IBM Security Identity Manager
Version 6.0

Active Directory Adapter with 64-bit Support User Guide

SC27-4385-02

IBM Security Identity Manager
Version 6.0

Active Directory Adapter with 64-bit Support User Guide

SC27-4385-02

Note
Before using this information and the product it supports, read the information in "Notices" on page 85.

Edition notice

Note: This edition applies to version 6.0 of IBM Security Identity Manager (product number 5724-C34) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures v

Tables vii

Preface ix
About this publication ix
Access to publications and terminology ix
Accessibility x
Technical training x
Support information x
Statement of Good Security Practices x

Chapter 1. Introduction to the Active Directory Adapter 1
Features of the Active Directory Adapter 1

Chapter 2. Checklist for configuring IBM Security Identity Manager to run the adapter 3

Chapter 3. User account management tasks 5
Before you begin the adapter operations 5
User account reconciliation 5
Reconciled attributes. 6
Attributes not reconciled 8
Support data reconciliation 8
userAccountControl attribute reconciliation . . . 9
cn attribute reconciliation 9
Filter reconciliation 9
User account additions 14
Attributes for adding user accounts 14
CN attribute specification. 15
Distinguished name creation for a user account 16
User principal name of a user account 17
Control specifications for a user account. . . . 18
Creating a home directory for a user account . . 19
RAS attribute specification 20
User account enablement for mail 21
Proxy address creation for a user account . . . 22
User account modification 23
Container attribute modification 23
Home Directory attribute modification 24
User password modification. 27
Mailbox Store attribute modification 28
Mail status modification for a user account. . . 28
Mail status clearing for a user account 29
Mailbox support modification for Exchange 2010 30
Primary Group attribute modification 32
User account suspension 32
User account restoration 33
User account deletion 33
Enabling and disabling unified messaging 34
Modifying unified messaging 35

Chapter 4. Group management tasks 37
Adding groups on Active Directory 37
Support data attribute specification on the group form. 37
Accessibility attribute specification on the group form. 39
Modifying group attributes 40
Container attribute modification on the group form. 41
Scope modification for the group 41
Creating a group 42
Adding users to groups 43
Viewing information about members of a group 43
Removing users from a group 44
Deleting groups from Active Directory 44

Chapter 5. Troubleshooting the Active Directory Adapter errors 47
Techniques for troubleshooting problems 47
Active Directory Adapter errors 49
Log information format 56

Appendix A. Country and region codes 57

Appendix B. Active Directory Adapter attributes. 65
Active Directory account form attributes. 65
Active Directory group form attributes 69
Customizable attributes on the Active Directory group form 69
Mapping extended attributes 70

Appendix C. APIs used by the adapter 71
ADSI interfaces and the corresponding APIs used by the adapter 71
Windows APIs used by the adapter 73

Appendix D. PowerShell command-line functions used by the adapter 75

Appendix E. Conventions used in this publication 77
Typeface conventions 77
Operating system-dependent variables and paths. . 77

Appendix F. Support information . . . 79
Searching knowledge bases 79
Obtaining a product fix 80
Contacting IBM Support 80

Appendix G. Accessibility features for IBM Security Identity Manager 83

Notices 85

Index 89

Figures

1. Generating an RDN 16
2. Example of an Active Directory structure 23
3. Exchange server organization tree 28
4. Example of an Active Directory container structure 41

Tables

1. Checklist for configuring IBM Security Identity Manager . . . 3
2. Attributes supported by the adapter for filter reconciliation . . . 10
3. Attributes not supported by the adapter for filter reconciliation . . . 12
4. Objects and the corresponding object class 14
5. List of attributes and their default values on the Active Directory. . . . 15
6. The order of attributes on the Active Directory account form that the adapter checks to generate an RDN . . . 16
7. Attributes on the Active Directory account form and their corresponding property flags . 19
8. Home Directory attribute settings . . . 20
9. Home Directory NTFS Access attribute values and their corresponding permissions on the home directory . . . 20
10. Account form values . . . 24
11. Account form values . . . 24
12. Account form values . . . 25
13. Account form values . . . 25
14. Account form values . . . 26
15. Changed account form values . . . 26
16. Account form values . . . 26
17. Account form values . . . 27
18. New registry keys . . . 30
19. DisableMailboxOnSuspend registry key actions 30
20. ReconDisconnectedMailbox registry key actions during reconciliation . . . 31
21. Group membership details . . . 38
22. Accessibility attributes . . . 39
23. Troubleshooting the Active Directory Adapter errors . . . 49
24. Countries and regions and their corresponding codes . . . 57
25. Mapping of attributes on IBM Security Identity Manager to the attributes on the Active Directory . . . 65
26. Group form attributes . . . 69
27. Customizable group form attributes . . . 70
28. ADSI Interfaces and the corresponding APIs used by the Active Directory Adapter. . . . 71
29. Windows APIs used by the Active Directory Adapter. . . . 74
30. PowerShell cmdlets used by the Active Directory Adapterand their description . . . 75

Preface

About this publication

The *Active Directory Adapter with 64-bit Support User Guide* provides information that you can use to manage user accounts on the Active Directory with the IBM® Security Identity Manager. IBM Security Identity Manager was previously known as Tivoli® Identity Manager.

This guide describes user account management tasks, such as reconciliation, add, modify, suspend, restore, delete, and password change.

Access to publications and terminology

This section provides:

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

IBM Security Identity Manager library

For a complete listing of the IBM Security Identity Manager and IBM Security Identity Manager Adapter documentation, see the online library (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0/ic-homepage.htm).

Online publications

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

IBM Security Identity Manager library
The product documentation site (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0/ic-homepage.htm) displays the welcome page and navigation for the library.

