IBM Security Verify Governance Identity Manager

Lotus Notes Adapter Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server.

Adapters can be installed on the managed resource. The Identity server manages access to the resource by using the security system. Adapters function as trusted virtual administrators on the target operating system. The adapter creates, suspends, restores user accounts, and other functions that administrators run manually. The adapter runs as a service, independently of whether you are logged on to the Identity server.

Features of the adapter

You can use the Lotus Notes Adapter to automate administrative tasks.

- Registering new users with:
  - Domino access, Sametime® access, Roaming access, only Sametime access
  - Explicit policies
  - Roaming feature
  - Full Name, Short Name, Custom attribute, or ITIM_ERUID as a User ID (eruid)
  - Mail file by using a mail template from Mail Template Server
  - Mail Replica file on Replica Server
  - Ability to create two replica mail files.
  - Multiple Certifier ID files and multiple passwords for the Certifier ID files
  - Custom attributes
  - Mail file creation immediately or in background by using the Administration Process (AdminP) command
- Modifying Lotus Notes user attributes
  - Upgrading users from non-roaming to Roaming profile
- Changing the Lotus Notes user account passwords, such as:
  - ID file passwords or Internet/HTTP passwords or both
  - Changing the ID file passwords at various locations, such as, File system, Person Document, Shadow Database (NoteIDsAddressBook), or Log Database
- Support for Notes ID Vault
- Suspending user accounts
- Restoring suspended user accounts with old or new passwords
- Deleting users with or without Mail file immediately or in the background by using the AdminP command
- Reconciling Lotus Notes user accounts and support data
- Adding groups, modifying group attributes, deleting groups
- Assigning users to groups and unassigning users from groups
- Running the following AdminP commands:
  - Renaming a user
  - Recertifying a user
  - Move user in hierarchy
  - Creating a replica of database
  - Moving a replica of database
  - Deleting an Access Control List (ACL)

  - Delete person in NAB
- Using multiple passwords for the Workstation ID file
- Support for non-English (for example, Chinese) characters as the Lotus Domino server name

Deprecation of Notes Shadow Adapter Utility, Shadow NAB, and Notes Shuttle Utility

The **`Notes Shadow Adapter`** utility and **`Notes Shuttle`** utility are deprecated in this version of the Lotus Notes Adapter. These utilities are no longer bundled with the adapter. No technical support is provided for problems that might occur.

To manage ID files and passwords, use the Notes ID Vault.

This version of the Lotus Notes Adapter continues to support the Shadow NAB utility. However, Lotus Notes Adapter no longer supports new implementations of the Notes Shadow adapter. For ease in migration, customers that upgrade from IBM® Security Identity Manager 5.x can use the Shadow utility with this version of the Lotus Notes Adapter.

Supported configurations

You can install the Lotus Notes Adapter in four different configurations.

The fundamental components in each environment are a IBM Security Verify Identity server, a Notes client, the Lotus Notes Adapter, and a Lotus Domino server. In each configuration, the Lotus Notes Adapter uses the Notes client to communicate with the Lotus Domino server.

Note: The following schematics show the Notes client and Lotus Notes Adapter on a separate workstation from the Lotus Domino server. Both components can reside on the same workstation as the Lotus Domino server.

Configuration 1: A single Lotus Notes Adapter

The first supported configuration includes a single Identity server, a single workstation running the Notes client with one instance of the Lotus Notes Adapter, and a single Lotus Domino server.

Figure 1. Single Lotus Notes Adapter configuration

Configuration 2: Multiple instances of the Lotus Notes Adapter

The second supported configuration includes a single Identity server, a single workstation running the Notes client with multiple instances of the Lotus Notes Adapter on different ports, and a single Lotus Domino server.

Figure 2. Multiple instances of Lotus Notes Adapter configuration

Configuration 3: Multiple instances of the Identity server

The third supported configuration includes multiple Identity server communicating with a single workstation running the Notes client with one instance of the Lotus Notes Adapter, and a single Lotus Domino server.

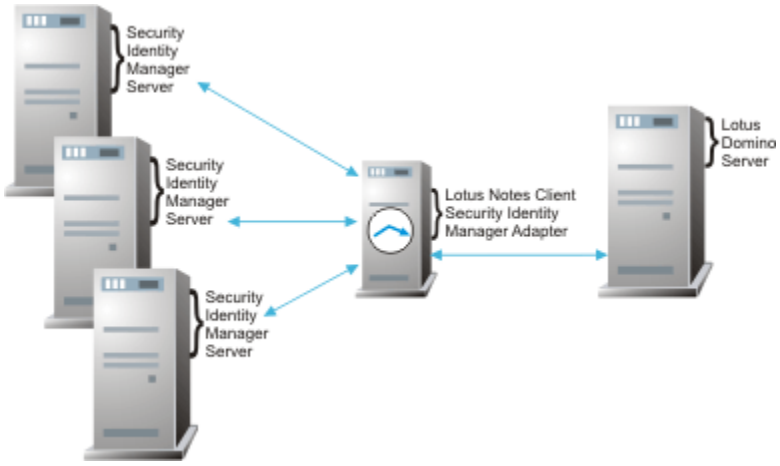


Figure 3. Multiple instances of the Identity server configuration

Configuration 4: Multiple instances of the Lotus Domino server

The fourth supported configuration includes a single Identity server, a single workstation running the Notes client with one instance of the Lotus Notes Adapter, and multiple instances of the Lotus Domino server.

While the Lotus Notes Adapter can work with multiple instances of the Lotus Domino server, it cannot do so simultaneously.

For more information on configuring the Lotus Notes Adapter to work with multiple instances of the Lotus Domino server, see "Configuring the adapter to run multiple Lotus Domino servers" on page 62.

Figure 4. Multiple instances of the Lotus Domino server configuration

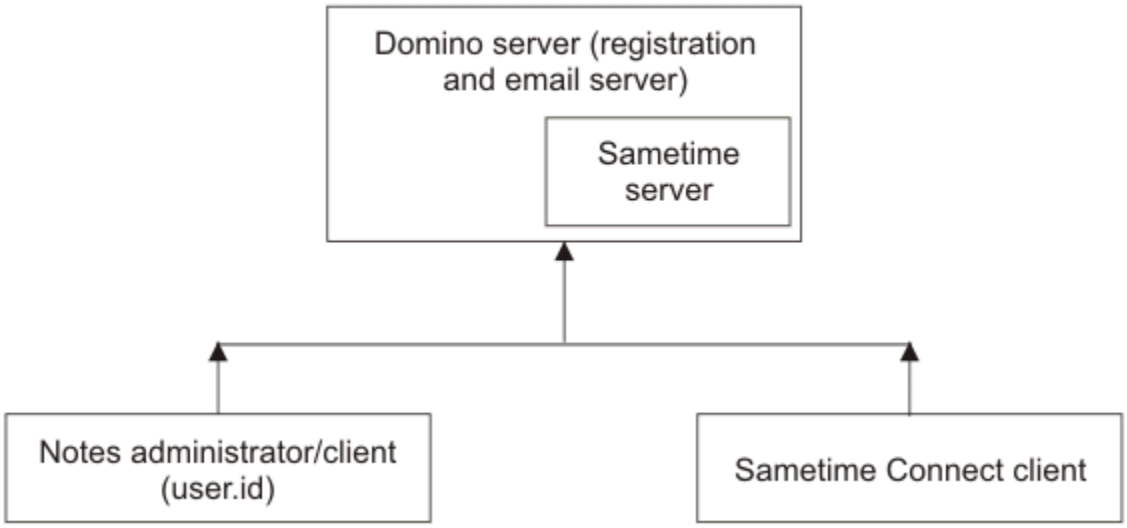
Supported Sametime configurations

The Lotus Notes Adapter supports Domino+Sametime and Only Sametime accounts management on the following Lotus Domino server configurations:

Configuration 1: A single Domino server

The first configuration involves a single Domino registration server that is also acting as a Domino email server.

The Sametime server is installed on the Domino registration server.

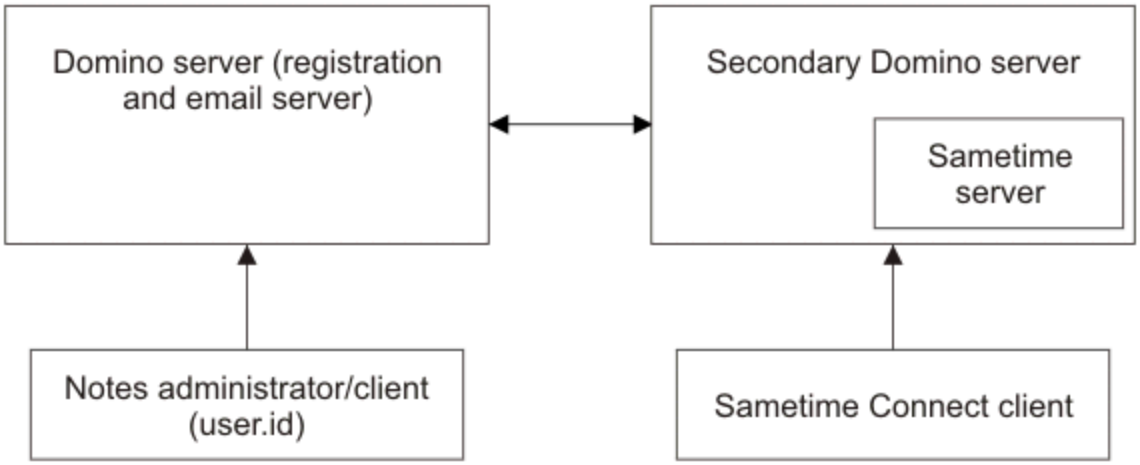


The illustration shows a single Domino server acting as a registration and e-mail server with the Sametime server installed on it. The server is connected to the Notes administrator or client and to the Sametime Connect client.

Configuration 2: Multiple Domino servers - case I

In this configuration, a Domino server acts as the registration and email server.

The Sametime server is installed on a secondary Domino server.

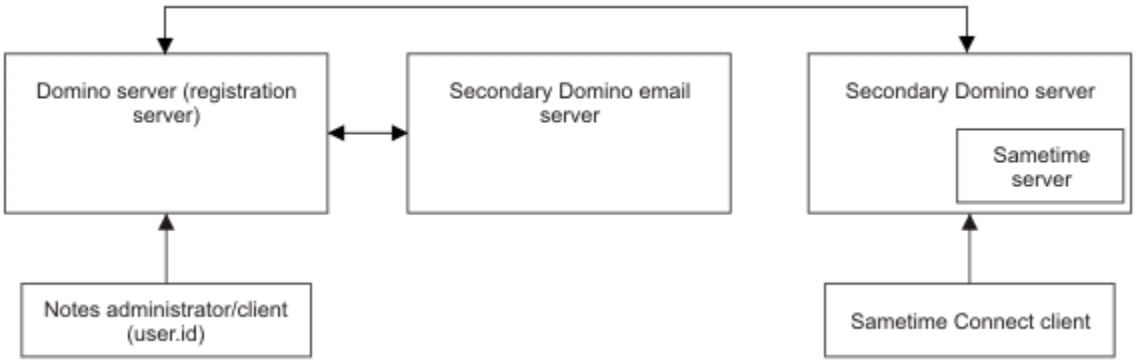


The illustration shows a single Domino server acting as a registration and email server with the Sametime server installed on a separate secondary Domino server. The primary Domino server is connected to the Notes administrator or client and the secondary Domino server is connected to the Sametime Connect client.

Configuration 3: Multiple Domino servers - case II

In this configuration, a Domino server acts as the registration server. A secondary Domino server acts as the email server.

The Sametime server is installed on another separate secondary Domino server.

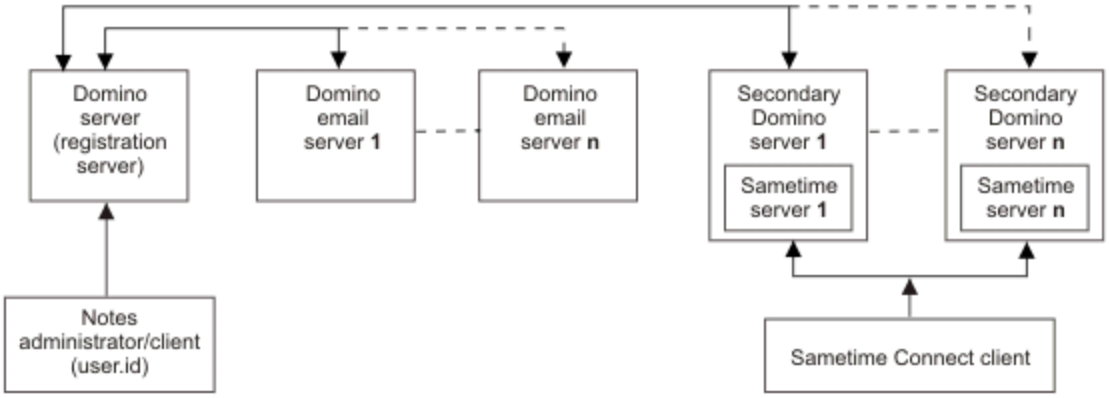


The illustration shows three Domino servers. The primary Domino server acts as the registration server and connects to secondary Domino server acting as the email server and to a separate secondary Domino server where the Sametime server is installed. The primary Domino server is connected to the Notes administrator or client. The secondary Domino e-mail server is connected only to the primary Domino server. The separate secondary Domino server with the Sametime server is connected to the Sametime Connect client.

Configuration 4: Multiple Domino servers - case III

In this configuration, a single Domino server acts as the registration server. Multiple secondary Domino servers act as email servers.

Multiple Sametime servers are installed on multiple separate secondary Domino servers.



The illustration shows five Domino servers. The primary Domino server acts as the registration server and connects to two secondary Domino servers acting as the e-mail servers and to two separate secondary Domino server where the Sametime servers are installed. The primary Domino server is connected to the Notes administrator or client. The secondary Domino e-mail servers connect to each other and to the primary Domino server. The separate secondary Domino servers with the Sametime servers connect to each other and to the Sametime Connect client.

Non-supported configurations

The Lotus Notes Adapter has non-supported configurations.

Configuration 1: Multiple Lotus Domino servers and multiple instances of the Identity server

The first non-supported configuration includes multiple Identity server, a single workstation running the Notes client with one instance of the Lotus Notes Adapter, and multiple Lotus Domino servers.

Configuration 2: Universal Provisioning Adapter on the same server as the Lotus Notes Adapter

The second non-supported configuration includes a Identity server, a single workstation that is running the Notes client with one instance of the Universal Provisioning Adapter and one instance of the Lotus Notes Adapter, and one Lotus Domino server.

The Universal Provisioning Adapter can be used to send email using the Notes client, therefore both adapters require the use of an ID file.

Configurations in which both adapters have the same ID file, or in which both adapters are installed on the same server, have not been tested and as such remain unsupported.

Configuration 3: Lotus Notes Adapter on Remote DeskTop or any other similar feature

Running Lotus Notes Adapter on Remote DeskTop is a non-supported configuration.

The Lotus Notes Adapter has not been tested on Remote DeskTop. These known issues might occur when Remote DeskTop is used:

- When Domino Server is running in Application Mode, Lotus Notes Adapter is running in Service Mode, and Domino Administrator is opened on Remote DeskTop, Lotus Notes Adapter throws a generic exception for any operation.
- When Domino Server is running in Service Mode, Lotus Notes Adapter is running in Service Mode, and Domino Administrator is opened on Remote DeskTop, Lotus Notes Adapter completes the first operation but stops during the second operation, "Opening Mail Database File (...) on Server (...)".

Implementing possible workarounds

You might need a workaround. Keep Domino Administrator closed on Remote DeskTop.

About this task

Note: This is a non-supported configuration and additional issues might be found after applying the workarounds.

Procedure

- If you have already opened Domino Administrator on Remote DeskTop:
  1. Close Domino Administrator.
  2. Restart Lotus Notes Adapter in Service Mode.
- If you are using Remote DeskTop and you need to keep Domino Administrator opened:
  1. Stop the Lotus Notes Adapter service.
  2. Run Lotus Notes Adapter in Console Mode from a command prompt. For example,`C:\Tivoli \Agents\NotesAgent\bin>NotesAgent.exe -name NotesAgent -console`

Configuration 4: Lotus Notes Adapter on VMware or any other Virtual Machine environment

The Lotus Notes Adapter is not supported on a VMware or any other virtual machine environment.

These tools are incompatible with the Notes client. In this case, the adapter crashes and transactions fail.

Configuration 5: Lotus Notes Adapter v5.*x* and v6.*x* on the same server

Adapters from different releases that are installed on the same server might share common components or runtime environments; however, some components might not be compatible.

Components of adapter version 5.*x* might not be compatible with the adapter version 6.*x* components. The adapters might not operate as expected after the installation of the adapter version 6.*x*. You must upgrade the 5.*x* adapters to the 6.*x* adapters.

Note: On Windows servers all the adapters must be upgraded simultaneously because of Dynamic Link Library (DLL) sharing.

Adapter interactions with the Identity server and the Lotus Domino server

There are multiple adapter interactions with the Identity server and the Lotus Domino server.

Data transfer to the adapter

The Lotus Notes Adapter is an individual IBM Security Verify Governance Identity Manager software program that must reside on a workstation where the Notes client is installed.

That workstation can be the Lotus Domino server. Data is transferred between the Lotus Notes Adapter and the Identity server using the Directory Access Markup Language (DAML) protocol. DAML uses Secure Sockets Layer (SSL) to send XML-formatted messages between the adapter and the server.

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

Communication between the adapter and the Lotus Domino server

The Lotus Notes Adapter uses a configuration port to listen to requests from the IBM Security Verify Governance Identity Manager.

After receiving a request from the IBM Security Verify Governance Identity Manager, the Lotus Notes Adapter:

1. Gathers the server name, the administrator ID file path, and the administrator password from the registry.
2. Initializes a session with the Lotus Domino server.
3. Opens the address book on the Lotus Domino server using the password that is found in the registry, after the administrator ID is authenticated.
4. Performs the operation that the IBM Security Verify Governance Identity Manager has requested and sends the status of the operation to the IBM Security Verify Governance Identity Manager.
5. Ends the session with the Lotus Domino server.

Basic configuration for server-to-adapter SSL communication

There can be an Identity server configuration on either the WebSphere® or the WebLogic application server.

In this scenario, the Identity server initiates communication with the adapter (server-to-adapter) using one-way authentication over SSL. The version of the SSL protocol that is used is Open SSL.

For more information on SSL, see “SSL authentication configuration” on page 63.

