
You must have root or Administrator authority on the IBM Security Identity Manager server.

The adapter profile is included in the JAR file for the adapter:

\texttt{adapternameProfile.jar}

**Procedure**

1. Log in to the IBM Security Identity Manager server with an account that has the authority to do administrative tasks.
2. Import the adapter profile (or service type) by using the import service type feature for your IBM Security Identity Manager product. Refer to the online help or the product documentation for specific instructions about importing service types.

**What to do next**

If you receive an error that is related to the schema when you import the adapter profile, refer to the \texttt{trace.log} file for information about the error. The \texttt{trace.log} file location is specified with the \texttt{handler.file.fileDir} property that is defined in the IBM Security Identity Manager enRoleLogging.properties file. The \texttt{enRoleLogging.properties} file is installed in the IBM Security Identity Manager \texttt{\data} directory.

**Verifying the Active Directory Adapter profile installation**

After you install the adapter profile, verify that the adapter profile was successfully installed.

**About this task**

If the adapter profile is not installed correctly, the adapter might not function as it is intended to function. If the Active Directory Adapter profile is not already installed on your system, you must import the adapter profile. See "Importing the adapter profile into the IBM Security Identity Manager server" on page 13 for information about importing the adapter profile.

To verify that the adapter profile was successfully installed, complete these steps.

**Procedure**

1. Create a service using the Active Directory Adapter profile. See "Creating an adapter service" for information about this task.
2. Create a user account by using the service. See "Adapter user account creation" on page 13 for information about this task.

   If you are unable to create a service by using the Active Directory Adapter profile or you are unable to create a user account, the adapter profile is not installed correctly. You might need to import the adapter profile again.

**Creating an adapter service**

After the adapter profile is imported on IBM Security Identity Manager, you must create a service so that IBM Security Identity Manager can communicate with the adapter.
About this task

To create or change a service, you must use the service form to provide information for the service. Service forms might vary depending on the adapter.

Procedure

1. Log on to the IBM Security Identity Manager server with an account that has the authority to perform administrative tasks.
2. In the My Work pane, click Manage Services and click Create.
3. On the Select the Type of Service page, select Active Directory Profile.
4. Click Next to display the adapter service form.
5. Complete the following fields on the service form:

   On the General Information tab:

   Service Name
   Specify a name that defines this adapter service on the IBM Security Identity Manager server.

   Description
   Optional: Specify a description for this service.

   URL
   Specify the location and port number of the adapter. The port number is defined in the protocol configuration by using the agentCfg program. For more information, see “Modifying protocol configuration settings” on page 21. URL is a required field.

   If https is specified as part of the URL, the adapter must be configured to use SSL authentication. If the adapter is not configured to use SSL authentication, specify http for the URL. For more information, see Chapter 7, “SSL authentication configuration,” on page 47.

   User Id
   Specify the DAML protocol user name. The user name is defined in the protocol configuration by using the agentCfg program. For more information, see “Modifying protocol configuration settings” on page 21.

   Password
   Specify the password for the DAML protocol user name. This password is defined in the protocol configuration by using the agentCfg program. For more information, see “Modifying protocol configuration settings” on page 21.

   Owner
   Optional: Specify the service owner, if any.

   Service Prerequisite
   Optional: Specify an existing IBM Security Identity Manager service that is a prerequisite for the adapter service.

   On the Status and information tab
   This page contains read only information about the adapter and managed resource. These fields are examples. The actual fields vary depending on the type of adapter and how the service form is configured. The adapter must be running to obtain the information. Click Test Connection to populate the fields.
Last status update: Date  
Specifies the most recent date when the Status and information tab was updated.

Last status update: Time  
Specifies the most recent time of the date when the Status and information tab was updated.

Managed resource status  
Specifies the status of the managed resource that the adapter is connected to.

Adapter version  
Specifies the version of the adapter that the IBM Security Identity Manager service uses to provision request to the managed resource.

Profile version  
Specifies the version of the profile that is installed in the IBM Security Identity Manager server.

ADK version  
Specifies the version of the ADK that the adapter uses.

Installation platform  
Specifies summary information about the operating system where the adapter is installed.

Adapter account  
Specifies the account that running the adapter binary file.

Adapter up time: Date  
Specifies the date when the adapter started.

Adapter up time: Time  
Specifies the time of the date when the adapter started.

Adapter memory usage  
Specifies the memory usage for running the adapter.

If the connection fails, follow the instructions in the error message. Also
• Verify the adapter log to ensure that the IBM Security Identity Manager test request was successfully sent to the adapter.
• Verify the adapter configuration information.
• Verify IBM Security Identity Manager service parameters for the adapter profile. For example, verify the work station name or the IP address of the managed resource and the port.

6. Click Finish.
Chapter 5. Installation and uninstallation of the Active Directory Adapter with 64-bit support in silent mode

You can install and uninstall the Active Directory Adapter with 64-bit support by using the silent mode.

Silent installation suppresses the wizard and the Launcher User Interfaces (UIs) that do not display any information or require interaction. You can use the –i silent option to install or uninstall the adapter in silent mode.

Note: If you install the adapter in silent mode, the uninstaller runs in silent mode irrespective of whether you use the –i silent option or not.

Adapter installation in silent mode

You can install the adapter by using the silent mode.

Installing the adapter with default options

Run the following command from command line to install the Active Directory Adapter with 64-bit support by using the –i silent option:

```bash
SetupAD64.exe -i silent -DLICENSE_ACCEPTED=TRUE
```

When you install the adapter by using the specified command, the adapter is installed with these default values.

<table>
<thead>
<tr>
<th>Table 4. Default values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Installation directory</strong></td>
</tr>
<tr>
<td><strong>Adapter name</strong></td>
</tr>
<tr>
<td><strong>Installation option</strong></td>
</tr>
</tbody>
</table>

Installing the adapter with command line options

You can specify the listed installation options from the command line when you install the adapter by using the silent mode. For example, if you want to override the default installation directory path, run the following command:

```bash
SetupAD64.exe -i silent -DLICENSE_ACCEPTED=TRUE -DUSER_INSTALL_DIR="c:\tivoli\MyFolder"
```

Note:

- The -D option is followed by a variable and a value pair without any space after the -D option.
- You must wrap arguments with quotation marks when the arguments contain spaces.

<table>
<thead>
<tr>
<th>Table 5. Installation options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td>-DUSER_INSTALL_DIR= Value</td>
</tr>
</tbody>
</table>
Table 5. Installation options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>-DLICENSE_ACCEPTED=Value</td>
<td>Accept the IBM license for the adapter, the value must be TRUE.</td>
</tr>
<tr>
<td></td>
<td>When you do not specify this option, the default value is FALSE.</td>
</tr>
</tbody>
</table>

Installing the adapter by using the response file

Generating the response file

You can use response file to provide inputs during silent installation. Generate the response file by running the following command, which runs the installer in interactive mode and installs the adapter.

```
SetupAD64.exe –r "Full path of response file"
```

For example:

```
SetupAD64.exe –r "c:\temp\WinAD64Response.txt"
```

Note: If you run this command to only generate the response file, you must uninstall the adapter by using the uninstaller.

Creating the response file manually

You can also manually create the response file with the following content:

```
#Start of Response file
#Choose Install Folder
#---------------------
USER_INSTALL_DIR=c:\tivoli\agents\ADAgent
#Has the license been accepted
#-----------------------------
LICENSE_ACCEPTED=TRUE
#End of Response file
```

After you create the response file, you can use it as:

```
SetupAD64.exe –i silent -f "Full path of response file"
```

Adapter uninstallation in silent mode

Run the following command from the command line to uninstall the Active Directory Adapter with 64-bit support by using the –i silent option.

```
Specify the full path when you are not running the command from the Uninstall IBM Windows AD Adapter for ITIM (64 Bit) directory in the installation directory of the adapter.
"Uninstall IBM Windows AD Adapter for ITIM (64 Bit).exe" -i silent
```

For example, "C:\tivoli\agents\ADAgent\Uninstall IBM Windows AD Adapter for ITIM (64 Bit)\Uninstall IBM Windows AD Adapter for ITIM (64 Bit).exe" -i silent.

Note: Restart the workstation after you install or uninstall the adapter.
Chapter 6. Configuring the adapter for IBM Security Identity Manager

After you install the adapter, configure the adapter to function correctly.

About this task

Note: The screens displayed in these tasks are examples, the actual screens displayed might differ.

To configure the adapter, perform the following steps:

Procedure

1. Start the adapter service. Use the Windows Services tool.
3. Configure the adapter for event notification. See “Configuring event notification” on page 25.
4. Install a certificate on the workstation where the adapter is installed and also on the IBM Security Identity Manager server to establish secure communication between them. See Chapter 7, “SSL authentication configuration,” on page 47.
5. Install the adapter profile on the IBM Security Identity Manager server. See “Importing the adapter profile into the IBM Security Identity Manager server” on page 13.
6. Configure the adapter service form. See “Creating an adapter service” on page 14.
7. Use the adapter configuration program, agentCfg, to view or modify the adapter parameters. See “Starting the adapter configuration tool.”
8. Configure the adapter account form. See the product documentation.
9. Restart the adapter service after you modify the adapter configuration settings.

Starting the adapter configuration tool

Use the adapter configuration program, agentCfg, to view or modify the adapter parameters.

About this task

All the changes that you make to the parameters with agentCfg take effect immediately. You can also use agentCfg to view or modify configuration settings from a remote workstation.

Procedure

1. Browse to the Windows command prompt.
2. In the command prompt, change to the bin subdirectory of the adapter. Run the following command if the adapter is in the default location:
   ```
   cd C:\Program Files\IBM\ISIM\Agents\adapter_nameAgent\bin\n   ```
3. Run the following command:
agentCfg -agent adapter_nameAgent

4. At the **Enter configuration key for Agent 'adapter_nameAgent'** prompt, type the configuration key for the adapter.

The default configuration key is **agent**. To prevent unauthorized access to the configuration of the adapter, you must modify the configuration key after the adapter installation completes.

The Agent Main Configuration menu is displayed.

```
adapter_nameAgent 6.0.4.1200 Agent Main Configuration Menu
-------------------------------------------
A. Configuration Settings.
B. Protocol Configuration.
C. Event Notification.
D. Change Configuration Key.
E. Activity Logging.
F. Registry Settings.
G. Advanced Settings.
H. Statistics.
I. Codepage Support.
X. Done.
```

Select menu option:

**Results**

From the Main Configuration menu screen, you can configure the protocol, view statistics, and modify settings, including configuration, registry, and advanced settings.

**Table 6. Options for the main configuration menu**

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Viewing configuration settings</td>
</tr>
<tr>
<td>B</td>
<td>Changing protocol configuration settings</td>
</tr>
<tr>
<td>C</td>
<td>Configuring event notification</td>
</tr>
<tr>
<td>D</td>
<td>Changing the configuration key</td>
</tr>
<tr>
<td>E</td>
<td>Changing activity logging settings</td>
</tr>
<tr>
<td>F</td>
<td>Changing registry settings</td>
</tr>
<tr>
<td>G</td>
<td>Changing advanced settings</td>
</tr>
<tr>
<td>H</td>
<td>Viewing statistics</td>
</tr>
<tr>
<td>I</td>
<td>Changing code page settings</td>
</tr>
</tbody>
</table>

**Related tasks:**

**“Accessing help and other options” on page 44**

Use the agentCfg help menu to display the help arguments that you can use to find information about the adapter.

**“Modifying protocol configuration settings” on page 21**

The adapter uses the DAML protocol to communicate with the IBM Security Identity Manager server.

**Viewing configuration settings**

View the adapter configuration settings for information about the adapter, including version, ADK version, and adapter log file name.
Procedure
1. Access the Agent Main Configuration menu.
2. Type A to display the configuration settings for the adapter.

<table>
<thead>
<tr>
<th>Configuration Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Version</td>
</tr>
<tr>
<td>ADK Version</td>
</tr>
<tr>
<td>ERM Version</td>
</tr>
<tr>
<td>Adapter Events</td>
</tr>
<tr>
<td>License</td>
</tr>
<tr>
<td>Asynchronous ADD Requests</td>
</tr>
<tr>
<td>Asynchronous MOD Requests</td>
</tr>
<tr>
<td>Asynchronous DEL Requests</td>
</tr>
<tr>
<td>Asynchronous SEA Requests</td>
</tr>
<tr>
<td>Available Protocols</td>
</tr>
<tr>
<td>Configured Protocols</td>
</tr>
<tr>
<td>Logging Enabled</td>
</tr>
<tr>
<td>Logging Directory</td>
</tr>
<tr>
<td>Log File Name</td>
</tr>
<tr>
<td>Max. log files</td>
</tr>
<tr>
<td>Max.log file size (Mbytes)</td>
</tr>
<tr>
<td>Debug Logging Enabled</td>
</tr>
<tr>
<td>Detail Logging Enabled</td>
</tr>
<tr>
<td>Thread Logging Enabled</td>
</tr>
</tbody>
</table>

Press any key to continue

3. Press any key to return to the Main menu.

Related tasks:
“Starting the adapter configuration tool” on page 19

Use the adapter configuration program, agentCfg, to view or modify the adapter parameters.

Modifying protocol configuration settings

The adapter uses the DAML protocol to communicate with the IBM Security Identity Manager server.

About this task

By default, when the adapter is installed, the DAML protocol is configured for a nonsecure environment. To configure a secure environment, use Secure Socket Layer (SSL) and install a certificate.

The DAML protocol is the only supported protocol that you can use. Do not add or remove a protocol.

Procedure
1. Access the Agent Main Configuration menu.
2. Type B. The DAML protocol is configured and available by default for the adapter.
3. At the Agent Protocol Configuration menu, type C to display the Configure Protocol Menu.

Configure Protocol Menu
-----------------------------------
A. DAML
X. Done
Select menu option:

4. Type a letter to display the Protocol Properties menu for the configured protocol with protocol properties.

The following screen is an example of the DAML protocol properties.

DAML Protocol Properties
--------------------------------------------------------
A. USERNAME ****** ;Authorized user name.
B. PASSWORD ****** ;Authorized user password.
C. MAX_CONNECTIONS 100 ;Max Connections.
D. PORTNUMBER 45580 ;Protocol Server port number.
E. USE_SSL TRUE ;Use SSL secure connection.
F. SRV_NODENAME ––––– ;Event Notif. Server name.
G. SRV_PORTNUMBER 9443 ;Event Notif. Server port number.
H. HOSTADDR ANY ;Listen on address < or "ANY" >
I. VALIDATE_CLIENT_CE FALSE ;Require client certificate.
J. REQUIRE_CERT_REG FALSE ;Require registered certificate.
K. READ_TIMEOUT 0 ;Socked read timeout (seconds)
X. Done
Select menu option:

5. Follow these steps to change a protocol value:
   • Type the letter of the menu option for the protocol property to configure. The following table describes each property.
   • Take one of the following actions:
     – Change the property value and press Enter to display the Protocol Properties menu with the new value.
     – If you do not want to change the value, press Enter.

Table 7. Options for the DAML protocol menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Displays the following prompt: Modify Property 'USERNAME': Type a user ID, for example, agent. The IBM Security Identity Manager server uses this value to connect to the adapter. The default user ID is agent.</td>
</tr>
</tbody>
</table>
### Table 7. Options for the DAML protocol menu (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
</table>
| B      | Displays the following prompt:  
Modify Property 'PASSWORD':  
Type a password, for example, agent. The IBM Security Identity Manager server uses this value to connect to the adapter. The default password is agent. |
| C      | Displays the following prompt:  
Modify Property 'MAX_CONNECTIONS':  
Enter the maximum number of concurrent open connections that the adapter supports. The default number is 100. |
| D      | Displays the following prompt:  
Modify Property 'PORTNUMBER':  
Type a different port number.  
This value is the port number that the IBM Security Identity Manager server uses to connect to the adapter. The default port number is 45580. |
| E      | Displays the following prompt:  
Modify Property 'USE_SSL':  
TRUE specifies to use a secure SSL connection to connect the adapter. If you set USE_SSL to TRUE, you must install a certificate. FALSE, the default value, specifies not to use a secure SSL connection.  
**Note:** By default event notification requires USE_SSL set to TRUE. To use event notification, you must set USE_SSL to TRUE and add a certificate and key from the PKCS12 file in the adapter. |
| F      | Displays the following prompt:  
Modify Property 'SRV_NODENAME':  
Type a server name or an IP address of the workstation where you installed the IBM Security Identity Manager server.  
This value is the DNS name or the IP address of the IBM Security Identity Manager server that is used for event notification and asynchronous request processing.  
**Note:** If your operating system supports Internet Protocol version 6 (IPv6) connections, you can specify an IPv6 server. |
| G      | Displays the following prompt:  
Modify Property 'SRV_PORTNUMBER':  
Type a different port number to access the IBM Security Identity Manager server.  
The adapter uses this port number to connect to the IBM Security Identity Manager server. The default port number is 9443. |
| H      | The HOSTADDR option is useful when the system where the adapter is running has more than one network adapter. You can select which IP address the adapter must listen to.  
The default value is ANY. |
### Table 7. Options for the DAML protocol menu (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
</table>
| I      | Displays the following prompt:<br>

Modify Property 'VALIDATE_CLIENT_CE':

Specify TRUE for the IBM Security Identity Manager server to send a certificate when it communicates with the adapter. When you set this option to TRUE, you must configure options D through I.

Specify FALSE, the default value to enable the IBM Security Identity Manager server to communicate with the adapter without a certificate.<br>
**Note:**<br>
- The property name is VALIDATE_CLIENT_CERT; however, it is truncated by the agentCfg to fit in the screen.<br>
- You must use certTool to install the appropriate CA certificates and optionally register the IBM Security Identity Manager server certificate. |
| J      | Displays the following prompt:<br>

Modify Property 'REQUIRE_CERT_REG':

This value applies when option I is set to TRUE.<br>

Type TRUE to register the adapter with the client certificate from the IBM Security Identity Manager server before it accepts an SSL connection.<br>

Type FALSE to verify the client certificate against the list of CA certificates. The default value is FALSE. |
| K      | Displays the following prompt:<br>

Modify Property 'READ_TIMEOUT':

Type the timeout value in seconds for IBM Security Identity Manager and the adapter connection.<br>

This option applies to setups that have a firewall between IBM Security Identity Manager and the adapter. This firewall has a timeout value that is less than the maximum connection age DAML property on IBM Security Identity Manager. When your transactions run longer than the firewall timeout, the firewall terminates the connection. The sudden termination of connections might leave the adapter with incorrect connection threads causing the adapter to crash.<br>

When the adapter halts randomly because of the specified setup, change the value for the READ_TIMEOUT. The value must be in seconds and less than the timeout value of the firewall. |

6. Follow these steps at the prompt:<br>
   - Change the property value and press Enter to display the Protocol Properties menu with the new value.<br>
   - If you do not want to change the value, press Enter.<br>
7. Repeat step 5 to configure the other protocol properties.<br>
8. At the Protocol Properties menu, type X to exit.<br>

**Related concepts:**

“SSL certificate management with certTool” on page 53<br>
Use the certTool utility to manage private keys and certificates.
You can provide SSL authentication, certificates, and enable SSL authentication with the certTool utility.

**Related tasks:**

* "Starting the adapter configuration tool" on page 19
  Use the adapter configuration program, agentCfg, to view or modify the adapter parameters.
* "Installing the certificate" on page 57
  After you receive your certificate from your trusted CA, install it in the registry of the adapter.

---

**Configuring event notification**

When you enable event notification, the workstation on which the adapter is installed maintains a database of the reconciliation data.

**About this task**

The adapter updates the database with the changes that are requested by the IBM Security Identity Manager server and remains synchronized with the server. You can specify an interval for the event notification process to compare the database to the data that currently exists on the managed resource. When the interval elapses, the adapter forwards the differences between the managed resource and the database to IBM Security Identity Manager and updates the local snapshot database.

**Note:** This adapter supports adapter-based event notification.

To enable event notification, ensure that the adapter is deployed on the managed host and is communicating successfully with IBM Security Identity Manager. You must also configure the host name, port number, and login information for the server and SSL authentication.

**Procedure**

- To identify the server that uses the DAML protocol and to configure SSL authentication, take the following steps:
  1. Access the Agent Main Configuration menu.
  2. At the Agent Protocol Configuration menu, select **Configure Protocol**.
  3. Change the USE_SSL property to **TRUE**.
  4. Install a certificate by using the certTool.
  5. Type the letter of the menu option for the SRV_NODENAME property.
  6. Specify the IP address or server name that identifies the server and press **Enter** to display the Protocol Properties menu with new settings.
  7. Type the letter of the menu option for the SRV_PORTNUMBER property.
  8. Specify the port number that the adapter uses to connect to the server for event notification.
  9. Press **Enter** to display the Protocol Properties menu with new settings.

The example menu describes all the options that are displayed when you enable event notification. If you disable event notification, none of the options are displayed.

- To set event notification for the IBM Security Identity Manager server, take the following steps:
1. Access the Agent Main Configuration menu.

2. At the Agent Main Configuration menu, type C to display the Event Notification menu.

   Event Notification Menu
   ----------------------------------------------------------------------------------
   * Password attributes : eradapterPassword
   * Reconciliation interval : 1 hour(s)
   * Next Reconciliation time : 57 min(s). 36 sec(s).
   * Configured Contexts : subtest, outtest, tradewinds
   A. Enabled - ADK
   B. Time interval between reconciliations.
   C. Set Processing cache size. (currently: 50 Mbytes)
   D. Start event notification now.
   E. Set attributes to be reconciled.
   F. Reconciliation process priority. (current: 1)
   G. Add Event Notification Context.
   H. Modify Event Notification Context.
   I. Remove Event Notification Context.
   J. List Event Notification Contexts.
   K. Set password attribute names.
   X. Done

   Select menu option:

3. At the Agent Main Configuration menu, type the letter of the menu option that you want to change.

   Note:
   – Enable option A for the values of the other options to take effect. Each time that you select this option, the state of the option changes.
   – Press Enter to return to the Agent Event Notification menu without changing the value.

   Table 8. Options for the event notification menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>If you select this option, the adapter updates the IBM Security Identity Manager server with changes to the adapter at regular intervals. If Enabled - Adapter is selected, the adapter code processes event notification by monitoring a change log on the managed resource. When the option is set to: • Disabled, all options except Start event notification now and Set attributes to be reconciled are available. Pressing the A key changes the setting to Enabled - ADK. • Enabled - ADK, all options are available. Pressing the A key changes the setting to Disabled or if your adapter supports event notification, changes to Enabled - Adapter. • Enabled - Adapter, all options are available except: Time interval between reconciliations, Set processing cache size, Start event notification now, Reconciliation process priority, and Set attributes to be reconciled. Pressing the A key changes the setting to Disabled. Type A to toggle between the options.</td>
</tr>
<tr>
<td>Option</td>
<td>Configuration task</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------</td>
</tr>
</tbody>
</table>
| B      | Displays the following prompt:  
|        | Enter new interval ([ww:dd:hh:mm:ss])  
|        | Type a different reconciliation interval. You can type this interval: [00:01:00:00:00]  
|        | This value is the interval to wait after the event notification completes before it is run again. The event notification process is resource intense, therefore, this value must not be set to run frequently. This option is not available if you select Enabled - Adapter. |
| C      | Displays the following prompt:  
|        | Enter new cache size [50]:  
|        | Type a different value to change the processing cache size. This option is not available if you select Enabled - Adapter. |
| D      | If you select this option, event notification starts. This option is not available if you select Disabled or Enabled - Adapter. |
| E      | Displays the Event Notification Entry Types menu. This option is not available if you select Disabled or Enabled - Adapter. |
| F      | Displays the following prompt:  
|        | Enter new thread priority [1-10]:  
|        | Type a different thread value to change the event notification process priority.  
|        | Setting the thread priority to a lower value reduces the impact that the event notification process has on the performance of the adapter. A lower value might also cause event notification to take longer. |
| G      | Displays the following prompt:  
|        | Enter new context name:  
|        | Type the new context name and press Enter. The new context is added. |
| H      | Displays a menu that lists the available contexts. |
| I      | Displays the Remove Context menu. This option displays the following prompt:  
|        | Delete context context1? [no]:  
|        | Press Enter to exit without deleting the context or type Yes and press Enter to delete the context. |
| J      | Displays the Event Notification Contexts in the following format:  
|        | Context Name : Context1  
|        | Target DN : erservicename=context1,o=IBM,ou=IBM,dc=com  
|        | --- Attributes for search request ---  
|        | {search attributes listed} ---  
| K      | When you select the Set password attribute names, you can set the names of the attributes that contain passwords. These values are not stored in the state database and changes are not sent as events. This option avoids the risk of sending a delete request for the old password in clear text when IBM Security Identity Manager changes a password. Changes from IBM Security Identity Manager are recorded in the local database for event notification. A subsequent event notification does not retrieve the password. It sends a delete request for the old password in clear text that is listed in the IBM Security Identity Manager logs. |
4. If you changed the value for options B, C, E, or F, press Enter. The other options are automatically changed when you type the corresponding letter of the menu option.

The Event Notification menu is displayed with your new settings.

Related concepts:

“SSL certificate management with certTool” on page 53
Use the certTool utility to manage private keys and certificates.

Related tasks:

“Modifying an event notification context” on page 30
Some adapters support multiple services.

“Setting event notification triggers”
By default, all the attributes are queried for value changes.

“Modifying protocol configuration settings” on page 21
The adapter uses the DAML protocol to communicate with the IBM Security Identity Manager server.

“Starting the adapter configuration tool” on page 19
Use the adapter configuration program, agentCfg, to view or modify the adapter parameters.

Setting event notification triggers
By default, all the attributes are queried for value changes.

About this task

These triggers apply only to ADK-based event notifications. The triggers are not used by adapter-based notifications.

Attributes that change frequently, for example, Password age or Last successful logon, must be omitted.

Note: Attributes for your adapter might be different than the attributes used in these examples.

Procedure

1. Access the Agent Main Configuration Menu. See “Starting the adapter configuration tool” on page 19.

2. At the Event Notification Menu, type E to display the Event Notification Entry Types Menu.

<table>
<thead>
<tr>
<th>Event Notification Entry Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. erADGroup</td>
</tr>
<tr>
<td>B. erADAccount</td>
</tr>
<tr>
<td>C. erADContainer</td>
</tr>
<tr>
<td>D. erADMailStore</td>
</tr>
<tr>
<td>X. Done</td>
</tr>
</tbody>
</table>

Select menu option:

Your adapter types might be different from this example. The types are not displayed in the menu until the following conditions are met:

a. Enable event notification
b. Create and configure a context
c. Perform a full reconciliation operation
3. Type A for a list of attributes returned during a group reconciliation. Type B for a list of attributes returned during a user reconciliation. Type C for a list of the container attributes returned during reconciliation. Type D for a list of the mail store attributes returned during reconciliation.

The Event Notification Attribute Listing for the selected type is displayed. The default setting lists all attributes that the adapter supports. The following list is an example of attributes. The attributes might be different for other adapters.

<table>
<thead>
<tr>
<th>Event Notification Attribute Listing</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) **erADEAlias</td>
</tr>
<tr>
<td>(b) **erADAllowDialin</td>
</tr>
<tr>
<td>(c) **erADBadLoginCount</td>
</tr>
<tr>
<td>(d) **erADBasePoint</td>
</tr>
<tr>
<td>(e) **erCompany</td>
</tr>
<tr>
<td>(f) **erADContainer</td>
</tr>
<tr>
<td>(g) **erADContainerCN</td>
</tr>
<tr>
<td>(h) **erADContainerDN</td>
</tr>
<tr>
<td>(i) **erADContainerRDN</td>
</tr>
</tbody>
</table>

4. To exclude an attribute from an event notification, type the letter of the menu option.

   **Note:** Attributes that are marked with two asterisks (**) are returned during the event notification. Attributes that are not marked with ** are not returned during the event notification.

**Adapter-based event notification: Configuring domain controllers**

The adapter-based event notification requires configuration on all domain controllers in the managed domain.

**About this task**

When a user is added to a group on the Active Directory, the group object is updated, not the user object. The adapter uses the event log entries on each domain controller to determine whether to add or remove a user from a group. To enable the log for the group membership modification of users in the event log, take the following steps.

**Procedure**

1. On Windows operating systems, click **Start > Programs > Administrative Tools > Domain Security Policy** to display the Default Domain Security Settings page.
2. Expand **Local Policy** and then select **Audit Policy**.
3. Double-click the **Audit account management** policy to display the Audit account management Properties page.
4. Select the **Define these policy settings** check box and then select **Success** and **Failure** check boxes.
5. Click **OK**.

**Setting the event viewer**

You can set the size of the Security log file, which must be at least 2 MB. Setting the log size to more than 2 MB allows the log file to collect more event data.
**Procedure**

1. On a Windows operating system, click **Start > Programs > Administrative Tools > Event Viewer** to display the Event Viewer (Local) page.
2. Right-click **Security** and then select **Properties** to display the Security Properties page.
3. On the General tab, set the log size to at least 2048 KB in the **Maximum log size** field.
4. Click **OK**.

**Results**

The adapter creates these registry keys under `\HKEY_LOCAL_MACHINE\SOFTWARE\Access360\adapter_name\Agent\CTXT_Context_Name`.

<table>
<thead>
<tr>
<th>Registry key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LastChanged_Context_Name</td>
<td>The highest changed number for the object class User.</td>
</tr>
<tr>
<td>LastChanged_Context_Name_CNT</td>
<td>The highest changed number for the object class Container.</td>
</tr>
<tr>
<td>LastChanged_Context_Name_GRP</td>
<td>The highest changed number for the object class Group.</td>
</tr>
<tr>
<td>LastChanged_Context_Name_EMB</td>
<td>The highest changed number for the object class Exchange Mailbox.</td>
</tr>
<tr>
<td>LastChanged_Context_Name_GRP_CNT</td>
<td>The highest changed number for the object class Group Container.</td>
</tr>
</tbody>
</table>

### Modifying an event notification context

Some adapters support multiple services.

### About this task

An event notification context corresponds to a service on the IBM Security Identity Manager server. If you want to enable event notification for a service, then you must create a context for the service. You can have multiple event notification contexts.

To modify an event notification context, do the following steps. In the following example screen, Context1, Context2, and Context3 are different contexts that have a different base point.

**Procedure**

1. Access the **Agent Main Configuration** menu.
2. From Event Notification, type the **Event Notification** menu option.
3. From the **Event Notification** menu, type the **Modify Event Notification Context** option to display a list of available contexts. For example:
4. Type the option of the context that you want to modify.

Options:

Table 10. Options for modify context

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Adding search attributes for event notification</td>
</tr>
<tr>
<td>B</td>
<td>Configuring the target DN for event notification contexts</td>
</tr>
<tr>
<td>C</td>
<td>Removing the baseline database for event notification contexts</td>
</tr>
</tbody>
</table>

Related tasks:

“Starting the adapter configuration tool” on page 19

Use the adapter configuration program, agentCfg, to view or modify the adapter parameters.

Adding search attributes for event notification

For some adapters, you can specify an attribute-value pair for one or more contexts.

About this task

These attribute-value pairs, which are defined by completing the following steps, serve multiple purposes:

- When a single adapter supports multiple services, each service must specify one or more attributes to differentiate the service from the other services.
- The adapter passes the search attributes to the event notification process either after the event notification interval occurs or the event notification starts manually. For each context, a complete search request is sent to the adapter. Additionally, the attributes that are specified for that context are passed to the adapter.
- When the IBM Security Identity Manager server initiates a reconciliation process, the adapter replaces the local database that represents this service with the new database.

To add search attributes, do the following steps:

Procedure

1. Access the Agent Main Configuration menu.
2. At the Modify Context menu for the context, type A to display the Reconciliation Attribute Passed to Agent menu.
Reconciliation Attributes Passed to Agent for Context: Context1
----------------------------------------------------
A. Add new attribute
B. Modify attribute value
C. Remove attribute
X. Done
Select menu option:

The valid values for the Active Directory adapter are:
- erADBasePoint
- erADGroupBasePoint
- erADDomainUser
- erADDomainPassword
- erADPreferredExchangeServers
- erADPreferredExchangeServersOnly
- erADPreferredLyncServers
- erADPreferredLyncServersOnly

If you modify these attributes, the new value must be the same as what is entered on the adapter service form. If the field is blank on the service form, you do not have to specify an attribute value.

Related tasks:
“Starting the adapter configuration tool” on page 19
Use the adapter configuration program, agentCfg, to view or modify the adapter parameters.

Configuring the target DN for event notification contexts
During event notification configuration, the adapter sends requests to a service that runs on the IBM Security Identity Manager server.

About this task
You must configure target DN for event notification contexts for the adapter to know which service the adapter must send the request to. Configuring the target DN for event notification contexts involves specifying parameters, such as the adapter service name, organization (o), and organization name (ou).

Procedure
1. Access the Agent Main Configuration menu.
2. Type the option for Event Notification to display the Event Notification menu.
3. Type the option for Modify Event Notification Context, then enter the option of the context that you want to modify.
4. At the Modify Context menu for the context, type B to display the following prompt:
   Enter Target DN:
5. Type the target DN for the context and press Enter. The target DN for the event notification context must be in the following format:
   erservicename=erservicename,o=organizationname,ou=tenantname,rootsuffix
Table 11 on page 33 describes each DN element.
Table 11. DN elements and definitions

<table>
<thead>
<tr>
<th>Element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>erservicename</td>
<td>Specifies the name of the target service.</td>
</tr>
<tr>
<td>o</td>
<td>Specifies the name of the organization.</td>
</tr>
<tr>
<td>ou</td>
<td>Specifies the name of the tenant under which the organization is. If this installation is an enterprise, then ou is the name of the organization.</td>
</tr>
<tr>
<td>rootsuffix</td>
<td>Specifies the root of the directory tree. This value is the same as the value of Identity Manager DN Location that is specified during the IBM Security Identity Manager server installation.</td>
</tr>
</tbody>
</table>

Results

The Modify Context Menu displays the new target DN.

Related tasks:

“Starting the adapter configuration tool” on page 19

Use the adapter configuration program, `agentCfg`, to view or modify the adapter parameters.

Removing the baseline database for event notification contexts

You can remove the baseline database for event notification contexts only after you create a context. You must also do a reconciliation operation on the context to create a Baseline Database file.

Procedure

1. From the Agent Main Configuration menu, type the Event Notification option.
2. From Event Notification, type the Remove Event Notification Context option to display the Modify Context menu.
3. Select the context that you want to remove.
4. Confirm that you want to remove a context and press Enter to remove the baseline database for event notification contexts.

Changing the configuration key

Use the configuration key as a password to access the configuration tool for the adapter.

Procedure

1. Access the Agent Main Configuration Menu.
2. At the Main Menu prompt, type 0.
3. Do one of the following actions:
   - Change the value of the configuration key and press Enter. The default configuration key is agent. Ensure that your password is complex.
   - Press Enter to return to the Main Configuration Menu without changing the configuration key.
Results

The following message is displayed:
Configuration key is successfully changed.

The configuration program returns to the **Main Menu** prompt.

**Related tasks:**

“Starting the adapter configuration tool” on page 19

Use the adapter configuration program, agentCfg, to view or modify the adapter parameters.

---

**Changing activity logging settings**

When you enable logging, the adapter maintains a log file of all transactions, `adapter_nameAgent.log`.

**About this task**

By default, the log file is in the `\log` directory.

To change the adapter **activity logging** settings, take the following steps:

**Procedure**

1. Access the Agent Main Configuration menu.
2. At the **Main Menu** prompt, type **E** to display the Agent Activity Logging menu. The following screen displays the default **activity logging** settings.

   ![Agent Activity Logging Menu]

   Select menu option:

3. Perform one of the following steps:
   - Type the value for menu option B, C, D, or E and press **Enter**. The other options are changed automatically when you type the corresponding letter of the menu option. The following table describes each option.
   - Press **Enter** to return to the Agent Activity Logging menu without changing the value.

   **Note:** Ensure that Option **A** is enabled for the values of other options to take effect.
### Table 12. Options for the activity logging menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
</table>
| A      | Set this option to enabled to have the adapter maintain a dated log file of all transactions.  
When the option is set to:  
• Disabled, pressing the A to key changes to enabled.  
• Enabled, pressing the A to key changes to disabled.  
Type A to toggle between the options. |
| B      | Displays the following prompt:  
Enter log file directory:  
Type a different value for the logging directory, for example, C:\Log.  
When the logging option is enabled, details about each access request are stored in the logging file that is in this directory. |
| C      | Displays the following prompt:  
Enter log file name:  
Type a different value for the log file name. When the logging option is enabled, details about each access request are stored in the logging file. |
| D      | Displays the following prompt:  
Enter maximum size of log files (mbytes):  
Type a new value such as 10. The oldest data is archived when the log file reaches the maximum file size. File size is measured in megabytes. It is possible for the activity log file size to exceed disk capacity. |
| E      | Displays the following prompt:  
Enter maximum number of log files to retain:  
Type a new value up to 99 such as 5. The adapter automatically deletes the oldest activity logs beyond the specified limit. |
| F      | If this option is set to enabled, the adapter includes the debug statements in the log file of all transactions.  
When the option is set to:  
• Disabled, pressing the F key changes the value to enabled.  
• Enabled, pressing the F key changes the value to disabled.  
Type F to toggle between the options. |
| G      | If this option is set to enabled, the adapter maintains a detailed log file of all transactions. The **detail logging** option must be used for diagnostic purposes only. Detailed logging enables more messages from the adapter and might increase the size of the logs.  
When the option is set to:  
• Disabled, pressing the G key changes the value to enabled.  
• Enabled, pressing the G key changes the value to disabled.  
Type G to toggle between the options. |
Table 12. Options for the activity logging menu (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
</table>
| **H**  | If this option is set to enabled, the adapter maintains a log file of all transactions in the Adapter Development Kit (ADK) and library files. Base logging substantially increases the size of the logs. When the option is set to:  
  • Disabled, pressing the **H** key changes the value to enabled.  
  • Enabled, pressing the **H** key changes the value to disabled.  
  Type **H** to toggle between the options. |
| **I**  | If this option is enabled, the log file contains thread IDs, in addition to a date and timestamp on every line of the file. When the option is set to:  
  • Disabled, pressing the **I** key changes the value to enabled.  
  • Enabled, pressing the **I** key changes the value to disabled.  
  Type **I** to toggle between the options. |

Related tasks:

“Starting the adapter configuration tool” on page 19

Use the adapter configuration program, agentCfg, to view or modify the adapter parameters.

### Modifying registry settings

Use the Agent Registry Menu to change the adapter registry settings.

**Procedure**

1. Type **F** (Registry Settings) at the main menu prompt to display the Registry menu:

```
adapter_name and version Agent Registry Menu
-------------------------------------------
A. Modify Non-encrypted registry settings.
B. Modify encrypted registry settings.
C. Multi-instance settings.
X. Done
Select menu option:
```

2. See the following procedures for modifying registry settings.

### Modifying non-encrypted registry settings

To modify the non-encrypted registry settings, complete the following steps:

**Procedure**

1. At the Agent Registry Menu, type **A** to display the Non-encrypted Registry Settings Menu.
Agent Registry Items

- 01. CreateUNCHomeDirectories 'FALSE'
- 02. DeleteUNCHomeDirectories 'FALSE'
- 03. delRoamingProfileOnDeprov 'FALSE'
- 04. delUNCHomeDirOnDeprov 'FALSE'
- 05. ForceRASServerLookup 'FALSE'
- 06. ForceTerminalServerLookup 'FALSE'
- 07. ManageHomeDirectories 'FALSE'
- 08. NotifyIntervalSeconds '300'
- 09. ReconHomeDirSecurity 'FALSE'
- 10. ReconPrimaryGroup 'TRUE'

---

Page 1 of 3

A. Add new attribute
B. Modify attribute value
C. Remove attribute
D. Next Page
X. Done

Select menu option:

Agent Registry Items

- 11. SearchPasswordSettings 'FALSE'
- 12. UnlockOnPasswordReset 'FALSE'
- 13. useDefaultDC 'FALSE'
- 14. useSSL 'FALSE'
- 15. WtsDisableSearch 'TRUE'
- 16. WtsEnabled 'FALSE'

---

Page 2 of 3

A. Add new attribute
B. Modify attribute value
C. Remove attribute
E. Prev Page
X. Done

Select menu option:

2. Type the letter of the menu option for the action that you want to perform on an attribute.

Table 13. Attribute configuration option descriptions

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Add new attribute</td>
</tr>
<tr>
<td>B</td>
<td>Modify attribute value</td>
</tr>
<tr>
<td>C</td>
<td>Remove attribute</td>
</tr>
</tbody>
</table>

3. Type the registry item name, and press Enter.
4. If you selected option A or B, type the registry item value and press Enter.
   The non-encrypted registry settings menu reappears and displays your new settings.
**Results**

The following table describes the registry keys and their available settings:

Table 14. Registry key descriptions

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateUNCHomeDirectories</td>
<td>If this key is set to <strong>TRUE</strong>, the key enables creation of the UNC home directory. The default value is <strong>FALSE</strong>.</td>
</tr>
<tr>
<td>DeleteUNCHomeDirectories</td>
<td>If this key is set to <strong>TRUE</strong>, the key enables deletion of the UNC home directory on delete. The default value is <strong>FALSE</strong>.</td>
</tr>
<tr>
<td>delRoamingProfileOnDeprovision</td>
<td>If this key is set to <strong>TRUE</strong>, the key enables user profile directory deletion when the user is de-provisioned. After successfully deleting the user from the Active Directory, the adapter deletes the user home directory, subdirectories, and files. If this key is set to <strong>FALSE</strong>, or if the key does not exist, the adapter does not delete the user home directory. The default value is <strong>FALSE</strong>.</td>
</tr>
<tr>
<td>delUNCHomeDirOnDeprovision</td>
<td>If this key is set to <strong>TRUE</strong>, the key enables UNC Home directory deletion when the user is de-provisioned. After successfully deleting the user from the Active Directory, the adapter deletes the user home directory, subdirectories, and files. If this key is set to <strong>FALSE</strong>, or if the key does not exist, the adapter does not delete the user home directory. The default value is <strong>FALSE</strong>.</td>
</tr>
<tr>
<td>ForceRASServerLookup</td>
<td>If this key is set to <strong>TRUE</strong>, the RASServer is always found from the domain information. If this key is set to <strong>FALSE</strong>, one of these conditions exist: • If the target server is specified in the base point, the target server is used as the RAS server. • If the target server is not specified in the base point, the RAS server is found from the domain information. The default value is <strong>FALSE</strong>.</td>
</tr>
<tr>
<td>ForceTerminalServerLookup</td>
<td>If this key is set to <strong>TRUE</strong>, the terminal server is always found from the domain information. If this key is set to <strong>FALSE</strong>, one of these conditions exist: • If the target server is specified in the base point, the target server is used as the terminal server. • If the target server is not specified in the base point, the terminal server is found from the domain information. The default value is <strong>FALSE</strong>.</td>
</tr>
<tr>
<td>ManageHomeDirectories</td>
<td>If this key is set to <strong>TRUE</strong>, the adapter performs Add and Delete operations for actual directories. If this key is set to <strong>FALSE</strong>, the adapter updates only the home directory information in the Active Directory. The default value is <strong>FALSE</strong>.</td>
</tr>
<tr>
<td>NotifyIntervalSeconds</td>
<td>This key specifies the interval (in seconds) after which the adapter enabled event notification process starts. It can be modified by using the agentCfg tool. The default value is 300 seconds.</td>
</tr>
<tr>
<td>ReconHomeDirSecurity</td>
<td>If this key is set to <strong>TRUE</strong>, the adapter brings the Home Security information (NTFS security, share name, and share security) during a reconciliation. The default value is <strong>FALSE</strong>. The reconciliation operation is fast when this key is set to <strong>FALSE</strong>.</td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ReconPrimaryGroup</td>
<td>The recon operation does not add the primary group to the group list. The <code>memberof</code> attribute in Active Directory stores the user’s group membership, except the primary group. The <code>primaryGroupID</code> attribute in Active Directory stores the primary group of the user. As a result the primary group must be explicitly added to group list. If this key is set to TRUE, the primary group is added to the group list. If this key is set to FALSE, the primary group is not added to the group list. The default value is FALSE.</td>
</tr>
<tr>
<td>SearchPasswordSettings</td>
<td>Most of the password attributes are stored in the Active Directory and are directly retrieved. But some (for example, Require Unique Password and User Cannot Change Password) are not stored in the Active Directory. These attributes must be retrieved by using APIs. If this key is set to TRUE, the password attributes are retrieved by using the respective API. If this key is set to FALSE, the attributes are not retrieved. The default value is FALSE. When this key is set to FALSE, the password flag attributes are not retrieved and the reconciliation operation is fast.</td>
</tr>
<tr>
<td>UnlockOnPasswordReset</td>
<td>If this key is set to TRUE, the adapter activates the user on a password change request. The default value is FALSE.</td>
</tr>
<tr>
<td>useDefaultDC</td>
<td>This key provides failover capability for the adapter when the host specified in the base point is not available. If the adapter cannot connect to the host specified in the base point and the key is set to TRUE, the adapter connects to the base point without the host name. If this key is set to TRUE, the key affects RASServer and Terminal server lookup behavior. The default value is FALSE.</td>
</tr>
<tr>
<td>useSSL</td>
<td>This key enables SSL communication between the adapter and the Active Directory. If this key is set to TRUE, the adapter uses SSL to communicate with the Active Directory. If this key is set to FALSE or does not exist, the adapter does not use SSL. The default value is FALSE.</td>
</tr>
<tr>
<td>WtsDisableSearch</td>
<td>This key takes effect only if WtsEnabled is set to TRUE. If set to FALSE, this key enables a reconciliation of the WTS attributes. If set to TRUE, the reconciliation is faster. The default value is FALSE.</td>
</tr>
<tr>
<td>WtsEnabled</td>
<td>If this key is set to TRUE, the key enables processing of Windows Terminal Server (WTS) attributes. The default value is FALSE.</td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>UseGroup</td>
<td>You can set this key to one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• CN:</td>
</tr>
<tr>
<td></td>
<td>When you set this key to CN, the adapter performance for add, modify, and reconciliation is lesser compared to the DN option. This lessening of performance is because adapter must perform extra binds to the Active Directory.</td>
</tr>
<tr>
<td></td>
<td>• DN:</td>
</tr>
<tr>
<td></td>
<td>When you set this key to DN, the adapter performance for add, modify, and reconciliation is higher compared to the CN and GUID options.</td>
</tr>
<tr>
<td></td>
<td>• GUID:</td>
</tr>
<tr>
<td></td>
<td>When you set this key to GUID, the adapter performance for add, modify, and reconciliation lesser compared to DN, however, higher compared to CN.</td>
</tr>
<tr>
<td></td>
<td>Depending on the key the adapter retrieves the value for group during the reconciliation operation and processes during the add and modify operation of the adapter. When you change the value of this key, you must modify the profile and import it again on IBM Security Identity Manager.</td>
</tr>
<tr>
<td></td>
<td>The default value is DN.</td>
</tr>
<tr>
<td>ReconMailboxPermissions</td>
<td>When this key is set to FALSE, the adapter does not retrieve the Mailbox Permission information. The reconciliation operation is fast when this key is set to FALSE. The default value is TRUE.</td>
</tr>
<tr>
<td>UPNSearchEnabled</td>
<td>When the registry key UPNSearchEnabled is set to FALSE, the adapter does not perform a search on the User Principal Name for uniqueness. It creates the user account with the supplied or generated value of the User Principal Name.</td>
</tr>
<tr>
<td></td>
<td>When the registry key UPNSearchEnabled is set to TRUE, the adapter performs a search on the User Principal Name to ensure the uniqueness. The default value is TRUE.</td>
</tr>
<tr>
<td></td>
<td>Note: This key is used only for the user add operation.</td>
</tr>
<tr>
<td>UseITIMCNAttribute</td>
<td>When this key is set to TRUE, the adapter uses IBM Security Identity Manager common schema attribute cn. The adapter processes the cn attribute for add, modify, and reconciliation operations. When this key is set to FALSE, the adapter uses the erADFullName attribute for add, modify, and reconciliation operations. When you set this registry key to FALSE, you must customize the account form.</td>
</tr>
<tr>
<td></td>
<td>For more information, see “Configuring the cn attribute” on page 74.</td>
</tr>
<tr>
<td></td>
<td>The default value is TRUE.</td>
</tr>
<tr>
<td>MailUserRenameDelay</td>
<td>When you rename a user account with mail status, the Active Directory might take time to reestablish the user account mail status. This behavior causes the adapter to fail the exchange attributes in the rename request with the error message Error setting attribute name. User does not have a mailbox. In this case, renaming means modifying the Eruid and the User Principal Name attribute.</td>
</tr>
<tr>
<td></td>
<td>When you use this key, the adapter waits before it modifies the exchange attribute when a user account is renamed. For example, set this key is set to 10 seconds. Submit a user account rename request. The adapter waits for 10 seconds before modifying the exchange attributes that are in the request.</td>
</tr>
<tr>
<td></td>
<td>The default value of the registry key is 0 seconds.</td>
</tr>
<tr>
<td></td>
<td>Note: The adapter uses this key only when the Eruid, User Principal Name, and the exchange attributes are modified.</td>
</tr>
<tr>
<td>Key</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SearchTimeout</td>
<td>In some of the Active Directory setups, the adapter might not complete the reconciliation operation. This failure occurs when the Microsoft ADSI API GetNextRow halts indefinitely. The adapter monitors the reconciliation operation. Set this registry key to a non-zero value. The adapter process ends if there is no activity by the adapter in the reconciliation operation for the time in seconds specified in this key. When you set the value of this registry key to 0 and if the adapter halts during the reconciliation operation, the reconciliation operation does not complete and the operation is timed out on IBM Security Identity Manager. In this case, restart the adapter service. The default value of the registry key is 0 seconds.</td>
</tr>
</tbody>
</table>

**Note:** The following registry keys are no longer used:

- AbortReconOnFailure
- OverrideX500Addresses

In addition to the listed adapter registry keys, you can add registry keys with a name as the value of **Users BasePoint DN** on the service form. You can also provide additional target servers for that service. Each target server must be separated by a |.

**Example 1**

When a **Users BasePoint DN** specified on service form isOU=TestOU,DC=MyDomain,DC=com, you can specify the list of target server(s) in the adapter registry by using agentCfg.exe as:

- Create the registry with name OU=TestOU,DC=MyDomain,DC=com.
- Specify the value for the key as DC01|DC02|DC03.

**Example 2**

When a Users BasePoint DN specified on service form isDC01|DC02|DC03/DC=MyDomain,DC=com, you can specify the list of additional target server(s) in the adapter registry by using agentCfg.exe as:

- Create the registry with name DC=MyDomain,DC=com.
- Specify the value for the key as DC04|DC05|DC06.

**Note:** When the base point or target server has Unicode characters, use the regedit to create registry keys under HKEY_LOCAL_MACHINE\SOFTWARE\Access360\ADAgent\Specific. For more information, see “Users Base Point configuration for the adapter” on page 66.

---

**Modifying encrypted registry settings**

You can access registry settings.

**Procedure**

1. Type 8 (Modifying Encrypted Registry Settings) at the Registry menu prompt to display the Encrypted Registry settings menu.
Encrypted Registry Items
-------------------------------------------
A. Add new attribute
B. Modify attribute value.
C. Remove attribute.
X. Done
Select menu option:

2. Type one of the following options:
   A) Add new attribute
   B) Modify attribute value
   C) Remove attribute
   X) Done

3. Type the registry item name, and press Enter.
4. Type the registry item value, if you selected option A or B, and press Enter.
   The encrypted registry settings menu reappears and displays your new settings.

Modifying advanced settings

You can change the adapter thread count settings.

About this task

You can change the thread count settings for the following types of requests:
   • System Login Add
   • System Login Change
   • System Login Delete
   • Reconciliation

These settings determine the maximum number of requests that the adapter processes concurrently. To change these settings, take the following steps:

Procedure

1. Access the Agent Main Configuration menu.
2. At the Main Menu prompt, type 6 to display the Advanced Settings menu.
   The following screen displays the default thread count settings.

---

**adapter_name and version number**
Advanced settings menu
-------------------------------------------
A. Single Thread Agent (current:FALSE)
B. ADD max. thread count. (current:3)
C. MODIFY max. thread count. (current:3)
D. DELETE max. thread count. (current:3)
E. SEARCH max. thread count. (current:3)
F. Allow User EXEC procedures (current:FALSE)
G. Archive Request Packets (current:FALSE)
H. UTF8 Conversion support (current:TRUE)
I. Pass search filter to agent (current:FALSE)
J. Thread Priority Level (1-10) (current:4)
X. Done
Select menu option:
Table 15. Options for advanced settings menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Forces the adapter to allow only 1 request at a time. The default value is FALSE.</td>
</tr>
<tr>
<td>B</td>
<td>Limits the number of ADD requests that can run simultaneously. The default value is 3.</td>
</tr>
<tr>
<td>C</td>
<td>Limits the number of MODIFY requests that can run simultaneously. The default value is 3.</td>
</tr>
<tr>
<td>D</td>
<td>Limits the number of DELETE requests that can run simultaneously. The default value is 3.</td>
</tr>
<tr>
<td>E</td>
<td>Limits the number of SEARCH requests that can run simultaneously. The default value is 3.</td>
</tr>
<tr>
<td>F</td>
<td>Determines whether the adapter can do the pre-exec and post-exec functions. The default value is FALSE. Note: Enabling this option is a potential security risk.</td>
</tr>
<tr>
<td>G</td>
<td>This option is no longer supported.</td>
</tr>
<tr>
<td>H</td>
<td>This option is no longer supported.</td>
</tr>
<tr>
<td>I</td>
<td>Active Directory Adapter supports processing filters directly. If you enable this option by setting it to TRUE, the adapter filters the results instead of the ADK. By default, this option is set to FALSE and the ADK does the filtering.</td>
</tr>
<tr>
<td>J</td>
<td>Sets the thread priority level for the adapter. The default value is 4.</td>
</tr>
</tbody>
</table>

3. Type the letter of the menu option that you want to change.
4. Change the value and press Enter to display the Advanced Settings menu with new settings.

Related tasks:
- “Starting the adapter configuration tool” on page 19

Use the adapter configuration program, agentCfg, to view or modify the adapter parameters.

Viewing statistics

You can view an event log for the adapter.

Procedure
1. Access the Agent Main Configuration Menu.
2. At the Main Menu prompt, type H to display the activity history for the adapter.
3. Type 3 to return to the Main Configuration Menu.

Related tasks:

"Starting the adapter configuration tool" on page 19

Use the adapter configuration program, agentCfg, to view or modify the adapter parameters.

Modifying code page settings

You can change the code page settings for the adapter.

About this task

To list the supported code page information for the adapter, the adapter must be running. Run the following command to view the code page information:

```
agentCfg -agent [adapter_name] -codepages
```

Procedure

1. Access the Agent Main Configuration menu.
2. At the Main Menu prompt, type 1 to display the Code Page Support menu.

```
adapter_name and version number Codepage Support Menu
---------------------------------------------
* Configured codepage: US-ASCII
---------------------------------------------
*
*************************************************
* Restart Agent After Configuring Codepages
*************************************************
A. Codepage Configure.
X. Done
Select menu option:
```

3. Type A to configure a code page.

Note: The code page uses Unicode, therefore this option is not applicable.

4. Type X to return to the Main Configuration menu.

Related tasks:

"Starting the adapter configuration tool" on page 19

Use the adapter configuration program, agentCfg, to view or modify the adapter parameters.

Accessing help and other options

Use the agentCfg help menu to display the help arguments that you can use to find information about the adapter.
Procedure

1. At the Main Menu prompt, type X to display the DOS command prompt.
2. Type agentCfg -help at the prompt to display the help menu and list of commands.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-version</td>
<td>Use this argument to display the version of the agentCfg tool.</td>
</tr>
<tr>
<td>-hostname &lt; value&gt;</td>
<td>Target nodename to connect to (Default: Local host IP address)</td>
</tr>
<tr>
<td>-findall</td>
<td>Find all agents on target node</td>
</tr>
<tr>
<td>-list</td>
<td>List available agents on target node</td>
</tr>
<tr>
<td>-agent &lt; value&gt;</td>
<td>Name of agent</td>
</tr>
<tr>
<td>-tail</td>
<td>Display agent's activity log</td>
</tr>
<tr>
<td>-portnumber &lt; value&gt;</td>
<td>Specified agent's TCP/IP port number</td>
</tr>
<tr>
<td>-netsearch &lt; value&gt;</td>
<td>Lookup agents hosted on specified subnet</td>
</tr>
<tr>
<td>-codepages</td>
<td>Display list of available codepages</td>
</tr>
<tr>
<td>-help</td>
<td>Display this help screen</td>
</tr>
</tbody>
</table>

Table 16. Arguments and descriptions for the agentCfg help menu

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-version</td>
<td>Use this argument to display the version of the agentCfg tool.</td>
</tr>
<tr>
<td>-hostname &lt; value&gt;</td>
<td>Target nodename to connect to (Default: Local host IP address)</td>
</tr>
<tr>
<td>-findall</td>
<td>Find all agents on target node</td>
</tr>
<tr>
<td>-list</td>
<td>List available agents on target node</td>
</tr>
<tr>
<td>-agent &lt; value&gt;</td>
<td>Name of agent</td>
</tr>
<tr>
<td>-tail</td>
<td>Display agent's activity log</td>
</tr>
<tr>
<td>-portnumber &lt; value&gt;</td>
<td>Specified agent's TCP/IP port number</td>
</tr>
<tr>
<td>-netsearch &lt; value&gt;</td>
<td>Lookup agents hosted on specified subnet</td>
</tr>
<tr>
<td>-codepages</td>
<td>Display list of available codepages</td>
</tr>
<tr>
<td>-help</td>
<td>Display this help screen</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
</table>

Chapter 6. Configuring the adapter for IBM Security Identity Manager 45
Table 16. Arguments and descriptions for the agentCfg help menu (continued)

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-netsearch</td>
<td>Use this argument with the -findall argument to display all active adapters on the managed resource. You must specify a subnet address as the value.</td>
</tr>
<tr>
<td>-codepages</td>
<td>Use this argument to display a list of available code pages.</td>
</tr>
<tr>
<td>-help</td>
<td>Use this argument to display the Help information for the agentCfg command.</td>
</tr>
</tbody>
</table>

3. Type agentCfg before each argument you want to run, as shown in the following examples.

*agentCfg -list*

Displays:

- A list of all the adapters on the local host
- The host IP address, the IP address of the local host
- The node on which the adapter is installed.

The default node for the server must be 44970. The output is like the following example:

```
Agents installed on node '127.0.0.1'
------------------------
agentnameAgent (44970)
```

*agentCfg -agent agentnameAgent*

Displays the Main menu of the agentCfg tool, which you can use to view or modify the adapter parameters.

*agentCfg -list -hostname 192.9.200.7*

Displays a list of the adapters on a host with the IP address 192.9.200.7. Ensure that the default node for the adapter is 44970. The output is like the following example:

```
Agents installed on node '192.9.200.7'
------------------------
agentnameAgent (44970)
```

*agentCfg -agent agentnameAgent -hostname 192.9.200.7*

Displays the agentCfg tool Main menu for a host with the IP address 192.9.200.7. Use the menu options to view or modify the adapter parameters.
Chapter 7. SSL authentication configuration

You can provide SSL authentication, certificates, and enable SSL authentication with the certTool utility.

For secure connection between the adapter and the server, configure the adapter and the server to use the Secure Sockets Layer (SSL) authentication with the DAML default communication protocol. Typically, SSL is used to establish a secure connection that encrypts the data that is being exchanged. While it can assist in authentication, you must enable registered certificates in DAML to use SSL for authentication. By configuring the adapter for SSL, the server can verify the identity of the adapter before the server makes a secure connection.

You can configure SSL authentication for connections that originate from the IBM Security Identity Manager server or from the adapter. The IBM Security Identity Manager server initiates a connection to the adapter to set or retrieve the value of a managed attribute on the adapter. Depending on the security requirements of your environment, you might configure SSL authentication for connections that originate from the adapter. For example, adapter events can notify the IBM Security Identity Manager server of changes to attributes on the adapter. In this case, configure SSL authentication for web connections that originate from the adapter to the web server used by the IBM Security Identity Manager server.

In a production environment, you must enable SSL security. If an external application communicates with the adapter (for example, the IBM Security Identity Manager server) and uses server authentication, enable SSL on the adapter. Enabling SSL verifies the certificate that the application presents.

Running the adapter in SSL mode

You can run the adapter in Secure Socket Layer (SSL) mode.

About this task

Note: If you do not do these steps, the certificate is not installed completely and the SSL is not enabled. See [http://en.wikipedia.org/wiki/User_Account_Control](http://en.wikipedia.org/wiki/User_Account_Control).

Procedure

1. Disable the User Account Control (UAC) security.
2. Install the required certificate.
3. (Optional) If required, enable the UAC security.

Related concepts:

“SSL certificate management with certTool” on page 53

Use the certTool utility to manage private keys and certificates.

Overview of SSL and digital certificates

In an enterprise network deployment, you must provide secure communication between the IBM Security Identity Manager server and the software products and components with which the server communicates.
SSL protocol uses signed digital certificates from a certificate authority (CA) for authentication. SSL secures communication in a configuration. SSL provides encryption of the data that is exchanged between the applications. Encryption makes data that is transmitted over the network intelligible only to the intended recipient.

Signed digital certificates enable two applications that connect in a network to authenticate their identity. An application that acts as an SSL server presents its credentials to verify to an SSL client. The SSL client then verifies that the application is the entity it claims to be. You can configure an application that acts as an SSL server so that it requires the application that acts as an SSL client to present its credentials in a certificate. In this way, the two-way exchange of certificates is completed. A third-party certificate authority issues signed certificates for a fee. Some utilities, such as those provided by OpenSSL, can also provide signed certificates.

You must install a certificate authority certificate (CA certificate) to verify the origin of a signed digital certificate. When an application receives a signed certificate from another application, it uses a CA certificate to verify the certificate originator. A certificate authority can be:

- Well-known and widely used by other organizations.
- Local to a specific region or a company.

Many applications, such as web browsers, use the CA certificates of well-known certificate authorities. Using a well-known CA eliminates or reduces the task of distributing CA certificates throughout the security zones in a network.

**Private keys, public keys, and digital certificates**

Keys, digital certificates, and trusted certificate authorities establish and verify the identities of applications.

SSL uses public key encryption technology for authentication. In public key encryption, a public key and a private key are generated for an application. The data encrypted with the public key can be decrypted only with corresponding private key. Similarly, the data encrypted with the private key can be decrypted only by using the corresponding public key. The private key is password-protected in a key database file. Only the owner can access the private key to decrypt messages that are encrypted with the corresponding public key.

A signed digital certificate is an industry-standard method of verifying the authenticity of an entity, such as a server, a client, or an application. To ensure maximum security, a third-party certificate authority provides a certificate. A certificate contains the following information to verify the identity of an entity:

**Organizational information**

This certificate section contains information that uniquely identifies the owner of the certificate, such as organizational name and address. You supply this information when you generate a certificate with a certificate management utility.

**Public key**

The receiver of the certificate uses the public key to decipher encrypted text that is sent by the certificate owner to verify its identity. A public key has a corresponding private key that encrypts the text.
Certificate authority's distinguished name
The issuer of the certificate identifies itself with this information.

Digital signature
The issuer of the certificate signs it with a digital signature to verify its authenticity. The corresponding CA certificate compares the signature to verify that the certificate is originated from a trusted certificate authority.

Web browsers, servers, and other SSL-enabled applications accept as genuine any digital certificate that is signed by a trusted certificate authority and is otherwise valid. For example, a digital certificate can be invalidated for the following reasons:

• The digital certificate expired.
• The CA certificate that is used to verify that it is expired.
• The distinguished name in the digital certificate of the server does not match with the distinguished name specified by the client.

Self-signed certificates
You can use self-signed certificates to test an SSL configuration before you create and install a signed certificate that is provided by a certificate authority.

A self-signed certificate contains a public key, information about the certificate owner, and the owner signature. It has an associated private key; however, it does not verify the origin of the certificate through a third-party certificate authority. After you generate a self-signed certificate on an SSL server application, you must:

1. Extract it.
2. Add it to the certificate registry of the SSL client application.

This procedure is equivalent to installing a CA certificate that corresponds to a server certificate. However, you do not include the private key in the file when you extract a self-signed certificate to use as the equivalent of a CA certificate.

Use a key management utility to:

• Generate a self-signed certificate.
• Generate a private key.
• Extract a self-signed certificate.
• Add a self-signed certificate.

Usage of self-signed certificates depends on your security requirements. To obtain the highest level of authentication between critical software components, do not use self-signed certificates or use them selectively. You can authenticate applications that protect server data with signed digital certificates. You can use self-signed certificates to authenticate web browsers or adapters.

If you are using self-signed certificates, you can substitute a self-signed certificate for a certificate and CA certificate pair.

Certificate and key formats
Certificates and keys are stored in the files in several formats.

.pem format
A privacy-enhanced mail (.pem) format file begins and ends with the following lines:

-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
A .pem file format supports multiple digital certificates, including a certificate chain. If your organization uses certificate chaining, use this format to create CA certificates.

.arm format
An .arm file contains a base-64 encoded ASCII representation of a certificate, including its public key, not a private key. The .arm file format is generated and used by the IBM Key Management utility.

.der format
A .der file contains binary data. You can use a .der file for a single certificate, unlike a .pem file, which can contain multiple certificates.

.pfx format (PKCS12)
A PKCS12 file is a portable file that contains a certificate and a corresponding private key. Use this format to convert from one type of SSL implementation to another. For example, you can create and export a PKCS12 file with the IBM Key Management utility. You can then import the file to another workstation with the certTool utility.

The use of SSL authentication
When you start the adapter, it loads the available connection protocols.

The DAML protocol is the only available protocol that supports SSL authentication. You can specify DAML SSL implementation.

The DAML SSL implementation uses a certificate registry to store private keys and certificates. The certTool key and certificate management tool manages the location of the certificate registry. You do not have to specify the location of the registry when you do certificate management tasks.

Configuring certificates for SSL authentication
You can configure the adapter for one-way or two-way SSL authentication with signed certificates.

About this task
Use the certTool utility for these tasks:
- "Configuring certificates for one-way SSL authentication"
- "Configuring certificates for two-way SSL authentication" on page 51
- "Configuring certificates when the adapter operates as an SSL client" on page 53

Configuring certificates for one-way SSL authentication
In this configuration, the IBM Security Identity Manager server and the IBM Security Identity Manager adapter use SSL.

About this task
Client authentication is not set on either application. The IBM Security Identity Manager server operates as the SSL client and initiates the connection. The adapter operates as the SSL server and responds by sending its signed certificate to the IBM Security Identity Manager server. The IBM Security Identity Manager server uses the installed CA certificate to validate the certificate that is sent by the adapter.
In Figure 1, Application A operates as the IBM Security Identity Manager server, and Application B operates as the IBM Security Identity Manager adapter.

Procedure

1. On the adapter, complete these steps:
   a. Start the certTool utility.
   b. To configure the SSL-server application with a signed certificate issued by a certificate authority:
      1) Create a certificate signing request (CSR) and private key. This step creates the certificate with an embedded public key and a separate private key and places the private key in the PENDING_KEY registry value.
      2) Submit the CSR to the certificate authority by using the instructions that are supplied by the CA. When you submit the CSR, specify that you want the root CA certificate to be returned with the server certificate.

2. On the IBM Security Identity Manager server, do one of these steps:
   • If you used a signed certificate that is issued by a well-known CA:
     a. Ensure that the IBM Security Identity Manager server stored the root certificate of the CA (CA certificate) in its truststore.
     b. If the truststore does not contain the CA certificate, extract the CA certificate from the adapter and add it to the truststore of the server.
   • If you generated the self-signed certificate on the IBM Security Identity Manager server, the certificate is installed and requires no additional steps.
   • If you generated the self-signed certificate with the key management utility of another application:
     a. Extract the certificate from the keystore of that application.
     b. Add it to the truststore of the IBM Security Identity Manager server.

Related tasks:
“Starting certTool” on page 54

To start the certificate configuration tool named certTool for the adapter, complete these steps:

Configuring certificates for two-way SSL authentication

In this configuration, the IBM Security Identity Manager server and adapter use SSL.
About this task

The adapter uses client authentication. After the adapter sends its certificate to the server, the adapter requests identity verification from the IBM Security Identity Manager server. The server sends its signed certificate to the adapter. Both applications are configured with signed certificates and corresponding CA certificates.

In the following figure, the IBM Security Identity Manager server operates as Application A and the adapter operates as Application B.

Before you do the following procedure, configure the adapter and IBM Security Identity Manager server for one-way SSL authentication. If you use signed certificates from a CA:

- The CA provides a configured adapter with a private key and a signed certificate.
- The signed certificate of the adapter provides the CA certification for the IBM Security Identity Manager server.

To complete the certificate configuration for two-way SSL, do the following tasks:

Procedure

1. On the IBM Security Identity Manager server, create a CSR and private key. Next, obtain a certificate from a CA, install the CA certificate, install the newly signed certificate, and extract the CA certificate to a temporary file.
2. On the adapter, add the CA certificate that was extracted from the keystore of the IBM Security Identity Manager server to the adapter.

Results

After you configure the two-way certificate, each application has its own certificate and private key. Each application also has the certificate of the CA that issued the certificates.

Related tasks:

- "Configuring certificates for one-way SSL authentication" on page 50

In this configuration, the IBM Security Identity Manager server and the IBM Security Identity Manager adapter use SSL.
Configuring certificates when the adapter operates as an SSL client

In this configuration, the adapter operates as both an SSL client and as an SSL server.

About this task

This configuration applies if the adapter initiates a connection to the web server (used by the IBM Security Identity Manager server) to send an event notification. For example, the adapter initiates the connection and the web server responds by presenting its certificate to the adapter.

Figure 3 describes how the adapter operates as an SSL server and an SSL client. When communicating with the IBM Security Identity Manager server, the adapter sends its certificate for authentication. When communicating with the web server, the adapter receives the certificate of the web server.

Figure 3. Adapter operating as an SSL server and an SSL client

If the web server is configured for two-way SSL authentication, it verifies the identity of the adapter. The adapter sends its signed certificate to the web server (not shown in the illustration). To enable two-way SSL authentication between the adapter and web server, perform the following process:

Procedure

1. Configure the web server to use client authentication.
2. Follow the procedure for creating and installing a signed certificate on the web server.
3. Install the CA certificate on the adapter with the certTool utility.
4. Add the CA certificate corresponding to the signed certificate of the adapter to the web server.

What to do next

If you want the software to send an event notification when the adapter initiates a connection to the web server (used by the IBM Security Identity Manager server), see the IBM Security Identity Manager product documentation.

SSL certificate management with certTool

Use the certTool utility to manage private keys and certificates.
Starting certTool

To start the certificate configuration tool named certTool for the adapter, complete these steps:

Procedure

1. Click Start > Programs > Accessories > Command Prompt.
2. At a DOS command prompt, change to the bin directory for the adapter. If the directory is in the default location, type the following command:
   \n   cd C:\Program Files\IBM\ISIM\Agents\adapter_nameAgent\bin\ 
3. Type CertTool -agent agent_name at the prompt.

   For example, to display the main menu, type: CertTool -agent NotesAgent

<table>
<thead>
<tr>
<th>Main menu - Configuring agent: agentnameAgent</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Generate private key and certificate request</td>
</tr>
<tr>
<td>B. Install certificate from file</td>
</tr>
<tr>
<td>C. Install certificate and key from PKCS12 file</td>
</tr>
<tr>
<td>D. View current installed certificate</td>
</tr>
<tr>
<td>E. List CA certificates</td>
</tr>
<tr>
<td>F. Install a CA certificate</td>
</tr>
<tr>
<td>G. Delete a CA certificate</td>
</tr>
<tr>
<td>H. List registered certificates</td>
</tr>
<tr>
<td>I. Register certificate</td>
</tr>
<tr>
<td>J. Unregister a certificate</td>
</tr>
<tr>
<td>K. Export certificate and key to PKCS12 file</td>
</tr>
<tr>
<td>X. Quit</td>
</tr>
</tbody>
</table>

   Choice:

Results

From the Main menu, you can generate a private key and certificate request, install and delete certificates, register and unregister certificates, and list certificates. The following sections summarize the purpose of each group of options.

By using the first set of options (A through D), you can generate a CSR and install the returned signed certificate on the adapter.

A. Generate private key and certificate request

   Generate a CSR and the associated private key that is sent to the certificate authority.

B. Install certificate from file

   Install a certificate from a file. This file must be the signed certificate that is returned by the CA in response to the CSR that is generated by option A.

C. Install certificate and key from a PKCS12 file

   Install a certificate from a PKCS12 format file that includes both the public certificate and a private key. If options A and B are not used to obtain a certificate, the certificate that you use must be in PKCS12 format.

D. View current installed certificate

   View the certificate that is installed on the workstation where the adapter is installed.
With the second set of options, you can install root CA certificates on the adapter. A CA certificate validates the corresponding certificate that is presented by a client, such as the IBM Security Identity Manager server.

**E. List CA certificates**
Show the installed CA certificates. The adapter communicates only with IBM Security Identity Manager servers whose certificates are validated by one of the installed CA certificates.

**F. Install a CA certificate**
Install a new CA certificate so that certificates generated by this CA can be validated. The CA certificate file can either be in X.509 or PEM encoded formats.

**G. Delete a CA certificate**
Remove one of the installed CA certificates.

Options H through K apply to adapters that must authenticate the application to which the adapter is sending information. An example of an application is the IBM Security Identity Manager server or the web server. Use these options to register certificates on the adapter. For IBM Security Identity Manager version 4.5 or earlier, register the signed certificate of the IBM Security Identity Manager server with an adapter to enable client authentication on the adapter. If you do not upgrade an existing adapter to use CA certificates, you must register the signed certificate that is presented by the IBM Security Identity Manager server with the adapter.

If you configure the adapter for event notification or enable client authentication in DAML, you must install the CA certificate. The CA certificate must correspond to the signed certificate of the IBM Security Identity Manager server. Use option F, **Install a CA certificate**.

**H. List registered certificates**
List all registered certificates that are accepted for communication.

**I. Register a certificate**
Register a new certificate. The certificate for registration must be in Base 64 encoded X.509 format or PEM.

**J. Unregister a certificate**
Unregister (remove) a certificate from the registered list.

**K. Export certificate and key to PKCS12 file**
Export a previously installed certificate and private key. You are prompted for the file name and a password for encryption.

**Related concepts:**
“View of the installed certificate” on page 58
To list the certificate on your workstation, type `0` at the Main menu of certTool.

**Related tasks:**
“Generating a private key and certificate request” on page 56
A certificate signing request (CSR) is an unsigned certificate that is a text file.
“Installing the certificate” on page 57
After you receive your certificate from your trusted CA, install it in the registry of the adapter.
“Installing the certificate and key from a PKCS12 file” on page 57
If the certTool utility did not generate a CSR to obtain a certificate, you must install both the certificate and private key.
Installing a CA certificate” on page 58
If you use client authentication, you must install a CA certificate that is provided by a certificate authority vendor. You can install a CA certificate that was extracted in a temporary file.

“Deleting a CA certificate” on page 59
You can delete a CA certificate from the adapter directories.

“Viewing registered certificates” on page 59
The adapter accepts only the requests that present a registered certificate when client validation is enabled.

“Registering a certificate” on page 59
You can register a certificate for the adapter.

“Unregistering a certificate” on page 60
You can unregister a certificate for the adapter.

“Exporting a certificate and key to a PKCS12 file” on page 60
You can export a certificate and key to a PKCS12 file.

Generating a private key and certificate request
A certificate signing request (CSR) is an unsigned certificate that is a text file.

About this task
When you submit an unsigned certificate to a certificate authority, the CA signs the certificate with the private digital signature. The signature is included in their corresponding CA certificate. When the CSR is signed, it becomes a valid certificate. A CSR contains information about your organization, such as the organization name, country, and the public key for your web server.

Procedure
1. At the Main Menu of the certTool, type A. The following message and prompt are displayed:
   Enter values for certificate request (press enter to skip value)
   ---------------------------------------------------------------
2. At Organization, type your organization name and press Enter.
3. At Organizational Unit, type the organizational unit and press Enter.
4. At Agent Name, type the name of the adapter for which you are requesting a certificate and press Enter.
5. At email, type the email address of the contact person for this request and press Enter.
6. At State, type the state that the adapter is in and press Enter. For example, type TX if the adapter is in Texas. Some certificate authorities do not accept two letter abbreviations for states; type the full name of the state.
7. At Country, type the country that the adapter is in and press Enter.
8. At Locality, type the name of the city that the adapter is in and press Enter.
9. At Accept these values, take one of the following actions and press Enter:
   - Type Y to accept the displayed values.
   - Type N and specify different values.
   The private key and certificate request are generated after the values are accepted.
10. At Enter name of file to store PEM cert request, type the name of the file and press Enter. Specify the file that you want to use to store the values you specified in the previous steps.
11. Press Enter to continue. The certificate request and input values are written to the file that you specified. The file is copied to the adapter bin directory and the Main menu is displayed again.

Results

You can now request a certificate from a trusted CA by sending the .pem file that you generated to a certificate authority vendor.

Example of certificate signing request

Here is an example certificate signing request (CSR) file.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB1jCCAT8CAQAwZxUExEjAQBgNVBAoTCWFjY2Vzc2VzclM2MDEuMBIGA1UECz/clmZWhn
akS1ZXJpbnVzaW9uMjAwMCgwFgExCzAJBgNVBAYTAndroidCwYIKwYBBQUHAgEBMAkGA1UEBh
MAkHAgEBMAgTAwggAcAgEAMB0GA1UdDwEB/wQEAwIFMBEB/wYIKwYBBQUHAgEIfSkDASBB
-----END CERTIFICATE REQUEST-----
```