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

IBM Publications Center
The IBM Publications Center site (http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss) offers customized search functions to help you find all the IBM publications you need.

IBM Terminology website

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

Accessibility

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

Technical training

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

Support information

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

Appendix F, "Support information," on page 79 provides details about:

- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

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

Statement of Good Security Practices

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

Chapter 1. Introduction to the Active Directory Adapter

The Active Directory Adapter provides connectivity between IBM Security Identity Manager and the network of systems that run the Active Directory.

The adapter runs as a service, independently of whether you are logged on to IBM Security Identity Manager.

The Active Directory Adapter automates the following user account management tasks:

- Adding Active Directory user accounts
- Creating a home directory for a user account
- Modifying attributes of Active Directory user accounts
- Changing passwords of Active Directory user accounts
- Suspending, restoring, and deleting Active Directory user accounts
- Retrieving user accounts from the Active Directory
- Managing mailboxes on the Exchange server
- Moving a user in the Active Directory hierarchy

The adapter also automates the following group management tasks:

- Retrieving groups from the Active Directory
- Adding groups on Active Directory
- Modifying group attributes
- Deleting groups from the Active Directory
- Adding users to a group
- Removing users from a group
- Moving a group in the Active Directory hierarchy

Features of the Active Directory Adapter

The Active Directory Adapter supports the following functions:

- Reconciliation of user accounts and groups from the Active Directory to the directory server of IBM Security Identity Manager.
- User account management tasks, such as add, modify (including password change), suspend, restore, and delete to manage accounts on the Active Directory by using IBM Security Identity Manager.
- Group account management tasks, such as add, modify, and delete groups on the Active Directory.
- Management of the Exchange 2010 mailboxes.
- Customization of the Active Directory account form.
- Customization of the Active Directory group form.
- Password synchronization of different accounts of a domain user by providing registry access to the Password Synchronization plug-in.

Chapter 2. Checklist for configuring IBM Security Identity Manager to run the adapter

Use this checklist to configure IBM Security Identity Manager to run the adapter.

Table 1 provides an overview of the process to configure IBM Security Identity Manager.

Table 1. Checklist for configuring IBM Security Identity Manager

Task	**See this documentation:**
Install the Active Directory Adapter	Installing the adapter in the *Active Directory Adapter Installation and Configuration Guide*
Import the adapter profile into IBM Security Identity Manager	Importing the adapter profile into the IBM Security Identity Manager server in the *Active Directory Adapter Installation and Configuration Guide*
Create a service for the Active Directory Adapter	Creating the service in the *Active Directory Adapter Installation and Configuration Guide* **Note:** After you create a Active Directory Adapter service, the IBM Security Identity Manager server creates a default provisioning policy for the adapter service. You can customize a provisioning policy for the Active Directory Adapter service according to the requirements of your organization. For more information, see the section about customizing a provisioning policy in the IBM Security Identity Manager product documentation.
Configure the Active Directory Adapter	Configuring the Active Directory Adapter in the *Active Directory Adapter Installation and Configuration Guide*
Perform a reconciliation operation to retrieve user accounts and store them in the IBM Security Identity Manager server	Managing reconciliation schedules in the IBM Security Identity Manager product documentation
Adopt orphan accounts on IBM Security Identity Manager	Assigning an orphan account to a user in the IBM Security Identity Manager product documentation

Chapter 3. User account management tasks

IBM Security Identity Manager manages user accounts stored on the Active Directory by using the Active Directory Adapter.

You can do various operations, such as reconciliation, add, modify (including password change), suspend, restore, and delete to manage your accounts.

You can manage:

- Accounts for a specific person
- Accounts for a service instance
- Specific accounts using the search function of IBM Security Identity Manager

Before you begin the adapter operations

Before you use the adapter to do any operations, complete the preliminary tasks.

1. Perform the steps in Chapter 2, "Checklist for configuring IBM Security Identity Manager to run the adapter," on page 3.
2. Use one of the following methods to start the Active Directory Adapter:
   - Windows services in service mode
     a. In the Windows control panel, double-click **Administrative Tools**.
     b. Double-click **Services**.
     c. Right-click the **Active Directory Agent service**, and click **Start**.
   - Windows command prompt in console mode

     Go to the adapter installation directory and run the following command:

     ```
     adagent -console
     ```
3. Verify that the Active Directory Adapter registry key settings are configured according to your requirements. To modify the values of the registry keys, use the Active Directory Adapter configuration tool, **agentCfg**. For more information, see the *Active Directory Adapter Installation and Configuration Guide* and search for "Registry key descriptions" and "Starting the adapter configuration tool."

User account reconciliation

The reconciliation operation retrieves the user account information from the Active Directory and stores it in the directory server of IBM Security Identity Manager.

You can schedule reconciliation to run at specific times and to return specific parameters. Running a reconciliation before its schedule time does not cancel the scheduled reconciliation. For more information about scheduling reconciliation and running a scheduled reconciliation, see the IBM Security Identity Manager product documentation.

You can also perform the following reconciliation tasks at any time from IBM Security Identity Manager:

- Reconciling support data
- Reconciling a single user account

When a user account is reconciled, the adapter returns all the groups of which the user is a member of by using the **erGroup** attribute. The adapter refers to **UseGroup** registry key. This key determines which attribute of a group that the user belongs to is added to the **erGroup** attribute of a user account. You can set the registry key **UseGroup** to:

- CN
- DN
- GUID

The following table specifies the results of setting the registry key UseGroup

Set to	Result
CN	The adapter adds the CN of the groups of which the user is member of to erGroup attribute.
DN	The adapter adds the DN of the groups of which the user is member of to erGroup attribute
GUID	The adapter adds the GUID of the groups of which the user is member of to erGroup attribute

The Group Unique Name is used to display the groups on the account form. It maps the **CN, DN**, or **GUID** of the group to the group unique name attribute of the respective groups reconciled for the same service.