Chapter 2. Planning

Installing and configuring the adapter involves several steps that you must complete in a specific sequence. Follow the roadmap for the main tasks.

Roadmap for Adapter Development Kit based adapters, using `Setup.exe`

Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Pre-installation

Complete these tasks.

1. Verify that your environment meets the software and hardware requirements for the adapter. See *Prerequisites*.
2. Obtain the installation software. See *Software downloads*.
3. Obtain the necessary information for the installation and configuration. See *Installation worksheet*.

Installation

Complete these tasks.

1. Install the adapter binary.
2. Install 3rd party client libraries.
3. Set up the adapter environment.
4. Import the adapter profile.
5. Restart the adapter service.
6. Create an adapter service/target.
7. Install the adapter language package.
8. Verify that the adapter is working correctly.

Upgrade

You can do an upgrade or do a full installation. Review the *Release Notes*® for the specific adapter before you proceed.

Configuration

Complete these tasks.

1. Configure secure communication between the Identity server and the adapter.
    a. Configure 1-way authentication.
    b. Configure 2-way authentication.
2. Configure secure communication between the adapter and the managed target.
    a. Configure 1-way authentication.
    b. Configure 2-way authentication.
3. Configure the adapter.
4. Modify the adapter profiles.
5. Customize the adapter.

Troubleshooting

See the following topics.

- Techniques for troubleshooting problems
- Configure debugging
- Logs
- Error messages and problem solving

Uninstallation

Complete these tasks.

1. Stop the adapter service.
2. Uninstall the adapter binary
3. Remove 3rd party client libraries.
4. Delete the adapter service/target.
5. Delete the adapter profile.

Reference

See the following topics.

- Adapter attributes and object classes
- Adapter attributes by operations
- Special attributes

Prerequisites

Verify that all of the prerequisites are met before installing the Lotus Notes Adapter. Also, complete the installation worksheet before installing the adapter.

Table 1 on page 10 identifies the system prerequisites to install the Lotus Notes Adapter.

Table 1. Prerequisites for installing the adapter

Prerequisite	Description
System, memory, and disk space	• A 32-bit x86-based microprocessor • A minimum of 256 MB of memory • At least 300 MB of free disk space
Operating System	• Windows 2008 • Windows 2008 R2 • Windows Vista • Windows 7

Table 1. Prerequisites for installing the adapter (continued)	
Prerequisite	**Description**
Lotus Notes Software	One of the following versions of Notes client software: • Notes client 8.5.0 for Windows • Notes client 8.5.2 for Windows • Notes client 8.5.3 for Windows Domino Administrator 8.5.*x* for Windows **Note:** The Notes client is required for the adapter to run and manage email. The Domino Administrator is required for and administrative user to manage the Lotus Domino server .
Lotus Notes Managed Resource	One of the following Lotus Domino server: • Lotus Domino server 8.5.0 with optional Lotus Sametime version 8.0 • Lotus Domino server 8.5.1with optional Lotus Sametime version 8.0 • Lotus Domino server 8.5.2 with optional Lotus Sametime version 8.0 • Lotus Domino server 8.5.3 with optional Lotus Sametime version 8.0
Network Connectivity	• Internet Protocol network • SSL enabled • For security purposes, install the adapter on a Windows NT file system (NTFS)
Identity server	The following servers are supported: • Identity server Version 10.0 • Identity server Version 10.0 • IBM Security Privileged Identity Manager Version 2.0 • Identity server Version 10.0

Software downloads

Download the software through your account at the IBM Passport Advantage® website.

Go to IBM Passport Advantage.

See the corresponding *IBM Security Verify Governance Identity Manager Download Document* for instructions.

Note:

You can also obtain additional adapter information from IBM Support.

Installation worksheet

The installation worksheet lists the information that is required to install and configure the adapter. Complete this worksheet before you start the installation procedure for ease of reference. Make a copy of the worksheet for each adapter instance you install.

Complete this worksheet before starting the installation procedure. The worksheet identifies the information you need to modify during the installation process.

Make a copy of the worksheet for each server where you are installing the Lotus Notes Adapter. For example, if you have five Windows servers where you are installing the Lotus Notes Adapter, you need five copies of the worksheet.

Table 2. Installation worksheet

Option	**Description, default, notes**
Installation option	The type of adapter installation, such as, full installation or update installation. If the adapter is already installed on the workstation, then select the **Update Installation** option. If it is a first time installation of the adapter on the workstation, then select the **Full Installation** option.
Adapter name	The name of the adapter that is used as the: • Key in the registry settings for the adapter • Directory name to install the adapter

Lotus Domino server name	The name of the Lotus Domino server that the Lotus Notes Adapter connects to. The format of the Lotus Domino server name must be:
	`CN=<Server Name>/O=<Organization Name>`
	For example,
	`CN=Condor/O=IBM`

Workstation ID file location	The location of the user ID file, which the Administrator uses to access to the Lotus Domino server.
Lotus Domino server password	The password that corresponds to the user ID that the Lotus Notes Adapter uses to connect to the Lotus Notes or Lotus Domino server.
Certification file location and password	Typically, the certification file is installed in the data directory under the directory where the Lotus Notes or Lotus Domino server is installed. In most cases, the `cert.id` file is installed in a directory called `Notes\Data\` on a shared drive. The certification password is created by the Lotus Notes network administrator during installation of the Lotus Notes server. Therefore, you must ask your Lotus Notes network administrator for the certification file location and password information.
Lotus Domino version number	The version number for your Lotus Domino server.
Lotus Domino server address book	The name of the Lotus Domino server address book that the adapter uses, if it is any address book other than the default (`NAMES.NSF`).
Suspend group name	The name of the group to which suspended users are added.
Suspend HTTP group name	The name of the group to which the suspended users are added for HTTP access.
Delete group name	The name of the group to which the deleted users are added.

Table 2. Installation worksheet (continued)	
Option	**Description, default, notes**
Deny access log name	The name of the database file that lists the user documents that are deleted or suspended.
Attributes to be reconciled	A list of attributes to include in the reconciliation process.
Not reconciled attributes list	A list of attributes to exclude from the reconciliation process.
Notes IDs address book	The name of the database file to use to store ID file and password information for newly created users in IBM Security Verify Governance Identity Manager. **Note:** The Notes IDs address book value must be different from the **Notes Address Book** value. For example, if your Notes address book name is `names.nsf`, then do not use the same name for the Notes IDs address book.
Synchronize HTTP password	Specifies whether to synchronize the user password with the Internet/HTTP password for the user.
Short name	Specifies whether to use short names as user IDs in IBM Security Verify Governance Identity Manager.
Audit short name	Specifies whether to use internet addresses as user IDs in IBM Security Verify Governance Identity Manager. The internet address is used only when the short name of a user is not present on the resource.
Delete mail database file	Specifies whether to delete the mail database file of a user when an account is deleted in IBM Security Verify Governance Identity Manager.
Custom Eruid	The name of the custom field used for Eruid.
Use ITIM_ERUID	Specifies whether to use the ITIM_ERUID to store the Eruid value.
Refresh ITIM_ERUID	Specifies whether to delete the ITIM_ERUID field from each person document for the user.
HTTP password only	Specifies whether to set the HTTP password only in the Password Change operation.
HTTP password first	Specifies whether to set the HTTP password first in the Password Change operation.
Eruid in full name	Specifies whether to add the eruid attribute in full name.
Update server document	Specifies whether to update the server document with the Suspend Groups.
Lotus Domino server for Mail File template	Specifies the name of Lotus Domino server from which the Mail File templates are used for Mail file creation during the User Registration process.
Run the AdminP commands for the User Delete operation	Specifies whether to run AdminP commands for the User Delete operation
Create group if not present on the Lotus Domino server	Specifies whether to create a group during the USER Add or Modify operations if the group is not available on the Lotus Domino server. Avoid selecting the **Yes** option because the adapter supports creation of a group directly from IBM Security Verify Governance Identity Manager.

Chapter 3. Installing

Installing the adapter mainly involves importing the adapter profile and creating an adapter service. Depending on the adapter, several other tasks can be involved to completely install it.

If the Lotus Notes Adapter is not automatically installed with your IBM Security Verify Governance Identity Manager product, use the adapter installer to manually install the adapter.

The installation program for the Lotus Notes Adapter is available for download from the IBM Web site. Contact your IBM account representative for the Web address and download instructions.

Before you begin to install the Lotus Notes Adapter, verify that the following conditions are met:

- Any existing instance of the Lotus Notes Adapter must not be running.

  If the Lotus Notes Adapter is running, use the Services window to stop the adapter.
- When you are installing the Lotus Notes Adapter, you must use the Administrator's ID file, so that the adapter has administrator privileges.
- The ID file that is specified during installation must have system administrator authority.
- You must verify that the Domino Administrator can communicate with the Lotus Domino server. Use a low-level communications ping to ensure that the client can communicate with the server appropriately.
- The workstation ID must have *Full Remote Console Access* to perform the AdminP operations successfully. The adapter uses the ID to authenticate with the Lotus Domino server. If you do not provide the required permissions:
  - All the AdminP commands fail that the adapter submits.
  - IBM Security Verify Governance Identity Manager generates the following message: `Unable to process the Administration Request. You are not authorized to use the remote console on this server.`

  Note:
  - The adapter creates the AdminP request in the `admin4.nsf` database and successfully completes the AdminP operation.
  - You can verify the errors in the IBM Security Verify Governance Identity Manager audit log.

Installing the adapter

Download the adapter installation software from Passport Advantage and then install the adapter.

About this task

Before you install the Lotus Notes Adapter, ensure that 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.
- 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. Extract the contents of the download file. Take these 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 *setup*.exe file in the temporary directory.
3. Click **Next** on the Welcome window.
4. Do the following:
   - Review the license agreement and select **Accept**.
   - Click **Next**.
5. Select either Full installation or Update installation and click **Next** to display the Select Destination Directory window. Remember that the adapter must already exist if you want to perform an updated installation
6. Specify the name of the adapter instance in the **Adapter Name** field. This name is used in the adapter registry settings, for the name of the installation folder, and as the service name for the Lotus Notes Adapter. Then, click **Next**.
7. Specify where you want to install the adapter in the Directory Name field.

   Do one of the following:
   - Click **Next** to accept the default location.
   - Click **Browse** and navigate to a different directory and click **Next**.
8. Specify the required information about your Lotus Domino server in these fields in the Domino Server Name window:

   Domino Version Number
   The version number of your Lotus Domino server.

   Domino Server Name
   Type the Lotus Domino server name that the adapter uses. Enter the server name in the following format:

   ```
   CN=<Server Name>/O=<Organization Name>
   ```

   For example,

   ```
   CN=Condor/O=IBM
   ```

   Domino Server Address Book
   If the adapter use any address book other than the default NAMES.NSF, type the name of the Lotus Domino server address book.

   Then, click **Next**.
9. Specify the login information for the Domino Administrator in these fields in the Workstation Information window:

   File Location
   Type the workstation ID file that the adapter uses. Enter the fully qualified name of the file, for example, `D:\Lotus\Notes\Data\user.id`

   Workstation Password
   Type the password associated with the ID file, which is used to access the Lotus Domino server, through the Domino Administrator. Passwords are case-sensitive.

   Then, click **Next**.
10. Specify the groups where suspended users are added in these fields in the Suspend Group and Suspend HTTP Group Name window:

    Suspend Group Name
    Type the name of the group to which suspended users are added. The default value is SuspendGroup.

Suspend HTTP Group Name
Type the name of the group to which suspended users are added for HTTP access. The default value is HTTPSuspendGroup.

Then, click **Next**.

11. In the **Delete Group Name and Deny Access Log** window, complete the following fields:

Delete Group Name
Type the name of the group to which deleted users are added. For example,

```
Deleted Users
```

Deny Access Log Name
Type the name of the database file that lists the deleted or suspended user documents. User documents are removed from this database file when a user is added or restored. For example, LogDB.nsf

Note: If Log DB is in a multilevel directory structure in the data directory of Lotus Domino server at \admindatabases\adapterdatabases, then the value of registry key Log DB must be admindatabases\adapterdatabases\logdb.nsf

Then, click **Next**.

12. In the **Attributes to be Reconciled, Not Reconciled Attributes, and Synchronize HTTP Password** window complete the following fields:

Attributes to be Reconciled
Specify a list of attributes to include in the reconciliation process. Separate the attributes with a semicolon (;) if you list more than one attribute, for example, Certificate;$UpdatedBy;$Revisions. If you leave the Reconciled Attributes field blank, all attributes except the ones specified in the Not Reconciled Attributes List are returned during reconciliation.

Not Reconciled Attributes List
Specify a list of attributes to exclude from the reconciliation process. Separate the attributes with a semicolon (;) if you list more than one attribute, for example, Certificate;$UpdatedBy;$Revisions.

Synchronize HTTP Password
Select **Yes** to synchronize the user password as the Internet/HTTP password for the user. Select **No** to not synchronize the user password. The default is Yes.

Then, click **Next**.

13. Specify how you want to use short names in these fields in the Use Short Name and Audit Short Name window:

Use Short Name
Select **Yes** to use short names as user IDs in IBM Security Verify Governance Identity Manager. Select **No** to not use short names. The default is No.

Note: When **Yes** is selected during this step, do not use the **Short Name** field on the IBM Security Verify Governance Identity Manager GUI Account form.

Audit Short Name
Select **Yes** to use internet addresses as user IDs in IBM Security Verify Governance Identity Manager. The internet address is used only when a user's short name is not present on the resource. Select **No** to not use internet addresses. The default is No.

Then, click **Next**.

14. Specify information about the user address book and mail file in these fields in the **Note IDs Address Book and Delete Mail Database File** window:

Note IDs Address Book
Type the name of the database file to use to store ID file and password information for newly created users in IBM Security Verify Governance Identity Manager. For example,

```
NoteIDsAddressBook.nsf
```

Note: If **NoteIDsAddressBook** is in a multilevel folder directory structure in the data directory of Lotus Domino server at \admindatabases\adapterdatabases, then the value of registry key **NoteIDsAddressBook** must be admindatabases\adapterdatabases \NoteIDsAddressBook.NSF.

Delete Mail Database File
Select **Yes** to delete the mail database file of a user when an account is detected in IBM Security Verify Governance Identity Manager. Select **No** to keep the mail database file. The default is Yes.

Then, click **Next**.

15. Specify information in these fields in the Change HTTPPassword Only, Change HTTPPassword First, Store ERUID in FullName, and Update Server Doc window:

Change HTTPPassword Only
Specify whether only HTTP password is changed in the password change operation from IBM Security Verify Governance Identity Manager. Select **YES** if only HTTP password is to be changed in the password change operation. The default value is NO.

Change HTTPPassword First
Specify how to store the HTTP password during a change operation. Select **Yes** if you want to change the HTTP password first before changing the user password. The default value is No.

Store ERUID in FullName
Specify whether you want to store the ERUID or User ID attribute in the FullName field in the person document. Select **Yes** if you want to store the attribute in the FullName field. The default value is Yes.

This registry key can be used only when either the ShortName, Custom Attribute, or ITIM_ERUID fields are used to store the ERUID attribute.

Update Server Doc
Specify whether you want to include all suspended groups in the Not Access Server field of the server document. Select **Yes** include all suspended groups in the Not Access Server field. The default value is NO.

Then, click **Next**.

16. If the default Certifier ID file is used for ADD operations, complete the following fields in the **Certifier ID File Path and Certifier password** window:

Certifier ID File Path
Optional: Specify the file path for the certifier ID file. The certifier ID file is the default file used for ADD operations. If the file path for the certifier file is not specified when you add a user, the file path from this field is used. If you specify the path for the certifier file when you add a user, the file path in this field is ignored. For example, you might specify the certifier ID file path as C:\Lotus\Domino\cert.id.

Certification Password
Specify the password for the certifier ID file that is provided in the Certifier ID File Path field. If a file path is not provided in this field, then you do not need to provide a password.

Use the agentCfg to change the value of the Certification Password registry key.

Then, click **Next**.

17. Specify information in these fields in the **Mail Template Server and Execute AdminP Operation** window:

Mail Template Server
Specify the server name for mail template files to be used by the adapter. If a value is not specified for this registry key, the adapter uses the mail template files from the Domino

Registration Server. The files for the Domino Registration Server are specified for the Domino Server registry key.

Execute AdminP Operation
Specify whether the AdminP operation is used to deprovision a user. Select **Yes** if you want the AdminP operation to be used when deprovisioning a user from IBM Security Verify Governance Identity Manager. The default value is NO. For Domino Version 6.5 and later **Delete Person in NAB** is used to deprovision a user.

Then, click **Next**.

18. Specify the **`Create Group If Not Present`** attribute if the group is not available on the Lotus Domino server. Select **Yes** if you want the adapter to create a group on the Lotus Domino server when you perform the add or modify user account operation from IBM Security Verify Governance Identity Manager. Select **No** if you do not want the adapter to create a group on the Lotus Domino server if the group is not available on the Lotus Domino server when you perform the add or modify user account operation from IBM Security Verify Identity. The default value is **No**.
19. Specify whether the ID Vault is configured on the Lotus Domino server.
    The default setting is No.
20. Review the installation settings in the **Install Summary** window. Take one of the following actions:
    - Click **Back** and return to a previous window to change any of these settings.
    - Click **Next** when you are ready to begin the installation.
21. Click **Finish** when the software displays the **Install Completed** window.

Importing the adapter profile

You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

Before you begin

- The Identity server is installed and running.
- You have administrator authority on the Identity server.
- The file to be imported must be a Java™ archive (JAR) file. The `<Adapter>Profile.jar` file includes all the files that are required to define the adapter schema, account form, service/target form, and profile properties. If necessary, you can extract the files from the JAR file, modify the files, and repackage the JAR file with the updated files.

About this task

Target definition files are also called adapter profile files. The profile definition files are provided with the various IBM Security Verify Adapter. The adapter profile must be imported because it defines the types of resources that the Verify Governance Identity Manager server can manage.

The adapter profile definition file is used to create a target profile on the Verify Governance Identity Manager server and to establish communication with the adapter. If the adapter profile is not imported, you cannot create a connector for that adapter type.

An upload error might occur when no file is selected, or when the file is empty, or due to any upload operation error, such as a timeout or connection error. If the adapter profile is not installed correctly, the adapter cannot function correctly. You cannot create a connector with the adapter profile or open and account on the service. You must import the adapter profile again.

This task can be completed from the Enterprise Connectors module in the Administration Console. To import an adapter target profile, complete these steps:

Procedure

1. Log in to the Verify Governance Identity Manager Administration Console.

2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Profiles**.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Click **Actions** > **Import**.
6. On the **Import** page, complete these steps:
   a) Select **Profile**.
   b) Click **Browse** to locate the JAR file that you want to import.
   c) Click **Upload file**.
   A message indicates that you successfully imported a profile.
7. Click **Close**.
   The new profile is displayed in the list of profiles.