Installing the certificate

After you receive your certificate from your trusted CA, install it in the registry of the adapter.

Procedure

1. If you received the certificate as part of an email message, do the following actions.
   a. Copy the text of the certificate to a text file.
   b. Copy that file to the bin directory of the adapter.
      For Windows operating systems:
      C:\Program Files\IBM\ISIM\Agents\adapter_name\Agent\bin

2. At the Main Menu prompt of the certTool, type B. The following prompt is displayed:

```
Enter name of certificate file:
```

3. At Enter name of certificate file, type the full path to the certificate file and press Enter.
   The certificate is installed in the registry for the adapter, and Main Menu is displayed again.

Installing the certificate and key from a PKCS12 file

If the certTool utility did not generate a CSR to obtain a certificate, you must install both the certificate and private key.

About this task

Store the certificate and private key in a PKCS12 file. The CA sends a PKCS12 file that has a .pfx extension. The file might be a password-protected file and it includes both the certificate and private key.
Procedure

1. Copy the PKCS12 file to the bin directory of the adapter.
   For Windows operating systems:
   C:\Program Files\IBM\ISIM\Agents\adapter_nameAgent\bin
2. At the Main Menu prompt for the certTool, type C to display the following prompt:
   Enter name of PKCS12 file:
   Enter password
3. At Enter name of PKCS12 file, type the name of the PKCS12 file that has the certificate and private key information and press Enter. For example, DamlSrvr.pfx.
4. At Enter password, type the password to access the file and press Enter.

Results

After you install the certificate and private key in the adapter registry, the certTool displays Main Menu.

View of the installed certificate

To list the certificate on your workstation, type D at the Main menu of certTool.

The utility displays the installed certificate and the Main menu. The following example shows an installed certificate:
The following certificate is currently installed.
Subject: c=US,st=California,l=Irvine,o=DAML,cn=DAML Server

Installing a CA certificate

If you use client authentication, you must install a CA certificate that is provided by a certificate authority vendor. You can install a CA certificate that was extracted in a temporary file.

Procedure

1. At the Main Menu prompt, type F (Install a CA certificate).
   The following prompt is displayed:
   Enter name of certificate file:
2. At Enter name of certificate file, type the name of the certificate file, such as DamlCACerts.pem and press Enter.
   The certificate file opens and the following prompt is displayed:
   e=admin@ibm.com,c=US,ct=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng
   Install the CA? (Y/N)
3. At Install the CA, type Y to install the certificate and press Enter.
   The certificate file is installed in the CACerts.pem file.

Viewing CA certificates

Use the certTool utility to view a private key and certificate that are installed the adapter.

About this task

The certTool utility installs only one certificate and one private key.
**Procedure**

Type E at the **Main Menu** prompt.

**Results**

The certTool utility displays the installed CA certificates and the **Main** menu. The following example shows an installed CA certificate:

Subject: o=IBM,ou=SampleCACert,cn=TestCA

**Deleting a CA certificate**

You can delete a CA certificate from the adapter directories.

**Procedure**

1. At the **Main Menu** prompt, type G to display a list of all CA certificates that are installed on the adapter.

   0 - e=admin@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng
   1 - e=support@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Support,cn=Support

   Enter number of CA certificate to remove:

2. At **Enter number of CA certificate to remove**, type the number of the CA certificate that you want to remove and press **Enter**.

**Results**

After the CA certificate is deleted from the CACerts.pem file, the certTool displays the Main menu.

**Viewing registered certificates**

The adapter accepts only the requests that present a registered certificate when client validation is enabled.

**Procedure**

To view a list of all registered certificates, type H on the **Main Menu** prompt.

The utility displays the registered certificates and the **Main** menu. The following example shows a list of the registered certificates:

0 - e=admin@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng
1 - e=support@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Support,cn=Support

**Registering a certificate**

You can register a certificate for the adapter.

**Procedure**

1. At the **Main Menu** prompt, type I to display the following prompt:

   Enter name of certificate file:

2. At **Enter name of certificate file**, type the name of the certificate file that you want to register and press **Enter**.

   The subject of the certificate is displayed, and a prompt is displayed, for example:

   e=admin@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng

   Register this CA? (Y/N)

3. At **Register this CA**, type Y to register the certificate, and press **Enter**.
Results

After you register the certificate to the adapter, the certTool displays the Main menu.

Unregistering a certificate

You can unregister a certificate for the adapter.

Procedure

1. At the Main Menu prompt, type J to display the registered certificates. The following example shows a list of lists registered certificates:

0 - e=admin@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng
1 - e=support@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Support,cn=Support

2. Type the number of the certificate file that you want to unregister and press Enter. For example:

   e=admin@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng
   Unregister this CA? (Y/N)

3. At Unregister this CA, type Y to unregister the certificate and press Enter.

Results

After you remove the certificate from the list of registered certificate for the adapter, the certTool displays the Main Menu.

Exporting a certificate and key to a PKCS12 file

You can export a certificate and key to a PKCS12 file.

Procedure

1. At the Main Menu prompt, type K to display the following prompt:

   Enter name of PKCS12 file:

2. At the Enter name of PKCS12 file prompt, type the name of the PKCS12 file for the installed certificate or private key and press Enter.

3. At the Enter Password prompt, type the password for the PKCS12 file and press Enter.

4. At the Confirm Password prompt, type the password again and press Enter.

Results

After the certificate or private key is exported to the PKCS12 file, the certTool displays the Main menu.
Chapter 8. Customizing the Active Directory Adapter

Active Directory can support custom attributes for the user class. The Active Directory Adapter only supports standard Windows attributes by default. However, you can customize the adapter to support custom (extended) attributes.

Before you begin

Before customizing an adapter, you must have working knowledge of these concepts:

- LDAP schema management
- LDAP object classes and attributes
- Scripting language that is appropriate for the installation system
- XML document structure

Note: The Active Directory Adapter supports customization only with the use of pre-Exec and post-Exec scripting. IBM does not support the your individual customization, scripts, or other modifications. If you experience a customization problem, IBM Support can require problem demonstration on the released version of the adapter before opening a problem report. For more information, see the IBM Security Identity Manager Support website.

About this task

Complete the steps to customize the Active Directory Adapter to support the extended attributes in the Active Directory.

Procedure

1. Extend the Active Directory Adapter schema and add the custom attributes to the Active Directory Server. For more information on extending the schema, see “Step 1: Extend the schema and add the extended attributes” on page 62. For information on the files that you can modify to customize the Active Directory Adapter, see Appendix A, “Files” on page 101.

2. Copy the JAR file to a temporary directory and extract the files. For more information on extracting the files, see “Step 2. Copy the ADprofile.jar file and extract the files” on page 62.

3. Add the extended attributes to the exschema.txt file. For more information on extending the attributes, see “Step 3. Modify the exschema.txt file” on page 63.

4. Update the schema.dsml file on the IBM Security Identity Manager server. For more information on updating this file, see “Step 4: Update the schema.dsml file” on page 63.

5. Update the customlabels.properties file on the IBM Security Identity Manager server. For more information on updating this file, see “Step 5: Modify the CustomLabels.properties file” on page 64.

6. Install the new attributes on the IBM Security Identity Manager server. For more information on updating this file, see “Step 6: Create a JAR file and install the new attributes on the IBM Security Identity Manager server” on page 64.

7. Modify the form for the account. For more information on updating the form, see “Step 7: Optionally modify the adapter form” on page 65.
Step 1: Extend the schema and add the extended attributes

Extend the Windows Active Directory schema and add the custom attributes to the Active Directory Server using the tools provided by Windows.

Refer to the Microsoft Windows Server documentation for more information about adding new attributes to the Active Directory.

The Active Directory Adapter supports the following types of custom attributes:

- Boolean
- Integer
- Case sensitive string
- Case insensitive string
- UTC coded time

Consider prefixing the attribute names with erAD in order to easily identify the attributes that are used with IBM Security Identity Manager.

Note:

- If Tivoli® Directory Server is being used as the directory server application, the name of the attribute must be unique within the first 16 characters.
- The Active Directory Adapter supports a multiline value for extended attributes with string syntax.
- The extended attributes are supported only for the User account class.

Step 2. Copy the ADprofile.jar file and extract the files

The profile JAR file, ADprofile.jar, is included in the Active Directory Adapter compressed file that you downloaded from the IBM website.

About this task

The ADprofile.jar file contains the following files:

- CustomLabels.properties
- erADAAccount.xml
- erADDAMLService.xml
- erADGroup.xml
- resource.def
- schema.dsml

You can modify these files to customize your environment.

To modify the ADprofile.jar file, complete the following steps:

Procedure

1. Log in to the system where the Active Directory Adapter is installed.
2. On the Start menu, click Programs > Accessories > Command Prompt.
3. Copy the ADprofile.jar file into a temporary directory.
4. Extract the contents of the ADprofile.jar file into the temporary directory by running the following command:
   ```
   cd c:\temp
   jar -xvf ADprofile.jar
   ```
The jar command will create the c:\temp\ADprofile directory.

5. Edit the appropriate file.

6. When you finish updating the profile JAR file, install it on the IBM Security Identity Manager. For more information on profile installation, see “Importing the adapter profile into the IBM Security Identity Manager server” on page 13.

### Step 3. Modify the exschema.txt file

The exschema.txt file lists all extended attributes in the Active Directory Server.

**About this task**

Modify this file to allow the Active Directory Adapter to recognize an extended attribute in the Windows Active Directory Server.

To modify the exschema.txt file, complete the following steps:

**Procedure**

1. Change to the data directory for the adapter.
2. Create or open the exschema.txt file in a text editor.
3. Add the extended attributes to the file. List only 1 attribute per line. For example:
   - erADString1
   - erADInteger
   - erADDate
   - erADBoolean
   - erADMultiValueString
4. Save the changes, and close the file.
5. Start the adapter again.
   - Start the adapter by using the Windows Services Console.

### Step 4: Update the schema.dsml file

The Active Directory Adapter schema.dsml file identifies all of the standard Windows account attributes.

**About this task**

Modify this file to identify the new extended attributes in the Active Directory Server. For more information about the attributes in this file, see “schema.dsml file” on page 101.

To update the schema.dsml file, complete the following steps:

**Procedure**

1. Change to the ADprofile directory, where the schema.dsml file has been created.
2. Edit the schema.dsml file to add an attribute definition for each extended attribute. The Object Identifier (OID) must be incremented by 1, based on the last entry in the file. For example, if the last attribute in the file uses the OID 1.3.6.1.4.1.6054.3.125.2.67, the first new attribute uses the OID 1.3.6.1.4.1.6054.3.125.2.68.

   Consider starting a new range of numbers for your custom attributes. For example, start custom attributes with OID 1.3.6.1.4.1.6054.3.125.2.100. This...
prevents duplicate OIDs if the adapter is upgraded to support new attributes that are standard for newer versions of Windows.

**Note:** The Active Directory Adapter does not support xforms.xml. Use the same attribute name in eschema.txt and schema.dsm1.

3. Add each of the new attributes to the account class. For example, add the following attribute definition under the erADAccount section of the schema.dsm1 file:

```xml
<attribute ref="erADDate" required="false"/>
```

---

**Step 5: Modify the CustomLabels.properties file**

After you add the extended attributes to the schema.dsm1 file, the attributes are available for use on the Active Directory Adapter form.

**About this task**

The attributes appear in the attribute list by their directory server name. You can modify the attribute names that appear in the attribute list. For more information about the attributes that appear on the adapter form, see “CustomLabels.properties file” on page 104.

To add an attribute and its corresponding label to the CustomLabels.properties file, complete the following steps:

**Procedure**

1. Change to the ADprofile directory where the CustomLabels.properties file has been created.
2. Edit the CustomLabels.properties file to add the attribute and its corresponding label using the following format:

```plaintext
attribute=label
```

**Note:** The attribute name must be in lower case.

For example:

```plaintext
#
# ADAgent Labels definitions
#
eradstring1=ADString1
eradinteger=ADInteger
eraddate=ADDate
eradboolean=ADBoolean
eradmultivaluestring=ADMultivalueString
```

---

**Step 6: Create a JAR file and install the new attributes on the IBM Security Identity Manager server**

After you modify the schema.dsm1 and CustomLabels.properties files, import these files and any other files in the profile that were modified for the adapter, into the IBM Security Identity Manager server to cause the changes to take effect.

**About this task**

To install the new attributes, complete the following steps:
Procedure
1. Create a new JAR file using the files in the `\temp` directory by running the following commands:
   ```bash
   cd c:\temp
   jar -cvf ADprofile.jar ADprofile
   ```
2. Import the `ADprofile.jar` file into the IBM Security Identity Manager server. For more information on importing the file, see "Importing the adapter profile into the IBM Security Identity Manager server" on page 13.
3. Stop and start the IBM Security Identity Manager server.

   Note: If you are upgrading an existing adapter profile, the new adapter profile schema is not immediately used. Stop and start the IBM Security Identity Manager server to refresh the cache and the adapter schema. For more information on upgrading an existing adapter, see "Updating the Active Directory Adapter" on page 93.

Step 7: Optionally modify the adapter form

After the changes are available in the IBM Security Identity Manager server, you can modify the Active Directory Adapter forms to use the new extended attributes.

The attributes do not need to be added to the Active Directory Adapter form unless you want them to be available. The attributes will be returned during reconciliations unless you explicitly exclude them.

For more information on how to modify the adapter form, see the IBM Security Identity Manager product documentation.

Managing passwords when you restore accounts

When a person’s accounts are restored from being previously suspended, you are not prompted to supply a new password for the reinstated accounts. However, there are circumstances when you might want to circumvent this behavior.

About this task

The password requirement to restore an account on Active Directory Server falls into two categories: allowed and required. How each restore action interacts with its corresponding managed resource depends on either the managed resource, or the business processes that you implement. Certain resources will reject a password when a request is made to restore an account. In this case, you can configure IBM Security Identity Manager to forego the new password requirement. If your company has a business process in place that dictates that the account restoration process must be accompanied by resetting the password, you can set the Active Directory Adapter to require a new password when the account is restored.

In the `resource.def` file, you can define whether or not a password is required as a new protocol option. When you import the adapter profile, if an option is not specified, the adapter profile importer determines the correct restoration password behavior. Adapter profile components also enable remote services to find out if you discard a password that is entered by the user in a situation where multiple accounts on disparate resources are being restored. In this scenario, only some of
the accounts being restored might require a password. Remote services will discard the password from the restore action for those managed resources that do not require them.

To configure the Active Directory Adapter to prompt for a new password when restoring accounts:

**Procedure**

1. Stop the IBM Security Identity Manager server.
2. Extract the files from the ADprofile.jar file. For more information on customizing the adapter profile file, see "Step 2. Copy the ADprofile.jar file and extract the files" on page 62.
3. Change to the \ADprofile directory, where the resource.def file has been created.
4. Edit the resource.def file to add the new protocol options. For example:

```
<Property Name = "com.ibm.itim.remoteservices.ResourceProperties.PASSWORD_NOT_REQUIRED_ON_RESTORE" Value = "FALSE"/>
<Property Name = "com.ibm.itim.remoteservices.ResourceProperties.PASSWORD_NOT_ALLOWED_ON_RESTORE" Value = "FALSE"/>
```

Adding the two options in the example above ensures that you are prompted for a password when an account is restored.
5. Create a new ADprofile.jar file using the resource.def file and import the adapter profile file into the IBM Security Identity Manager server. For more information, see "Step 6: Create a JAR file and install the new attributes on the IBM Security Identity Manager server" on page 64.
6. Start the IBM Security Identity Manager server again.

**Note:** If you upgrade an existing adapter profile, the new adapter profile schema is not immediately used. Stop and start the IBM Security Identity Manager server to refresh the cache and therefore the adapter schema. For more information on upgrading an existing adapter, see "Updating the Active Directory Adapter" on page 93.

---

**Users Base Point configuration for the adapter**

You can configure the Active Directory Adapter to support both sub-domains and multiple domains through the base point feature on the adapter service form.

For more information on configuring the service form, see the IBM Security Identity Manager product documentation.

The base point for the Active Directory Adapter is the point in the directory server that is used as the root for the adapter. This point can be an OU or DC point. Because the base point is an optional value, if a value is not specified, the adapter uses the default domain of the workstation on which it is installed.

The following definition is an example of a base point defined from the root of the directory server:

```
dc=irvine,dc=IBM,dc=com
```

The following definition is an example of a base point defined from an organizational unit level:

```
ou=engineering,dc=irvine,dc=IBM,dc=com
```
The syntax of the base point also allows for an optional workstation name to prefix the base point DN, for example server1/dc=ibm,dc=com. This causes the adapter to bind to a specific server instead of connecting to the first available server when responding to an active directory bind request.

You can specify more than one target server for the base point on the Active Directory Adapter service form on IBM Security Identity Manager and in the Active Directory Adapter registry. Each target server must be separated by | as a delimiter. For example,

**Base Point DN on the service form with more than one target server:**
DC01|DC02|DC03/OU=engineering,DC=irvine,DC=IBM,DC=com

**Base Point DN on the service form with only one target server:**
DC01/OU=engineering,DC=irvine,DC=IBM,DC=com

**Base Point DN on the service form with no target server:**
OU=engineering,DC=irvine,DC=IBM,DC=com

You can also specify target servers for the base point in the Active Directory Adapter registry. For example,

**Example 1**
If the BasePoint specified on the service form is OU=engineering,DC=irvine,DC=IBM,DC=com, you can specify the list of target servers in the adapter registry by using the agentCfg.exe as you:

1. Create an Active Directory Adapter registry key, for example,
   OU=engineering,DC=irvine,DC=IBM,DC=com.
2. Specify the value for the created registry key as DC01|DC02|DC03.

**Example 2**
If the BasePoint specified on the service form is DC01|DC02|DC03/
OU=engineering,DC=irvine,DC=IBM,DC=com, you can specify the list of target servers in the adapter registry by using the agentCfg.exe as you:

1. Create an Active Directory Adapter registry key, for example,
   OU=engineering,DC=irvine,DC=IBM,DC=com.
2. Specify the value for the created registry key as DC04|DC05|DC06.

The adapter iterates through all the target servers specified in the base point on the service form, and then through the target servers specified in the adapter registry key. The adapter uses the first available target server. You can specify the base point without the target servers on the service form and use the registry key to specify the target servers. The adapter uses the base point specified on the service form to search a key with this base point value in the registry to get the target servers specified as the value for this registry key.

**Note:**
- There is a limit of 240 characters for the Base Point DN attribute on the adapter service form.
- The adapter service form and registry can specify their own set of target servers. However, the target servers specified on the service form are considered a high priority.
- When you do not provide a base point on the service form, the adapter does not use the registry.
Specify the target server by using the adapter registry because it is cached to improve the performance compared to specifying on the adapter service form. The target server list on the service form is not cached and is parsed in each request to find all target servers.

Use the `agentCfg.exe` to create and modify adapter registry keys. Restart the adapter service after you add or modify the registry keys. When the base point or target server have Unicode characters, use `regedit` to create registry keys under `HKEY_LOCAL_MACHINE\SOFTWARE\Access360\ADAgent\Specific`.

Also, on the service form are the Admin User Account and Admin User Password values. These optional values are only required if an administrator account is defined for the base point of the adapter, and you want to use this account for logging purposes. If these values are not defined, the adapter will use the account assigned to the adapter service.