Because the **CN** value is not guaranteed to be unique, use the **DN** as the group name value. Although the **GUID** value is always unique, groups that have the same **DN** in test and production do not have the same **GUID**. Use the **DN** value to allow membership to cross domain groups.

When the **Base Point DN** attributes are specified on the account form, the reconciliation operation returns to IBM Security Identity Manager:

- All the user accounts under the **Users Base Point DN**
- All the groups under the **Groups Base Point DN**

Note: You might not see the unique name of a group if the following conditions occur:

- The user account is viewed from the account form.
- The **UseGroup** registry key is set to DN or GUID.
- The user is a member of a group that is not in the **Groups Base Point DN**.

Reconciled attributes

During reconciliation, the value of the sAMAccountName attribute of the Active Directory is returned to IBM Security Identity Manager as the User Id attribute.

When you perform a reconciliation, the Active Directory Adapter returns all containers to the base point that is specified in the Active Directory Adapter service form. If you do not specify a base point at the time of creating an Active Directory service, then the adapter returns all containers to the Active Directory.

In a reconciliation operation, you can configure the adapter to return:

- The Windows Terminal services (WTS) attributes
- The attributes that are related to the home directory security.

To reconcile the WTS attributes, set the registry key WtsDisableSearch to FALSE and WtsEnabled to TRUE.

The Active Directory Adapter retrieves the following WTS attributes from the Active Directory:

- Allow Logon
- Initial Program
- Inherit Initial Program
- Profile Path
- Connect Client Drives
- Connect Client Printers
- Client Printer Is Default
- Working Directory
- WTS Home Directory
- WTS Home Directory Drive
- WTS Callback Settings
- WTS Callback Number
- Idle Timeout
- Connection Timeout
- Disconnection Timeout
- Broken Timeout Setting
- Reconnect Settings
- Shadow Settings
- WTS Home Directory NTFS Access
- WTS Home Directory Share
- WTS Home Directory Share Access
- WTS Remote Home Directory

The default value of the registry key WtsDisableSearch is TRUE. If you retain the default value, then the adapter does not return the WTS attributes to IBM Security Identity Manager and the reconciliation takes less time.

Use the registry key ReconHomeDirSecurity to retrieve the attributes that are related to the home directory security, such as NTFS security, share name, and share security from the Active Directory. Attributes corresponding to the home directory security are:

- Home Directory NTFS Access
- Home Directory Share
- Home Directory Share Access

The default value of the registry key ReconHomeDirSecurity is FALSE. If you retain the default value, the adapter does not retrieve the attributes that are related to the home directory security. The reconciliation takes less time. To reconcile the attributes that are related to the home directory security, set the value of the registry key ReconHomeDirSecurity to TRUE.

You must provide either Full or Change access rights to a home directory on the Active Directory. Otherwise, the following attributes remain blank on the account form after the adapter performs the reconciliation operation:

- Home Directory NTFS Access
- WTS Home Directory NTFS Access
- Home Directory Share Access
- WTS Home Directory Share Access

The default value of the registry key ReconMailboxPermissions is TRUE. If you set the value of the registry key ReconMailboxPermissions to FALSE, then the adapter does not retrieve the mailbox security permission attributes for the mailbox enabled user accounts from the Active Directory. To reconcile the following mailbox security permission attributes for the mailbox enabled user accounts, set the value of the ReconMailboxPermissions to TRUE:

- Delete Mailbox Storage
- Read Permissions
- Change Permissions
- Take Ownership
- Full Mailbox Access
- Associated External Acc
- Apply Onto (for Allow)
- Apply Onto (for Deny)
- Apply Permissions To One Level Only (for Allow)
- Apply Permissions To One Level Only (for Deny)

To reconcile the following password-related attributes, set the registry key SearchPasswordSettings to TRUE:

- Password Minimum Length
- Require Unique Password
- User Cannot Change Password

The default value of the registry key SearchPasswordSettings is FALSE. When you retain the default value, the adapter does not retrieve the listed password-related attributes to IBM Security Identity Manager and the reconciliation operation takes less time.

Attributes not reconciled

Except for these attributes and the attributes that are retrieved depending on the values of the registry keys, all other attributes are always reconciled.

The Active Directory Adapter does not return the following attributes to IBM Security Identity Manager after reconciliation:

- User password
- System Call (This attribute is not supported by the Active Directory Adapter.)
- WTS Server Name
- RAS Saved IPv4 Address
- RAS Saved IPv4 Address

Support data reconciliation

In addition to reconciling user accounts, theActive Directory Adapter also reconciles support data to IBM Security Identity Manager.

Support data might be:

- Groups
- Containers
- Mailbox stores

The support data is reconciled only when you perform a full reconciliation.

userAccountControl attribute reconciliation

The user account status on IBM Security Identity Manager can be either active or inactive.

During reconciliation, the Active Directory Adapter retrieves the status of a user account from the userAccountControl attribute on the Active Directory. The ACCOUNTDISABLE property flag value of the userAccountControl attribute determines the status of a user account. For more information about property flags of the userAccountControl attribute, see the Microsoft Windows Server documentation.

cn attribute reconciliation

You can configure the attribute corresponding to CN that is returned to IBM Security Identity Manager in a user entry during a reconciliation operation.

You can configure the account form to use either the IBM Security Identity Manager schema cn attribute or the erADFullName attribute. When the compliance alerts on IBM Security Identity Manager are enabled, do not use the cn attribute on the account form. To use either the cn attribute or the erADFullName attribute, you must customize the account form and set the registry key UseITIMCNattribute. For more information about the cn attribute configuration, see the *Active Directory Adapter Installation and Configuration Guide*.