Results

The upload is synchronous but has a timeout. The progress bar on the **Import** page accurately indicates the upload status. However, when a timeout is reached, the following message occurs: "The import is still in progress and will complete shortly. Close this window to proceed." If you see that message, allow a few minutes for the upload to complete and for the profile to be available.

What to do next

After the target profile is imported successfully, complete these tasks.

- Import the attribute mapping file. See “Importing attribute mapping file” on page 20.
- Create a connector that uses the target profile. See “Adding a connector” on page 21.

Importing attribute mapping file

After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

About this task

This task involves importing an account attribute mapping definition file, which is included in the adapter package. The imported file must be a DEF file.

Procedure

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Profiles**.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Click **Actions** > **Import**.
6. On the **Import** page, complete these steps:
   a) Select **Attribute Mapping**.
   b) Click **Browse** to locate the attribute mapping file that you want to import.
   c) Click **Upload file**.
   A message indicates that you successfully imported the file.
7. Click **Close**.

Adding a connector

After you import the adapter profile on the Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager server can communicate with the managed resource.

Before you begin

Complete Importing the adapter profile.

Note: If you migrated from Verify Governance Identity Manager V5.2.2 or V5.2.2.1 and want to add or configure a connector, see *Adding and configuring a connector for each target* in the IBM Security Verify Governance Identity Manager product documentation.

About this task

The connectors consolidate, extract, and reconcile user identities, organization units, permissions, and user entitlements with the most common enterprise applications. Configure a connector to keep the Access Governance Core repository synchronized with the target system.

This task can be completed from the Enterprise Connectors module in the Administration Console.

Procedure

To add a connector, complete these steps.

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.
   A list of connectors is displayed on the **Connectors** tab.
4. Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Click **Actions** > **Add**.
   The **Connector Details** pane is enabled for your input.
7. On the **Connector Details** tab, complete these steps:
   a) Assign a name and description for the connector.
   b) Select the target profile type as `Identity Brokerage` and its corresponding target profile.
   c) Select the entity, such as **Account** or **User**.
      Depending on the connector type, this field might be preselected.
   d) Optional: Select **Trace ON** and the corresponding **Trace Level** to enable trace logs.
      The available trace levels are DEBUG, INFO, and ERROR.
   e) Optional: Select **History ON** to save and track the connector usage.
   f) Click **Save**.
      The fields for enabling the channels for sending and receiving data are now visible.
   g) Select and set the connector properties in the **Global Config** accordion pane.
      For information about the global configuration properties, see Global Config accordion pane.
   h) Click **Save**. The fields for enabling the channels for sending and receiving data are now visible.

Results

The connector is saved and added to the list of connectors in the **Connectors** pane.

If you cannot create a connector with the target profile or open an account on an existing connector, the target profile was not installed correctly during the import. You must import the target profile again.

What to do next

Enable the channel modes to synchronize the data between the target systems and Verify Governance Identity Manager. For more information, see "Enabling connectors" on page 22.

Enabling connectors

After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Before you begin

Table 3. Prerequisites for enabling a connector

Prerequisite	Find more information
A connector must exist in Verify Governance Identity Manager.	"Adding a connector" on page 21.
Ensure that you enabled the appropriate channel modes for the connector.	"Reviewing and setting channel modes for each new connector" on page 23.

Procedure

To enable a connector, complete these steps:

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.

   A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:
   a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed.

   Enable write-to channel
   Propagates every change in the Access Governance Core repository into the target system.

   For connectors that are not HR feed, the check boxes for enabling the read-from channel and the write-to channel are available.

   Enable read-from channel
   Reads the INPUT EVENTS and USER DATA from the target system. Imports data from the target system to the Access Governance Core repository.

   For HR feed connectors, only the check box for enabling the read-from channel is available.

   Enable reconciliation
   Synchronizes the modified data between the Access Governance Core repository and the target system.

Results

The connector is enabled

What to do next

Enable the channel modes to synchronize the data between the target systems and Verify Governance Identity Manager.

Reviewing and setting channel modes for each new connector

Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

About this task

Note: Legacy Verify Governance Identity Manager Enterprise connectors use `Reconciliation` channel, whereas Identity Brokerage Enterprise connectors use `Read From Channel` and `Change Log Sync`.

For more information about any of tasks in the following steps, see the IBM® Security Identity Governance and Intelligence product documentation.

Procedure

To enable the read-from and write-to channels, and to set the change log synchronization schedule for each new connector, complete these steps in Verify Governance Identity Manager V5.2.3:

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.

   A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:
   a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed, in which you can do more configuration, such as mapping attributes and setting up rules.

      Enable write-to channel
      Propagates every change in the Access Governance Core repository into the target system.

      Enable read-from channel
      Reads the INPUT EVENTS and USER DATA from the target system. Imports data from the target system to the Access Governance Core repository.

      Enable reconciliation
      Synchronizes the modified data between the Access Governance Core repository and the target system.
8. Select **Monitor** > **Change Log Sync Status**.

   A list of connectors is displayed.
9. On the **Change Log Sync Status** tab, complete these steps:
   a) Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
   b) Select a connector, and click **Actions** > **Sync Now**.

      The synchronization process begins.
   c) Optional: To view the status of the synchronization request, select **Sync History** in the right pane.

      Information about the synchronization is displayed in the **Sync History** tab.

10. Set the change log synchronization schedule for each new connector that you migrated.
11. When the connector configuration is complete, enable the connector by completing these steps:
    a) Select **Manage** > **Connectors**.
    b) Select the connector that you want to enable, and then select the **Enable** check box in the **Connector Details** tab.
    c) Click **Save**.

    For more information, see “Enabling connectors” on page 22.

    For Identity Brokerage connectors that are not HR feed, the check boxes for enabling the read-from channel and the write-to channel are available.

    For Identity Brokerage HR feed connectors, only the check box for enabling the read-from channel is available.
12. Start the connector by selecting **Monitor** > **Connector Status**. Select the connector that you want to start, and then select **Actions** > **Start**.

Service/Target form details

Complete the service/target form fields.

On the General Information tab:

Service Name
Specify a name that defines this adapter service on the Identity 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 37. 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 “SSL authentication configuration” on page 63.

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 37.

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 37.

Owner
Optional: Specify the service owner, if any.

Service Prerequisite
Optional: Specify an existing 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 service uses to provision request to the managed resource.

Profile version
Specifies the version of the profile that is installed in the Identity 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 test request was successfully sent to the adapter.
- Verify the adapter configuration information.
- Verify service parameters for the adapter profile. For example, verify the work station name or the IP address of the managed resource and the port.

Verifying the adapter installation

You can verify that the adapter is installed correctly by checking the components in a specific directory.

32-bit systems
`C:\Program Files\IBM\ISIM\Agents\NotesAgent\bin`

64-bit systems
`C:\Program Files (x86)\IBM\ISIM\Agents\NotesAgent\bin`

- NotesAgent.exe
- agentCfg.exe
- CertTool.exe
- regis.exe
- Isamtool.exe
- fipsEnable.exe
- DelRegKey.exe
- NotesRegID.exe
- RemoveReg.cmd
- icudt32.dll icuuc32.dll
- xml4c_5_5.dll
- XML4CMessages5_5.DLL

The following components exist in the one of the following directories:

32-bit systems
`C:\WINDOWS\system32`

64-bit systems
`C:\WINDOWS\SysWOW64`

- AdkApi.dll
- ErmApi.dll
- ErmApiDaml.dll
- icudt36.dll
- icuuc36.dll
- ssleay32.dll
- libeay32.dll
- NotesAuth.dll
- lcppn.dll

Review the installer log files (`NotesAgentSetup.log`) located in the following directories for any errors.

32-bit systems
`C:\Program Files\IBM\ISIM\Agents\NotesAgent`

64-bit systems
`C:\Program Files (x86)\IBM\ISIM\Agents\NotesAgent`

If this installation is to upgrade an adapter, send a request from IBM Security Verify Governance Identity Manager. Verify that the version number in the `NotesAgent.log` matches the version of the adapter

Note: The Lotus Notes Adapter does not use an `xforms.xml` file. Ignore the errors in the adapter log that are related to xforms.

Using the Lotus Notes Adapter on a Japanese operating system

After you successfully install the Lotus Notes Adapter on a Japanese operating system, set the code page.

Procedure

1. At the command prompt, navigate to the `agentCfg.exe` file that is located in the `\bin` directory of the adapter and run the following command: `agentCfg.exe -a NotesAgent`.
2. From the Main Configuration Menu, select option I. Codepage Support.
3. From the Code Page Support Menu, select option A. Codepage Configure.
4. Enter the value for the code page. For example, you can enter `ibm-943_P14A-1999`.

   Note: Find a list of supported code pages by using the -codepage option of the `agentCfg.exe` file. For example, run the following command from the command prompt after you navigate to the `agentCfg.exe` file: `agentCfg.exe -a NotesAgent -codepage`
5. Restart the Lotus Notes Adapter.

Installing and uninstalling in silent mode

You can install and uninstall the Lotus Notes Adapter 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 **`-silent`** option to install or uninstall the adapter in silent mode.

You must create a response file, before you can install with silent mode.

Note:

- The adapter installer also installs run time libraries from Microsoft. The user interface of the installer for these run time libraries is also suppressed during silent installation of the adapter. The Microsoft installer for these run time libraries creates a log file `vcredist_x86.log` under the `temp` directory of

the user home directory (%temp%). For example, `C:\Documents and Settings\Administrator\Local Settings\Temp\vcredist_x86.log`. You can check this file for any errors.

- If you install adapter in silent mode, the uninstaller runs in silent mode irrespective of whether you are using **`-i silent`** option.

Response file creation and silent installation

You can use response files to provide inputs during silent installation. You can either generate a response file or create one manually.

A response file contains the information necessary to answer the prompts during the installation of the adapter. You can do multiple installations without having to resupply the same information.

Generating the response file

You can generate a response file by running the following command.

```
setup.exe -r "Full path of response file"
```

This command runs the installer in interactive mode and installs the adapter. You must supply information for each of the installation prompts. After the installation is completed, the file specified as *Full path of response file* is created. It contains the information you supplied for the required parameters. You can use this file for later installations.

Example

```
setup.exe -r "C:\Notes60resp.txt"
```

Creating the response file manually

You can also manually create the response file and add the required parameters to the file.

Attributes with names like *attrName*_YES and *attrName*_NO are related to a registry key with the name *attrName*. For example DeleteMailDB_YES and DeleteMailDB_NO are related to a registry key with the name DeleteMailDB. The combination of the attribute values set the value for the registry key.

Table 4. Attribute settings and registry key values

Attribute setting	Attribute setting	Registry key value
*attrName*_YES=1	*attrName*_NO=0	TRUE
*attrName*_YES=0	*attrName*_NO=1	FALSE

Note: The value for *attrName*_YES and *attrName*_NO must not be the same.

Create a text file, for example `C:\Notes60resp.txt` with the following content:

```
#Select Install Type
#-------------------
USER_INPUT_INSTALL_TYPE=\"Full Installation\",\"\"
USER_INPUT_INSTALL_TYPE_1=Full Installation
USER_INPUT_INSTALL_TYPE_2=
USER_INPUT_INSTALL_TYPE_BOOLEAN_1=1
USER_INPUT_INSTALL_TYPE_BOOLEAN_2=0

#Adapter Name
#------------
AgentName=\"NotesAgent\"
AgentName_1=NotesAgent
AgentName_BOOLEAN_1=

#Choose Install Folder
#---------------------
USER_INSTALL_DIR=C:\\Program Files\\IBM\\ISIM\\Agents\\NotesAgent
```

```
#Notes Adapter Configuration Settings
#----------------------------------
DominoVersionNumber_8.5=1
DominoServerName=CN=mymailserver/O=myorg
AddressBookName=
WkStnIDFile=C:\\Program Files\\IBM\\Lotus\\Notes\\Data\\user.id
WkStnPass=password
SuspendGroupName=SuspendGroup
SuspendHTTPGroupName=HTTPSuspendGroup
DeleteGroupName=
LogDBName=
ReconAttribs=
NotReconAttribs=Certificate;$UpdatedBy;$Revisions
SynchroniseHTTPPwd_YES=1
SynchroniseHTTPPwd_NO=0
UseShortName_YES=0
UseShortName_NO=1
UseInetAddrForShortName_YES=0
UseInetAddrForShortName_NO=1
IdsAddressBookName=
DeleteMailDB_YES=1
DeleteMailDB_NO=0
SetHTTPPswdOnly_YES=0
SetHTTPPswdOnly_NO=1
SetHTTPPswdFirst_YES=0
SetHTTPPswdFirst_NO=1
AddEruidToFullName_YES=1
AddEruidToFullName_NO=0
UpdateServerDoc_YES=0
UpdateServerDoc_NO=1
CertIDPath=C:\\Program Files\\IBM\\Lotus\\Notes\\Data\\cert.id
CertIDPassword=password
MailTemplateServer=
ExecAdminpOperation_YES=0
ExecAdminpOperation_NO=1
CreateGroupIfNotPresent_YES=0
CreateGroupIfNotPresent_NO=1
IsIDVaultConfigured_YES=1
IsIDVaultConfigured_NO=0
```

If you do not want to restart the server after the adapter is installed, add this line to the end of the response file.

```
USER_REQUESTED_RESTART=NO
```

For a list of available attributes, see “Installation attributes” on page 100. If optional attributes are not specified in the response file, a default value is assigned to the associated registry key. See “Default values for optional registry keys” on page 108 for a list of the default values.

After you create the response file, you can use it to provide parameters to the installer for silent installation:

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

Example

```
setup.exe -i silent -f "C:\Notes60resp.txt"
```

Installing in silent mode

To use the command line, each attribute must be prefixed with the `-D` switch. No space exists in between D and the attribute.

The following example illustrates the installation command with some of the required attributes. For a list of the available attributes, see “Installation attributes” on page 100.

Issue the installation command on a single line.

```
setup.exe -i silent -DUSER_INSTALL_DIR="c:\\ISIM\\agent\\NotesAgent"
-DUSERINPUT_INSTALL_TYPE_1=1
-DUSERINPUT_INSTALL_TYPE_2=0
```

Note: The installation path must be marked with quotation marks. The path separator is \\ (double backslash).

Uninstalling in silent mode

Run the **uninstaller.exe** command with the `-silent` option to uninstall the Lotus Notes Adapter.

At the command line, type:

```
uninstaller.exe –silent
```

Specify the full path when you are not running the command from the `_uninst` directory of the adapter installation directory.

```
C:\Program Files\IBM\ISISM\Agents\NotesAgent\_uninst\uninstaller.exe -i silent
```

Chapter 4. Upgrading

You can upgrade either the Lotus Notes Adapter or the Adapter Development Kit (ADK).

If you upgrade the adapter, as opposed to reinstalling it, you can keep your configuration settings. Additionally, you do not have to uninstall the current adapter and install the newer version.

Note: If your existing adapter version is earlier than 6.*x*, you must uninstall the older version of the adapter before you can install the 6.*x* adapter. You cannot migrate from an earlier version to 6.*x*.

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. You can perform an adapter upgrade to migrate your current adapter installation to a newer version, for example version 6.*x* to version 6.*x*.

If only a code fix is made to the ADK, instead of upgrading the entire adapter, you can upgrade just the ADK to the newer version. See “Upgrading the ADK” on page 32.

Upgrading the Lotus Notes Adapter

For adapter versions 6 and higher, use the adapter upgrade option.

About this task

Use this option:

- If you want to keep the adapter configuration (registry keys and certificates) unchanged.
- If the installed adapter is FIPS enabled. The Update Installation option keeps FIPS configurations such as the CA certificates, `fipsdata.txt`, the (key generated by running `fipsenable.exe`) and the registry keys encrypted with `fipsdata.txt` unchanged.

If 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 a service for the adapter.

During an upgrade, to maintain all of your current configuration settings, the certificate, and private key, do not uninstall the old version of the adapter before installing the new version. During the installation, specify the same installation directory where the previous adapter was installed. For more information about how to install the adapter, see Chapter 3, “Installing,” on page 15.

To upgrade an existing adapter, complete the following steps:

Procedure

1. Stop the Lotus Notes Adapter service.
2. Install the new version of the adapter.

Results

When the upgraded adapter starts for the first time, new log files are created that replace the old files.

The adapter installer allows an update installation of the adapter, for adapters versions 6.0 or later. The upgrade option is applicable only for the adapter version 6*x* maintenance upgrades. The upgrade option is not designed for the adapter versions 5.*x* to version 6.*x* migrations.

Upgrading the ADK

You can use the ADK upgrade program to update the ADK portion of the adapters that are currently installed on a workstation.

About this task

You can install just the ADK, and not the entire adapter. As part of the ADK upgrade, the ADK library and the DAML protocol library are updated. In addition, the agentCfg and certTool binary files are updated.

The ADK consists of the runtime library, filtering, and event notification functionality, protocol settings, and logging information. The remainder of the adapter is composed of the Add, Modify, Delete, and Search functions. While all adapters have the same ADK, the remaining functionality is specific to the managed resource.

Before upgrading the ADK files, the upgrade program checks the current version of the ADK. A warning message occurs if the current level is higher than what you are attempting to install.

To upgrade the Lotus Notes Adapter ADK, complete the following steps:

Procedure

1. Download the ADK upgrade program compressed file from the IBM website.
2. Extract the contents of the compressed file into a temporary directory.
3. Stop the Lotus Notes Adapter service.
4. Start the upgrade program with the `adkinst_win32.exe` file in the temporary directory. For example, select **Run** from the **Start** menu, and type `C:\TEMP\adkinst_win32.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. On the Installation Information window, click **Next** to begin the installation.
7. On the **Install Completed** window, click **Finish** to exit the program.

Location of the ADK log files

Logging entries are stored in the *ADKVersion*`Installer.log` and *ADKVersion*`Installeropt.log` files, where *ADKVersion* is the version of the ADK. For example, `ADK50Installer.log` and `ADK50Installeropt.log`.

These files are created in the folder where you run the installation program.

Adapter upgrade by using the silent mode

Use the **`-i silent`** option to update the Lotus Notes Adapter in 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 **`-silent`** option to upgrade the adapter in silent mode. See "Installation attributes" on page 100 for information about the command-line parameters for silent mode.

You must create a response file, before you can install with silent mode.

Note:

- When performing an update installation in silent mode, the **`USER_INSTALL_DIR`** parameter indicates directory for update installation. Make sure that adapter is already installed at the location specified in **`USER_INSTALL_DIR`**.