**Note:** Do not create services that overlap in scope in the directory tree. This could result in duplicate account creation during reconciliation.

---

### Configuring the source attribute of `erGroup` and `erADGroupIsMemberOf`

You can configure Group CN, Group DN, or Group GUID for the Source Attribute of `erGroup` and `erADGroupIsMemberOf` on the account form and group form to meet the requirements of your organization.

**About this task**

The source attribute identifies the name of the group class attribute for which the value is supplied in the request when groups are added or removed from the account form and group form. The default configuration is DN. The adapter uses the Group DN to bind to a group for adding or removing members. Also, the adapter adds the Group DN to the `erGroup` attribute of user object and `erADGroupIsMemberOf` attribute of group object during the reconciliation operation.

The CN value is not required to be unique.

The GUID value is not human readable.

It is possible to set up a test environment that uses the same DN values as the production environment. Any customization based on the DN works in both environments because the DNs are the same. However, if you use the same GUID in both environments, the values are different even if the DN values are the same.

To use the Group CN, Group DN, or Group GUID, perform the following steps.

**Procedure**

- Set the UseGroup registry key to one of the following options by using the `agentCfg`:
  - CN
  - DN
  - GUID
- Modify the profile files `erADAccount.xml`, `erADGroup.xml`, and `resource.def`. For information about profile file modifications, see Table 17 on page 70.
• Build the ADprofile.jar and import the new profile on IBM Security Identity Manager.

• Perform a full reconciliation operation.

**Note:** If an event notification is enabled, delete the event notification database and perform a full reconciliation operation. When you do so, you are ensuring that a new database is created with correct values.

• Modify the profile files erADAccount.xml, erADGroup.xml, and resource.def as specified in the following table:
### Table 17. Profile files

<table>
<thead>
<tr>
<th>Value of the UseGroup registry key</th>
<th>Modifications required in</th>
<th>Expected modification</th>
</tr>
</thead>
</table>
| DN                               | erADAccount.xml           | `<formElement direction="inherit" label="$ergroup" name="data.ergroup">
<searchFilter multiple="true" type="select">
<filter>(objectclass=eradgroup)</filter>
<base>contextual</base>
<attribute>erADGroupSamAccountName</attribute>
<sourceAttribute>erADGroupDN</sourceAttribute>
<delimiter></delimiter>
<size></size>
<width>300</width>
<objectClass>erADGroup</objectClass>
<showQueryUI>false</showQueryUI>
<paginateResults>true</paginateResults>
</searchFilter>
</formElement>` |
| erADGroup.xml                    | erADGroup.xml             | `<formElement direction="inherit" label="$eradgroupismemberof" name="data.eradgroupismemberof">
<searchFilter multiple="true" type="select">
<filter>(objectclass=eradgroup)</filter>
<base>contextual</base>
<attribute>erADGroupSamAccountName</attribute>
<sourceAttribute>erADGroupDN</sourceAttribute>
<delimiter></delimiter>
<size></size>
<width>300</width>
<objectClass>erADGroup</objectClass>
<showQueryUI>false</showQueryUI>
<paginateResults>true</paginateResults>
</searchFilter>
</formElement>` |
| resource.def                     | ServiceGroups             | `<ServiceGroups>
  <GroupDefinition ProfileName="ADGroupProfile"
    ClassName = "erADGroup"
    RdnAttribute = "erADGroupSamAccountName"
    AccountAttribute = "erGroup">
    <AttributeMap>
      <Attribute Name = "erGroupId" Value="erADGroupDN" />
      <Attribute Name = "erGroupName" Value="erADGroupSamAccountName" />
      <Attribute Name = "erGroupDescription" Value="erADGroupDescription" />
    </AttributeMap>
    <BehaviorProperties>
      <Property Name = "Managed" Value = "true"/>
    </BehaviorProperties>
  </GroupDefinition>
</ServiceGroups>` |
<table>
<thead>
<tr>
<th>Value of the UseGroup registry key</th>
<th>Modifications required in</th>
<th>Expected modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN</td>
<td>erADAccount.xml</td>
<td><code>&lt;formElement direction=&quot;inherit&quot; label=&quot;$ergroup&quot; name=&quot;data.ergroup&quot;&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;searchFilter multiple=&quot;true&quot; type=&quot;select&quot;&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;filter&gt;(objectclass=eradgroup)&lt;/filter&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;base&gt;contextual&lt;/base&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;attribute&gt;erADGroupSamAccountName&lt;/attribute&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;sourceAttribute&gt;erADGroupCN&lt;/sourceAttribute&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;delimiter&gt;&lt;/delimiter&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;size&gt;&lt;/size&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;width&gt;300&lt;/width&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;objectClass&gt;erADGroup&lt;/objectClass&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;showQueryUI&gt;false&lt;/showQueryUI&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;paginateResults&gt;true&lt;/paginateResults&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/searchFilter&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/formElement&gt;</code></td>
</tr>
<tr>
<td>erADGroup.xml</td>
<td></td>
<td><code>&lt;formElement direction=&quot;inherit&quot; label=&quot;$eradgroupismemberof&quot; name=&quot;data.ergadgroup&quot;&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;searchFilter multiple=&quot;true&quot; type=&quot;select&quot;&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;filter&gt;(objectclass=eradgroup)&lt;/filter&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;base&gt;contextual&lt;/base&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;attribute&gt;erADGroupSamAccountName&lt;/attribute&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;sourceAttribute&gt;erADGroupCN&lt;/sourceAttribute&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;delimiter&gt;&lt;/delimiter&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;size&gt;&lt;/size&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;width&gt;300&lt;/width&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;objectClass&gt;erADGroup&lt;/objectClass&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;showQueryUI&gt;false&lt;/showQueryUI&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;paginateResults&gt;true&lt;/paginateResults&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/searchFilter&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/formElement&gt;</code></td>
</tr>
<tr>
<td>resource.def</td>
<td></td>
<td><code>&lt;ServiceGroups&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;GroupDefinition ProfileName=&quot;ADGroupProfile&quot;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>ClassName = &quot;erADGroup&quot;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>RdnAttribute = &quot;erADGroupSamAccountName&quot;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>AccountAttribute = &quot;erGroup&quot;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/AttributeMap&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;Attribute Name = &quot;erGroupId&quot; Value=&quot;erADGroupCN&quot; /&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;Attribute Name = &quot;erGroupName&quot; Value=&quot;erADGroupSamAccountName&quot; /&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;Attribute Name = &quot;erGroupDescription&quot; Value=&quot;erADGroupDescription&quot; /&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/AttributeMap&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;BehaviorProperties&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;Property Name = &quot;Managed&quot; Value = &quot;true&quot;/&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/BehaviorProperties&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/GroupDefinition&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/ServiceGroups&gt;</code></td>
</tr>
<tr>
<td>Value of the UseGroup registry key</td>
<td>Modifications required in</td>
<td>Expected modification</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>GUID</td>
<td>erADAccount.xml</td>
<td><code>&lt;formElement direction=&quot;inherit&quot; label=&quot;$ergroup&quot; name=&quot;data.ergroup&quot;&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;searchFilter multiple=&quot;true&quot; type=&quot;select&quot;&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;filter&gt;(objectclass=#1;eradgroup)&lt;/filter&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;base&gt;contextual&lt;/base&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;attribute&gt;erADGroupSamAccountName&lt;/attribute&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;sourceAttribute&gt;erADGroupGUID&lt;/sourceAttribute&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;delimiter&gt;&lt;/delimiter&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;width&gt;300&lt;/width&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;objectClass&gt;erADGroup&lt;/objectClass&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;showQueryUI&gt;false&lt;/showQueryUI&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;paginateResults&gt;true&lt;/paginateResults&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;searchFilter&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/searchFilter&gt;</code></td>
</tr>
<tr>
<td></td>
<td>erADGroup.xml</td>
<td><code>&lt;formElement direction=&quot;inherit&quot; label=&quot;$eradgroupismemberof&quot; name=&quot;data.eradgroupismemberof&quot;&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;searchFilter multiple=&quot;true&quot; type=&quot;select&quot;&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;filter&gt;(objectclass=#1;eradgroup)&lt;/filter&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;base&gt;contextual&lt;/base&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;attribute&gt;erADGroupSamAccountName&lt;/attribute&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;sourceAttribute&gt;erADGroupGUID&lt;/sourceAttribute&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;delimiter&gt;&lt;/delimiter&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;width&gt;300&lt;/width&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;objectClass&gt;erADGroup&lt;/objectClass&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;showQueryUI&gt;false&lt;/showQueryUI&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;paginateResults&gt;true&lt;/paginateResults&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;searchFilter&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/searchFilter&gt;</code></td>
</tr>
<tr>
<td></td>
<td>resource.def</td>
<td><code>&lt;ServiceGroups&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;GroupDefinition ProfileName=&quot;ADGroupProfile&quot;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>ClassName = &quot;erADGroup&quot;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>RdnAttribute = &quot;erADGroupSamAccountName&quot;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>AccountAttribute = &quot;erGroup&quot;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;AttributeMap&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;Attribute Name = &quot;erGroupId&quot; Value=&quot;erADGroupGUID&quot; /&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;Attribute Name = &quot;erGroupName&quot; Value=&quot;erADGroupSamAccountName&quot;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;Attribute Name = &quot;erGroupDescription&quot; Value=&quot;erADGroupDescription&quot;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;AttributeMap&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;BehaviorProperties&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;Property Name = &quot;Managed&quot; Value = &quot;true=&quot;/&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/BehaviorProperties&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/GroupDefinition&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/ServiceGroups&gt;</code></td>
</tr>
</tbody>
</table>

### Configuring the Proxy Addresses attribute

You can modify the Proxy Addresses attribute of a user account. In this case, IBM Security Identity Manager sends the erADEProxyAddresses attribute in the modify operation with an attribute operation type of replace.
About this task

When the attribute operation type is replace, the adapter resets the proxy addresses for the user account on the Active Directory. You do not get the proxy addresses that are added to the user account by using the external application with an attribute operation type of replace when:

- You have additions to the Proxy Addresses attribute of a user account on the Active Directory by using an external application.
- The user accounts are not reconciled frequently.

To avoid a reset of the Proxy Addresses attribute on the Active Directory, modify the adapter profile for sending the erADEProxyAddresses attribute in the modify operation with an attribute operation type of Add or Delete. To handle the erADEProxyAddresses attribute with an attribute operation type of Add or Delete, modify the profile for Active Directory. The adapter profile (ADprofile.jar) is included in the JAR file for the adapter.

To modify the ADprofile.jar file for handling the erADEProxyAddresses attribute with an attribute operation type of Add or Delete, perform the following steps:

Procedure

1. Copy the ADprofile.jar file to a temporary directory, for example, C:\Temp directory.
2. Extract the contents of the ADprofile.jar file into the temporary directory by running the following command:
   ```
   cd C:\Temp
   jar -xvf ADprofile.jar
   ```
   The jar command creates the C:\Temp\ADprofile directory that has all the profile files.
3. From the extracted ADprofile directory, open the resource.def file in a text editor and search for this entry:
   ```
   <Parameter Name="erADEProxyAddresses" Source="account" ReplaceMultiValue="true" />
   ```
4. Delete all the occurrences of the above entry from the resource.def file and save the file.
5. Run the following command to create the new jar file:
   ```
   cd C:\Temp
   jar -cvf ADprofile.jar ADprofile
   ```
6. Import the new ADprofile.jar file on IBM Security Identity Manager. For more information about importing the adapter profile, see "Importing the adapter profile into the IBM Security Identity Manager server" on page 13.
7. After you import the adapter profile, restart IBM Security Identity Manager to reflect the updates.

Configuring the erGroup attribute

When you modify the Groups attribute of a user account, IBM Security Identity Manager sends the erGroup attribute in the modify operation with an attribute operation type of replace.

About this task

When the attribute operation type is replace, the adapter removes the membership of the user from the groups of which the user is a member on the Active Directory.
and that are not included in the modify request. You do not get the membership of a user account to groups that are added to the user account by using the external application when:

- You modify the user account membership on the Active Directory by using an external application.
- The user accounts are not reconciled frequently.

When you modify the user account membership on the Active Directory, modify the profile for sending the erGroup attribute in the modify request with an attribute operation type of Add or Delete. To handle the erGroup attribute with attribute operation type as Add or Delete, modify the profile for Active Directory.

The adapter profile (ADprofile.jar) is included in the JAR file for the adapter.

To modify the ADprofile.jar file for handling the erGroup attribute with an attribute operation type of Add or Delete, perform the following steps:

**Procedure**

1. Copy the ADprofile.jar file to a temporary directory, for example, C:\Temp directory.
2. Extract the contents of ADprofile.jar file into the temporary directory by running the following command:

   ```
   cd C:\Temp
   jar -xvf ADprofile.jar
   ```

   The jar command creates the C:\Temp\ADprofile directory that has all the profile files.
3. From the extracted ADprofile directory, open the resource.def file in a text editor and search for the entry `<Parameter Name="erGroup" Source="account" ReplaceMultiValue="true" />`.
4. Delete all the occurrences of the above entry from the resource.def file and save the file.
5. Run the following command to create a new jar file:

   ```
   cd C:\Temp
   jar -cvf ADprofile.jar ADprofile
   ```
6. Import the new ADprofile.jar file on IBM Security Identity Manager. For more information about importing the adapter profile, see "Importing the adapter profile into the IBM Security Identity Manager server" on page 13.
7. After you import the adapter profile, restart IBM Security Identity Manager to reflect the updates.

**Configuring the cn attribute**

You can configure the cn attribute.

**About this task**

The Active Directory Adapter user account class contains the following attributes for the attribute cn defined in the Active Directory:

- IBM Security Identity Manager common schema attribute cn
- erADFullName.

The cn attribute is used on the account form, by default. The adapter processes the cn attribute in the user add, modify, and reconciliation operations. The adapter
uses the registry key UseITIMCNAttribute to use either the cn or the erADFullName attribute. When the compliance alerts on IBM Security Identity Manager are enabled, avoid using the cn attribute on the account form. To use the erADFullName attribute, you must customize the account form and set the registry key UseITIMCNAttribute.

When you set the registry key UseITIMCNAttribute to FALSE, the adapter uses the erADFullName attribute for the cn attribute defined in the Active Directory for the user add, modify, and reconciliation operations.

To use the erADFullName attribute on the account form, perform the following steps:

**Procedure**

1. Add the erADFullName attribute to the user account form by customizing the Active Directory account form. For more information about customizing the user account form, see the IBM Security Identity Manager product documentation.
2. Set the registry key UseITIMCNAttribute to FALSE by using the agentCfg utility.
Chapter 9. Taking the first steps after installation

After you install and configure the adapter, take these steps:

**Procedure**
1. Test the connection for the service that you have created on IBM Security Identity Manager.
2. Perform a full reconciliation from the IBM Security Identity Manager server.
3. Perform all supported operations (add, change and delete) on one account and examine the WinADAgent.log file after each operation to ensure that no errors were reported.
Chapter 10. Troubleshooting

Use this information to identify and resolve problems that are related to the adapter, including errors that might occur during installation because of incorrect input.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem.

The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When starting to describe a problem, the most obvious question is “What is the problem?” This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?
• Do all users have the problem?
• (For multi-site installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration; many problems can be traced back to incompatible levels of software that are not intended to run together or have not been fully tested together.

**When does the problem occur?**

Develop a detailed timeline of events leading up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:
• Does the problem happen only at a certain time of day or night?
• How often does the problem happen?
• What sequence of events leads up to the time that the problem is reported?
• Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

**Under which conditions does the problem occur?**

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:
• Does the problem always occur when the same task is being performed?
• Does a certain sequence of events need to happen for the problem to occur?
• Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.

**Can the problem be reproduced?**

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Consequently, problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible,
re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

For information about obtaining support, see Appendix C, “Support information,” on page 119.

---

**Known behaviors**

The following behaviors and limitations are known to exist in the operation of the Active Directory Adapter.

**Directory NTFS and share access**

The agent returns the actual, effective permissions that are granted to a user and not the specific access that is assigned to the user account.

**Expiration date**

The Active Directory Users and Computers Microsoft Management Console (MMC) snap-in displays the account expiration date as one day earlier than the date contained in the `accountExpires` attribute. The IBM Security Identity Manager server displays the value that is contained in the `account expires` attribute.

**Password properties**

The password properties are specific to the account. However, these properties can be overridden by the security policies of the managed resource.

For example:

- Domain controller security policies
- Domain security policies
- Local security policies

**Language preference settings for accounts**

The languages attribute `eradlanguage` is an Exchange attribute. If you are using a configuration without Exchange, setting this attribute returns a warning.

**Log message: Error More Data**

The `Error_More_Data` message might be in the adapter log if a reconciliation is run while the Active Directory server is under load.

The Active Directory Adapter is designed to retry the query three times before terminating the Reconciliation. For more information, see the Microsoft Knowledge base.

---

**Replication delay solutions for a mailbox addition on Microsoft Exchange**

Requesting a user account on Active Directory with mail status on Exchange might generate the error `User does not exist`. 
This behavior is caused by replication delay. Exchange might not find the user account on a domain controller, if the account is created on another domain.

The solution here is to target both the following operations to the same Domain Controller:
- Create user account operation.
- The Exchange operation, to either mailbox enable or mail-enable the user account.

To specify a target server use the **Users Base Point DN** on IBM Security Identity Manager Active Directory profile service form. The Base Point must contain the name of the domain controller. For more information about how to specify **Users Base Point DN**, see “**Users Base Point configuration for the adapter**” on page 66.

**Example**

Users Base Point DN: DC01/ou=Test,dc=MyDomain,dc=com.

---

### Errors in Exchange mailbox permissions

The adapter might not set the mailbox permissions correctly, even though the request generates a **SUCCESS** message.

If multiple permissions are set in a modify request but only the last permission takes effect, you must modify the **SetMailboxPermissionDelay** registry key.

The **SetMailboxPermissionDelay** registry key cause the adapter to wait a specified time in seconds before processing the next permission. The default setting of this key is 0 or no delay. Typically setting this registry to 20 resolves the problem.

For information about setting registry keys, see “**Modifying registry settings**” on page 36.

---

### No provisioning provider installed

This error is a known configuration issue with Exchange.

This error is misleading in that it is typically caused by a lack of permissions by the adapter logon account. Typically the error is not because a “provisioning provider” is installed.

To provision mailboxes to Exchange, the logon account must be a member of the appropriate security groups. Because of these variations, it is not possible to provide a definitive list of group memberships that are required by the adapter logon account:
- Active Directory installations can be on single domains, multiple domains, or sub domains.
- Groups can be customized, that is added to other groups.

Membership in the Domain Admins group is required to provision accounts.

Typically, membership in the following Exchange groups is sufficient for the adapter to provision mailboxes:
- Recipient Management
- Organization Management
• Exchange Windows Permissions

If the adapter logon account is a member of these groups and the error persists, add a membership to Enterprise Admins group. This action can determine if the problem is due to permissions. If adding this membership resolves the issue, see the Microsoft documentation about trial and error to determine which group memberships are needed.

Warnings and error messages

A warning or error message might be displayed in the user interface to provide information about the adapter or when an error occurs.

These errors might be displayed in the user interface when the adapter is installed on your system.

Table 18. Troubleshooting the Active Directory Adapter errors

<table>
<thead>
<tr>
<th>Error message</th>
<th>Corrective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unable to bind to base point</td>
<td>Ensure that:</td>
</tr>
<tr>
<td></td>
<td>• The Users Base Point is correctly specified on the adapter service form.</td>
</tr>
<tr>
<td></td>
<td>• The target servers are up and reachable when they are specified in the base point.</td>
</tr>
<tr>
<td></td>
<td>• The user ID is correctly specified on the adapter service form.</td>
</tr>
<tr>
<td></td>
<td>• The password is correctly specified on the adapter service form.</td>
</tr>
<tr>
<td></td>
<td>• The Active Directory Server is reachable from the workstation where the adapter is installed.</td>
</tr>
<tr>
<td>Unable to bind to group base point</td>
<td>Ensure that:</td>
</tr>
<tr>
<td></td>
<td>• The Groups Base Point is correctly specified on the adapter service form.</td>
</tr>
<tr>
<td></td>
<td>• The user ID is correctly specified on the adapter service form.</td>
</tr>
<tr>
<td></td>
<td>• The password is correctly specified on the adapter service form.</td>
</tr>
<tr>
<td></td>
<td>• The target servers are up and reachable when they are specified in the base point.</td>
</tr>
<tr>
<td></td>
<td>• The Active Directory Server is reachable from the workstation where the adapter is installed.</td>
</tr>
<tr>
<td>Unable to determine default domain</td>
<td>This error occurs when the Active Directory Adapter fails to:</td>
</tr>
<tr>
<td></td>
<td>• Bind to root DSE</td>
</tr>
<tr>
<td></td>
<td>• Get the default naming context</td>
</tr>
<tr>
<td></td>
<td>Ensure that:</td>
</tr>
<tr>
<td></td>
<td>• The Users Base Point is correctly specified on the adapter service form.</td>
</tr>
<tr>
<td></td>
<td>• The user ID is correctly specified on the adapter service form.</td>
</tr>
<tr>
<td></td>
<td>• The password is correctly specified on the adapter service form.</td>
</tr>
<tr>
<td></td>
<td>• The Active Directory Server is reachable from the workstation where the adapter is installed.</td>
</tr>
<tr>
<td>Error binding to DN: DN String</td>
<td>This error occurs when the Active Directory Adapter fails to bind to a user object of the Active Directory Server for processing.</td>
</tr>
<tr>
<td></td>
<td>Ensure that the user processed in the Active Directory Server is not deleted by any other process simultaneously.</td>
</tr>
<tr>
<td>Error message</td>
<td>Corrective action</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Extended attribute <em>attribute name</em> has unsupported syntax</td>
<td>The Active Directory Adapter does not support the data type used for the extended attribute. Use one of the following data types:</td>
</tr>
<tr>
<td></td>
<td>•                                                                       Integer</td>
</tr>
<tr>
<td></td>
<td>•                                                                       Case-sensitive string</td>
</tr>
<tr>
<td></td>
<td>•                                                                       Not case-sensitive string</td>
</tr>
<tr>
<td></td>
<td>•                                                                       Numerical string</td>
</tr>
<tr>
<td></td>
<td>•                                                                       Unicode string</td>
</tr>
<tr>
<td></td>
<td>•                                                                       Distinguished name</td>
</tr>
<tr>
<td></td>
<td>•                                                                       UTC coded time</td>
</tr>
<tr>
<td></td>
<td>For more information about customizing the adapter to use the extended attributes, see Chapter 8, “Customizing the Active Directory Adapter,” on page 61.</td>
</tr>
<tr>
<td>Extended attribute <em>attribute name</em> not found in Active Directory schema</td>
<td>The extended attribute specified in the <em>exschema.txt</em> file does not exist on the Active Directory Server.</td>
</tr>
<tr>
<td>Error message</td>
<td>Corrective action</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Error determining RAS server name                                            | Check the value of the registry key `ForceRASServerLookup`. If the value of the key is `TRUE`, the Active Directory Adapter determines the RAS server regardless of whether you specify the server name on the adapter service form.  
This error might be because the domain does not exist or the domain controller is not available for the specified domain.  
Ensure that the Active Directory Server is reachable from the workstation where the adapter is installed. |
| Unable to get domain name. Terminal and RAS servers cannot be determined.    | This error occurs when the Active Directory Adapter fails to get the domain name from the specified base point or from the default domain.  
Ensure that a base point is specified with a correct domain name.             |
| Invalid domain name syntax                                                  | Use one of the following formats to specify the domain name:  
• Server name/ou=org1,dc=ibm,dc=com  
• ou=org1,dc=ibm,dc=com                                                          |
| User not found                                                               | Ensure that the user exists on the Active Directory Server and is not directly deleted or modified on the Active Directory Server.                     |
| Group not found.                                                             | Ensure that the group exists on the Active Directory Server and is not directly deleted or modified on the Active Directory Server.                     |
| Error setting attributes `country`. Unknown country code.                    | The country code specified for the user is not valid.  
Specify a valid country code and submit the request again. For information about valid country codes, see the country and region codes section in the `Active Directory Adapter User Guide`. |
| Could not modify the attribute–msExchUserAccountControl                     | This warning occurs when the user mailbox is not disabled on suspending a user account.                                                            |
| Error removing membership from group `group name`                           | The Active Directory Adapter failed to remove the membership of a user or group from the group `group name`.  
Ensure that:  
• The user or group exists on the Active Directory Server.  
• The user or group is a member of the group `group name`.  
• The group specified exists on the Active Directory Server.                      |
| Error adding membership to group `group name`                               | The Active Directory Adapter failed to add membership of the user or group to the group `group name`.  
Ensure that:  
• The user or group exists on the Active Directory Server.  
• The user or group is not already a member of the group `group name`.  
• The group specified exists on the Active Directory Server.                      |
| Unable to get info on share `share name`                                     | This error occurs when the Active Directory Adapter fails to retrieve share information from the home directory of the user.  
Ensure that:  
• The user account under which the adapter is running has access to the home directory.  
• The share name exists on the workstation where the home directory is created.   |
<table>
<thead>
<tr>
<th>Error message</th>
<th>Corrective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid home directory path <em>path name</em></td>
<td>The Active Directory Adapter supports creation and deletion of only UNC home directories. Specify the UNC home directory path in the following format:</td>
</tr>
<tr>
<td></td>
<td>\servername\sharename\foldername</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>• NTFS security and Shares can be set only on the Home Directories that are a UNC path.</td>
</tr>
<tr>
<td></td>
<td>• Share Access can be set only on the Home Directories that are a UNC path that have a share created.</td>
</tr>
<tr>
<td>Unable to delete home directory <em>home directory name</em></td>
<td>The Active Directory Adapter is not able to delete the specified home directory. If the adapter is unable to delete the UNC home directory, ensure that:</td>
</tr>
<tr>
<td></td>
<td>• The value of the registry key <strong>DeleteUNCHomeDirectories</strong> is TRUE.</td>
</tr>
<tr>
<td></td>
<td>• The user account under which the adapter is running has permissions to delete the directory.</td>
</tr>
<tr>
<td>Home directory deletion is not enabled.</td>
<td>To enable home directory deletion, set the values of <strong>DeleteUNCHomeDirectories</strong> and <strong>ManageHomeDirectories</strong> registry keys to TRUE. Resend the modify request from IBM Security Identity Manager.</td>
</tr>
<tr>
<td>Homedirectory will not be deleted.</td>
<td></td>
</tr>
<tr>
<td>Home directory creation not enabled.</td>
<td>To enable home directory creation, set the values of <strong>CreateUNCHomeDirectories</strong> and <strong>ManageHomeDirectories</strong> registry keys to TRUE. Resend the modify request from IBM Security Identity Manager.</td>
</tr>
<tr>
<td>Directory will not be created.</td>
<td></td>
</tr>
<tr>
<td>Error creating home directory <em>home directory name</em></td>
<td>The Active Directory Adapter is not able to create home directory.</td>
</tr>
<tr>
<td>Unable to set Home Directory Drive. Failed to create Home Directory.</td>
<td>Ensure that:</td>
</tr>
<tr>
<td>Unable to set Home Directory NTFS security. Failed to create Home Directory.</td>
<td>• A directory with the same name does not exist.</td>
</tr>
<tr>
<td>Unable to set Home Directory Share. Failed to create Home Directory.</td>
<td>• The user account has permissions to create home directory.</td>
</tr>
<tr>
<td>Unable to set Home Directory Share Access. Failed to create Home Directory.</td>
<td>• Intermediate directories exist. The adapter creates only the final directory in the specified path.</td>
</tr>
<tr>
<td>Error deleting share <em>share name</em></td>
<td>The Active Directory Adapter is not able to delete the share when you clear the value of the share-related attributes from the Active Directory Server account form.</td>
</tr>
<tr>
<td></td>
<td>Ensure that:</td>
</tr>
<tr>
<td></td>
<td>• The user account has access to the specified share.</td>
</tr>
<tr>
<td></td>
<td>• The specified share name exists.</td>
</tr>
<tr>
<td></td>
<td>• The user account under which the adapter is running has permissions to create home directory.</td>
</tr>
</tbody>
</table>
Table 18. Troubleshooting the Active Directory Adapter errors (continued)