Filter reconciliation

The Active Directory Adapter can reconcile users, groups, containers, and mail stores from the Active Directory based on the filters that are specified for the reconciliation.

To enable the Active Directory Adapter for filter reconciliation, set the value of the Pass search filter to agent registry key to `TRUE`. To set the value of the Pass search filter to agent registry key, use the adapter configuration tool, agentCfg. For more information about using the agentCfg tool, see the *Active Directory Adapter Installation and Configuration Guide*. Search for the section "Starting the adapter configuration tool."

The search filter must be a Lightweight Directory Access Protocol (LDAP) version 2 filter. For information about specifying filters, see the IBM Security Identity Manager product documentation.

Supported attributes for filtering

The following table lists the attributes on the Active Directory account form that the adapter supports for filter reconciliation.

Table 2. Attributes supported by the adapter for filter reconciliation

- cn
- description
- erADExDialin
- erADBadLoginCount
- erADCallbackNumber
- erADCountryCode
- erADDialinCallback
- erADDisplayName
- erADEAlias
- erADEDaysBeforeGarbage
- erADEEnableStoreDeflts
- erADEExtension1
- erADEExtension10
- erADEExtension11
- erADEExtension12
- erADEExtension13
- erADEExtension14
- erADEExtension15
- erADEExtension2
- erADEExtension3
- erADEExtension4
- erADEExtension5
- erADEExtension6
- erADEExtension7
- erADEExtension8
- erADEExtension9
- erADEHardLimit
- erADEHideFromAddrsBk
- erADEIncomingLimit
- erADELanguages
- erADEmployeeID
- erADEOutgoingLimit
- erADEOverQuotaLimit
- erADEOverrideGarbage
- erADEProxyAddresses (Not supported for X400 type addresses)
- erADERecipientLimit
- erADESMTPEmail
- erADEStoreQuota
- erADETargetAddress
- erADEX400Email
- erADfax
- erADHomeDir
- erADHomeDirDrive
- erADHomePage
- erADInitial
- erADLoginScript
- erADLoginWorkstations
- erADNamePrefix
- erADNameSuffix
- erADOfficeLocations
- erADOtherName
- erADPasswordForceChange
- erADPrimaryGroup
- erADUPN
- erCompany
- erDepartment
- erDivision
- erMaxStorage
- erProfile
- eruid
- givenName
- homePhone
- l
- mail
- mobile
- pager
- postalCode
- postOfficeBox
- sn
- st
- street
- telephoneNumber
- title
- erADFullName

Note: The adapter supports extended attributes with the following syntax types:

- String
- Integer
- Boolean

Examples of supported filters

Example 1:

To retrieve user accounts that have the value of the employeeID attribute on the Active Directory account form as 1, specify the filter as

```
(erADEmployeeID=1)
```

Example 2:

To retrieve user accounts that have the value of the cn attribute on the Active Directory account form as thomas, specify the filter as

```
(cn=thomas)
```

Example 3:

To retrieve user accounts that have the value of the Department name attribute as ibm and the Country attribute as United States, specify the filter as

```
(&(erADDepartment=ibm*)(erADCountryCode=840))
```

Non-supported attributes for filtering

The following table lists the attributes on the Active Directory account form that the adapter does not support for filter reconciliation.

Table 3. Attributes not supported by the adapter for filter reconciliation

- All WTS attributes
- erAccountStatus
- erADAllowEncryptedPassword
- erADCannotBeDelegated
- erADContainer
- erADDistinguishedName
- erADEApplyOntoAllow
- erADEApplyOntoDeny
- erADEAssociatedExtAcc
- erADEAutoGenEmailAddrs
- erADEChgPermissions
- erADEDelegates
- erADEDelMailboxStorage
- erADEDenyPermTo1Level
- erADEFullMailboxAccess
- erADEGarbageAfterBckp
- erADEHomeMDB
- erADEMailBoxStore
- erADEReadPermissions
- erADERstrctAdrsLs
- erADEShowInAddrBook
- erADETakeOwnership
- erADEForwardTo
- erADEForwardingStyle
- erADExpirationDate
- erADIsAccountLocked
- erADLastFailedLogin
- erADLastLogoff
- erADLastLogon
- erADLastLogonTimeStamp
- erADManager
- erADNoChangePassword
- erADPasswordLastChange
- erADPasswordMinimumLength
- erADPasswordNeverExpires
- erADPasswordRequired
- erADRequireUniquePassword
- erADSmartCardRequired
- erADTrustedForDelegation
- erGroup
- erLogonTimes
- erPassword
- erADHomeDirShare
- erADHomeDirAccessShare
- erADHomeDirNtfsAccess
- erADEAllowPermTo1Level
- erADRadiusFramedIPv4Addr
- erADEAllowedAddressList
- erADEOutlookWebAccessEnabled
- erADEActiveSyncEnabled
- erADEMAPIEnabled
- erADEEnableRetentionHold
- erADEStartRetentionHold
- erADEEndRetentionHold

Examples of non-supported filters

Example 1: Filter reconciliation of attributes not supported

The adapter does not support filter reconciliation of attributes, such as manager, **distinguishedName**, and **memberOf**, because the values of these attributes are stored in the distinguished name (DN) format in the Active Directory.

A group, group1, exists inside the organization unit Test under the domain adlab. This domain lies inside the parent domain com that exists on the Active Directory. The Group attribute on the Active Directory account form is mapped to the **memberOf** attribute of the Active Directory.

If you specify the value of the Group attribute on the Active Directory account form as group1, then the adapter sets the value of the **memberOf** attribute in the DN format as `CN=group1,OU=Test,DC=adalb,DC=com.`

To retrieve users that are members of the group, group1, specify the filter as (ergroup=group1). The adapter searches for the value group1 in the **memberOf** attribute. Because the value of the **memberOf** attribute is stored in the DN format, the adapter fails to retrieve users that are members of the group, group1.