- When **USER_INSTALL_DIR** not specified in the response file, adapter identifies the correct directory for the installation.
- If multiple instances of the $AgentName are installed, **USER_INSTALL_DIR** typically has the value `C:\Program Files\IBM\ISIM\\agents\$AgentName`. `$AgentName` is name of the Lotus Notes Adapter specified at the time of the installation.
- When updating the adapter with silent installation, the parameter `DUSER_INPUT_INSTALL_TYPE_BOOLEAN_1=0` must be used to overwrite the default value of this parameter.
- The `AgentName` must be specified and must match the installed adapter `AgentName`. The `AgentName` can be specified as **–DagentName=NotesAgent**.
- The adapter installer also installs run time libraries from Microsoft. The user interface of the installer for these run time libraries is also suppressed during silent installation of the adapter. The Microsoft installer for these run time libraries creates a log file `vcredist_x86.log` under the `temp` directory of the user home directory (%temp%). For example, `C:\Documents and Settings\Administrator \Local Settings\Temp\vcredist_x86.log`. You can check this file for any errors.

Response file creation

You can use response files to provide inputs during silent installation upgrade. You can either generate a response file or create one manually.

A response file contains the information necessary to answer the prompts during the upgrade of the adapter. You can do multiple upgrades without having to resupply the same information.

Generating the response file

You can generate a response file by running the following command.

```
setup.exe -r "Full path of response file"
```

This command runs the installer in interactive mode and installs the adapter. You must supply information for each of the installation prompts. After the installation is completed, the file specified as *Full path of response file* is created. It contains the information you supplied for the required parameters. You can use this file for later upgrade installations.

Example

```
setup.exe -r "C:\Notes60UpdateResp.txt"
```

Creating the response file manually

You can also manually create the response file and add the required parameters to the file.

Attributes with names like *attrName*_YES and *attrName*_NO are related to a registry key with the name *attrName*. For example `DeleteMailDB_YES` and `DeleteMailDB_NO` are related to a registry key with the name `DeleteMailDB`. The combination of the attribute values set the value for the registry key.

Table 5. Attribute settings and registry key values

Attribute setting	**Attribute setting**	**Registry key value**
*attrName*_YES=1	*attrName*_NO=0	TRUE
*attrName*_YES=0	*attrName*_NO=1	FALSE

Note: The value for *attrName*_YES and *attrName*_NO must not be the same.

Create a text file, for example `C:\Notes60UpdateResp.txt` with the following content:

```
#Select Install Type
#-------------------
USER_INPUT_INSTALL_TYPE=\"\",\"Update Installation\"
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

#Adapter Name
#------------
AgentName=\"NotesAgent\"
AgentName_1=NotesAgent
AgentName_BOOLEAN_1=

#Choose Install Folder
#---------------------
USER_INSTALL_DIR=C:\\Program Files\\IBM\\ISIM\\Agents\\NotesAgent
```

If you do not want to restart the server after the adapter is installed, add this line to the end of the response file.

```
USER_REQUESTED_RESTART=NO
```

For a list of available attributes, see "Installation attributes" on page 100. If optional attributes are not specified in the response file, a default value is assigned to the associated registry key. See "Default values for optional registry keys" on page 108 for a list of the default values.

After you create the response file, you can use it to provide parameters to the installer for updating the adapter in silent installation:

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

Example

```
setup.exe -i silent -f "C:\Notes60UpdateResp.txt"
```

After the adapter is updated, an installation log file is created to replace the old file in the installation directory.

Adapter upgrade by using silent mode command parameters

You can upgrade the adapter with the use of silent mode command parameters.

To use the command line, prefix each attribute with the `-D` switch. No space exists in between D and the attribute. For example, issue the following command on a single line:

```
Setup.exe –i silent -DUSER_INPUT_INSTALL_TYPE=\"\",\"Update Installation\"
-DUSER_INPUT_INSTALL_TYPE_2=Update Installation
-DUSER_INPUT_INSTALL_TYPE_BOOLEAN_1=0
-DUSER_INPUT_INSTALL_TYPE_BOOLEAN_2=1
-DAgentName=\"NotesAgent9\"
-DAgentName_1=NotesAgent9
```

Note: The installation path must be marked with quotation marks. The path separator is \\ (double backslash).

The installer detects whether the adapter is installed on the system. To determine the installation location, the installer refers to the adapter registry keys. The installer updates the adapter only after it detects a prior installation of the adapter on the system. Otherwise the installation ends and a log file `IBM_Security_Lotus_Notes_Adapter_InstallLog.log` is generated.

Chapter 5. Configuring

After you install the adapter, configure it to function correctly. Configuration is based on your requirements or preference.

Configuring the adapter

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

About this task

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

Before you begin to configure the adapter, verify that you meet the following conditions:

- The Administrator ID must previously log on the client, on the same workstation where the adapter is running. The adapter requires that the last ID logged on the Notes client is the Administrator ID. For more information, see the first bullet in the installation verification topic.
- You must obtain a production certificate from a well-known certificate authority or create your own certificate with your own certificate authority. The adapter does not come prepackaged with a certificate.

To configure the adapter, take the following steps:

Procedure

1. Start the adapter service. Use the Windows Services tool.
2. Configure the Directory Access Markup Language (DAML) protocol for the adapter to establish communication with the Identity server.
3. Configure the adapter for event notification.
4. Install a certificate on the workstation where the adapter is installed and also on the Identity server to establish secure communication between them.
5. Install the adapter profile on the Identity server.
6. Configure the adapter service form.
7. Use the adapter configuration program, **agentCfg**, to view or modify the adapter parameters.
8. Configure the adapter account form.
9. Restart the adapter service after you modify the adapter configuration settings.

Related concepts

"SSL authentication configuration" on page 63
You can provide SSL authentication, certificates, and enable SSL authentication with the certTool utility.

Related tasks

"Configuring event notification" on page 41
When you enable event notification, the workstation on which the adapter is installed maintains a database of the reconciliation data.

"Modifying protocol configuration settings" on page 37
The adapter uses the DAML protocol to communicate with the Identity server.

Importing the adapter profile

"Starting the adapter configuration tool" on page 36

Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Starting the adapter configuration tool

Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

About this task

Note: The screens displayed in the tasks topics are examples. Information in the actual screens might be different.

Procedure

1. Browse to the Windows Command Prompt.
2. In the command prompt, change to the read/write `/bin` subdirectory of the adapter.If the adapter is installed in the default location for the read/write directory, run the following command.

   ```
   cd C:\Program Files\IBM\ISIM\Agents\adapter_name\bin\
   ```

3. Run the following command

   ```
   agentCfg -agent adapterAGNT
   ```

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

   The default configuration key is `agent`.

   Note: 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.

   ```
   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:
   ```

   The following table lists the different options available in the **Agent Main Configuration Menu**.

Table 6. Options for the main configuration menu	
Option	**Configuration task**
A	Viewing configuration settings
B	Changing protocol configuration settings
C	Configuring event notification
D	Changing the configuration key
E	Changing activity logging settings
F	Changing registry settings

Table 6. Options for the main configuration menu (continued)	
Option	**Configuration task**
G	Changing advanced settings
H	Viewing statistics
I	Changing code page settings

Related tasks

"Accessing help and other options" on page 60
Access the **agentCfg** help menu to view the list of available argument that you can use.

"Modifying protocol configuration settings" on page 37
The adapter uses the DAML protocol to communicate with the Identity 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.

```
Configuration Settings
----------------------------------------
Name            : adapter_nameAgent
Version         : 6.0.4.1200
ADK Version     : 6.0.1017
ERM Version     : 6.0.4.1200
Adapter Events  :
License         : NONE
Asynchronous ADD Requests  :  (Max.Threads:3)
Asynchronous MOD Requests  : (Max.Threads:3)
Asynchronous DEL Requests  :  (Max.Threads:3)
Asynchronous SEA Requests  :  (Max.Threads:3)
Available Protocols        : DAML
Configured Protocols       : DAML
Logging Enabled            : TRUE
Logging Directory          : C:\Program Files\IBM\ISIM\Agents\adapter_name\log
Log File Name              : adapter_name.log
Max. log files             : 3
Max.log file size (Mbytes) : 1
Debug Logging Enabled      : TRUE
Detail Logging Enabled     : FALSE
Thread Logging Enabled     : FALSE

Press any key to continue
```

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

Related tasks

"Starting the adapter configuration tool" on page 36
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Modifying protocol configuration settings

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

About this task

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.

```
Agent Protocol Configuration Menu
---------------------------------
Available Protocols: DAML
Configured Protocols: DAML
A. Add Protocol.
B. Remove Protocol.
C. Configure Protocol.

X. Done

Select menu option
```

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            FALSE  ;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)
L. DISABLE_SSLV3      TRUE   ;Disable SSLv3 and earlier
M. DISABLE_TLS10      FALSE  ;Disable TLS 1.0 and earlier
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	
Option	**Configuration task**
A	Displays the following prompt: `Modify Property 'USERNAME':` Type a user ID, for example, `agent`. The Identity server uses this value to connect to the adapter. The default user ID is `agent`.
B	Displays the following prompt: `Modify Property 'PASSWORD':` Type a password, for example, `agent`. The Identity 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 Identity 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 Identity server. This value is the DNS name or the IP address of the Identity 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 Identity server. The adapter uses this port number to connect to the Identity server. The default port number is 9443.

Table 7. Options for the DAML protocol menu (continued)

Option	Configuration task
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.
I	Displays the following prompt: `Modify Property 'VALIDATE_CLIENT_CE':` Specify TRUE for the Identity 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 Identity server to communicate with the adapter without a certificate. **Note:** – The property name is VALIDATE_CLIENT_CERT; however, it is truncated by the `agentCfg` to fit in the screen. – You must use certTool to install the appropriate CA certificates and optionally register the Identity server certificate.
J	Displays the following prompt: `Modify Property 'REQUIRE_CERT_REG':` This value applies when option I is set to TRUE. Type TRUE to register the adapter with the client certificate from the Identity server before it accepts an SSL connection. Type FALSE to verify the client certificate against the list of CA certificates. The default value is FALSE.
K	Displays the following prompt: `Modify Property 'READ_TIMEOUT':` Type the timeout value in seconds for IBM Security Verify Governance Identity Manager and the adapter connection. This option applies to setups that have a firewall between IBM Security Verify Governance Identity Manager and the adapter. This firewall has a timeout value that is less than the maximum connection age DAML property on IBM Security Verify Governance 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. 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.

Table 7. Options for the DAML protocol menu (continued)	
Option	**Configuration task**
L	Displays the following prompt: `Modify Property 'DISABLE_SSLV3':` SSLv3 is considered an unsecured protocol and is disabled by default. To enable SSLv3, set this value to FALSE. If this value does not exist or is not FALSE, the SSLv3 protocol will be disabled when using SSL. The DAML checks for an environment variable called *ISIM_ADAPTER_CIPHER_LIST*. This variable can contain a list of ciphers for the SSL protocol. DAML uses the openSSL library to support SSL. The cipher string is passed to openSSL during initialization. See the OpenSSL website at https://www.openssl.org/docs/apps/ciphers.html for the available cipher names and syntax. When this string is used, it only fails if none of the ciphers can be loaded. It is considered successful if at least one of the ciphers is loaded.
M	Displays the following prompt: `Modify Property 'DISABLE_TLS10':` Among other weaknesses, TLS 1.0 is vulnerable to man-in-the-middle attacks, risking the integrity and authentication of data communication. Disabling TLS 1.0 support on your server is sufficient to mitigate this issue. To disable TLS 1.0, set this value to TRUE. If this value does not exist or is not FALSE, the TLS 1.0 protocol is disabled when you are using SSL. **Note:** Use TLS 1.2 for all SSL communications. See "Enabling TLS 1.2 in Identity Manager" on page 51.

6. Follow these steps at the prompt:
   - 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**.
7. Repeat step 5 to configure the other protocol properties.
8. At the Protocol Properties menu, type X to exit.

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 Identity 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 Identity server and updates the local snapshot database.

Note: This adapter does not support 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 Verify Governance 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 Identity 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

Option	Configuration task
A	If you select this option, the adapter updates the Identity 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.

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.

Table 8. Options for the event notification menu (continued)	
Option	**Configuration task**
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 Verify Governance Identity Manager changes a password. Changes from IBM Security Verify Governance 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 Verify Governance 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.

Setting event notification triggers

By default, all the attributes are queried for value changes.

About this task

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

```
Event Notification Entry Types
----------------------------------------
A. erAceServerAccount
B. erAceServerGroups
C. erAceServerClients
D. erAceServerTokens
E. erAceProfiles
X. Done
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 the attributes that are returned during a user reconciliation. Type B for attributes that are returned during a group reconciliation. Type C for a list of the attributes that are returned during client reconciliation. Type D for a list of the attributes that are returned during tokens reconciliation. Type E for a list of the attributes that are returned during profiles 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 that might be different for other adapters.

```
Event Notification Attribute Listing
------------------------------------
(a) **erAceGroupName     (b) **erAceToken3ActivatedDate      (c) **erAceTokenAssign
(d) **erAceToken2Assign  (e) **erAceToken2EnableDisableDate  (f) **erAceClearPin
(g) **erAceClearPin2     (h) **erAceClearPin3                (i) **erAceClient
(j) **erAceCreatePin     (k) **erAceToken1ActivatedDate      (l) **erAceDays
(m) **erAceTokenName     (o) **erAcePasswdActivatedDate      (p) **erAceDuration
(q) **erAceToken3Assign  (r) **erAceToken3EnableDisableDate  (s) **erAceTokenEnable

(p)rev    page 1 of 3  (n)ext
----------------------------

X. Done
Select menu option:
```

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.

“Starting the adapter configuration tool” on page 36
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Configuring domain controllers for adapter-based event notification

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 9. Registry keys and description

Registry key	Description
LastChanged_*Context_Name*	The highest changed number for the object class User.
LastChanged_*Context_Name*_CNT	The highest changed number for the object class Container.
LastChanged_*Context_Name*_ GRP	The highest changed number for the object class Group.
LastChanged_*Context_Name*_EMB	The highest changed number for the object class Exchange Mailbox.
LastChanged_*Context_Name*_GRPCNT	The highest changed number for the object class Group Container.

Modifying an event notification context

Some adapters support multiple services.

About this task

An event notification context corresponds to a service on the Identity 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:

```
Modify Context Menu
-----------------------------
A. Context1
B. Context2
C. Context3
X. Done
Select menu option:
```

4. Type the option of the context that you want to modify.

```
A. Set attributes for search
B. Target DN:
C. Delete Baseline Database
X. Done
Select menu option:
```

   Options:

Table 10. Options for modify context	
Option	**Configuration task**
A	Adding search attributes for event notification
B	Configuring the target DN for event notification contexts
C	Removing the baseline database for event notification contexts

Related tasks

“Starting the adapter configuration tool” on page 36
Start the **agentCfg** tool to access the configuration menu, where you can modify the different 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 Identity 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 adapter does not have any attributes that you must specify for Event Notification.

Related tasks

"Adding search attributes for event notification" on page 47

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

Configuring the target DN for event notification contexts

During event notification configuration, the adapter sends requests to a service that runs on the Identity 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 48 describes each DN element.

Table 11. DN elements and definitions

Element	Definition
erservicename	Specifies the name of the target service.
o	Specifies the name of the organization.
ou	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.
rootsuffix	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 Identity server installation.

Results

The Modify Context Menu displays the new target DN.

Related tasks

"Starting the adapter configuration tool" on page 36

Start the **agentCfg** tool to access the configuration menu, where you can modify the different 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 D.
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 36
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Changing `activity logging` settings

When you enable logging, the adapter maintains a log file of all transactions, *`adapter_name`*`Agent.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
-----------------------------------
A. Activity Logging (Enabled).
B. Logging Directory (current: C:\Program Files\IBM\ISIM\Agents\adapter_nameAgent\log).
C. Activity Log File Name (current: adapter_nameAgent.log).
D. Activity Logging Max. File Size ( 1 mbytes)
E. Activity Logging Max. Files ( 3 )
F. Debug Logging (Enabled).
G. Detail Logging (Disabled).
H. Base Logging (Disabled).
I. Thread Logging (Disabled).
X. Done
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*

Option	Configuration task
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.

*Table 12. Options for the **activity logging** menu (continued)*	
Option	**Configuration task**
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.
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 36
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Enabling TLS 1.2 in Identity Manager

After Setting up certificates in Identity Manager and Adapter, Enable TLS 1.2 by adding or modifying the following line in `enRole.properties` file in ISIM (equivalent for ISPIM and IGI).

com.ibm.daml.jndi.DAMLContext.SSL_PROTOCOL=TLSv1.2

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

You can modify the non-encrypted registry settings.

Procedure

1. At the Agent Registry Menu, type A. The Non-encrypted Registry Settings Menu is displayed.