<table>
<thead>
<tr>
<th>Error message</th>
<th>Corrective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search failed. Unable to retrieve additional data after 3 retries.</td>
<td>The Active Directory Adapter retrieves data from the Active Directory Server in a paged manner. The adapter reconciles users, groups, and containers and attempts to retrieve data in a maximum of three attempts. If all three attempts fail, the adapter abandons the search.</td>
</tr>
<tr>
<td>User search failed</td>
<td></td>
</tr>
<tr>
<td>Group search failed. Error code: error code - error description. Provider: provider name.</td>
<td>The adapter cannot retrieve data because of one of the following reasons: • The network response is slow. • The Active Directory Server is busy. • The Active Directory Adapter installed on the Active Directory Server server is overloading the server. For information about configuring the Active Directory Server, see <a href="http://support.microsoft.com">http://support.microsoft.com</a>.</td>
</tr>
<tr>
<td>Error performing User Lookup</td>
<td></td>
</tr>
<tr>
<td>errorMessage=&quot;Unsupported filter&quot;</td>
<td>The adapter does not support the attribute specified in the filter. For the list of supported attributes, see supported attributes in the Active Directory Adapter User Guide.</td>
</tr>
<tr>
<td>Error setting attribute eradprimarygroup. ADSI Result code: 0x80072035 - The server is unwilling to process the request.</td>
<td>Ensure that: • The user is a member of the specified group. • The specified group is either a universal security group or a global security group.</td>
</tr>
<tr>
<td>ADSI Result code: 0x80072014 - The requested operation did not satisfy one or more constraints associated with the class of the object.</td>
<td>These errors occur when the specified value for the attribute violates any constraint associated with that attribute. For example, a constraint might be: • Minimum or maximum length of characters the attribute can store. • Minimum or maximum value the attribute can accept. Ensure that the specified value for the attribute does not violate these constraints. Note: If any one of the attribute specified in the request violates a constraint, the adapter gives the same error for all the subsequent attributes. This error is issued even though they do not violate any constraint. For example, the Title attribute on the Active Directory Server can store a description of maximum of 64 characters. If you specify a description of more than 64 characters, the adapter gives these errors for the Title attribute and for all the other attributes specified in the request.</td>
</tr>
<tr>
<td>ADSI Result code: 0x8007202f - A constraint violation occurred.</td>
<td></td>
</tr>
<tr>
<td>Request for proxy email types should contain at least one primary SMTP address</td>
<td>Verify that the request for proxy email types contains a primary SMTP address.</td>
</tr>
<tr>
<td>Unable to load XML transformation buffer from adapter installation directory\data\xforms.xml</td>
<td>The Active Directory Adapter does not use the xforms.xml file. Therefore, you can safely ignore the xforms-related errors that are recorded in the WinADAgent.log file.</td>
</tr>
<tr>
<td>Unable to bind to group group name.</td>
<td>This error occurs when the Active Directory Adapter fails to connect to a group object in the Active Directory Server for processing. Ensure that the group group name exists on the Active Directory Server.</td>
</tr>
<tr>
<td>Error message</td>
<td>Corrective action</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Unable to contact Exchange services. ADSI Result code: 0x80004002</td>
<td>The Exchange provider uses Collaboration Data Objects for Exchange Management (CDOEXM) for a user object. CDOEXM uses several static variables.  The lifetimes of these variables last until the process ends. These static variables are reallocated every time CDOEXM is loaded. Because all CDOEXM work is done in the lifetime of the worker thread, CDOEXM is loaded and unloaded repeatedly. Under certain conditions, CDOEXM is incorrectly marked as initialized, though CDOEXM is not fully initialized. Therefore, later attempts to use CDOEXM fail. To avoid this error, use the new feature “Thread Pooling” of Windows Active Directory Adapter.</td>
</tr>
</tbody>
</table>
| The specified User Principal Name (UPN) UPN values already exists in the enterprise. Specify a new one. | This error occurs when an attempt is made to create user request and the user account exists in the Active Directory Server with the same value for User Principal Name attribute. Ensure that: 
  - The value specified for the User Principal Name attribute when you create a user account is not already used by an existing user account on the Active Directory Server. 
  - You set the registry key UPNSearchEnabled to FALSE when you do not want the adapter to check the uniqueness of the User Principal Name attribute. For more information about usage of the registry key UPNSearchEnabled, see "User Principal Name of a user account" in the *Active Directory Adapter User Guide*. |
| Error while fetching the group interface for group DN.                       | This error occurs when the Active Directory Adapter fails to bind to a group object on the Active Directory Server for processing. Ensure that the group processed in the Active Directory Server is not deleted by any other process simultaneously. |
| Unable to bind to the container object in move operation.                   | This error occurs when the Active Directory Adapter binds to the requested container when a user or group object is moved in the Active Directory Server hierarchy. Ensure that the container exists on the Active Directory Server. |
| Cannot set Fixed Callback without Callback number. Callback number not found in the request. | When you select Callback Settings as Fixed Callback, you must specify the Callback Number.                                                                                                                              |
| Error setting the RAS attribute RAS attribute name. Error reading RAS info.  | Ensure that: 
  - The user account under which the adapter is running has administrator rights to the Active Directory Server. 
  - The RAS service is running on the Domain Controller. |
| Not a valid IPv4 address.                                                    | The IP address specified for the Static IPv4 Address is in an incorrect format. Specify the IP address in the IPv4 format.                                                                                             |
### Table 18. Troubleshooting the Active Directory Adapter errors (continued)

<table>
<thead>
<tr>
<th>Error message</th>
<th>Corrective action</th>
</tr>
</thead>
</table>
| Agent ADAgent is not installed.                         | This error occurs when an attempt is made to run the certTool utility by running the following command: CertTool -agent ADAgent  
Ensure that:  
• The user who runs the certTool utility has administrator permissions.  
• You disabled the User Account Control (UAC) security feature before you run the certTool utility on the workstation where the adapter is installed. |
| Home Directory will not be created. Home directory management is disabled. | Set the adapter registry keys CreateUNCHomeDirectories and ManageHomeDirectories to TRUE to:  
• Create a home directory  
• Create home directory share  
• Set share access  
• Set home directory NTFS access for a user account. For more information about creating the home directory and modifying the home directory attribute, see Active Directory Adapter User Guide. |
| Cannot create share share name. Home directory management is disabled. | For extended attribute of type DNWithBinary, verify that value given in the binary value contains only hexadecimal character. Valid characters are numerals 0 through 9 and letters A through F. The value can be a combination of valid numerals and letters. |
| Cannot set share access. Home directory management is disabled. | For extended attribute of type DNWithBinary, verify that value given in the binary value contains only hexadecimal character. Valid characters are numerals 0 through 9 and letters A through F. The value can be a combination of valid numerals and letters. |
| Cannot set NTFS access. Home directory management is disabled. | For extended attribute of type DNWithBinary, verify that value given in the binary value contains only hexadecimal character. Valid characters are numerals 0 through 9 and letters A through F. The value can be a combination of valid numerals and letters. |
| Value specified is not in the proper format.           | Ensure that the value format of extended attribute of type DNWithBinary is $B:\text{char count}:\text{binary value:object DN}$                                                                                         |
| Value specified for the attribute does not start with character ‘B’. | Ensure that value specified for extended attribute of type DNWithBinary is start with the character ‘B’ only.                                                                                                      |
| Value given after ‘B:’ is not correct. Expected value is the total number of Hexadecimal Digit count | For extended attribute of type DNWithBinary, verify that value given for the char count is the total number of Hexadecimal Digit count. Ensure that it does not contain any alphabetical characters or any special characters. |
| Hexadecimal value does not contain the number of characters specified in the character count. | For extended attribute of type DNWithBinary, verify that total hexadecimal digit count specified in the char count is equal to number of hexadecimal characters. |
| Wrong Digit in Hex String.                             | For extended attribute of type DNWithBinary, verify that value given in the binary value contains only hexadecimal character. Valid characters are numerals 0 through 9 and letters A through F. The value can be a combination of valid numerals and letters. |
| Value is not set on resource due to invalid constraint. | This error occurs when the specified value for the extended attribute of type DNWithBinary violates any constraint associated with that attribute. For example, some constraints might be:  
• The object DN in the value must be a distinguished name of existing user object.  
• The maximum or minimum number of bits in the hexadecimal value.  
Ensure that the specified value for the attribute does not violate any constraints. |
<p>| Hexadecimal value should always contain even number of characters. | For extended attribute of type DNWithBinary, verify that value given in the binary value contains an even number of hexadecimal characters. |</p>
<table>
<thead>
<tr>
<th>Error message</th>
<th>Corrective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute can be set only if Mailbox is enabled for Unified Messaging.</td>
<td>Ensure that valid values of both UMMailbox Policy and UM Addresses(Extensions) are specified in the request to enable the user for Unified Messaging.</td>
</tr>
<tr>
<td>Attribute Operation Type is not supported.</td>
<td>Ensure that the value specified for UM Addresses (Extensions) is not of operation type, MODIFY.</td>
</tr>
<tr>
<td>Attribute cannot be set. Mailbox is Disabled for Unified Messaging.</td>
<td>Ensure that the request does not contain Unified Messaging attributes with operation ADD or MODIFY when the MailBox of the user is disabled for Unified Messaging.</td>
</tr>
<tr>
<td>Attribute cannot be set. Error occurred while trying to Disable MailBox for</td>
<td>This error occurs if disable Unified Messaging is failed and if request contains UM Addresses (Extensions) attribute with operation types ADD or MODIFY.</td>
</tr>
<tr>
<td>Unified Messaging.</td>
<td></td>
</tr>
<tr>
<td>Attribute cannot be delete. Error occurred while trying to Disable MailBox</td>
<td>This error occurs if disable Unified Messaging is failed and if the request contains UM Addresses (Extensions) attribute with operation type DELETE.</td>
</tr>
<tr>
<td>for Unified Messaging.</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 11. Language package installation for the Active Directory Adapter

The adapters use a separate language package from the IBM Security Identity Manager.

See the IBM Security Identity Manager library and search for information about installing the adapter language pack.
Chapter 12. Updates for the Active Directory Adapter or the Adapter Development Kit (ADK)

You can either update the Active Directory Adapter or the Adapter Development Kit (ADK).

The ADK is the base component of the adapter. While all adapters have the same ADK, the remaining adapter functionality is specific to the managed resource.

Updating an adapter is only supported for the current IBM Security Identity Manager release. If your current adapter is version 5.x, you must uninstall the adapter first.

If only a code fix has been made to the ADK, instead of upgrading the entire adapter, you can upgrade just the ADK to the newer version. See "Updating the ADK" on page 96.

Updating the Active Directory Adapter

You can update the Active Directory Adapter.

About this task

For adapter versions 6.x and later, use the adapter update option if you want to keep the adapter configuration (registry keys and certificates) unchanged.

If the update installation option is selected, the path of the existing installed adapter is required. The installer replaces the binary files and the DLLs of the adapter and the ADK. The installer does not prompt for any configuration information during an update installation.

Note: Adapter-related registry keys are not modified. The update installation does not create an additional service for the adapter.

When you update to a higher version of the adapter, first install the new version of the adapter before you uninstall the old version. Installing the update in this sequence maintains all of your current configuration settings, the certificate, and private key. When you install the adapter, specify the same installation directory where the previous adapter was installed. For more information about installing the adapter, see Chapter 4, "Adapter installation," on page 11.

To update an existing adapter, complete the following steps:

Procedure

1. Stop the Active Directory Adapter service.
2. Install the new version of the adapter.
   - When the upgraded adapter starts for the first time, new log files are created, replacing the old files.
   - The adapter installer allows an update installation of the adapter, for adapters versions 6.0 or later.
Upgrading the Windows Active Directory in graphical user interface mode

Use the adapter update option, if you want to keep the adapter configuration (registry keys and certificates) unchanged.

**About this task**

If the update installation option is selected, the installer detects the path of the existing installed adapter. If no prior installation of the adapter is found on the system, the installer displays an error message. The installer replaces the binary files and the DLLs of the adapter and the ADK. The installer does not prompt for any configuration information during an update installation.

**Note:** Adapter-related registry keys are not modified. The update installation does not create a service for the adapter.

To maintain your current configuration settings, and the certificate and private key during an update, do not uninstall the old version of the adapter. For more information about installing the adapter, see “Installing the adapter” on page 11.

**Procedure**

1. Downloaded the installation software from Passport Advantage.
   a. Create a temporary directory on the computer on which you want to install the software.
   b. Extract the contents of the compressed file into the temporary directory.
2. Run the SetupAD64.exe file in the temporary directory to start the installation program.
3. Select the language and click OK to display the Introduction window.
5. Select **Update installation** option and click Next.

   **Note:** The adapter must exist, if you want to perform an update installation. If it does not exist, the software generates the following message: *Update not supported when the adapter is not previously installed. Cannot perform Update Installation. IBM Tivoli Windows Active Directory Adapter (64 Bit) is not installed on this machine. Please select Full Installation.* The adapter displays the path of the adapter installation that is to be updated.
6. Click OK to view the pre-Installation Summary window.
7. Review the installation settings on the pre-Installation Summary window and click Install.
8. Click Done on the Install Complete window.

Upgrading Windows Active Directory in silent mode by using command-line parameters

You can use the `-i` silent option to update the adapter in silent mode.

**About this task**

**Note:** If you install adapter in silent mode, the uninstaller runs in silent mode irrespective of whether you are using `-i` silent option.
The installer refers to the adapter registry keys to detect if the adapter is installed on the system where you are running the command. The installer updates the adapter only if it successfully detects a prior installation of the adapter on the system. If no prior installation is found on the system, the installation ends. A log file IBM_Tivoli_Windows_Active_Directory_Adapter_(64_Bit)_InstallLog is generated with this information in the Desktop.

**Note:** When performing an update installation the -DUSER_INSTALL_DIR parameter must not be used.

**Procedure**

Issue one of the following commands on a single line:

- SetupAD64.exe -i silent -DLICENSE_ACCEPTED=TRUE
  -DUSER_INPUT_INSTALL_TYPE_1=
  -DUSER_INPUT_INSTALL_TYPE_2="Update Installation"
  -DUSER_INPUT_INSTALL_TYPE_BOOLEAN_1=0
  -DUSER_INPUT_INSTALL_TYPE_BOOLEAN_2=1

- SetupAD64.exe -i silent -DLICENSE_ACCEPTED=TRUE
  -DUSER_INPUT_INSTALL_TYPE_BOOLEAN_1=0
  -DUSER_INPUT_INSTALL_TYPE_BOOLEAN_2=1

---

**Upgrading Windows Active Directory in silent mode by using a response file**

You can use response file to provide inputs during silent installation.

**Procedure**

1. Use one of these actions to create a response file.
   - Generate a response file by issuing the command:
     
     ```
     SetupAD64.exe -r "Full path of response file"
     ```

     This command runs the installer in interactive mode and installs the adapter. After the installation completes, the file specified as "Full path of response file" is created. The file contains the required parameters.

   **Note:** If you are running this command to generate only the response file, you must uninstall the adapter by using the uninstaller.

   - Manually create a response file:
     Use a text editor to create a text file. For example create a file WinAD64InstallParameters.txt, with the following content:

     ```
     #Has the license been accepted
     LICENSE_ACCEPTED=TRUE

     #Select Install Type
     USER_INPUT_INSTALL_TYPE_1=
     USER_INPUT_INSTALL_TYPE_2="Update Installation"
     USER_INPUT_INSTALL_TYPE_BOOLEAN_1=0
     USER_INPUT_INSTALL_TYPE_BOOLEAN_2=1
     ```

2. Issue the command:

   ```
   SetupAD64.exe -i silent -f "Full path of response file"
   ```

   For example:

   ```
   SetupAD64.exe -i silent -f "C:\WinAD64InstallParameters.txt"
   ```
3. Restart the workstation.

Updating the ADK

You can use the ADK update program to update the ADK portion of the adapters that are currently installed on a workstation. You can install just the ADK, and not the entire adapter.

About this task

The ADK consists of the runtime library, filtering, and event notification functions, protocol settings, and logging information. The remainder of the adapter contains the Add, Modify, Delete, and Search functions. While all adapters have the same ADK, the remaining function is specific to the managed resource. As part of the ADK update, the ADK library and the DAML protocol library are updated. In addition, the agentCfg and certTool binary files are updated.

Note: Upgrading the ADK from only versions 6.0 or a later version is supported.

Before updating the ADK files, the update program checks the current version of the ADK. If the current level is higher than what you are attempting to install, a warning message is displayed.

To update the Active Directory Adapter ADK on a Windows based operating system, complete the following steps:

Procedure

1. Download the ADK update program compressed file from the IBM website.
2. Extract the contents of the compressed file into a temporary directory.
3. Stop the Active Directory Adapter service.
4. Start the update program by using the adkinst_win64.exe file in the temporary directory. For example, select Run from the Start menu, and type C:\TEMP\adkinst_win64.exe in the Open field.
   If no adapter is installed, you receive the following error message, and the program exits:
   No Agent Installed - Cannot Install ADK.
5. In the Welcome window, click Next.
6. In the Installation Information window, click Next to begin the installation.
7. In the Install Completed window, click Finish to exit the program.

Upgrading the adapter profile from an earlier version of IBM Security Identity Manager

When you upgrade the IBM Security Identity Manager server to version 6.0, perform the following steps to install the Active Directory Adapter version 5.0 or version 5.1.

About this task

The Active Directory Adapter version 6.0 supports group management tasks, such as adding, modifying, and deleting Active Directory groups. To support this feature, the 5.1 adapter profile and the adapter are modified; however, they are not compatible with the adapter version 5.0 or 4.6.
The earlier version of the adapter functions correctly on IBM Security Identity Manager version 5.1 during the upgrade; however, group management is not available. Support for the 5.0 or 4.6 versions of the adapter that run on IBM Security Identity Manager version 5.1 is limited to the upgrade period only.

Perform the following steps to install the Active Directory Adapter version 6.0.

**Procedure**

1. Create a backup of your directory schema and objects.
2. Run the upgradeGroups tool without the update parameter to verify that the environment is correct.
3. Run the upgradeGroups tool with the update parameter to update the Active Directory Adapter group object class (erADGroup) to make it compatible with the 6.0 adapter profile.
4. Import the version 5.0 or 5.1 adapter profile on IBM Security Identity Manager. For specific information, see "Importing the adapter profile into the IBM Security Identity Manager server" on page 13.
5. Install version 6.0 of the adapter. For specific procedures, see "Installing the adapter" on page 11 and the adapter Release Notes.

**Note:** Ensure that you select the Full Installation option during the adapter installation.

6. Perform Support data reconciliation or a full reconciliation operation.

**The upgradeGroups tool**

The upgradeGroups tool updates the IBM Security Identity Manager server.

The tool acts by:

- Creating and adding the following attributes to the erADGroup object class:
  - erADGroupSamAccountName: Unique group name used by the Active Directory
  - erADGroupDescription: Group description

- Updating all objects of the erADGroup class by:
  - Setting the value of the erADGroupSamAccountName attribute to the value of erADGroupCN.
  - Setting a value of the erADGroupDescription attribute to the value of description.
  - Deleting the object and creating it again by using erADGroupSamAccountName as the naming attribute.

- Removing the description (used for group description in earlier adapter version) attribute from the erADGroup object class.

**Note:** The upgradeGroups tool is packaged with the Active Directory Adapter package.

**Run the upgradeGroups tool**

Run the upgradeGroups tool to update the IBM Security Identity Manager server.

**About this task**

Before you run the upgradeGroups tool, ensure that:
You run the upgradeGroups tool on the workstation where the IBM Security Identity Manager server is installed.

The CLASSPATH includes itim_common.jar, tim_server.jar, jlog.jar, and IBM Security Identity Manager data directory. These jar files are located under the IBM Security Identity Manager lib directory.

You provide the IBM Security Identity Manager home directory and the key value AD on the command line.

You provide the update parameter only when the environment is correct.

**Note:** On a Windows operating system, run the command or the batch file from a command prompt to obtain the output of the tool.