Example 2: Bit-level filtering not supported

The adapter does not support bit-level filtering. The **userAccountControl** attribute in Active Directory is a bit-mapped value attribute. Active Directory Adapter retrieves the status of a user account from the **userAccountControl** attribute on the Active Directory. The attribute is of data type integer and its value can be zero or a combination of one or more of the property flags. For more information about the property flags of the **userAccountControl** attribute, see the Microsoft Windows Server documentation.

To reconcile status of user accounts, specify the filter as (eraccountstatus=1). Because the value of the **userAccountControl** is a combination of one or more property flags, the adapter fails to retrieve any of the user accounts.

Example 3: Attribute format differences not supported

The adapter supports the format of the attributes displayed on the Active Directory account form. It does not support filter reconciliation for attributes that have their values stored in the Active Directory in a different format. For example, if India is specified as the country on the Active Directory account form, the adapter sets the three-digit code 356 as the value of the **countryCode** attribute in the Active Directory. The countryCode attribute on the Active Directory is mapped to the Country attribute on the Active Directory account form. To reconcile all objects that have the Country attribute set to India, specify the filter as (eradcountrycode=India). The adapter searches for the value India in the **countryCode** attribute. Because the value of the country India is stored as 356 in the **countryCode** attribute, the adapter returns success, but does not reconcile any user accounts. For a successful reconciliation, specify the country code of India as 356 in the filter in the following format:

```
(eradcountrycode=356)
```

Example 4: Not format filtering leads to unexpected results

A filter that uses the not format (!(Attribute name=Value)) leads to unexpected results. The format of the filter is valid and the search is successful. However, the adapter retrieves entire sets of data for all objects for which the specified attribute is not set. For example, to retrieve user accounts that have the **empoyeeID** attribute not equal to 1000, specify the filter as (!(erADEmployeeID=1000)). The adapter retrieves:

- All user accounts that have the **empoyeeID** attribute not equal to 1000.
- All groups because the group object does not contain the **empoyeeID** attribute.
- All containers because the container object does not contain the **empoyeeID** attribute.
- All mail stores because the mail stores object does not contain the **empoyeeID** attribute.

For a successful reconciliation, specify the object class with the attribute name. To retrieve user accounts that have **empoyeeID** attribute not equal to 1000, specify the **erADAccount** object class with the **employeeID** attribute in the following format:

```
(&((!(erADEmployeeID=1000))(objectclass=erADAccount)))
```

The following table lists the objects and their corresponding object class that you must specify in addition to the attribute name for a successful filter reconciliation.

Table 4. Objects and the corresponding object class

Object	Object class
Group	erADGroup
Group container	erADGroupContainer
User	erADAccount
User container	erADContainer
Mail store	erADMailStore
Mailbox Folder Policy	erADMBFldPolicy
Mailbox Unified Messaging Policy	erADMBUMPolicy
Disconnected Mailbox	erADDisabledMB

User account additions

You can add user accounts at any time for either an existing person or a new person in the organization.

This section describes the adapter attributes that define the accounts on the account form. For specific procedures, see the IBM Security Identity Manager product documentation.

Attributes for adding user accounts

Specify a value for the **User Id** attribute to add a user account on the Active Directory.

The **User Id** attribute is limited to 20 characters. This attribute can contain:

- Alphabetic characters
- Unicode characters
- Numbers
- Special characters, such as _ # - $ % ^ ` ( ) ! ~ . ' { }

Note: The period (.) is an exception. It must be surrounded by valid characters; that is, you must specify a valid character before and after the period. For example, 6.7.8.9 is a valid user ID, however, 6.7.8.9. is not a valid user ID.

The **User Id** attribute cannot include control characters, or any other special characters other than ' ` ~ ! $ % ^ . & { } ( ) - _. If the **User Id** attribute contains non-supported characters, the Active Directory gives an error message. The adapter stores the value of the **User Id** attribute in the sAMAccountName attribute on the Active Directory.

Note: The **User Id** attribute is the only attribute that is required to add an Active Directory account.

To add a user account, if you specify only the **User Id** attribute on the account form, these attributes are set on the Active Directory.

Table 5. List of attributes and their default values on the Active Directory

Attribute	Default value	Set by
cn	Value of the User Id attribute on the Active Directory account form.	Active Directory Adapter
countryCode	0 If country is specified on the Active Directory account form, then the corresponding three-digit code is set on the Active Directory.	Active Directory
lastLogoff	0	Active Directory
lastLogon	0	Active Directory
distinguishedName	`cn=`*`RDN`*`,cn=Users,`*`domain name`* if no base point is specified on the Active Directory Adapter service form. `cn=`*`RDN`*`,`*`container`*`,`*`base point`* if the base point is specified on the Active Directory Adapter service form.	Active Directory Adapter
primaryGroupID	513	Active Directory
sAMAccountName	Value of the **User Id** attribute on the Active Directory account form.	Active Directory Adapter
name	Value of the **User Id** attribute on the Active Directory account form.	Active Directory
userPrincipalName	*UserId@domain*	Active Directory Adapter
badPwdCount	0	Active Directory
objectCategory	`CN=Person,CN=Schema,` `CN=Configuration,DC=`*`domain name`*	Active Directory
msNPAllowDialin	FALSE	Active Directory Adapter
msRADIUSServiceType	4	Active Directory Adapter

CN attribute specification

You can configure to use either the IBM Security Identity Manager schema cn attribute or the erADFullName attribute on the account form.