```
Agent Registry Items
--------------------------------
01. group_name            'TRUE'
--------------------------------
           Page 1 of 1

A. Add new attribute
B. Modify attribute value
C. Remove attribute
X. Done
Select menu option:
```

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

Table 13. Attribute configuration option descriptions

Option	Configuration task
A	Add new attribute
B	Modify attribute value The adapter does not have any encrypted registry settings; therefore, option B is not applicable.
C	Remove attribute

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.

   The following table lists the registry keys and the available settings. Example settings are for Lotus Notes:

Table 14. Registry key descriptions

Key	Description

Table 14. Registry key descriptions (continued)	
Attributes not RECONCILED	Specifies a list of attribute names to exclude from the reconciliation process. If more than one name is listed, separate them by semicolon. The default values are **Certificate;$UpdatedBy;$Revisions**.
Attributes Reconciled	Specifies a list of attribute names to include in the reconciliation process. If more than one name is listed, separate them by semicolon. If this field is left blank, all attributes except those attributes specified in the Attributes not reconciled list are returned during a reconciliation.
AuditShortName	Specifies whether your adapter needs the IP address to be a unique ID on the Identity server when the short name value is NULL. Set this key to **TRUE** only when the Use ShortName key is also set to **TRUE**. The default value is **FALSE**.
Certification File Location	Specifies the file path for the certifier ID file. The certifier ID file is the default file used for ADD operations. If the file path for the certifier file is not specified when you add a user, the file path from this field is used. If you specify the path for the certifier file when you add a user, the file path in this field is ignored. For example, you might specify the certifier ID file path as `C:\Lotus\Domino\cert.id`.
Change HTTPPassword First	Specifies how to store the HTTP password during a change operation. Set the value of this registry key to **TRUE**, if you want to change the HTTP password first before changing the user password. The default value is **FALSE**.
Change HTTPPassword Only	Specifies whether to change only the HTTP password of the user in the Change Password operation from IBM Security Verify Governance Identity Manager. Set the value of the registry key to **TRUE** if only the HTTP password of the user is to be changed in password change operation from IBM Security Verify Governance Identity Manager. The default value is **FALSE**.
CopyIDFileFromStore	Specifies whether to copy the ID file from the NotesIdsAddressBook or the `Certlog.nsf` file to the specified location. The location is specified by the User ID file path attribute in the account form of the user. If the value of the registry key is **TRUE**, the adapter copies the ID file of the user from the NotesIDsAddressBook or the `Certlog.nsf` file to the location specified by the attribute, User ID file Path. The copy occurs only if the ID file is not present at the location specified by the User ID file path. The default value of the registry key is **FALSE**.

Table 14. Registry key descriptions (continued)	
CustomEruid	Specifies the resource name of the Custom ERUID attribute. The following data types are supported: • Single value STRING attribute • Multiple value STRING attribute • Single value NUMERIC attribute
Delete Group	Specifies the name of the group that is used by the adapter to keep the CN values of the deleted users. This group must be created on the adapter before running the adapter.
Delete Mail DB	Specifies whether your adapter requires the deletion of the mail database file when a user deletion occurs. The default value is **TRUE**.
Domino Server	Specifies the Lotus Domino Registration Server name that the adapter uses.
Domino Version Number	Specifies the version number of your Lotus Domino server. The default value is **version 6**.
Execute AdminP Operation	Specifies whether the AdminP operation is to be used to deprovision a user. Set the value of this registry key to **TRUE** if you want AdminP to be used when deprovisioning a user from IBM Security Verify Governance Identity Manager. The default value is **FALSE**.
IsIDVaultConfigured	Specifies whether ID Vault is configured on the Domino Server. The default value is FALSE.
Log DB	Specifies the name of a Lotus Notes database. This database file must be created on the Lotus Domino server before running the Lotus Notes Adapter. If Log DB is in a multilevel directory structure in the data directory of Lotus Domino server at `\admindatabases\adapterdatabases`, then the value of registry key Log DB must be `admindatabases\adapterdatabases\logdb.nsf`
Mail Template Server	Specifies the server name for the mail template files that are used by the adapter. If a value is not specified for this registry key, the adapter uses the mail template files from the Domino Registration Server. The files for the Domino Registration Server are specified for the Domino Server registry key.

Table 14. Registry key descriptions (continued)	
NoteIDsAddressBook	Specifies the name of the Lotus Notes database file that is used by the adapter to store the user information (ID file, password in ADK encrypted form and the CN name of the user). This database file must be created on the Lotus Domino server before running the Lotus Notes Adapter. If `NoteIDsAddressBook` is in a multilevel folder directory structure in the data directory of the Lotus domino server at `\admindatabases\adapterdatabases`, then the value of registry key `NoteIDsAddressBook` must be `admindatabases\adapterdatabases \NoteIDsAddressBook.NSF`.
Notes Address Book	If the name of the Lotus Notes Address Book is anything other than `names.nsf`, specifies the name of the Lotus Notes Address Book. The Lotus Notes Address Book database file is different from the NoteIdsAddressBook database file.
Refresh ITIM_ERUID	Specifies whether to delete the ITIM_ERUID filed from the person document for all users, during a reconciliation. The value for ITIM_ERUID comes from the Full name, Short name, or Custom field. The default value is **FALSE**.
Store ERUID in FullName	Specifies whether to store the ERUID or User ID attribute in the FullName field in the person document. Set the value of this registry key to **TRUE**, if you want to store the attribute in the FullName field. The default value is **TRUE**. This registry key can be used only when the ShortName, Custom Attribute, or ITIM_ERUID fields are used to store the ERUID attribute.
Suspend Group	Specifies the name of the group that is used by the Lotus Notes Adapter to keep the CN values of the suspended users. This group must be created on the Lotus Domino server before running the adapter.
Suspend HTTPPassword	Specifies the name of the group that is used by the Lotus Notes Adapter to keep the CN values of the suspended users for restricting Internet access. This group must be created on the Lotus Domino server before running the adapter.
Synchronize HTTPPassword	Specifies whether your Lotus Notes Adapter requires the User Password to be set to Internet Password during an ADD or MODIFY request. The default value is **TRUE**.
Update ServerDoc	Specifies whether to include all suspended groups in the Not Access Server field of the server document. Set the value of this registry key to **TRUE** to include all suspended groups in the Not Access Server field. The default value is **FALSE**.

Table 14. Registry key descriptions (continued)	
UpdateShadowNAB	Specifies whether to create a user entry in the NotesIdsAddressBook, if it does not exist. Set the value of this registry key to **TRUE**, if the user's entry is to be created when the user is reregistered and the user's entry does not exist in the NotesIdsAddressBook. The default value is **FALSE**.
Use ITIM_ERUID	Specifies whether: a. The Lotus Notes Adapter creates an ITIM_ERUID field in the person document when a new user ID is created b. The Lotus Notes Adapter will save the value of Eruid from the Identity server; to the ITIM_ERUID field in the person document of a user ID c. During the first reconciliation after this key is set to **TRUE**, the Lotus Notes Adapter will create the ITIM_ERUID field in the person document for each user. The value from the Full name, Short name, or Custom field will be used for the Eruid. The default value is **FALSE**.
Use ShortName	Specifies whether your Lotus Notes Adapter is configured to use the short name value as a unique ID on the Identity server. If you set this value to TRUE, do not use the short name attribute that is on the Lotus Notes account form. The adapter will ignore the specified value of the Short Name field during an ADD or MODIFY request. The default value is **FALSE**.
Workstation ID File Location	Specifies the path to the Lotus Domino server Administrator ID file. The adapter uses this Administrator ID file to connect to the Lotus Domino server.
Workstation Password	Specifies the password for the Lotus Domino server Administrator ID file. The adapter will use this password to connect to the Lotus Domino server. The password is in ADK encrypted format and can be changed using the agentCfg tool.
CreateGroupIfNotPresent	Specifies whether to create a group on the Lotus Domino server if not available on the Lotus Domino server when you perform the user add or user modify operation from IBM Security Verify Governance Identity Manager. If you set the value to **TRUE**, the adapter creates the group if not available on the Lotus Domino server when you perform the user add or user modify operation. If you set the value to **FALSE**, the adapter does not create the group on the Lotus Domino server if not available on the Lotus Domino server when you perform the user add or user modify operation. The default value is **FALSE**.
PasswordCountStatusAdmin	The adapter uses this registry key. Do not modify the registry key.

Table 14. Registry key descriptions (continued)	
PasswordCountStatusCert	The adapter uses this registry key. Do not modify the registry key.

Modifying encrypted registry settings

You can access registry settings.

Procedure

1. Type B (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 G 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

Option	Description
A	Forces the adapter to allow only 1 request at a time. The default value is FALSE.
B	Limits the number of ADD requests that can run simultaneously. The default value is 3.
C	Limits the number of MODIFY requests that can run simultaneously. The default value is 3.
D	Limits the number of DELETE requests that can run simultaneously. The default value is 3.
E	Limits the number of SEARCH requests that can run simultaneously. The default value is 3.
F	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.
G	This option is no longer supported.
H	This option is no longer supported.
I	Currently, this adapter does not support processing filters directly. This option must always be FALSE.
J	Sets the thread priority level for the adapter. The default value is 4.

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.

"Starting the adapter configuration tool" on page 36

Start the **agentCfg** tool to access the configuration menu, where you can modify the different 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.

```
  Agent Request Statistics
-------------------------------------------------------------------
Date       Add       Mod       Del       Ssp       Res       Rec


-------------------------------------------------------------------

02/15/06  000001    000000    000000     000000    000000    000001

-------------------------------------------------------------------

X. Done
```

3. Type X to return to the **Main Configuration Menu**.

Related tasks

“Starting the adapter configuration tool” on page 36
Start the **agentCfg** tool to access the configuration menu, where you can modify the different 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 I 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 36
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Accessing help and other options

Access the **agentCfg** help menu to view the list of available argument that you can use.

About this task

Note: The screens displayed in the tasks topics are examples. Information in the actual screens might be different.

Procedure

1. Access the **Agent Main Configuration Menu**.
2. Type X to display the command prompt.
3. Type **agentCfg** `-help` at the prompt to display the help menu and list of arguments.

```
Usage:
-version               ;Show version
-hostname <value>      ;Target nodename to connect to (Default:Local host IP address)
-findall               ;Find all agents on target node
-list                  ;List available agents on target node
-agent <value>         ;Name of agent
-tail                  ;Display agent's activity log
-portnumber <value>    ;Specified agent's TCP/IP port number
-netsearch <value>     ;Lookup agents hosted on specified subnet.
-codepages             ;Display list of available codepages.
-help                  ;Display this help screen
```

The following table describes each argument.

*Table 16. Arguments and descriptions for the **agentCfg** help menu*

Argument	Description
-version	Use this argument to display the version of the **agentCfg** tool.
-hostname *value*	Use the **-hostname** argument with one of the following arguments to specify a different host: • **-findall** • **-list** • **-tail** • **-agent** Enter a host name or IP address as the value.
-findall	Use this argument to search and display all port addresses 44970 - 44994 and their assigned adapter names. This option times out the unused port numbers, therefore, it might take several minutes to complete. Add the **-hostname** argument to search a remote host.

*Table 16. Arguments and descriptions for the **agentCfg** help menu (continued)*	
Argument	**Description**
-list	Use this argument to display the adapters that are installed on the local host of the adapter. By default, the first time you install an adapter, it is either assigned to port address 44970 or to the next available port number. You can then assign all the later installed adapters to the next available port address. After the software finds an unused port, the listing stops. Use the **-hostname** argument to search a remote host.
-agent *value*	Use this argument to specify the adapter that you want to configure. Enter the adapter name as the value. Use this argument with the **-hostname** argument to modify the configuration setting from a remote host. You can also use this argument with the **-tail** argument.
-tail	Use this argument with the **-agent** argument to display the activity log for an adapter. Add the **-hostname** argument to display the log file for an adapter on a different host.
-portnumber *value*	Use this argument with the **-agent** argument to specify the port number that is used for connections for the **agentCfg** tool.
-netsearch *value*	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.
-codepages	Use this argument to display a list of available code pages.
-help	Use this argument to display the Help information for the **agentCfg** command.

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

agentCfg -list
Displays:

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

The default node for the Identity server must be 44970. The output is similar to the following example:

```
Agent(s) installed on node '127.0.0.1'
-----------------------
adapterAGNT   (44970)
```

agentCfg -agent ***adapterAGNT***
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 similar to the following example:

```
Agent(s) installed on node '192.9.200.7'
-----------------
agentname   (44970)
```

agentCfg -agent ***adapterAGNT*** **-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.

Configuring the adapter to run multiple Lotus Domino servers

After you configure the Lotus Notes adapter for IBM Security Verify Governance Identity Manager, more configuration is required to allow the adapter to work with multiple Lotus Domino servers.

About this task

While the Lotus Notes adapter can work with multiple Lotus Domino servers, it cannot do so simultaneously.

To configure the Lotus Notes adapter to work with multiple instances of the Lotus Domino server, complete the following steps:

Procedure

1. Log in to the Lotus Domino server as the Domino Administrator.
2. You can change the registry settings by using the adapter configuration tool agentCfg. Change the following registry settings:
   - Domino Server
   - Workstation ID File Location
   - Workstation Password
3. Verify that the other registry settings apply to the new Lotus Domino server.
   For example, ensure that the value of `NoteIdsAddressBook` applies to the new server settings. Refer to the installation worksheet for the registry settings for the Lotus Domino server.

Related tasks

"Starting the adapter configuration tool" on page 36
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Configuring the adapter to use Custom ERUID

After you install the Lotus Notes adapter, a new registry key named **CustomEruid** is created with an empty value.

About this task

The value of this key must be the resource field name of the attribute to be used as Custom ERUID.

Note: Existing user attributes that are supported by the Lotus Notes adapter are not allowed as Custom ERUID by the Lotus Notes adapter.

To use Custom ERUID, complete the following steps:

Procedure

1. Start the Lotus Notes adapter.

2. Start the agentCfg tool to add a value to the registry key **CustomEruid**.
3. Add the name of the field from Lotus Notes (to be used as Custom ERUID) to the **CustomEruid** registry key.

   Assume the following conditions:

   - A **DirSynchKey**field is on the Domino resource.
   - A **DirSynchKey** field is added to the `CustomAttributes.xml` file.
   - The **DirSynchKey** field is to be used as Custom ERUID.

   Add the value of **DirSynchKey** to the registry key **CustomEruid**.
4. Restart the adapter.

Configuring the adapter to use ITIM_ERUID

After you install the Lotus Notes adapter, two new registry keys, **Use ITIM_ERUID** and **Refresh ITIM_ERUID**, are created with a default value of FALSE.

About this task

The Lotus Notes adapter uses these registry keys as follows:

Use ITIM_ERUID

- To create the **ITIM_ERUID** field in the person document of each user during an ADD operation.
- To save the value of **Eruid** from the IBM Security Verify Identity server to the **ITIM_ERUID** field in the person document of each user.
- To use the value of the **ITIM_ERUID** field as the value of **Eruid** to be sent back to the IBM Security Verify Identity server.

Refresh ITIM_ERUID
During a reconciliation operation, to delete the **ITIM_ERUID** field from the person document for all users.

You can use the agentCfg utility, depending on your Lotus Notes adapter and Domino deployment of the UserID attribute storage location on the Lotus Domino server.

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 Identity server or from the adapter. The Identity 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 Identity 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 Identity server.

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

Running in SSL mode with Windows 2008

You can use Windows 2008 and 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.

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 69
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 Identity 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 with various 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” on page 66
- “Configuring certificates for two-way SSL authentication” on page 67
- “Configuring certificates when the adapter operates as an SSL client” on page 68

Configuring certificates for one-way SSL authentication

In this configuration, the Identity server and the adapter use SSL.

About this task

Client authentication is not set on either application. The Identity 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 Identity server. The Identity server uses the installed CA certificate to validate the certificate that is sent by the adapter.

In Figure 5 on page 67, Application A operates as the Identity server, and Application B operates as the adapter.

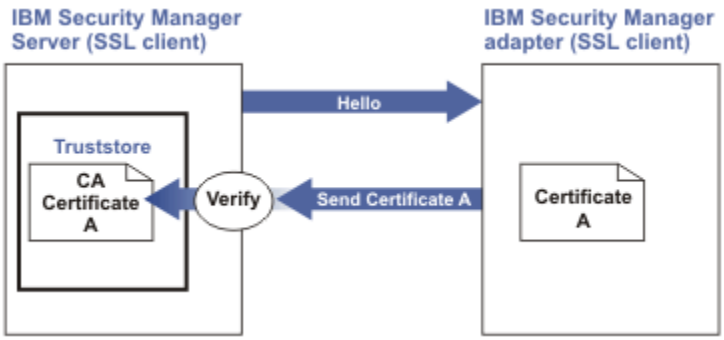


Figure 5. One-way SSL authentication (server authentication)

To configure one-way SSL, do the following tasks for each application:

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:
      i) 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.
      ii) 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 Identity server, do one of these steps:
   - If you used a signed certificate that is issued by a well-known CA:
     a. Ensure that the Identity 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 Identity 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 Identity server.

Related tasks

"Starting certTool" on page 69
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 Identity 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 Identity 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 Identity server operates as Application A and the adapter operates as Application B.

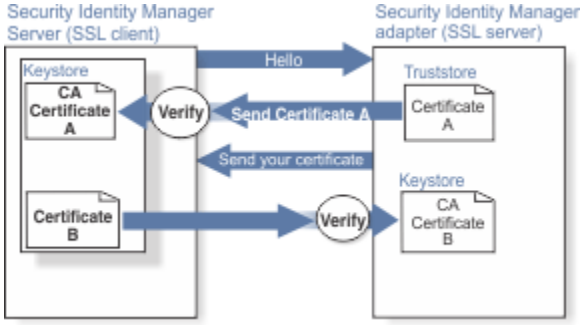


Figure 6. Two-way SSL authentication (client authentication)

Before you do the following procedure, configure the adapter and Identity 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 Identity server.

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

Procedure

1. On the Identity 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 Identity 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 66
In this configuration, the Identity server and the 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 Identity 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 7 on page 69 describes how the adapter operates as an SSL server and an SSL client. To communicate with the Identity server, the adapter sends its certificate for authentication. To communicate with the web server, the adapter receives the certificate of the web server.

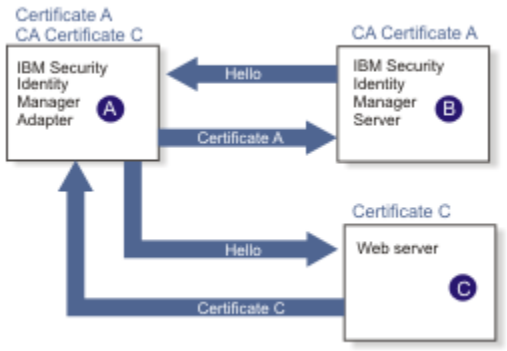


Figure 7. Adapter operating as an SSL server and an SSL client

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, take these steps:

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

You can have the software send an event notification when the adapter initiates a connection to the web server (used by the Identity server).

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:

   ```
   cd C:\Program Files\IBM\ISIM\Agents\adapter_name\bin\
   ```

3. Type `CertTool -agent` *`agent_name`* at the prompt.

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

```
Main menu - Configuring agent: agentnameAgent
 ------------------------------
A. Generate private key and certificate request
B. Install certificate from file
C. Install certificate and key from PKCS12 file
D. View current installed certificate

E. List CA certificates
F. Install a CA certificate
G. Delete a CA certificate

H. List registered certificates
I. Register certificate
J. Unregister a certificate

K. Export certificate and key to PKCS12 file

X. Quit

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 Identity server.

E. List CA certificates
Show the installed CA certificates. The adapter communicates only with Identity server 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 Identity server or the web server. Use these options to register certificates on 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 Identity 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 73
To list the certificate on your workstation, type D at the Main menu of certTool.

Related tasks

"Generating a private key and certificate request" on page 71
A certificate signing request (CSR) is an unsigned certificate that is a text file.

"Installing the certificate" on page 72
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 73
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 73
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 74
You can delete a CA certificate from the adapter directories.

"Viewing registered certificates" on page 74
The adapter accepts only the requests that present a registered certificate when client validation is enabled.

"Registering a certificate" on page 75
You can register a certificate for the adapter.