Perform these steps:

**Procedure**

1. Create a batch file or a script file to run the tool. The updateAD.bat file has the following content:

```
set JAVA=C:\Program Files\IBM\WebSphere\AppServer\java\bin\java
set TIM_HOME=C:\Program Files\IBM\itim
set TIM_DATA=%TIM_HOME%\data %JAVA% -cp "%TIM_HOME%\lib\itim_common.jar";
"%TIM_HOME%\lib\itim_server.jar"; "%TIM_HOME%\lib\jlog.jar";
upgradeGroups.jar; "%TIM_DATA%" upgradeGroups "%TIM_HOME%" AD
```

2. The following command in the batch file verifies that the CLASSPATH and the IBM Security Identity Manager installation location are correct:

```
"%JAVA%" -cp "%TIM_HOME%\lib\itim_common.jar";
"%TIM_HOME%\lib\itim_server.jar"; "%TIM_HOME%\lib\jlog.jar";
upgradeGroups.jar; "%TIM_DATA%" upgradeGroups "%TIM_HOME%" AD
```

If the environment is correct, the tool generates a message **Verification OK**.

3. Rerun the tool with the update parameter to commit the changes as:

```
"%JAVA%" -cp "%TIM_HOME%\lib\itim_common.jar";
"%TIM_HOME%\lib\itim_server.jar"; "%TIM_HOME%\lib\jlog.jar";
upgradeGroups.jar; "%TIM_DATA%" upgradeGroups "%TIM_HOME%" AD update
```

AD is a required value for the Active Directory Adapter and provides the update parameter to commit the LDAP changes.

You can modify the updateAD.bat file according to your IBM Security Identity Manager installation location and operating system. If there are any issues, the tool displays the appropriate error messages.

**Note:**

- The DOS batch file is supplied with the upgradeGroups tool.
- The upgradeGroups tool uses the value of the erADGroupCN attribute for the erADGroupSamAccountName attribute to replace a group object on IBM Security Identity Manager. When you perform support data reconciliation or full reconciliation, the access on groups that do not have the same value for erADGroupCN attribute and erADGroupSamAccountName attribute on the Active Directory is deleted from IBM Security Identity Manager.
Chapter 13. Adapter uninstallation

Before you remove the adapter, inform your users that the adapter is unavailable. If the server is taken offline, adapter requests that were completed might not be recovered when the server is back online.

Perform these steps:
1. “Uninstalling the adapter from the target server”
2. “Adapter profile removal from the IBM Security Identity Manager server”

Uninstalling the adapter from the target server

You can uninstall the adapter from the target server.

Procedure
1. Stop the adapter service.
2. Run the uninstaller. To run the uninstaller:
   a. Navigate to the adapter home directory. For example, Tivoli\agents\adaptername\Uninstall IBM Windows AD Adapter for ITIM (64 Bit)
   b. Double click the Uninstall IBM Windows AD Adapter for ITIM (64 Bit).exe file.
   c. On the Uninstall IBM Windows AD Adapter for ITIM (64 BIT) window, click Uninstall.
   d. On the Uninstall Complete window, click Done.

Adapter profile removal from the IBM Security Identity Manager server

Before you remove the adapter profile, ensure that no objects exist on your IBM Security Identity Manager server that reference the adapter profile.

Examples of objects on the IBM Security Identity Manager server that can reference the adapter profile are:
• Adapter service instances
• Policies referencing an adapter instance or the profile
• Accounts

For specific information on how to remove the adapter profile, see the online help or the IBM Security Identity Manager product documentation.
Appendix A. Files

You can configure several adapter-specific files.

This appendix includes information about the files that are associated with the Active Directory Adapter:
- “schema.dsml file”
- “CustomLabels.properties file” on page 104

schema.dsml file

The schema.dsml file contains all of the attributes that are common to all adapters.

This common file also contains IBM Security Identity Manager server attributes that can be used by any adapter. The schema.dsml file defines all of the classes used by the adapter. The classes are used to declare accounts, services, and supporting data.

The schema.dsml file defines the attributes and objects that the adapter supports and uses to communicate with the IBM Security Identity Manager server. All attributes must be unique; therefore, they are assigned an OID.

The OID is defined with the <object-identifier>...</object-identifier> tags.

The schema.dsml file has the following format:

```
<?xml version="1.0" encoding="UTF-8"?>
<directory-schema>
  <!-- Schema supported by the Windows adapter. -->
  <!-- erADString1-->
  <attribute-type single-value="true">
    <name>erADString1</name>
    <description/>
    <object-identifier>1.3.6.1.4.1.6054.3.125.2.100</object-identifier>
    <syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
  </attribute-type>
  <!-- erADInteger-->  
  <!-- erADDate-->  
  <attribute-type single-value="true">  
    <name>erADInteger</name>  
    <description/>  
    <object-identifier>1.3.6.1.4.1.6054.3.125.2.101</object-identifier>
    <syntax>1.3.6.1.4.1.1466.115.121.1.27</syntax>
  </attribute-type>
  <attribute-type single-value="true">  
    <name>erADDate</name>  
    <description/>  
    <object-identifier>1.3.6.1.4.1.6054.3.125.2.102</object-identifier>
  </attribute-type>
</directory-schema>
```

© Copyright IBM Corp. 2012, 2013
The sections of this schema file are described in the following sections.

**Object identifier**

The IBM Security Identity Manager server uses LDAP directory services to add, delete, modify, and search IBM Security Identity Manager data.

Each data item in an LDAP directory server must have a unique OID. Each attribute and class that is defined in the schema.dsml file in IBM Security Identity Manager has an OID.

OIDs have the following syntax:

```
enterprise ID.product ID.adapter ID.object ID.instance ID
```

The enterprise ID is always 1.3.6.1.4.1.6054 for IBM.

The product ID is always 3 because these schema.dsml files are used with adapters.

The adapter ID is 125 for the Active Directory Adapter.

The object ID is 2. An attribute uses 2 as the object ID.

The instance ID is a sequential number of the object.
Attribute definition

Before you define unique attributes for the adapter, ensure that the attribute does not exist in the common schema.dsml file.

The following example defines an attribute:

<!-- *********************************************** -->
<!-- erSampleHome -->
<!-- *********************************************** -->
<attribute-type single-value = "true">
  <name>erSampleHome</name>
  <description>User home directory</description>
  <object-identifier>1.3.6.1.4.1.6054.3.125.2.100</object-identifier>
  <syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
</attribute-type>

Comment lines are denoted by the <!-- ... --> markers.

The attribute type is defined as single-value or multivalue. A single-value attribute is denoted by the line: <attribute-type single-value ="true">. To denote a multivalued attribute, change the true value to false.

The name of the attribute that is used by the IBM Security Identity Manager server is defined in the schema. To simplify the tracking of new Active Directory Adapter attributes, use erAD as the preface for all new attributes, so that they can be easily identified in your Windows Active Directory. When attributes have already been defined in the Windows Active Directory, and they do not conflict with existing attributes, they can be used without changing their names.

The description of the attribute is denoted by the <description>...</description> tags.

The OID is defined using the <object-identifier>...</object-identifier> tags. Because OIDs are already assigned to the existing, standard attributes, the OID can be copied from the last attribute in the list. Increment the last number by a value of one for each new attribute that you add to the schema.dsml file.

The data type is defined using the <syntax>...</syntax> tags. The following table lists various data types and the value that you specify in the syntax tags.

**Table 19. Data types and values for syntax tags**

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit string</td>
<td>1.3.6.1.4.1.1466.115.121.1.6</td>
</tr>
<tr>
<td>Boolean</td>
<td>1.3.6.1.4.1.1466.115.121.1.7</td>
</tr>
<tr>
<td>Directory String</td>
<td>1.3.6.1.4.1.1466.115.121.1.15</td>
</tr>
<tr>
<td>UTC Coded Time</td>
<td>1.3.6.1.4.1.1466.115.121.1.24</td>
</tr>
<tr>
<td>Integer</td>
<td>1.3.6.1.4.1.1466.115.121.1.27</td>
</tr>
</tbody>
</table>
Classes

At least one account class and one service class must be defined in the schema.dsml file.

Each class requires at least one attribute to identify the class: a name attribute. Additional attributes might be required depending on the class defined.

The following syntax defines a class:

```xml
<class superior="top">
  <name> ... </name>
  <description> ... </description>
  <object-identifier> ... </object-identifier>
  <attribute ref = "..." required = "true" />
  <attribute ref = "..." required = "true" />
</class>
```

To make an attribute optional for a class, change required = "true" to required = "false" in the `<attribute ref>` tag.

An account class defines the attributes that are used to describe an account. An account class must be defined in the schema.dsml file.

The following example defines an account class:

```xml
<class superior="top">
  <name>erSampleAccount</name>
  <description>Sample Account</description>
  <object-identifier>1.3.6.1.4.1.6054.3.125.1.101</object-identifier>
  <attribute ref = "eruid" required = "true" />
  <attribute ref = "erAccountStatus" required = "false" />
  <attribute ref = "erSampleGroups" required = "false" />
  <attribute ref = "erSampleHome" required = "false" />
  <attribute ref = "erSampleDesc" required = "false" />
  <attribute ref = "erPassword" required = "false" />
</class>
```

In this example, the class name is `erSampleAccount` and the only required attribute is `eruid`. However, note that `erAccountStatus` is a required attribute to suspend or restore accounts.

CustomLabels.properties file

The CustomLabels.properties file is a text file that defines the labels on the form for the adapter.

The syntax for the information in the file is:

```plaintext
attribute=text
```

where `attribute` is the same attribute defined in the `schema.dsml` file and `text` is the label that appears on the form in the IBM Security Identity Manager user interface for the account.

The `attribute` must be in lowercase. This requirement comes from the IBM Security Identity Manager server.
Appendix B. Adapter attributes

As part of the adapter implementation, a dedicated account for IBM Security Identity Manager to access the Active Directory Server is created on the Active Directory Server.

The adapter consists of files and directories that are owned by the IBM Security Identity Manager account. These files establish communication with the IBM Security Identity Manager server.

Attribute descriptions

The IBM Security Identity Manager server communicates with the adapter by using attributes in transmission packets that are sent over a network.

The combination of attributes depends on the type of action that the IBM Security Identity Manager server requests from the adapter.

The next table lists the account form attributes that the adapter uses.

<table>
<thead>
<tr>
<th>Directory server attribute</th>
<th>Description</th>
<th>Data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn</td>
<td>Specifies the full name of the user (given name and surname)</td>
<td>String</td>
</tr>
<tr>
<td>erADFullName</td>
<td>Specifies the full name of the user (given name and surname)</td>
<td>String</td>
</tr>
<tr>
<td>description</td>
<td>Specifies the description for the user.</td>
<td>String</td>
</tr>
<tr>
<td>erADAllowEncryptedPassword</td>
<td>Specifies whether encrypted passwords are allowed.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADBadLoginCount</td>
<td>Specifies the number of invalid login attempts that are allowed since the last reset.</td>
<td>Long</td>
</tr>
<tr>
<td>erADBasePoint</td>
<td>Specifies the DN of the domain name, extended to allow any base point.</td>
<td>String</td>
</tr>
<tr>
<td>erADCACallbackNumber</td>
<td>Specifies the callback number for remote access services that is used when DialinCallBack is set to fixed.</td>
<td>String</td>
</tr>
<tr>
<td>erADCannotBeDelegated</td>
<td>Specifies that this account cannot be assigned for delegation by another account.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADContainer</td>
<td>Specifies the Relative Distinguished Name (RDN) of a container object in which to create the user account. The container is relative to the domain.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADContainerCN</td>
<td>Specifies the short name for the container object.</td>
<td>String</td>
</tr>
<tr>
<td>Directory server attribute</td>
<td>Description</td>
<td>Data type</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>erADContainerDN</td>
<td>Specifies the full DN for the container object.</td>
<td>String</td>
</tr>
<tr>
<td>erADContainerRDN</td>
<td>Specifies the container RDN.</td>
<td>String</td>
</tr>
<tr>
<td>erADCountyCode</td>
<td>Specifies the country where the user resides.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADDialinCallback</td>
<td>Sets the Dial-in Callback for the user.</td>
<td>Integer</td>
</tr>
<tr>
<td></td>
<td>1 - No Callback</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 - Fixed callback using erADcallbackNumber</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3 - This option is not used</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4 - User supplied callback</td>
<td></td>
</tr>
<tr>
<td>erADDisplayName</td>
<td>Specifies the Active Directory displayName attribute.</td>
<td>String</td>
</tr>
<tr>
<td>erADDistinguishedName</td>
<td>Specifies the distinguished name of the account on the Active Directory.</td>
<td>String</td>
</tr>
<tr>
<td>erADDomainPassword</td>
<td>Specifies the password for the user ID that is used to connect to the Active Directory.</td>
<td>String</td>
</tr>
<tr>
<td>erADDomainUser</td>
<td>Specifies the user ID that is used when connecting to the Active Directory.</td>
<td>String</td>
</tr>
<tr>
<td>erADEActiveSyncEnabled</td>
<td>Specifies whether to enable or disable Active Sync.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADEAlias</td>
<td>Specifies the alias for the Exchange Mailbox.</td>
<td>String</td>
</tr>
<tr>
<td>erADEAllowAddressList</td>
<td>Specifies a list of email IDs that the user accepts mail from.</td>
<td>String</td>
</tr>
<tr>
<td>erADEAssociatedExtAcc</td>
<td>Specifies whether the user has associated external account permission.</td>
<td>Integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erADEAutoGenEmailAddr</td>
<td>Specifies whether the recipient update services updates the email address.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADEChgPermissions</td>
<td>Specifies whether to change the user's Mailbox permission.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADEDaysBeforeGarbage</td>
<td>Specifies the number of days that deleted mail is retained before it is permanently deleted.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADEDelegates</td>
<td>Specifies the list of all users that have access to the Exchange Mailbox.</td>
<td>String</td>
</tr>
<tr>
<td>erADEDelMailboxStorage</td>
<td>Specifies whether the user has delete Mailbox storage permission.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADEEnableRetentionHold</td>
<td>Specifies whether to enable or disable Retention Hold.</td>
<td>Boolean</td>
</tr>
<tr>
<td>Directory server attribute</td>
<td>Description</td>
<td>Data type</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td>erADEEnableStoreDeflts</td>
<td>Specifies whether to use only default store values for storage limits, or to use other properties that pertain to the Mailbox.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADEEndRetentionHold</td>
<td>Specifies the date to stop retention hold.</td>
<td>Date</td>
</tr>
<tr>
<td>erADEExtension1</td>
<td>Specifies a user-defined extension attribute.</td>
<td>String</td>
</tr>
<tr>
<td>erADEExtension2</td>
<td>Specifies a user-defined extension attribute.</td>
<td>String</td>
</tr>
<tr>
<td>erADEExtension3</td>
<td>Specifies a user-defined extension attribute.</td>
<td>String</td>
</tr>
<tr>
<td>erADEExtension4</td>
<td>Specifies a user-defined extension attribute.</td>
<td>String</td>
</tr>
<tr>
<td>erADEExtension5</td>
<td>Specifies a user-defined extension attribute.</td>
<td>String</td>
</tr>
<tr>
<td>erADEExtension6</td>
<td>Specifies a user-defined extension attribute.</td>
<td>String</td>
</tr>
<tr>
<td>erADEExtension7</td>
<td>Specifies a user-defined extension attribute.</td>
<td>String</td>
</tr>
<tr>
<td>erADEExtension8</td>
<td>Specifies a user-defined extension attribute.</td>
<td>String</td>
</tr>
<tr>
<td>erADEExtension9</td>
<td>Specifies a user-defined extension attribute.</td>
<td>String</td>
</tr>
<tr>
<td>erADEExtension10</td>
<td>Specifies a user-defined extension attribute.</td>
<td>String</td>
</tr>
<tr>
<td>erADEExtension11</td>
<td>Specifies a user-defined extension attribute.</td>
<td>String</td>
</tr>
<tr>
<td>erADEExtension12</td>
<td>Specifies a user-defined extension attribute.</td>
<td>String</td>
</tr>
<tr>
<td>erADEExtension13</td>
<td>Specifies a user-defined extension attribute.</td>
<td>String</td>
</tr>
<tr>
<td>erADEExtension14</td>
<td>Specifies a user-defined extension attribute.</td>
<td>String</td>
</tr>
<tr>
<td>erADEExtension15</td>
<td>Specifies a user-defined extension attribute.</td>
<td>String</td>
</tr>
<tr>
<td>erADEForwardingStyle</td>
<td>Specifies whether email is also delivered to an alternate email address.</td>
<td>String</td>
</tr>
<tr>
<td>erADEForwardTo</td>
<td>Specifies the URL where email is to be forwarded.</td>
<td>String</td>
</tr>
<tr>
<td>erADEFullMailboxAccess</td>
<td>Specifies whether the user has full Mailbox access permission.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADEGarbageAfterBckp</td>
<td>Specifies whether deleted messages can be permanently deleted after the Mailbox is backed up.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADEHardLimit</td>
<td>Specifies the maximum Mailbox size in KB when sending and receiving email is disabled.</td>
<td>Integer</td>
</tr>
<tr>
<td>Directory server attribute</td>
<td>Description</td>
<td>Data type</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>erADEHideFromAddrBk</td>
<td>Specifies whether the address is displayed in the address book.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADEHomeMDB</td>
<td>Specifies the URL of the store for the recipient.</td>
<td>String</td>
</tr>
<tr>
<td>erADEIncomingLimit</td>
<td>Specifies the maximum size in KB of a message sent to the recipient.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADELanguages</td>
<td>Specifies an array of language names for the user.</td>
<td>String</td>
</tr>
<tr>
<td>erADEMailboxStore</td>
<td>Specifies the name of the mail store that holds the user Mailbox.</td>
<td>Binary</td>
</tr>
<tr>
<td>erADEMailStoreCN</td>
<td>Specifies the mail store common name (CN).</td>
<td>String</td>
</tr>
<tr>
<td>erADEMailStoreDN</td>
<td>Specifies the mail store DN.</td>
<td>Binary</td>
</tr>
<tr>
<td>erADEMailStoreGN</td>
<td>Specifies the mail store group name.</td>
<td>String</td>
</tr>
<tr>
<td>erADEMailStoreRDN</td>
<td>Specifies the mail store object relative directory name (RDN) attribute.</td>
<td>Binary</td>
</tr>
<tr>
<td>erADEAPIEnabled</td>
<td>Specifies whether to enable or disable MAPI support.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADEEmployeeID</td>
<td>Specifies the user's employee identifier.</td>
<td>String</td>
</tr>
<tr>
<td>erADEOutgoingLimit</td>
<td>Specifies the maximum size in KB of a message sent from the recipient.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADEOutlookWebAccessEnabled</td>
<td>Specifies whether to enable or disable Outlook Web Access.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADEOverQuotaLimit</td>
<td>Specifies the maximum size of a Mailbox in KB before sending messages is suspended.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADEOverrideGarbage</td>
<td>Specifies whether the store is prevented from permanently deleting messages.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADEProxyAddresses</td>
<td>Specifies a list of proxy addresses for the recipient.</td>
<td>String</td>
</tr>
<tr>
<td>erADEReadPermissions</td>
<td>Specifies whether the user has read Mailbox permission.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADERecipientLimit</td>
<td>Specifies the maximum number of people to whom the recipient can send email.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADERstrctAdrsLs</td>
<td>Specifies a list of email addresses to reject mail from.</td>
<td>String</td>
</tr>
<tr>
<td>erADEServerName</td>
<td>Specifies the name of the Microsoft Exchange Server.</td>
<td>String</td>
</tr>
<tr>
<td>erADEShowInAddrBook</td>
<td>Specifies the list of address books that the user is a member of.</td>
<td>String</td>
</tr>
<tr>
<td>Directory server attribute</td>
<td>Description</td>
<td>Data type</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>erADESMTPEmail</td>
<td>Specifies the primary SMTP address that is used for the recipient.</td>
<td>String</td>
</tr>
<tr>
<td>erADEStartRetentionHold</td>
<td>Specifies the date to start retention hold.</td>
<td>Date</td>
</tr>
<tr>
<td>erADEStoreQuota</td>
<td>Specifies a limit when the recipient receives a warning for exceeding their mail file storage allocation.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADETakeOwnership</td>
<td>Specifies whether the user has take Mailbox ownership permission.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADETargetAddress</td>
<td>Specifies the external email address to be used by the user.</td>
<td>String</td>
</tr>
<tr>
<td>erADEX400Email</td>
<td>Specifies the primary X.400 address that is used for the recipient.</td>
<td>String</td>
</tr>
<tr>
<td>erADExpirationDate</td>
<td>Specifies the date and time after which the user cannot log in.</td>
<td>Date</td>
</tr>
<tr>
<td>erADfax</td>
<td>Specifies the fax numbers of the user.</td>
<td>String</td>
</tr>
<tr>
<td>erADGroupCN</td>
<td>Specifies the short name for the group object.</td>
<td>String</td>
</tr>
<tr>
<td>erADGroupDN</td>
<td>Specifies the full DN for the group object.</td>
<td>String</td>
</tr>
<tr>
<td>erADHomeDir</td>
<td>Specifies a null-terminated string that contains the path of the user's home directory. This string can specify a local path or a UNC path. For example: \machine\share\path</td>
<td>String</td>
</tr>
<tr>
<td>erADHomeDirAccessShare</td>
<td>Specifies the user access level on the share.</td>
<td>String</td>
</tr>
<tr>
<td>erADHomeDirDrive</td>
<td>Specifies the drive letter to assign to a UNC-based home directory.</td>
<td>String</td>
</tr>
<tr>
<td>erADHomeDirNtfsAccess</td>
<td>Specifies the NTFS security level for the home directory of the user.</td>
<td>String</td>
</tr>
<tr>
<td>erADHomeDirShare</td>
<td>Specifies the name of the share to create for home directory. Append a dollar sign ($) to create a hidden share.</td>
<td>String</td>
</tr>
<tr>
<td>erADHomePage</td>
<td>Specifies the URL for the home page of the user.</td>
<td>String</td>
</tr>
<tr>
<td>erADInitial</td>
<td>Specifies the middle initials of the name of the user.</td>
<td>String</td>
</tr>
<tr>
<td>erADIsAccountLocked</td>
<td>Specifies whether the account is locked because of intruder detection.</td>
<td>Boolean</td>
</tr>
<tr>
<td>Directory server attribute</td>
<td>Description</td>
<td>Data type</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>erADLastFailedLogin</td>
<td>Specifies the date and time of the last failed network login.</td>
<td>Date</td>
</tr>
<tr>
<td>erADLastLogoff</td>
<td>Specifies the date and time of the last network logoff.</td>
<td>Date</td>
</tr>
<tr>
<td>erADLastLogon</td>
<td>Specifies the date and time of the last successful network login.</td>
<td>Date</td>
</tr>
<tr>
<td>erADLoginScript</td>
<td>Specifies the login script path.</td>
<td>String</td>
</tr>
<tr>
<td>erADLoginWorkstations</td>
<td>Specifies a comma-separated list of addresses or names of workstations from which the user can log in to.</td>
<td>String</td>
</tr>
<tr>
<td>erADManager</td>
<td>Specifies the user ID for the user's manager.</td>
<td>String</td>
</tr>
<tr>
<td>erADNamePrefix</td>
<td>Specifies the title of the user, for example Ms. or Mr.</td>
<td>String</td>
</tr>
<tr>
<td>erADNameSuffix</td>
<td>Specifies the name suffix of the user, for example Jr., or III.</td>
<td>String</td>
</tr>
<tr>
<td>erADNoChangePassword</td>
<td>Specifies whether the user can change their password.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADOOfficeLocations</td>
<td>Specifies the office location.</td>
<td>String</td>
</tr>
<tr>
<td>erADOtherName</td>
<td>Specifies an additional name, for example, the middle name, for the user.</td>
<td>String</td>
</tr>
<tr>
<td>erADPasswordForceChange</td>
<td>Specifies whether to force a password change on next login.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADPasswordLastChange</td>
<td>Specifies the last time that the password was changed.</td>
<td>Date</td>
</tr>
<tr>
<td>erADPasswordMinimumLength</td>
<td>Specifies the minimum length of the password.</td>
<td>Long</td>
</tr>
<tr>
<td>erADPasswordNeverExpires</td>
<td>Specifies whether a password can never expire.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADPasswordRequired</td>
<td>Specifies whether the password is required.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADPrimaryGroup</td>
<td>Specifies the primary group ID.</td>
<td>String</td>
</tr>
<tr>
<td>erADPrimaryGrpTknt</td>
<td>Specifies the ID of the group that is used to set primary group.</td>
<td>String</td>
</tr>
<tr>
<td>erADRequireUniquePassword</td>
<td>Specifies whether a new password must be different from those passwords known through a password history.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADSmartCardRequired</td>
<td>Specifies whether a smart card is required for login.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADTrustedForDelegation</td>
<td>Specifies that the user can assign responsibility for management and administration of a portion of the domain namespace to another user, group, or organization.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADUPN</td>
<td>Specifies the principal name for the user account.</td>
<td>String</td>
</tr>
<tr>
<td>Directory server attribute</td>
<td>Description</td>
<td>Data type</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td>erADWTSAllowLogon</td>
<td>Specifies whether the user account is permitted to log on to a terminal server.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADWTSServerTimeout</td>
<td>Specifies what happens when the connection or idle timers expire or when a connection is lost due to a connection error.</td>
<td>Boolean, Long</td>
</tr>
<tr>
<td>erADWTSCallbackNumber</td>
<td>Citrix ICA clients must specify a null-terminated string that contains the phone number to use for callback connections.</td>
<td>String</td>
</tr>
<tr>
<td>erADWTSCallbackSettings</td>
<td>Citrix ICA clients must specify a value that indicates the configuration for dialup connections in which the terminal server hangs up and then calls back the client to establish the connection. Valid values indicate: 1 - The server prompts the user to enter a phone number, and calls the user back at that phone number. You can use the WtsCallbackNumber value to specify a default phone number. 2 - The server automatically calls the user back at the phone number specified by the WtsCallbackNumber value.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADWTSClientDefaultPrinter</td>
<td>RDP 5.0 clients and Citrix ICA clients must specify whether the client printer is the default printer.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADWTSClientDrives</td>
<td>Citrix ICA clients must specify whether the terminal server automatically establishes client drive mappings at login.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADWTSClientPrinters</td>
<td>RDP 5.0 clients and Citrix ICA clients must specify whether the terminal server automatically establishes client printer mappings at login.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADWTSHomeDir</td>
<td>Specifies a null-terminated string for the path of the home directory of the user for terminal server login. This string can specify a local path or a UNC path (\machine\share\path).</td>
<td>String</td>
</tr>
<tr>
<td>erADWTSHomeDirAccessShare</td>
<td>Specifies the user access level to the share on the WTS home directory.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADWTSHomeDirDrive</td>
<td>Specifies a null-terminated string for a drive letter to which the UNC path specified in the WtsHomeDir string is mapped.</td>
<td>String</td>
</tr>
<tr>
<td>erADWTSHomeDirNtfsAccess</td>
<td>Specifies the NTFS access to the home directory.</td>
<td>String</td>
</tr>
<tr>
<td>erADWTSHomeDirShare</td>
<td>Specifies the name of a share to create the WTS home directory. Append a dollar sign ($) to create a hidden share.</td>
<td>String</td>
</tr>
<tr>
<td>Directory server attribute</td>
<td>Description</td>
<td>Data type</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td>erADWTSInheritInitialProg</td>
<td>Specifies whether the client can specify the initial program. If not set, WtsInitialProgram is the only program the user can run. The terminal server logs off the user when the user exits that program.</td>
<td>Boolean</td>
</tr>
<tr>
<td>erADWTSInitialProgram</td>
<td>Specifies a null-terminated string for the path of the initial program that Terminal Services runs when the user logs in. If the WtsInheritInitialProgram value is 1, the initial program can be any program specified by the client.</td>
<td>String</td>
</tr>
<tr>
<td>erADWTSProfilePath</td>
<td>Specifies a null-terminated string for the path of the profile of the user for terminal server login.</td>
<td>String</td>
</tr>
<tr>
<td>erADWTSReconnectSettings</td>
<td>Specifies a value that indicates how a disconnected session for a user can be reconnected. Valid values indicate: 0 - The user can log in to any client computer to reconnect to a disconnected session. Sessions started at clients other than the system console cannot be connected to the system console. Sessions started at the system console cannot be disconnected. 1 - The user can reconnect to a disconnected session by logging on to the client computer used to establish the disconnected session. If the user logs on from a different client computer, the user gets a new login session.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADWTSRemoteHomeDir</td>
<td>Specifies the home directory of the user on the Windows Server.</td>
<td>String</td>
</tr>
<tr>
<td>erADWTSShadowSettings</td>
<td>RDP 5.0 clients and Citrix ICA clients must specify a value that indicates whether the user session can be shadowed. Shadowing allows a user to remotely monitor the on-screen operations of another user.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADWTSTimeoutConnections</td>
<td>Specifies a value that specifies the maximum connection duration, in milliseconds. One minute before the connection timeout interval expires, the user is notified of the pending disconnection. The user session is disconnected or terminated depending on the WtsBrokenTimeout value. Every time the user logs on, the timer is reset. A value of zero indicates that the connection timer is disabled.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADWTSTimeoutDisconnections</td>
<td>Specifies the maximum duration, in milliseconds, that a WTS retains a disconnected session before the login is terminated. A value of zero indicates that the disconnection timer is disabled.</td>
<td>Integer</td>
</tr>
<tr>
<td>Directory server attribute</td>
<td>Description</td>
<td>Data type</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>erADWTSTimeoutIdle</td>
<td>Specifies the maximum idle time, in milliseconds. If there is no keyboard or mouse activity for the specified interval, the user's session is disconnected or terminated depending on the WtsBrokenTimeout value. A value of zero indicates that the idle timer is disabled.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADWTSWorkingDir</td>
<td>Specifies a null-terminated string for the path of the working directory for the initial program</td>
<td>String</td>
</tr>
<tr>
<td>erCompany</td>
<td>Specifies the name of the company that the user works for.</td>
<td>String</td>
</tr>
<tr>
<td>erDepartment</td>
<td>Specifies the department within the company to which the user belongs.</td>
<td>String</td>
</tr>
<tr>
<td>erDivision</td>
<td>Specifies the division within a company (organization) that the employee belongs to.</td>
<td>String</td>
</tr>
<tr>
<td>erGroup</td>
<td>Specifies names of groups.</td>
<td>String</td>
</tr>
<tr>
<td>erLogonTimes</td>
<td>Specifies the time periods for each day of the week during which logins are permitted for the user. Represented as a table of Boolean values for the week, each indicating whether that time slot is a valid login time.</td>
<td>Byte array</td>
</tr>
<tr>
<td>erMaxStorage</td>
<td>Specifies the maximum amount of disk space, in KB, that the user can have.</td>
<td>Long</td>
</tr>
<tr>
<td>erPassword</td>
<td>Specifies the password for the user account.</td>
<td>String</td>
</tr>
<tr>
<td>erProfile</td>
<td>Specifies the path to the profile of the user.</td>
<td>String</td>
</tr>
<tr>
<td>eruid</td>
<td>Specifies the user ID</td>
<td>String</td>
</tr>
<tr>
<td>givenName</td>
<td>Specifies the given name of the user.</td>
<td>String</td>
</tr>
<tr>
<td>homePhone</td>
<td>Specifies the home telephone number of the user.</td>
<td>String</td>
</tr>
<tr>
<td>l</td>
<td>Specifies the user's city or location (shown as the lowercase letter 'l').</td>
<td>String</td>
</tr>
<tr>
<td>mail</td>
<td>Specifies the email address of the user.</td>
<td>String</td>
</tr>
<tr>
<td>mobile</td>
<td>Specifies the mobile telephone number of the user.</td>
<td>String</td>
</tr>
<tr>
<td>pager</td>
<td>Specifies the pager number of the user.</td>
<td>String</td>
</tr>
<tr>
<td>postalCode</td>
<td>Specifies the user's postal code for their address</td>
<td>String</td>
</tr>
<tr>
<td>postOfficeBox</td>
<td>Specifies the user's Post Office Box</td>
<td>String</td>
</tr>
<tr>
<td>sn</td>
<td>Specifies the surname of the user.</td>
<td>String</td>
</tr>
</tbody>
</table>
### Table 20. Attributes, descriptions, and corresponding data types (continued)