When the compliance alerts on IBM Security Identity Manager are enabled, avoid using the cn attribute on the account form. To use either the cn attribute or the erADFullName attribute, you must customize the account form and set the registry key UseITIMCNattribute. For more information about the CN attribute configuration, see the *Active Directory Adapter Installation and Configuration Guide*.

Distinguished name creation for a user account

The Active Directory Adapter computes values of various attributes on the Active Directory account form to create a distinguished name (DN) for a user account.

To create a DN, the adapter:

1. Generates a Relative Distinguished Name (RDN) for the user account. The following table lists the order in which the Active Directory Adapter checks the values of the attributes on the Active Directory account form to generate an RDN.

Table 6. The order of attributes on the Active Directory account form that the adapter checks to generate an RDN

Attributes on the IBM Security Identity Manager			**RDN value**
Full Name			*Full Name*
Display Name			*Display Name*
First Name	Initial	Last Name	*First Name Initial*. Last Name
First Name	Initial		*First Name Initial*.
First Name	Last Name		*First Name Last Name*
First Name			*First Name*
Last Name			*Last Name*
User Id			*User Id*

The following figure displays the decision tree for the process of generating an RDN.

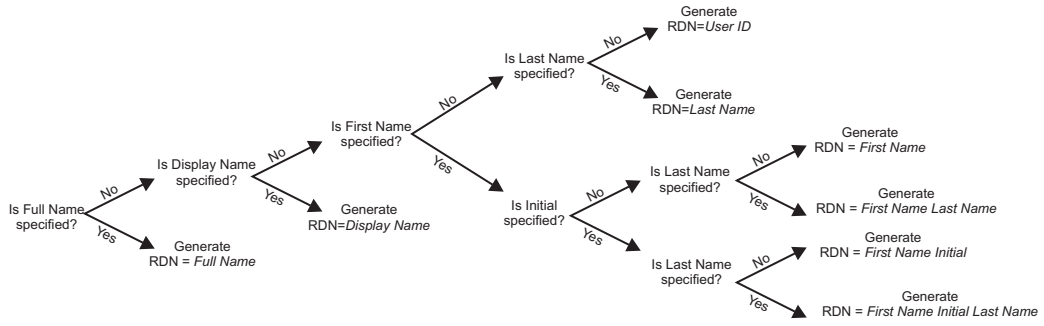

Figure 1. Generating an RDN

If the adapter finds an attribute value, that value is used for generating the RDN. For example, if the Full Name attribute is not found, then the adapter checks for the value in the Display Name attribute. If a value is found, the adapter uses the display name as the RDN. Otherwise, the adapter checks for the next attribute value in the First Name attribute, and so on. User Id is the default value of an RDN. The maximum length of an RDN is 64 characters.

2. Adds the string cn= as a prefix to the generated RDN. For example, cn=*RDN*.

3. Adds a container that contains the user account as a suffix to cn=*RDN*. The container is separated by a comma. The adapter adds the default user container cn=Users as a suffix, if:
   - You do not specify the Container attribute on the Active Directory account form.
   - You do not specify the Base Point DN attribute on the Active Directory Adapter service form.
   - The base point that you specify on the Active Directory Adapter service form does not contain a container.

   Containers other than the Users container are represented as ou=*organization unit*, where organization unit is the name of the container.
4. Adds a domain name as a suffix to cn=*RDN*,cn=Users. The domain name is separated by a comma. If a base point is specified on the Active Directory Adapter service form, then the domain name is the specified base point. However, if no base point is specified on the Active Directory Adapter service form, then the adapter finds the default domain name where the adapter is running. Therefore, the distinguished name is: cn=*RDN*,cn=Users,*domain name*.

User principal name of a user account

The user principal name is an account name of a user in an email address format.

A user principal name consists of two parts:

- User identification: Contains the user log-on name.
- Domain: Contains the domain name where the user account is located.

A user principal name is computed by separating these two parts by an @ symbol. For example, *username@domain name*.

If you specify the User Principal Name attribute on the Active Directory account form, then the adapter sets the specified value to the userPrincipalName attribute on the Active Directory. If the User Principal Name attribute is not specified, then the adapter uses the value of the User Id attribute as user principal name. The adapter also appends @*domain name* to the user principal name.

The Active Directory Adapter checks for the uniqueness of the User Principal Name (UPN) attribute within a forest when you create a user account from IBM Security Identity Manager. You can either provide the User Principal Name during the user add operation or the adapter generates the User Principal Name. The adapter performs this search on the User Principal Name in the forest to ensure that no two users have the same User Principal Name. The adapter performs the search first in the current managed domain and then in the forest.

The adapter uses the UPNSearchEnabled registry key to perform the uniqueness search. By default, this registry key is set to TRUE. When the registry key UPNSearchEnabled is set to FALSE, the adapter creates the user account without checking for the uniqueness of the User Principal Name.

Examples of when the registry key UPNSearchEnabled is set to TRUE:

Example 1

You provide the User Principal Name during the user add operation. The adapter uses the value of the User Principal Name attribute and performs

the search. When a user account with the same User Principal Name exists in the forest, the adapter fails the user add operation.

Example 2

You do not provide the User Principal Name during the user add operation. The adapter generates the User Principal Name to perform the search in the forest. When the adapter finds a user account with the generated User Principal Name, the adapter creates another User Principal Name. The adapter appends a number starting from 1 to the generated value to get a new User Principal Name.