"Unregistering a certificate" on page 75
You can unregister a certificate for the adapter.

"Exporting a certificate and key to a PKCS12 file" on page 75
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-----
MIIB1jCCAT8CAQAwgZUxEjAQBgNVBAoTCWFjY2VzczM2MDEUMBIGA1UECxMLZW5n
aW5lZXJpbmcxEDAOBgNVBAMTB250YWdlbnQxJDAiBgkqhkiG9w0BCQEWFW50YWdl
bnRAYWNjZXNzMzYwLmNvbTELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3Ju
aWExDzANBgNVBAcTBklydmluZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
mR6AcPnwf6hLLc72BmUkAwaXcebtxCoCnnTH9uc8VuMHPbIMAgjuC4s91hPrilG7
UtlbOfy6X3R3kbeR8apRR9uLYrPIvQ1b4NK0whsytij6syCySaFQIB6V7RPBatFr
6XQ9hpsARdkGytZmGTgGTJ1hSS/jA6mbxpgmttz9HPECAwEAAaAAMA0GCSqGSIb3
DQEBAgUAA4GBADxA1cDkvXhgZntHkwT9tCTqUNV9sim8N/U15HgMRh177jVaHJqb
N1Er46vQSsOOOk4z2i/XwOmFkNNTXRVl9TLZZ/D+9mGZcDobcO+lbAKlePwyufxK
Xqdpu3d433H7xfJJSNYLYBFkrQJesITqKft0Q45gIjywIrbctVUCepL2
 -----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_nameAgent\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
   ```

   For example: `C:\Program Files\IBM\ISIM\Agents\NotesAgent\bin`
2. At the **Main Menu** prompt for the certTool, type `C` to display the following prompt:

   ```
   Enter name of PKCS12 file:
   ------------------------------------------------------------------------
   ```
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,st=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
Valid To: Wed Jul 26 23:59:59 2006
```

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.

Managed resource configuration

Configuring the Domino server involves several steps that you must complete to ensure the correct set up for the Lotus Notes Adapter.

While these steps can be performed prior to installing the Lotus Notes Adapter, they must be performed before the adapter will function properly.

Configuration of the Windows server is also required.

Lotus Domino server configuration

In order for the Lotus Notes Adapter to work properly, do the following configuration on the Lotus Domino server.

Database creation on the Lotus Domino server

The following registry keys are created by the Lotus Notes Adapter installer.

The values of the registry keys are user-defined; the values listed in this table are examples:

Table 17. Registry keys and their values

Registry key	Key value/database name
NoteIDsAddressBook	NoteIDsAddressBook.nsf
Log DB	LogDB.nsf

Note:

- If `NoteIDsAddressBook.nsf` is in a multilevel folder directory structure in the data directory of Lotus Domino server at `\admindatabases\adapterdatabases`, then the value of registry key `NoteIDsAddressBook` must be `admindatabases\adapterdatabases \NoteIDsAddressBook.NSF`.
- If `LogDB.nsf` is in a multilevel directory structure in the data directory of the Lotus Domino server at `\admindatabases\adapterdatabases`, then the value of registry key Log DB must be `admindatabases\adapterdatabases\logdb.nsf`.

To create a database on the Lotus Domino server, complete the following steps for each registry key:

1. In the Domino Administrator console, click **File** > **Database** > **New**.
2. In the New Database window, set the parameters for database creation according to the following values:

Table 18. Values to specify during database creation

Field name	Value
Server	Name of the registration server.
Title	Title of the new database.
File name	File name of the database to be created. This value corresponds to the value of the registry key; for example, NoteIDsAddressBook and LogDB.

Table 18. Values to specify during database creation (continued)	
Field name	**Value**
Template	The suggested template for the NoteIDsAddressBook and LogDB database files is the **Personal Address Book** template.

Click **OK**.

3. Repeat steps 1 and 2 for each registry key.

Creating a group on the Lotus Domino server

Before you begin to create a group on the Lotus Domino server, set the values of the following registry keys.

About this task

The values of the registry keys are user defined; the values listed in the table are examples:

Table 19. Registry keys and their values	
Registry key	**Key value/group name**
Suspend Group	Suspended users
Suspend HTTPPassword	HTTP Suspended users
Delete Group	Deleted users

To create a new group on the Lotus Domino server, complete the following steps for each registry key:

1. In the Domino Administrator console, select the **People & Groups** tab.
2. In the left window pane, click on **Groups**.
3. In the Group View, click the Add Group icon.
4. In the New Group window, set the parameters for group creation according to the following values:

Table 20. Values to specify during group creation	
Field name	**Value**
Group name	Name of the group
Group type	Multi-purpose
Description	Brief description of the group

Click Save & Close.

5. Repeat steps 3 and 4 for each registry key.

MoveInHierarchy/RequestRename

When you are moving a person in hierarchy, it is now possible to perform a simultaneous rename operation.

To do this, do the following steps:

1. Issue the **Adminp** command **MoveUserInHierarchy** as described in the Notes Adapter Users Guide.
2. When you are issuing the **Adminp** command **MoveComplete**, specify the First Name, Middle Initial, and Last Name if you want to rename the user.

Note: Ensure that the `certlog.nsf` is available on the server that handles move user request.

The adapter fails the **Adminp MoveUserInHierarchy** request if the `certlog.nsf` is missing on the server that handles the move request. The domino document on the cert log states: "`Create a replica of the Certification Log on every server that is a registration server and on every server that stores a Domino Directory that is used for user management -- for example, renaming and recertifying users. If the server whose Domino Directory replica you are using does not have a Certification Log, user management actions will fail.`"

Notes API for cluster failover

IBM Notes adapter now takes advantage of special options in Notes API for cluster failover.

The failover occurs only when the Domino server is unavailable when you are opening a database. For example, `Names.nsf`. If the server is unavailable after the database is opened, the operation fails and no failover takes place. For more information on clustering and failover, see the Domino Administration Guide.

Specifying required environment settings on Windows

You can add the directory path of the `nnotes.dll` file to the environment path.

Procedure

1. On your desktop, right click on the **My Computer** icon and select the **Properties** menu.
2. In the System Properties window, click on the **Advanced** tab, then the **Environment Variables** button.
3. On the Advanced tab, select **Path** under the System variables section and click **Edit**.
4. In the Variable Value field, append the location of your Notes client. For example:

   ```
   C:\Lotus\Notes
   ```

5. In the Edit System Variable window, click **OK**.
6. In the Environment Variables window, click **OK**.
7. In the System Properties window, click **Apply** and then **OK**.
8. If the Lotus Notes Adapter is running, stop the adapter and restart it.

   Ensure that the `certlog.nsf` is available on the server that handles move user request.

   The adapter fails the `adminP MoveUser` request if the `certlog.nsf` is missing on the server that handles the move request. The domino document on the certlog states: "`Create a replica of the Certification Log on every server that is a registration server and on every server that stores a Domino Directory that is used for user management -- for example, renaming and recertifying users. If the server whose Domino Directory replica you are using does not have a Certification Log, user-management actions will fail.`".

   ITIM Notes Adapter needs to be notes cluster aware
   IBM Notes adapter now takes advantage of special options in Notes API for cluster failover. Note that the failover occurs only when the Domino server becomes unavailable while opening a database (e.g. Names.nsf). If the server becomes unavailable after the database is opened, then the operation would fail and no failover would take place. Please consult Domino Administration Guide to learn more about clustering and failover.

   Notes: Support for RequestRename/MoveInHierarchy combined adminp request type
   When you are moving a person in hierarchy, it is now possible to perform a simultaneous rename operation. To do this, do the following steps:

   a. Issue the Adminp command MoveUserInHierarchy as described in the Notes Adapter Users Guide.
   b. When Issuing the Adminp command MoveComplete, specify the First Name, Middle Initial, and Last Name if you want to rename the user.

Customizing the Lotus Notes Adapter

You can update the Lotus Notes Adapter JAR file, `NotesProfile.jar`, to change the adapter schema, account form, service form, and profile properties.

About this task

To make updates, extract the files from the JAR file, make changes to the necessary files, and repackage the JAR file with the updated files. Follow these steps in order to customize the Lotus Notes Adapter profile:

Procedure

1. Copy the JAR file to a temporary directory and extract the files.

   For more information on extracting the files, see "Copying the NotesProfile.jar file and extracting the files" on page 79.
2. Make the appropriate file changes.
3. Install the new attributes on the IBM Security Verify Governance Identity Manager.

   For more information on updating this file, see "Creating a JAR file and installing the new attributes" on page 80.

Copying the `NotesProfile.jar` file and extracting the files

You can modify the profile JAR file to customize your environment.

About this task

The profile JAR file, `NotesProfile.jar`, is included in the Lotus Notes Adapter compressed file that you downloaded from the IBM Web site. The `NotesProfile.jar` file contains the following files:

- `CustomLabels.properties`
- `erNotesAccount.xml`
- `erNotesDAMLService.xml`
- `resource.def`
- `schema.dsml`

When you finish updating the profile JAR file, install it on the IBM Security Verify Governance Identity Manager. For more information on the profile installation, see Importing the adapter profile.

To modify the `NotesProfile.jar` file, complete the following steps:

Procedure

1. Log in to the system where the Lotus Notes Adapter is installed.
2. On the **Start** menu, click **Programs** > **Accessories** > **Command Prompt**.
3. Copy the `NotesProfile.jar` file into a temporary directory.
4. Extract the contents of` the `NotesProfile.jar` file into the temporary directory by running the following command:

   ```
   cd c:\temp
   jar -xvf NotesProfile.jar
   ```

   The jar command will create the `c:\temp\NotesProfile` directory.
5. Edit the appropriate file.

Editing adapter profiles on the UNIX or Linux® operating system

The adapter profile `.JAR` file might contain ASCII files that are created by using the MS-DOS ASCII format (For example, `schema.dsml`, `CustomLabels.properties`, and `service.def`).

About this task

If you edit an MS-DOS ASCII file on the UNIX operating system, you see character *^M* at the end of each line. This is the extra character 0x0d that is used to indicate a new line of text in MS-DOS. Tools, such as, `dos2unix` are used to remove the *^M* character.

You might also want to use the text editors, such as, vi editor that ignore the *^M* character. In the mentioned command, the *^M* (or Ctrl-M) must be entered by pressing *^v^M* (or Ctrl V Ctrl M) in sequence.

Example

For example, if you are using the vi editor, you can remove the *^M* character by performing the following steps:

1. From the vi editor command mode, run the following command:

   ```
   :%s/^M//g
   ```

   and press **Enter**.

Enter the *^M* (or Ctrl-M) by pressing *^v^M* (or Ctrl V Ctrl M) in sequence. The *^v* preface indicates to the vi editor to use the next keystroke instead of considering the entry as a command.

Creating a JAR file and installing the new attributes

After you modify the `schema.dsml` and `CustomLabels.properties` files, you must import these files, and any other files that were modified for the adapter, into the IBM Security Verify Governance Identity Manager for 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:

   ```
   cd c:\temp
   jar -cvf NotesProfile.jar NotesProfile
   ```

2. Import the `NotesProfile.jar` file into the IBM Security Verify Governance Identity Manager Application Server.

   For more information on importing the file, see Importing the adapter profile.

3. Stop and start the Identity server.

What to do next

Note: If you are upgrading an existing adapter profile, the new adapter profile schema is not reflected immediately. Stop and start the Identity server to refresh the cache and the adapter schema. For more information on upgrading an existing adapter, see “Upgrading the Lotus Notes Adapter” on page 31.

Managing passwords for account restoration

When a person's accounts are restored from being previously suspended, you are 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 Lotus Domino 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 Identity server 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 Lotus Notes Adapter to require a new password when the account is restored.

In the `resource.def` file, you can define whether 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 Lotus Notes Adapter to *not* prompt for a new password when restoring accounts:

Note: If you are upgrading an existing adapter profile, the new adapter profile schema will not be reflected immediately. You need to stop and start the Identity server to refresh the cache and therefore the adapter schema. For more information on upgrading an existing adapter, see "Upgrading the Lotus Notes Adapter" on page 31.

Procedure

1. Stop the Identity server.
2. Extract the files from the `NotesProfile.jar` file.

   For more information on customizing the adapter profile file, see "Customizing the Lotus Notes Adapter" on page 79.
3. Change to the `\NotesProfile` 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 = "TRUE"/>
   <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 will *not* be prompted for a password when an account is restored.
5. Create a new `NotesProfile.jar` file using the `resource.def` file and import the adapter profile file into the Identity server.
6. Start the Identity server again.

Chapter 6. Troubleshooting

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. This topic provides information and techniques for identifying and resolving problems that are related to the adapter, including troubleshooting errors that might occur during the adapter installation.

Techniques for troubleshooting problems

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 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 you start 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 operating system, or is it common across multiple 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 are not fully tested together.

When does the problem occur?

Develop a detailed timeline of events that lead 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 use 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 done?
- Is a certain sequence of events required 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 occur 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. 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?
- Do multiple users or applications have the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

Troubleshooting the Lotus Notes Adapter installation

You can identify and resolve problems that are related to the Lotus Notes Adapter installation.

About this task

To troubleshoot the adapter installation, complete the following steps:

Procedure

- If the Lotus Notes Adapter installation fails or does not install correctly, check the adapter installer log file, `NotesAgentSetup.log`, for incorrect input and error messages.

  This log file is generated in the Lotus Notes Adapter installation directory. The name of the Lotus Notes Adapter directory, along with its path, is specified during the installation. Use the log file to find out what operation failed, not to get information on the correctness of the values entered.
- Verify that the input values given while installing the adapter are correct.

  Compare the values that you entered during the installation procedure with those specified in Adapter Installation.
- Check for the following error message to be displayed by the installer while inputting information for the Administrator ID file:

  ```
  "FileName" is not a valid file name or does not exist.
  Please specify a valid file name.
  ```

  To correct this error, correctly specify the Administrator ID file path.

Chapter 7. Uninstalling

To remove an adapter from the Identity server for any reason, you must remove all the components that were added during installation. Uninstalling the adapter involves running the uninstaller and removing the adapter profile from the Identity server.

Uninstalling the adapter from the target server

You can remove the Lotus Notes Adapter.

Procedure

1. Stop the adapter service.
2. Run the uninstaller. To run the uninstaller:
   a. Navigate to the adapter home directory. For example, navigate to the `ISIM/agents/adaptername/_uninst` directory.
   b. Double-click the `uninstaller.exe` file.
   c. In the Welcome window, click **Next**.
   d. In the uninstallation summary window, click **Next**.
   e. Click **Finish**.
   f. Inspect the directory tree for the adapter directories, subdirectories, and files to verify that uninstall is complete.

Deleting the adapter profile

Remove the adapter service/target type from the Identity server. Before you delete the adapter profile, ensure that no objects exist on the Identity server that reference the adapter profile.

About this task

Objects on the Identity server that can reference the adapter profile:

- Adapter service instances
- Policies referencing an adapter instance or the profile
- Accounts

Note: The Dispatcher component must be installed on your system for adapters to function correctly in a Security Directory Integrator environment. When you delete the adapter profile, do not uninstall the Dispatcher.

For specific information about how to delete the adapter profile, see the IBM Security Verify Governance Identity Manager product documentation.

Chapter 8. Reference

Reference information is organized to help you locate particular facts quickly, such as adapter attributes, registry settings, and environment variables.

Adapter attributes and object classes

Adapter attributes and object classes are required for customization, creating provisioning rules, and understanding what service/target attributes are supported by the adapter. The Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.

Adapter attributes and object classes

The Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.

As part of the adapter implementation, a dedicated account for IBM Security Verify Governance Identity Manager to access the Lotus Domino server is created on the Lotus Domino server.

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

Table 21. Attributes automatically defined for a newly created user ID

Attribute	Default Value
CertExpDate	If this value is not specified, the default of 2 years is taken.
CheckPassword	Do not check password.
Clean-up setting	Do not clean up.
Generational Qualifier	I
MailOwnerAccess	Designer
MailSystem	Notes
PersonalTitle	Mr.
User Can Roam	No

Attribute descriptions

The IBM Security Verify Governance 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 Identity server requests from the adapter. Table 22 on page 89 lists the account form attributes that the adapter uses.