<table>
<thead>
<tr>
<th>Directory server attribute</th>
<th>Description</th>
<th>Data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>st</td>
<td>Specifies the state where the user resides.</td>
<td>String</td>
</tr>
<tr>
<td>street</td>
<td>Specifies the street address where the user resides.</td>
<td>String</td>
</tr>
<tr>
<td>telephonenumber</td>
<td>Specifies the work telephone number of the user.</td>
<td>String</td>
</tr>
<tr>
<td>title</td>
<td>Specifies the title of the user.</td>
<td>String</td>
</tr>
<tr>
<td>erADExDialin</td>
<td>Specifies the dial-in access of the user, Allowed, Denied, or Control Access through Remote Access policy.</td>
<td>String</td>
</tr>
<tr>
<td>erADLastLogonTimeStamp</td>
<td>Specifies the times stamp of last network logon.</td>
<td>Date</td>
</tr>
<tr>
<td>erADRADIUSFramedIPv4Addr</td>
<td>Specifies the IPv4 address that is statically assigned when the user dials in to the network.</td>
<td>String</td>
</tr>
<tr>
<td>erADGroupBasePoint</td>
<td>Specifies the DN of the domain name for group management.</td>
<td>String</td>
</tr>
<tr>
<td>erADGrpContainerCN</td>
<td>Specifies the short name for the group container object.</td>
<td>String</td>
</tr>
<tr>
<td>erADGrpContainerDN</td>
<td>Specifies the full DN for the group container object.</td>
<td>String</td>
</tr>
<tr>
<td>erADGrpContainerRDN</td>
<td>Specifies the group container RDN.</td>
<td>String</td>
</tr>
<tr>
<td>erADGrpContainerDescription</td>
<td>Specifies a brief description for the group container object.</td>
<td>String</td>
</tr>
<tr>
<td>erADGroupSamAccountName</td>
<td>Specifies the unique name for the group object.</td>
<td>String</td>
</tr>
<tr>
<td>erADGroupGUID</td>
<td>Specifies the GUID for the group object.</td>
<td>String</td>
</tr>
<tr>
<td>erADGroupDlEmail</td>
<td>Specifies the email address associated with the group object.</td>
<td>String</td>
</tr>
<tr>
<td>erADGroupDescription</td>
<td>Specifies a brief description of the group object.</td>
<td>String</td>
</tr>
<tr>
<td>erADGroupType</td>
<td>Specifies the type of the group object as Security or Distribution.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADGroupScope</td>
<td>Specifies the scope of the group object as Global, Local, or Universal.</td>
<td>Integer</td>
</tr>
<tr>
<td>erADGroupIsMemberOf</td>
<td>Specifies the groups of which the current group is a member of.</td>
<td>String</td>
</tr>
</tbody>
</table>

### Lync account form attributes

The adapter uses Lync account form attributes.

### Table 21. Attributes, descriptions, and corresponding data types

<table>
<thead>
<tr>
<th>Directory server attribute</th>
<th>Description</th>
<th>Data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>erADLyncSipAdr</td>
<td>Specifies SIP address of the user.</td>
<td>String</td>
</tr>
<tr>
<td>erADLyncenable</td>
<td>Specifies whether the Lync account is enabled or not for a user.</td>
<td>Boolean</td>
</tr>
</tbody>
</table>
Table 21. Attributes, descriptions, and corresponding data types (continued)

<table>
<thead>
<tr>
<th>Directory server attribute</th>
<th>Description</th>
<th>Data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>erADLyncRegpool</td>
<td>Specifies to which registrar pool user is assigned.</td>
<td>String</td>
</tr>
<tr>
<td>erADLyncTelephony</td>
<td>Sets the Telephony for the user.</td>
<td>Integer</td>
</tr>
<tr>
<td></td>
<td>1. PC to PC only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Audio/video disabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Enterprise voice</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Remote call control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Remote call control only</td>
<td></td>
</tr>
<tr>
<td>erADLyncLineUri</td>
<td>Specifies telephone number of the user.</td>
<td>String</td>
</tr>
<tr>
<td>erADLyncLineSerUri</td>
<td>Specifies line server URI of user.</td>
<td>String</td>
</tr>
<tr>
<td>erADLyncConfPolicy</td>
<td>Specifies the features and capabilities that can be used in a conference.</td>
<td>String</td>
</tr>
<tr>
<td>erADLyncCvPolicy</td>
<td>Specifies the policy name that contains information about which client version is able to connect to the Lync Server and also do updates if it is a Lync Client.</td>
<td>String</td>
</tr>
<tr>
<td>erADLyncPnPolicy</td>
<td>Using this policy, the administrator can control PIN (Personal Identification Number) which can be used instead of user name and password when PIN authentication is enabled.</td>
<td>String</td>
</tr>
<tr>
<td>erADLyncExacPolicy</td>
<td>This policy allows an administrator to control if a specific user can communicate with federated organizations, Public IM providers, or access the Lync infrastructure from an external source without VPN.</td>
<td>String</td>
</tr>
<tr>
<td>erADLyncArchpolicy</td>
<td>This policy allows the administrator to control the archiving perspective of the communications. The scope can be Internal, External or both to be stored on an SQL database.</td>
<td>String</td>
</tr>
<tr>
<td>erADLyncLocPolicy</td>
<td>A location policy contains the settings that define how E9-1-1 is implemented.</td>
<td>String</td>
</tr>
<tr>
<td>erADLyncClntPolicy</td>
<td>Specifies client-related settings.</td>
<td>String</td>
</tr>
<tr>
<td>erADLyncDialpPolicy</td>
<td>Specifies dial plan policy of user.</td>
<td>String</td>
</tr>
<tr>
<td>erADLyncVoicePolicy</td>
<td>Specifies calling features that can be enabled or disabled and public switched telephone network (PSTN) usage records.</td>
<td>String</td>
</tr>
</tbody>
</table>

Active Directory Adapter attributes by action

The following lists are typical adapter actions by their functional transaction group. The lists include more information about required and optional attributes sent to the adapter to complete that action.

**System Login Add**

A System Login Add is a request to create a user account with the specified attributes.

*Table 22. Add request attributes*

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>All other supported attributes</td>
</tr>
</tbody>
</table>
System Login Change
A System Login Change is a request to change one or more attributes for the specified users.

Table 23. Change request attributes

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>All other supported attributes</td>
</tr>
</tbody>
</table>

System Login Delete
A System Login Delete is a request to remove the specified user from the directory.

Table 24. Delete request attributes

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>All other supported attributes</td>
</tr>
<tr>
<td>erEntProfileType</td>
<td></td>
</tr>
<tr>
<td>erEntUserState</td>
<td></td>
</tr>
<tr>
<td>erEntUserDN</td>
<td></td>
</tr>
</tbody>
</table>

System Login Suspend
A System Login Suspend is a request to disable a user account.

The user is neither removed nor are their attributes modified.

Table 25. Suspend request attributes

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>None</td>
</tr>
<tr>
<td>erEntProfileType</td>
<td></td>
</tr>
</tbody>
</table>

System Login Restore
A System Login Restore is a request to activate a user account that was previously suspended.

After an account is restored, the user can access the system using the same attributes as the ones before the Suspend function was called.

Table 26. Restore request attributes

<table>
<thead>
<tr>
<th>Required attribute</th>
<th>Optional attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>erUid</td>
<td>None</td>
</tr>
<tr>
<td>erEntProfileType</td>
<td></td>
</tr>
</tbody>
</table>
Reconciliation

The Reconciliation function synchronizes user account information between IBM Security Identity Manager and the adapter.

Table 27. Reconciliation attributes

<table>
<thead>
<tr>
<th>Attributes returned during reconciliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported attributes</td>
</tr>
</tbody>
</table>
Appendix C. Support information

You have several options to obtain support for IBM products.

- “Searching knowledge bases”
- “Obtaining a product fix” on page 120
- “Contacting IBM Support” on page 120

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the product documentation for IBM Security Identity Manager. However, sometimes you must look beyond the product documentation to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

1. Search for content by using the IBM Support Assistant (ISA).
   ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the ISA website.

2. Find the content that you need by using the IBM Support Portal.
   The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.

3. Search for content about IBM Security Identity Manager by using one of the following additional technical resources:
   - IBM Security Identity Manager version 6.0 technotes and APARs (problem reports)
   - IBM Security Identity Manager Support website
   - IBM Redbooks®
   - IBM support communities (forums and newsgroups)

4. Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the Search field at the top of any ibm.com® page.

5. Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to
include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

Tip: Include “IBM” and the name of the product in your search if you are looking for information about an IBM product.

### Obtaining a product fix

A product fix might be available to resolve your problem.

**About this task**

You can get fixes by following these steps:

**Procedure**

1. Obtain the tools that are required to get the fix. You can obtain product fixes from the Fix Central Site. See [http://www.ibm.com/support/fxcentral/](http://www.ibm.com/support/fxcentral/).
2. Determine which fix you need.
3. Download the fix. Open the download document and follow the link in the “Download package” section.
4. Apply the fix. Follow the instructions in the “Installation Instructions” section of the download document.

### Contacting IBM Support

IBM Support assists you with product defects, answers FAQs, and helps users resolve problems with the product.

**Before you begin**

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM software subscription and support contract, and you must be authorized to submit problems to IBM. For information about the types of available support, see the “Software Support Handbook”.

**Procedure**

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support topic in the Software Support Handbook.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA):
     Any data that has been collected can be attached to the service request. Using ISA in this way can expedite the analysis and reduce the time to resolution.
     b. Open ISA.
c. Click **Collection and Send Data**.

d. Click the **Service Requests** tab.

e. Click **Open a New Service Request**.

- Online through the IBM Support Portal. You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.

- By telephone for critical, system down, or severity 1 issues: For the telephone number to call in your region, see the Directory of worldwide contacts web page.

**Results**

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.
Appendix D. Accessibility features for IBM Security Identity Manager

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

**Accessibility features**

The following list includes the major accessibility features in IBM Security Identity Manager.
- Support for the Freedom Scientific JAWS screen reader application
- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

The IBM Security Identity Manager library, and its related publications, are accessible.

**Keyboard navigation**

This product uses standard Microsoft Windows navigation keys.

**Related accessibility information**

The following keyboard navigation and accessibility features are available in the form designer:
- You can use the tab keys and arrow keys to move between the user interface controls.
- You can use the Home, End, Page Up, and Page Down keys for more navigation.
- You can launch any applet, such as the form designer applet, in a separate window to enable the Alt+Tab keystroke to toggle between that applet and the web interface, and also to use more screen workspace. To launch the window, click **Launch as a separate window**.
- You can change the appearance of applets such as the form designer by using themes, which provide high contrast color schemes that help users with vision impairments to differentiate between controls.

**IBM and accessibility**

See the [IBM Human Ability and Accessibility Center](https://www.ibm.com/humanability) for more information about the commitment that IBM has to accessibility.
Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to
IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

If you are viewing this information softcopy, the photographs and color illustrations might not appear.

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

**Trademarks**

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [http://www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Cell Broadband Engine and Cell/B.E. are trademarks of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.
Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, and to tailor interactions with the end user or for other purposes. In many cases, no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.


Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Index

A
accessibility x, 123
account form
attributes 105
Lync 114
erADGroupsMemberOf, configuring 68
erGroup, configuring 68
accounts
password requirements, when restoring 65
user account, creating 13
action, adapter attributes 115
adapter ix
ADK upgrade 96
automating administration tasks 1
base point configuration 66
common attributes in schema.dsml file 101
communication
adapter to server 5
with Security Identity Manager Server 5
configurable files 101
configuration tool 19
configuration, required conditions 19
customization
ADProfile.jar file 62
CustomLabels.properties file 64
file import 64
schema extension 62
schema.dsml file 63
steps 61
domain boundaries 2
extend attributes 61
features 1
form, updating 65
help 45
installation 11, 13
preinstallation roadmap 9
prerequisites 10
roadmap 9
silent mode 17
interface, managed resource and server 1
limitations 2
Lync 3
overview 1
parameters
accessing 54
certTool 54
options 54
PowerShell session with Exchange server 2
profile
objects referencing 99
removal 99
verifying installation 14
registry settings, modifying 36
removal 99

B
behaviors, troubleshooting adapter 81

C
CA, see certificate authority 54
certificate
certTool 59
exporting to PKCS12 file 60

Certificate (continued)
installation on workstation with
adapter 7
registration 59
viewing 58

Certificate authority
adapter directories 59
available functions 54
definition 47
deleting 59
installing 58
from file 58
sample 58
viewing 58
viewing installed 58
certificate signing request
definition 56
examples 57
file, generating 56
certificates
definition 47
examples of signing request (CSR) 57
installing 57
key formats 49
management tools 50
overview 48
private keys and digital certificates 48
protocol configuration tool, see
certTool 48, 54
registering 55, 59
removing 60
self-signed 49
unregistering 60
viewing 58
viewing registered 59
certTool
registered certificates, viewing 59
starting 54
change request attributes 116
changing
adapter parameters 36
configuration key 33
registry settings 36
classes
account 104
definition 104
schema.dsml file
classes 104
service 104
client authentication 52
cn attribute 74
code page
listing information 44
modifying settings 44
viewing information 44
communication
SSL
between adapter and Active Directory 5, 6
server-to-adapter 5
communication (continued)
with IBM Security Identity Manager Server 5
configuration
base point 66
cn attribute 74
erADProxyAddresses attribute 73
erADGroupIsMemberOf attribute 68
erGroup attribute 68, 73
key, changing 33
one-way SSL authentication 50
required settings for adapter 19
settings, viewing 21
configuring
domain controllers 29
connectivity between server, resource ix
context
baseline database 33
definition 25
modifying 30
reconciliation data 25
target DN 32
CSR 56
customization
ADProfile.jar file 62
schema extension 62
CustomLabels.properties file 104
updating 64
D
DAML protocol
properties, changing with agentCfg 21
username 21
debug log
enable/disable with 34
purpose 34
delayed replication errors 82
delete request attributes 116
detail log
enable/disable with 34
purpose 34
Directory Access Markup Language (DAML) protocol 5
directory NTFS, known behaviors 81
disk space prerequisites 10
domain
controllers, configuring 29
event notification 29
managed 29
domain boundaries, adapter 2
domain controller, installing Enterprise CA 6
download
adapter software 10
E
education x
encryption
SSL 48
erADProxyAddresses attribute 73
erADGroupIsMemberOf attribute 68
erGroup attribute 68, 73
error messages 83
error more data message
known behaviors 81
errors
Exchange 82
event notification
ADK-based 28
context
baseline database 33
modifying 30
multiple 30
related to service 30
search attributes 31
target DN 32
domain controllers 29
reconciliation data 25
triggers 28
event viewer
log file size 30
setting 30
Exchange
errors 82
Exchange Mailbox prerequisites 10
expiration date
known behaviors 81
exschema.txt file 63
extending, schema 62
F
files
adapter-specific 101
CustomLabels.properties file 104
updating 64
examples
schema.dsml file 101
exschema.txt file 63
schema.dsml file 101
classes 104
object identifier 102
updating 63
first steps after installation 77
G
graphical user interface, updating the adapter 94
H
help
accessing 45
agentCfg menu 45
for adapter 45
I
IBM
Software Support x
Support Assistant x
IBM Security Identity Manager server, importing adapter profile 13
IBM Support Assistant 120
import
adapter profile 64
importing
adapter profile 13
installation
adapter 11, 13
adapter registry 57
certificate, on workstation with adapter 7
certificates 57
Enterprise CA on domain controller 6
first steps after 77
language pack 91
planning 9
prerequisites 10
profile 13
roadmap 9
sequence 9
silent mode 17
troubleshooting 79
verify 12
installation prerequisites
administrator authority 10
network connectivity 10
operating system 10
Security Identity Manager server 10
ISA 120
K
key
encrypted information 48
exporting to PKCS12 file 60
private 48
public 48
knowledge bases 119
known behaviors
directory NTFS 81
error more data message 81
expiration date 81
language preferences 81
password properties 81
share access 81
L
language pack
installation 91
same for adapters and server 91
language preference, known behaviors 81
logs
debug 34
detail 34
directory, changing with 34, 35
disable/enable, changing with 35
settings, changing with
agentCfg 34
log file name 34
max file size 34
settings, default values 34
trace.log file 13
viewing statistics 43
Lync
account limitations 3
attributes, account form 114
upgrading (continued)
  adapter form 65
  adapter profile 13, 61
  authority required 13
  service creation 13
upgrade
  ADK 96
  graphical user interface 94
upgradeGroups
  tool 97
upgradeGroups tool 97
upgrading
  adapter 93, 96
  Adapter Development Kit 93
  upgradeGroups tool 97
upgrading the adapter
  silent mode 94, 95
user account
  adapter 13
  creation 13
username, changing with agentCfg 21

V
  verifying
    adapter profile installation 14
  verifying
    installation 12

W
  warning messages 83
Windows Local Account Adapter 1