For example, the adapter generates the User Principal Name `TestUser@MyDomain.com`. When the adapter finds a user account with the generated User Principal Name, the adapter appends 1 to the name, `TestUser1@MyDomain.com`. When the adapter performs the search by using the new value and finds a user account with the generated User Principal Name, the adapter appends 2 to the name, `TestUser2@MyDomain.com`. When the adapter performs the search and finds a user account with the generated User Principal Name, the adapter fails the user add operation

Note:

- The User Principal Name search operation is expensive in terms of adapter performance.
- The adapter might not find a user with the current User Principal Name because of the replication delay. It adds the user account on the Active Directory.
- Two add operations are running simultaneously with the same User Principal Name. The adapter might not find a user with the User Principal Name and both the user accounts are added successfully.
- The existing version of the adapter does not perform the User Principal Name search for the modify operation. You can have a policy to generate a unique User Principal Name on IBM Security Identity Manager server and avoid relying on the adapter to generate the unique name.

Control specifications for a user account

You can set attributes on the Active Directory account form to specify controls for a user account.

Password Never Expires
Specifies whether a password can ever expire.

Password Required
Specifies whether a password is required.

Smart Card Required
Specifies whether a smart card is required for login.

User Cannot Change Password
Specifies whether the user can change their password.

Allow Encrypted Password
Specifies whether encrypted passwords are allowed.

These attributes correspond to the property flags of the userAccountControl attribute on the Active Directory. The attribute names and their corresponding property flags are listed in the following table.

Table 7. Attributes on the Active Directory account form and their corresponding property flags

Attribute	Property flag	Hexadecimal value for the property flag	Decimal value for the property flag
Password Never Expires	DONT_EXPIRE_PASSWORD	0x10000	65536
Password Required	PASSWD_NOTREQD	0x0000	0
Smart Card Required	SMARTCARD_REQUIRED	0x40000	262144
User Cannot Change Password	PASSWD_CANT_CHANGE	0x0040	64
Allow Encrypted Password	ENCRYPTED_TEXT_PWD_ALLOWED	0x0080	128

The value of the userAccountControl attribute is the sum of the values of the property flags that are enabled. For more information about property flags of the userAccountControl attribute, see the Microsoft Windows Server documentation.

You can force a user account to change the password on next logon. Select the Force Password Change check box on the PASSWORD page of the Active Directory account form. The Active Directory Adapter maps the Force Password Change attribute to the pwdLastSet attribute on the Active Directory. If you select the Force Password Change check box, then the adapter sets the value of the pwdLastSet attribute to -1. If you do not select the Force Password Change check box, then the adapter sets the value of the pwdLastSet attribute to 0.

Creating a home directory for a user account

Follow these steps to set the attributes that create and specify permissions for a user account home directory.

Before you begin

Before you create a home directory for a user account, ensure that you have:

- Created a shared directory on the Windows server.
- Provided full access rights on that shared directory to the user account under which Active Directory Adapter is running.

About this task

To create a home directory for a user account:

Procedure

1. Set the value of the following registry keys to `TRUE`
   - CreateUNCHomeDirectories
   - ManageHomeDirectories
2. Specify the following attributes on the Active Directory account form:
   - Home Directory
   - Home Directory Drive

   Note: The Home Directory attribute must be in the Universal Naming Convention (UNC) format. UNC is a format for specifying the location of resources in a Local Area Network (LAN). UNC uses the format: `\\HOME_AD_SERVER\ SHARED_DIR\HOME DIR`, where:

- HOME_AD_SERVER is the shared server name.
- SHARED_DIR is the shared directory.
- HOME DIR is the name of the home directory for the user account.

For example, consider a user account with the following attribute settings on the Active Directory account form.

Table 8. Home Directory attribute settings

User Id	Thomas
Home Directory	\\H20\homedir\thomas
Home Directory Drive	F:

Because the values of the registry keys CreateUNCHomeDirectories and ManageHomeDirectories are `TRUE`, the adapter:

- Creates on server H20 a UNC home directory `thomas` inside the shared directory `homedir`.
- Maps the home directory thomas with drive F.

3. Specify permissions on the home directory for a user account. Set the Home Directory NTFS Access attribute for the user on the Active Directory account form. The following table lists the values of the Home Directory NTFS Access attribute and their corresponding permissions on the home directory.

Table 9. Home Directory NTFS Access attribute values and their corresponding permissions on the home directory

Home Directory NTFS Access attribute value	**Permissions**
Full	You have full control over the home directory. You can: • Change permissions • Take ownership • Delete subfolders and files • Read, write, and change files
Change	You have following controls over files and subfolders in the home directory: • Read • Write • Modify

4. Optional: Share the home directory and provide full access rights to the user account on the home directory Specify the following attributes on the Active Directory account form:
   - Home Directory Share
   - Home Directory Share Access

RAS attribute specification

To specify the Remote Access Service (RAS) dial-in option, you can use attributes on the Active Directory Adapter account form.

Dial-in

The dial-in options maps to the Remote Access Permission (Dial-in or VPN) on the Dial-in tab of an Active Directory user account. The default option on the account form is Deny Access. You can select one of the following options on the account form:

- Allow Access
- Deny Access
- Control access through Remote Access Policy

Note: The option Control Access through Remote Access Policy is not available on the Active Directory when the Active Directory is in Mixed mode.

Callback Settings

The Callback Settings maps to the Callback Options on the Dial-in tab of an Active Directory user account. The default option on the account form is User supplied callback number. You can select one of the following options on the account form:

- No Callback
- User supplied callback number
- Fixed callback number

Callback Number

When you select the Callback Settings options as the Fixed callback number, you must specify the Callback Number. when you do not do so, the adapter generates an error.

Static IPv4 Address

The Static IPv4 Address accepts the IP address string in the IPv4 format. The Static IPv4 Address maps to the Assign a Static IP Address on the Dial-in tab of an Active Directory user account.

Note: The Assign a Static IP Address attribute is not available on the Active Directory when the Active Directory is in Mixed mode.

User account enablement for mail

Two types of mail enablement are available for user accounts.

Select the type of enablement you want for the user account.