Table 22. Notes user account form attributes, descriptions, and corresponding data types

Attribute	Directory server attribute	Description	Data type
$Conflict	erNotesReplicationConflict	Specifies whether there is a replication conflict	Boolean

Table 22. Notes user account form attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data type
AddCertPasswd	erNotesPasswdAddCert	Specifies the password of the certifier ID file	String
AddCertPath	erNotesAddCertPath	Specifies the path to the certifier ID	String
AdminpCertifier	erNotesAdminpCertifier	Specifies the ADMINP certifier ID	String
AdminpDBTitle	erNotesAdminpDBTitle	Specifies the database title	String
AdminpDestDBPath	erNotesDestDBPathAdminp	Specifies the destination database path, relative to `\data` directory on the Lotus Domino server	String
AdminpDestDBServer	erNotesDestDBServerAdminp	Specifies the destination database server	String
AdminpFirstName	erNotesAdminpFirstName	Specifies the given name of the ADMINP	String
AdminpLastName	erNotesAdminpLastName	Specifies the family name of the ADMINP	String
AdminpMiddleName	erNotesAdminpMiddleName	Specifies the middle name of the ADMINP	String
AdminpOrgUnitName	erNotesAdminpOrgUnitName	Specifies the organization unit name for the ADMINP	String
AdminPRequest	erNotesAdminPRequest	Specifies the ADMINP command to run	String???
AdminpSrcDBPath	erNotesSrcDBPathAdminp	Specifies the source database path, relative to `\data` directory on the Lotus Domino server	String
AdminpSrcDBServer	erNotesSrcDBServerAdminp	Specifies the source database server	String
AltFullName	erNotesAltFullName	Specifies the alternate full name of the user.	String
AltFullNameLanguage	erNotesAltLanguageFullName	Specifies the alternate full name language of the user.	String
AltFullNameSort	erNotesAltSortFullName	Specifies the phonetic name of the user	String

Table 22. Notes user account form attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data type
Assistant	erNotesAssistant	Specifies the assistant name of the user	String
CalendarDomain	erNotesCalendarDomain	Specifies the domain name of the alternate scheduling application	String
CellPhoneNumber	erNotesCellPhoneNumber	Specifies the cell phone number for the user	String
CertExpiryDate	erNotesCertExpiryDate	Specifies the expiration date of certifier	String
CheckPassword	erNotesCheckPassword	Specifies whether to require the user to enter a password to authenticate with servers that have **password checking** enabled	Boolean
Children	erNotesChildren	Specifies the name of the children of the user	String
City	erNotesCity	Specifies the city where the user works	String
ClientType	erNotesClientType	Specifies whether the user has full or limited Lotus Notes access	String
ClntBld	erNotesClientBuild	Specifies the list of client build versions that the user runs. This list is updated automatically by the Notes client.	String
ClntMachine	erNotesClientMachine	Specifies the list of workstations that the user runs the client on. This list is updated automatically by the Notes client.	String
ClntPltfrm	erNotesClientPlatform	Specifies the list of workstation platforms that the user runs. This list is updated automatically by the Notes client.	String

Table 22. Notes user account form attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data type
Comment	erNotesComment	Specifies a brief comment about the user (maximum size 2048 characters)	String
CompanyName	erNotesCompanyName	Specifies the name of the company where the user works	String
Country	erNotesCountry	Specifies the country where the user works	String
CreateNorthAmericanId	erNotesCreateNorthAmericanID	Specifies a North American ID	Boolean
Department	erNotesDepartment	Specifies the department name for the user	String
EmployeeID	erNotesEmployeeID	Specifies the employee ID of the user	String
EncryptIncomingMail	erNotesEncryptIncomingMail	Specifies whether the incoming mail is encrypted upon delivery	Boolean
FirstName	erNotesFirstName	Specifies the given name and nickname of the user	String
FullName	erNotesFullName	Specifies the full name of the user	String
HomeFAXPhoneNumber	erNotesHomeFAXPhoneNumber	Specifies the home FAX number for the user	String
HTTPPasswordForceChange	erNotesForceInetPwdChange	Specifies whether to force the user to change their HTTP password	Boolean
InternetAddress	erNotesInternetAddress	Specifies the internet email address of the user	String
InternetLockout	erNotesInetLockout	Specifies whether an internet account is locked	String
JobTitle	erNotesJobTitle	Specifies the job title of the user	String
LastName	erNotesLastName	Specifies the family name of the user	String

Table 22. Notes user account form attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data type
LocalAdmin	erNotesLocalAdmin	Specifies the local administrator of the user ID	String
Location	erNotesLocation	Specifies the office location or mail-stop for the user	String
MailAddress	erNotesMailAddress	Specifies the email address for the user	String
MailDomain	erNotesMailDomain	Specifies the domain name of the mail server for the user account	String
MailFile	erNotesMailFile	Specifies the path and file name for the mail file for the user account	String
MailFileOwnerAccess	erNotesMailFileOwnerAccess	Specifies the owner access of the mail file for the user account	String
MailFileQuotaSize	erNotesMailFileQuotaSize	Specifies the quota size of the mail file for the user account	String
MailServer	erNotesMailServer	Specifies the hierarchical name of the server that stores the mail file for the user account	String
MailSystem	erNotesMailSystem	Specifies the mail system for the user	Integer
MailTemplateName	erNotesMailTemplateName	Specifies the mail template file name for the user	String
Manager	erNotesManager	Specifies the name of the manager for the user	String
MemberOfGroups	erNotesMemberOfGroups	Specifies the list of groups that the user belongs to	String
MiddleInitial	erNotesMiddleInitial	Specifies the middle initial of the user	String
NetUserName	erNotesNetUserName	Specifies the public network, such as America Online or Prodigy, for the user name	String

Table 22. Notes user account form attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data type
NewCertExpiryDate	erNotesNewCertExpiryDate	Specifies the expiration date of the new certificate	String
NewCertPasswd	erNotesPasswdNewCert	Specifies the password of the new certificate ID file	String
NewCertPath	erNotesNewCertPath	Specifies the path to the new certificate ID file	String
OfficeCity	erNotesOfficeCity	Specifies the city in which the office of the user is located	String
OfficeCountry	erNotesOfficeCountry	Specifies the country in which the office of the user is located	String
OfficeFAXPhoneNumber	erNotesOfficeFAXPhoneNumber	Specifies the office fax number for the user	String
OfficeNumber	erNotesOfficeNumber	Specifies the office number of the user	String
OfficePhoneNumber	erNotesOfficePhoneNumber	Specifies the office phone number of the user	String
OfficeState	erNotesOfficeState	Specifies the state where the office is located for the user	String
OfficeStreetAddress	erNotesOfficeStreetAddress	Specifies the street address where the office is located for the user	String
OfficeZIP	erNotesOfficeZIP	Specifies the postal zip code of the office for the user	String
OrigCertifier	erNotesOrigCertifier	Specifies the path to the original certifier ID file	String
OrigCertPasswd	erNotesOrigCertPasswd	Specifies the password of the original certifier ID file	String
Owner	erNotesOwner	Specifies the hierarchical name of the user who created a document	String
Password	erNotesPassword	Specifies the HTTP password of the user	

Table 22. Notes user account form attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data type
PasswordChangeInterval	erNotesChangeIntervalPassword	Specifies the number of days that a password is valid	Integer
PasswordGracePeriod	erNotesPasswordGracePeriod	Specifies the number of days after a required change interval that the user can change the password	Integer
PasswordQualityScale	erNotesPasswordScale	Specifies the password quality that is to be set in the ID file of the user	Integer
PhoneNumber	erNotesPhoneNumber	Specifies the home telephone number for the user	String
PhoneNumber_6	erNotesPagerNumber	Specifies the pager number for the user	String
Policy	erNotesExplicitPolicy	Specifies the explicit policy that is to be used for the user	String
PreferredLanguage	erNotesPreferredLanguage	Specifies the preferred language for the user	String
Profiles	erNotesProfiles	Specifies the setup profile name. This name is used to specify the default settings for the user.	String
RASEXEC	erNotesRasExec	Specifies the system call that will be run after each Lotus Notes Adapter operation	String
ReplicationFileName	erNotesReplMailFileName	Specifies the mail file name of the replicated mail file	String
ReplicationServerName	erNotesReplServerName	Specifies the replication server name for the mail file replica	String
RoamCleanPer	erNotesRoamingIntervalCleanup	Specifies the roaming cleanup interval for the roaming user	String
RoamCleanSetting	erNotesRoamingCleanupSetting	Specifies the roaming cleanup setting for the roaming user	String

Table 22. Notes user account form attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data type
RoamingUser	erNotesRoamingAccess	Specifies whether the user is a roaming user	String
RoamRplSrvr	erNotesRoamingNewReplicaServers	Specifies the roaming replica server where the replica of the users roaming file is located	String
RoamSrvr	erNotesRoamingServer	Specifies the roaming server for the roaming user	String
RoamSubdir	erNotesRoamingUserSubFolder	Specifies roaming subfolder under which the roaming file of the user is created on the roaming server	String
SametimeACL	erNotesSametimeACL	Specifies the Sametime ACL of the user	String
SametimeLockAccount	erNotesSametimeLockAccount	Specifies whether to lock the Sametime access of the user	Boolean
SametimeOnlyAccount	erNotesSametimeOnlyAccount	Specifies whether the account is a Sametime only account or a Domino and Sametime account	Boolean
SaveIdInAddressBook	erNotesSaveIdInAddressBook	Specifies whether the ID file is stored in the Domino Address Book. If it is, the ID file is attached to the Person document of the User.	Boolean
ShortName	erNotesShortName	Specifies the short name that is used by a foreign mail system	String
Spouse	erNotesSpouse	Specifies the spouse name of the user	String
State	erNotesState	Specifies the state or province name where the user resides	String
StreetAddress	erNotesStreetAddress	Specifies the street address where the user resides	String
Suffix	erNotesSuffix	Specifies the suffix for the user	String

Table 22. Notes user account form attributes, descriptions, and corresponding data types (continued)			
Attribute	**Directory server attribute**	**Description**	**Data type**
Title	erNotesTitle	Specifies the title of the user	String
UniqueOrgUnit	erNotesUniqueOrgUnit	Specifies the unique organization unit for the user	String
UserIDfileName	erNotesUserIDfileName	Specifies the name of user ID file that stores access keys	String
UserIdInCertLog	erNotesUserIdInCertLog	Specifies the name that is stored in the CertLog.nsf file	String
UserName	erUid	Specifies the logon ID of the user	String
UserPassword	erPassword	Specifies the logon password that can be changed by the adapter	String
UserStatus	erAccountStatus	Specifies whether the user has account access	Boolean
WebSite	erNotesWebSite	Specifies the website for the user	String
x400Address	erNotesx400Address	Specifies additional x400 O/R attributes, excluding /C, /A, /P	String
Zip	erNotesZip	Specifies the postal code for the home address of the user	String
CreateAdminpMailfile	erNotesCreateAdminpMailfile	Specifies whether the Mail file is to be created by using the AdminP command	String

The following attributes are supported by the Lotus Notes Adapter, but they do nare not displayed on the Notes Account form. To view these attributes on the Notes Account form, additional configuration is required. For more information about how to view the hidden attributes, see the IBM Security Verify Governance Identity Manager product documentation.

Table 23. Notes user account form hidden attributes, descriptions, and corresponding data types			
Attribute	**Directory server attribute**	**Description**	**Data type**
$FILE	erNotesFILE	Specifies the $FILE value for the user account	String
Administrator	erNotesAdministrator	Specifies whether the user is also the administrator of the Lotus Domino server	Boolean

Table 23. Notes user account form hidden attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data type
AvailableForDirSync	erNotesAvailableForDirSync	Specifies whether Lotus Notes is available for directory synchronization	Boolean
ccMailLocation	erNotesccMailLocation	Specifies the ccMailLocation value for the user	String
ccMailUserName	erNotesccMailUserName	Specifies the ccMailUserName value for the user	String
CertIDfileName	erNotesCertIDfileName	Specifies the cert ID file name for the user	String
DocumentAccess	erNotesDocumentAccess	Specifies the access for a Lotus Notes document for the user	String
Form	erNotesForm	Specifies the form for the user	String
MessageStorage	erNotesMessageStorage	Specifies the message storage for the user account	String
OU	erNotesOU	Specifies the organization unit for the user	String
PasswordChangeDate	erNotesChangeDatePassword	Specifies the password change date for the user	String
PasswordDigest	erNotesPasswordDigest	Specifies the password digest for the user	String
PersonalID	erNotesPersonalID	Specifies the personal ID for the user	String
PostalAddress	erNotesPostalAddress	Specifies the postal address for the user	String
ProposedAlt CommonName	erNotesAltCommonNameProposed	Specifies the proposed alternate common name for the user	String
ProposedAlt FullNameLanguage	erNotesProposedAltFullNameLanguage	Specifies the proposed alternate full name language for the user	String
ProposedAltOrgUnit	erNotesAltOrgUnitProposed	Specifies the proposed alternate organization unit for the user	String
PublicKey	erNotesPublicKey	Specifies the public key for the user	String
Street	erNotesStreet	Specifies the street name for the user	String
Type	erNotesType	Specifies the type of user ID	String

Table 23. Notes user account form hidden attributes, descriptions, and corresponding data types (continued)			
Attribute	**Directory server attribute**	**Description**	**Data type**
IDFileDownloadCount	erNotesIDdownLoadCount	Specifies the download count of the ID file from the ID vault	Integer

Support for a Lotus Domino server name with non-English (for example, Chinese) characters

The Lotus Notes Adapter supports a unicode Lotus Domino server name.

About this task

The unicode Lotus Domino server name must be provided on the adapter service form on IBM Security Verify Governance Identity Manager. Specify the name of the server in the **Domino Server Name** field on the service form.

To add the **Domino Server Name** field on the adapter service form, perform the following steps:

Procedure

1. Log on to IBM Security Verify Governance Identity Manager as an administrator.
2. In the **My Work** pane, expand **Configure System** and click **Design Forms** to display the Design Forms page.
3. From the applet, double-click **Service** to display the service form profiles.
4. Double-click **Notes Profile** and from the Attribute List, double-click **$ernotesdominoserver**.
5. Click the **Save Form Template** icon.

Group form attributes

You can specify Lotus Notes group form attributes.

Table 24 on page 99 lists the group form attributes that are used by the adapter. The table gives a brief description and the data type for the value of the attribute.

Table 24. Lotus Notes group form attributes, description, and their corresponding data types			
Attribute	**Directory server attribute**	**Description**	**Data type**
ListName	erNotesGrpName	Specifies the name of the group.	String
GroupType	erNotesGroupType	Specifies the type of the group.	String
ListCategory	erNotesGroupCategory	Specifies the category of the group.	String
ListDescription	erNotesGrpDescription	Specifies a brief description about the group.	String
MailDomain	erNotesGroupMailDomain	Specifies the Mail Domain of the group.	String
InternetAddress	erNotesGrpInternetAddress	Specifies the Internet Address for the group.	String

Table 24. Lotus Notes group form attributes, description, and their corresponding data types (continued)			
Attribute	**Directory server attribute**	**Description**	**Data type**
Comments	erNotesGrpComment	Specifies comments for the group.	String
ListOwner	erNotesGrpOwner	Specifies owners of the group.	String
LocalAdmin	erNotesGroupAdmin	Specifies the names of the group administrators.	String
AvailableForDirSync	eNotesAvailForDirSync	Specifies whether the Group Document is available for Directory Synchronization.	Boolean
Members	erNotesGrpMemberGroups	Specifies groups that are members of this group	String

Installation attributes

The following table lists the attributes that are used during the installation of the adapter. If you are using a response file, you must include all of the attributes marked as required.

Table 25. Installation attributes. In this table, the heading **Rqd** means required.			
Rqd	**Attribute**	**Description**	**Example**
Yes	`USER_INSTALL_DIR`	The value of this parameter sets the installation directory path.	`USER_INSTALL_DIR="C:\\Program Files\\IBM\\ISIM\\agent\ \\NotesAgent"` **Note:** The installation path must be wrapped in quotation marks. And use path separator as \\
Yes	`USER_INPUT_INSTALL _TYPE`	The values of this parameter are `\"Full Installation\"` and `\"Update Installation\"`	`USER_INPUT_INSTALL_TYPE=Full Installation,\"\"` or `USER_INPUT_INSTALL_TYPE= \"\",\"Update Installation\"`
Yes	`USER_INPUT_INSTALL _TYPE_1`	When the value of this parameter is `Full Installation` the installer performs full installation of the adapter.	`USER_INPUT_INSTALL_TYPE_1= \Full Installation\` Set this variable as blank if you want perform an update operation. For example, `USER_INPUT_INSTALL_TYPE_1=`

Table 25. Installation attributes. In this table, the heading **Rqd** means required. *(continued)*

Rqd	Attribute	Description	Example
Yes	`USER_INPUT_INSTALL_TYPE_2`	When the value of this parameter is `Update Installation` the installer performs full installation of the adapter.	`USER_INPUT_INSTALL_TYPE_2=Update Installation` Set this variable as blank if you want perform a full operation. For example, `USER_INPUT_INSTALL_TYPE_2=` **Note:** When Update Installation is specified, the parameter **USER_INPUT_INSTALL_TYPE_1** must be blank. You must explicitly override the default value of **USER_INPUT_INSTALL_TYPE_BOOLEAN_1** to `0`.
Yes	`USER_INPUT_INSTALL_TYPE_BOOLEAN_1`	This parameter is associated with **USER_INPUT_INSTALL_TYPE_1**. When the value of this parameter is 1 the installer performs a full installation of the adapter.	`USER_INPUT_INSTALL_TYPE_BOOLEAN_1=1` Set this variable to 0 if you want to perform an update installation `USER_INPUT_INSTALL_TYPE_BOOLEAN_1=0`
	`USER_INPUT_INSTALL_TYPE_2`	When the value of this parameter is `Update Installation` the installer performs an update installation of the adapter.	`USER_INPUT_INSTALL_TYPE_2=Update Installation` **Note:** When `Update Installation` is specified, the parameter **USER_INPUT_INSTALL_TYPE_1** must be blank or not specified at all. You must explicitly override the default value of **USER_INPUT_INSTALL_TYPE_BOOLEAN_1** to `0`.
Yes	`USER_INPUT_INSTALL_TYPE_BOOLEAN_2`	This parameter is associated with **USER_INPUT_INSTALL_TYPE_2** When the value of this parameter is 1 the installer performs an update installation of the adapter.	`USER_INPUT_INSTALL_TYPE_BOOLEAN_2=1` Set this variable to `0` if you want to perform a full installation.
Yes	`AgentName`	Specifies the Lotus Notes Adapter name. You can install multiple instances of the adapter on different ports by providing different names to the adapter. For example, `NotesAgent1`, `NotesAgent2`. The default name is `NotesAgent`.	`AgentName=\"NotesAgent\"`
Yes	`AgentName_1`	Specifies the name of Lotus notes adapter. It is the same as that of **AgentName** but without quotation marks.	`AgentName_1=NotesAgent` **Note:** Value of **AgentName_1** must be same as that of **AgentName** but without quotation marks.
	`AgentName_BOOLEAN_1=`	Ignore this variable. Keep the value as blank. You can remove it from response file.	`AgentName_BOOLEAN_1=`

Table 25. Installation attributes. In this table, the heading **Rqd** means required. *(continued)*			
Rqd	**Attribute**	**Description**	**Example**
	`DominoVersionNumber_8.5`	This attribute is Boolean variable its value is either 0 or 1. If value of this variable is 1 then value of domino version Number is 8.5.	`DominoVersionNumber_8.5=1`
Yes	`DominoServerName`	Specifies the Lotus Domino Registration Server name that the adapter uses. The name is in format `CN=Server Name/O=org. name`.	`DominoServerName=CN=PS7636/O=psl`
Yes	`AddressBookName`	Specifies the name of the Lotus Notes Address Book when it is other than `names.nsf`. The Lotus Notes Address Book database file is different from the `NoteIdsAddressBook` database file.	`AddressBookName=` **Note:** Keep the value as blank if address book name is `names.nsf`.
Yes	`WkStnIDFile`	Specifies the path to the Lotus Domino Server Workstation ID file. The adapter uses the workstation ID file to connect to the Lotus Domino server. Specify the fully qualified name of the file	`WkStnIDFile=C:\\ID\\PS7636\\admin.id` **Note:** The path separator is \\ (double backslash).
Yes	`WkStnPass`	Specifies the password of the Workstation ID file.	`WkStnPass=password`
Yes	`SuspendGroupName`	Specifies the name of the group that the Lotus Notes Adapter uses to keep the CN values of the suspended users. Create this group on the Lotus Domino server before you run the adapter.	`SuspendGroupName=SuspendGroup`
Yes	`SuspendHTTPGroupName`	Specifies the name of the group that the Lotus Notes Adapter uses to keep the CN values of the suspended users to restrict Internet access. Create this group on the Lotus Domino server before you run the adapter.	`SuspendHTTPGroupName=HTTPSuspendGroup`
Yes	`DeleteGroupName`	Specifies the name of the group that the Lotus Notes Adapter uses to keep the CN values of the deleted users. Create this group on the Lotus Domino server before you run the adapter.	`DeleteGroupName=DelGroup`
Yes	`LogDBName`	Specifies the name of a Lotus Notes database. It lists the deleted or suspended user documents. The adapter removes the user documents from this database file when a user is added or restored.	`LogDBName=Logdb` **Note:** The value can be blank.

Table 25. Installation attributes. In this table, the heading **Rqd** means required. *(continued)*

Rqd	Attribute	Description	Example
Yes	`ReconAttribs`	Specifies the list of attribute names to include in the reconciliation process. When more than one name is listed, separate them by a semicolon. When you do not provide any value in the Reconciled Attributes field, all the attributes are returned during the reconciliation operation. Except for those attributes that are specified in the **NotReconAttribs** list. The default value is blank.	`ReconAttribs=`
Yes	`NotReconAttribs`	Specifies the list of attribute names to exclude from the reconciliation process. When more than one name is listed, separate them by a semicolon. The default values are `Certificate;$UpdatedBy;$Revisions`.	`NotReconAttribs=Certificate; $UpdatedBy;$Revisions`
	`SynchroniseHTTPPwd_YES`	This attribute is a Boolean variable. If value of **SynchroniseHTTPPwd_YES** is 1, the user password is set as Internet password during an Add or Modify request. When you do not specify this option during the installation the default value is TRUE.	`SynchroniseHTTPPwd_YES=1` or `SynchroniseHTTPPwd_YES=0` **Note:** The value of **SynchroniseHTTPPwd_YES** must be the opposite of **SynchroniseHTTPPwd_NO**. For example, if the value **SynchroniseHTTPPwd_YES** is 1 the value of **SynchroniseHTTPPwd_NO** must be `0`.
	`SynchroniseHTTPPwd_NO`	This Boolean variable is associated with **SynchroniseHTTPPwd_YES**. If value of **SynchroniseHTTPPwd_NO** is 1, the user password is not set as Internet password during an Add or Modify request.	`SynchroniseHTTPPwd_NO=1` or `SynchroniseHTTPPwd_NO=0` **Note:** The value of **SynchroniseHTTPPwd_NO** must be the opposite of **SynchroniseHTTPPwd_YES**. For example, if the value **SynchroniseHTTPPwd_NO** is 1 the value of **SynchroniseHTTPPwd_YES** must be `0`.
	`UseShortName_YES`	If the value is 1, the Lotus Notes Adapter is configured to use the short name value as a unique ID on the IBM Security Verify Identity server.	`UseShortName_YES=1` or `UseShortName_YES=0` **Note:** The value of **UseShortName_YES** must be the opposite of **UseShortName_NO** . For example, if the value **UseShortName_YES** is 1 the value of **UseShortName_NO** must be `0`.

Table 25. Installation attributes. In this table, the heading **Rqd** means required. *(continued)*			
Rqd	**Attribute**	**Description**	**Example**
	`UseShortName_NO`	If the value is 1, the Lotus Notes Adapter is not configured to use the short name value as a unique ID on the IBM Security Verify Identity server. When you do not specify this option during the installation the default value is FALSE.	`UseShortName_NO=1` or `UseShortName_NO=0` **Note:** The value of **UseShortName_NO** must be the opposite of **UseShortName_YES** . For example, if the value **UseShortName_NO** is 1 the value of **UseShortName_YES** must be 0.
	`UseInetAddrForShort Name_YES`	If the value is 1, the Lotus Notes Adapter requires a unique ID as the internet address on the IBM Security Verify Identity server when the short name value is NULL. Set only this key to 1 when the Use ShortName key is also set to 1.	`UseInetAddrForShortName_YES=1` or `UseInetAddrForShortName_YES=0` **Note:** The value of **UseInetAddrForShortName_YES** must be the opposite of **UseInetAddrForShortName_NO** . For example, if the value **UseInetAddrForShortName_YES** is 1 the value of **UseInetAddrForShortName_NO** must be 0.
	`UseInetAddrForShort Name_NO`	If the value is 1, the Lotus Notes Adapter does not require a unique ID as the internet address on the IBM Security Verify Identity server	`UseInetAddrForShortName_NO=1` or `UseInetAddrForShortName_NO=0` **Note:** The value of **UseInetAddrForShortName_NO** must be the opposite of **UseInetAddrForShortName_YES** . For example, if the value **UseInetAddrForShortName_NO** is 1 the value of **UseInetAddrForShortName_YES** must be 0.
Yes	`IdsAddressBookNa me`	Specifies the name of the Lotus Notes database file that the adapter uses to store the user information. For example, the username, password, and ID file. The value can be blank.	`IdsAddressBookName=`
	`DeleteMailDB_YES`	If the value is 1, the mail database file is deleted, when a user is deleted.	`DeleteMailDB_YES=1` or `DeleteMailDB_YES=0` **Note:** The value of **DeleteMailDB_YES** must be the opposite of **DeleteMailDB_NO** . For example, if the value **DeleteMailDB_YES** is 1 the value of **DeleteMailDB_NO** must be 0.

Table 25. Installation attributes. In this table, the heading **Rqd** means required. *(continued)*

Rqd	Attribute	Description	Example
	`DeleteMailDB_NO`	If the value is 1, the mail database file is not deleted, when a user is deleted	`DeleteMailDB_NO=1` or `DeleteMailDB_NO=0` **Note:** The value of **DeleteMailDB_NO** must be the opposite of **DeleteMailDB_YES** . For example, if the value **DeleteMailDB_NO** is 1 the value of **DeleteMailDB_YES** must be `0`.
	`SetHTTPPswdOnly_YES`	If the value is 1, only the HTTP password of the user is changed in the Change Password operation from IBM Security Verify Identity.	`SetHTTPPswdOnly_YES=1` or `SetHTTPPswdOnly_YES=0` **Note:** The value of **SetHTTPPswdOnly_YES** must be the opposite of **SetHTTPPswdOnly_NO** . For example, if the value **SetHTTPPswdOnly_YES** is 1 the value of **SetHTTPPswdOnly_NO** must be `0`.
	`SetHTTPPswdOnly_NO`	If the value is 1, the HTTP password of the user is not changed in the Change Password operation from IBM Security Verify Identity.	`SetHTTPPswdOnly_NO=1` or `DeleteMailDB_NO=0` **Note:** The value of **SetHTTPPswdOnly_NO** must be the opposite of **SetHTTPPswdOnly_YES** . For example, if the value **SetHTTPPswdOnly_NO** is 1 the value of **SetHTTPPswdOnly_YES** must be `0`.
	`SetHTTPPswdFirst_YES`	If the value is 1, the HTTP password is changed before the user password is changed.	`SetHTTPPswdFirst_YES=1` or `SetHTTPPswdFirst_YES=0` **Note:** The value of **SetHTTPPswdFirst_YES** must be the opposite of **SetHTTPPswdFirst_NO** . For example, if the value **SetHTTPPswdFirst_YES** is 1 the value of **SetHTTPPswdFirst_NO** must be `0`.
	`SetHTTPPswdFirst_NO`	If the value is 1, the HTTP password is not changed before the user password is changed.	`SetHTTPPswdFirst_NO=1` or `SetHTTPPswdFirst_NO=0` **Note:** The value of **SetHTTPPswdFirst_NO** must be the opposite of **SetHTTPPswdFirsty_YES** . For example, if the value **SetHTTPPswdFirst_NO** is 1 the value of **SetHTTPPswdFirst_YES** must be `0`.

Table 25. Installation attributes. In this table, the heading **Rqd** means required. *(continued)*			
Rqd	**Attribute**	**Description**	**Example**
	`AddEruidToFullName_YES`	If the value is 1, the **ERUID** or the **User ID** attribute is stored in the **FullName** field in the person document.	`AddEruidToFullName_YES=1` or `AddEruidToFullName_YES=0` **Note:** The value of **AddEruidToFullName_YES** must be the opposite of **AddEruidToFullName_NO** . For example, if the value **AddEruidToFullName_YES** is 1 the value of **AddEruidToFullName_NO** must be `0`.
	`AddEruidToFullName_NO`	If the value is 1, the **ERUID** or the **User ID** attribute is not stored in the **FullName** field in the person document.	`AddEruidToFullName_NO=1` or `AddEruidToFullName_NO=0` **Note:** The value of **AddEruidToFullName_NO** must be the opposite of **AddEruidToFullName_YES** . For example, if the value **AddEruidToFullName_NO** is 1 the value of **AddEruidToFullName_YES** must be `0`.
	`UpdateServerDoc_YES`	If the value is 1, all the suspended groups are included in the **Not Access Server** field.	`UpdateServerDoc_YES=1` or `UpdateServerDoc_YES=0` **Note:** The value of **UpdateServerDoc_YES** must be the opposite of **UpdateServerDoc_NO** . For example, if the value **UpdateServerDoc_YES** is 1 the value of **UpdateServerDoc_NO** must be `0`.
	`UpdateServerDoc_NO`	If the value is 1, the suspended groups are not included in the **Not Access Server** field.	`UpdateServerDoc_NO=1` or `UpdateServerDoc_NO=0` **Note:** The value of **UpdateServerDoc_NO** must be the opposite of **UpdateServerDoc_YES** . For example, if the value **UpdateServerDoc_NO** is 1 the value of **UpdateServerDoc_YES** must be `0`.
Yes	`CertIDPath`	Specifies the file path for the certifier ID file. The certifier ID file is the default file used for the User Add operations. When you do not specify the file path for the certifier file during the user add operation, the file path from this field is used to add the user. If you specify the path for the certifier file when you add a user, the file path in this field is ignored.	`CertIDPath=C:\\ID\\PS7636\\cert.id` **Note:** The file path separator is \\ (double backslash).
Yes	`CertIDPassword`	Specifies the password of the certifier ID file.	`CertIDPassword=password`

Table 25. Installation attributes. In this table, the heading **Rqd** means required. *(continued)*			
Rqd	**Attribute**	**Description**	**Example**
Yes	`MailTemplateServer`	The server name and the organization name for the mail template files that the adapter uses. When you do not specify a value for this registry key, the adapter uses the mail template files from the Domino Registration Server. The files for the Domino Registration Server are specified for the Domino Server registry key. The format of the name is `CN=Server Name/O=org. name`	`MailTemplateServer=CN=PS7636/O=psl`
	`ExecAdminpOperation_YES`	If the value is 1, the **AdminP** is used when you deprovision a user from IBM Security Verify Identity.	`ExecAdminpOperation_YES=1` or `ExecAdminpOperation_YES=0` **Note:** The value of **ExecAdminpOperation_YES** must be the opposite of **ExecAdminpOperation_NO** . For example, if the value **ExecAdminpOperation_YES** is 1 the value of **ExecAdminpOperation_NO** must be 0.
	`ExecAdminpOperation_NO`	If the value is 1, the **AdminP** is not used when you deprovision a user from IBM Security Verify Identity.	`ExecAdminpOperation_NO=1` or `ExecAdminpOperation_NO=0` **Note:** The value of **ExecAdminpOperation_NO** must be the opposite of **ExecAdminpOperation_YES** . For example, if the value **ExecAdminpOperation_NO** is 1 the value of **ExecAdminpOperation_YES** must be 0.
	`IsIDVaultConfigured_YES`	If the value is 1, the adapter can change the password of a user ID file in ID vault. **Note:** Lotus Notes version 8.5 is required to set this value to 1.	`IsIDVaultConfigured_YES=1` or `IsIDVaultConfigured_YES=0` **Note:** The value of **IsIDVaultConfigured_YES** must be the opposite of **IsIDVaultConfigured_NO** . For example, if the value **IsIDVaultConfigured_YES** is 1 the value of **IsIDVaultConfigured_NO** must be 0.

Table 25. Installation attributes. In this table, the heading **Rqd** means required. *(continued)*			
Rqd	**Attribute**	**Description**	**Example**
	`IsIDVaultConfigured_NO`	If the value is 1, the adapter cannot change the password of a user ID file in ID vault.	`IsIDVaultConfigured_NO=1` or `IsIDVaultConfigured_NO=0` **Note:** The value of **IsIDVaultConfigured_NO** must be the opposite of **IsIDVaultConfigured_YES** . For example, if the value **IsIDVaultConfigured_NO** is 1 the value of **IsIDVaultConfigured_YES** must be 0.
	`USER_REQUESTED_RESTART`	If this attribute has value NO, the server doesl not restart after adapter is install in silent mode. This variable is IA installer specific.	`USER_REQUESTED_RESTART=NO`

Default values for optional registry keys

If you do not set a value for the associated installation attributes, the registry keys have default values.

Table 26. Default values for optional registry keys	
Registry name	**Default value**
UseShortName	FALSE
UseInetAddrForShortName	FALSE
DeleteMailDB	TRUE
SetHTTPPswdOnly	FALSE
SetHTTPPswdFirst	FALSE
AddEruidToFullName	TRUE
UpdateServerDoc	FALSE
ExecAdminpOperation	FALSE
IsIDVaultConfigured	FALSE
SynchroniseHTTPPwd	TRUE

Adapter attributes by operations

Adapter attributes by operations refer to adapter actions by their functional transaction group. They are required for customization, creating provisioning rules, and understanding what service/target attributes are supported by the adapter.

System Login Add

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

Table 27. Add request attributes

Required attribute	Optional attribute
erUid erNotesLastName erNotesAddCertPath erNotesPasswdAddCert	All other supported attributes

System Login Change

A System Login Change is a request to change one or more attributes for the specified users.

Table 28. Change request attributes

Required attribute	Optional attribute
erUid erNotesLastName erNotesAddCertPath erNotesPasswdAddCert	All other supported attributes

System Login Delete

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

Table 29. Delete request attributes

Required attribute	Optional attribute
erUid	None

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 30. Suspend request attributes

Required attribute	Optional attribute
erUid erAccountStatus	None

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 31. Restore request attributes

Required attribute	Optional attribute
erUid erAccountStatus	erPassword

System Login Reconcile

The Reconciliation request synchronizes user account information between IBM Security Verify Governance Identity Manager and the adapter.

Table 32. Attributes returned during reconciliation

Required attribute	Optional attribute
None	None

System Login Group Add

A System Login Group Add is a request to create a new group with the specified attributes.

Table 33. Group Add request attributes

Required attribute	Optional attribute
erNotesGrpName	All other supported attributes

System Login Group Change

A System Login Group Change is a request to change one or more attributes for a group.

Table 34. Group Change request attributes

Required attribute	Optional attribute
erNotesGrpName	All other supported attributes

System Login Group Delete

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

Table 35. Group Delete request attributes

Required attribute	Optional attribute
erNotesGrpName	None

Special attributes

Certain attributes have special syntax and meaning that customers needs to be aware off. This information will be used to help the customer in how to supply the attribute value.This topic is not applicable for this adapter.

Federal Information Processing Standards compliance mode

IBM Security Verify Governance Identity Manager can be operated with FIPS 140-2 certified cryptographic modules.

FIPS 140-2 is a standard from the US National Institute of Standards and Technology (NIST) that applies to cryptographic modules.

Two FIPS 140-2 modules are used:

- IBM Java Crytographic Extension
- Open SSL module

As a user of these modules, there is no certification implied for IBM Security Verify Governance Identity Manager. However, for the correct use of these FIPS 14-2 modules IBM customers need to follow the instructions in this document.

The fipsEnable tool enables the adapter to be Federal Information Processing Standards (FIPS) compliant. The fipsEnable tool causes the adapter to use a FIPS certified encryption library so that all cryptographic keys that are used are generated by a FIPS compliant algorithm. Any communications with the adapter are also secured. The tool generates the FIPS master key, enables the FIPS mode setting, changes the USE_SSL parameter to TRUE and re-encrypts the existing encrypted values for:

- agentCfg key
- DAML user name and password
- Adapter specific encrypted registry items

Note: After FIPS mode is enable, it cannot be disabled. You must reinstall the adapter, if you want to disable FIPS mode.

Configuring the adapter to run in FIPS mode

To configure the adapter to run in FIPS mode, you must run the fipsEnable utility.

Procedure

1. Install the adapter.
2. Run the fipsEnable utility and issue the command:

   ```
   fipsEnable -reg agentName
   ```

3. Restart the adapter.

Operational differences when the adapter runs in FIPS mode

The DAML protocol used to communicate between the adapter and IBM Security Verify Governance Identity Manager must run in SSL mode.

The fipsEnable tool sets the DAML SSL mode to TRUE. In SSL mode, however, you must install a server certificate because the fipsEnable tool does not convert an existing DAML certificate and key.

Note: You cannot import a PKCS12 file that contains a certificate and key. You must use certTool (option A) to create a Certificate Signing Request (CSR) and have it signed by a certificate authority. You can then install the signed certificate with certTool (option B).

The agentCfg tool automatically detects when the adapter is running in FIPS mode and initializes the encryption library in FIPS mode. In addition, the ADK accepts only agentCfg connections from localhost (127.0.0.1).

Security policy

For FIPS compliance, a security policy must be defined that outlines the requirements for the user to operate the application in a FIPS-compliant mode.

The software ensures that the correct algorithms and keys are used. Requirements for the environment are the responsibility of the security officer. The security policy defines two roles, security officer and user. It defines the extent to which each of these persons can physically access the workstation, file system, and configuration tools. The security of the workstation, of the file system, and of the configuration is the responsibility of the security officer.

Authentication roles

The FIPS security policy normally defines separate roles for a security officer and a user. For an adapter, the user role is actually the Identity server. The installation and configuration of the adapter must be done by the security officer.

The security officer must ensure that the correct physical and logical security is in place to prevent access to the adapter by unauthorized personnel. The physical workstation must be in a secure location that is accessible only by persons with the authority and access privileges of the security officer. In addition, the security on the folder in which the adapter is installed must be configured to prevent access by personnel other than security officers.

For Window installations, the system registry must be secured at the top-level key for the adapter to prevent access by personnel other than security officers.

Rules of operation

You must follow certain rules and restrictions to operate in FIPS mode.

- The replacement or modification of the adapter by unauthorized intruders is prohibited.
- The operating system enforces authentication methods to prevent unauthorized access to adapter services.
- All critical security parameters are verified as correct and are securely generated, stored, and destroyed.
- All host system components that can contain sensitive cryptographic data, such as main memory, system bus, and disk storage, must be in a secure environment.
- The operating system is responsible for multitasking operations so that other processes cannot access the address space of the process that contains the adapter.
- Secret or private keys that are input to or output from an application must be encrypted by a FIPS approved algorithm.

Index

A

C

D

E

F

G

H

S

T

U

V

W