Mail-enabled

An Active Directory user account that has an email address associated with it, but has no mailbox on the Exchange server. A mail-enabled user can send and receive email with another messaging system. Messages sent to a mail-enabled user account, pass through the Exchange server, and are forwarded to an external email ID of that user account. For example, Thomas is an employee of company1, with a mailbox on the Exchange server of company1, and an email ID thomas1@company1.com. Company2 takes over company1. The employees of company1 have mail-enabled user accounts in the domain of company2. The new email ID of Thomas is thomas1@company2.com. Thomas can send and receive mail with the new

email ID, but the mailbox for Thomas is not on the Exchange server of company2. It is on the Exchange server of company1.

Mailbox-enabled
An Active Directory user account that has a mailbox on the Exchange server. A mailbox-enabled user can send and receive messages, and store messages on the Exchange server mailboxes.

To create a mail-enabled user account, you must specify a value for the Target Address attributes on the Active Directory account form.

To create a mailbox-enabled user account, you can optionally specify a value for the Mailbox Store attributes on the Active Directory account form. If the value is not specified, the Active Directory Adapter uses the default mailbox feature of Exchange 2010 to create a default mailbox for the user. You can view the value of the default mailbox in the IBM Security Identity Manager account form. The value is on the **Mailbox** tab in the **Mailbox Store** field.

You can also create a mailbox-enabled user account by connecting the disconnected mailbox to a user account. The name of the mailbox is changed according to the user account name. For more information about connecting a disconnected mailbox to a user account, see "Mailbox support modification for Exchange 2010" on page 30.

The Exchange server uses the value of the Alias attribute to generate an email ID for a user account. If you do not specify a value for the Alias attribute, the Exchange server uses a default alias. The value of the User Principal Name attribute becomes the default alias. For example, for a user account thomas with the user principal name thomasd@ibm.com, the Exchange server uses the value thomasd as the alias. If the value of the Alias attribute of another user account matches an existing alias, the Exchange server modifies the other user account email ID. The Exchange server appends a number to the email ID of the other user account. For example, a user account Thomas with alias thomas1 exists on the Active Directory. The email ID of Thomas is thomas1@ibm.com. If you create another user account Nancy with alias thomas1, then the Exchange server generates the email ID thomas12@ibm.com for Nancy.

Note: If you specify both the attributes, Mailbox Store and Target Address, the Active Directory Adapter returns an error.

Proxy address creation for a user account

By default, the Exchange server assigns a primary Simple Mail Transfer Protocol (SMTP) proxy address to a user account when a mailbox is created.

To create multiple proxy addresses for a user account, specify the Proxy Addresses attribute on the Active Directory account form. A primary proxy address for each type must be added before adding additional proxy addresses of the same type. The primary proxy address of an SMTP address type cannot be deleted.

Note: Always specify a primary proxy address in uppercase and a secondary proxy address in lowercase.

For example, a user account Thomas exists on the Active Directory with the following values in the Active Directory account form.

User Id	Thomas

Proxy Addresses	SMTP:Thomas@ibm.com smtp:Thomas2@ibm.com

In this example, SMTP:Thomas@ibm.com is the primary SMTP proxy address, and smtp:Thomas2@ibm.com is the secondary SMTP proxy address.

Note: To create an X400 proxy address for a user account, you must specify the primary SMTP proxy address.

User account modification

You can modify user account attributes at any time in IBM Security Identity Manager.

For specific procedures, see the IBM Security Identity Manager product documentation.

Container attribute modification

Modifying the Container attribute means moving a user from one container to another.

You can move a user between:

- Containers that are stored at the specified base point
- All containers, if no base point is specified.

  Note: If no base point is specified when creating an Active Directory service, the Active Directory Adapter creates users in the Users container of the Active Directory.

When you modify the Container attribute, the distinguished name of a user changes because the user moves to a different position in the Active Directory hierarchy. The following example illustrates changes in the distinguished name of a user, when you modify the Container attribute.

For example, a user account with the name Thomas Daniel exists on the Active Directory. The Active Directory has the following structure.

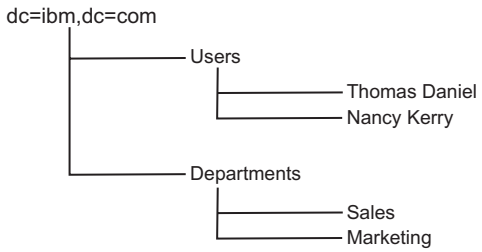

Figure 2. Example of an Active Directory structure

The distinguished name of Thomas Daniel is:

```
cn=Thomas Daniel,cn=Users,dc=ibm,dc=com
```

Modify the Container attribute on IBM Security Identity Manager from cn=Users to ou=Marketing. After this change, the distinguished name of Thomas Daniel changes to the following value:

```
cn=Thomas Daniel,ou=Marketing,ou=Departments,dc=ibm,dc=com
```

Home Directory attribute modification

The Active Directory Adapter supports creation and deletion of home directories only in the shared folders on the Windows server. The adapter does not support the creation and deletion of local home directories.

The following examples describe the behavior of the Active Directory Adapter when you modify the attributes that are related to the home directory on the Active Directory account form, for an existing user account.

Note: The request to create a home directory might fail because the shared directory does not have full access rights for the user account under which the adapter service is running.

Examples of Active Directory behavior when home directory attributes are modified.

Example 1

A user account Thomas Daniel exists on the Active Directory with the following values in the Active Directory account form.

Table 10. Account form values

Attribute	Value
Home Directory	\\H20\shareddir\thomas
Home Directory Drive	F:
Home Directory Share	homedirshare1

The values of the registry keys are:

- ManageHomeDirectories = TRUE
- DeleteUNCHomeDirectories = FALSE
- CreateUNCHomeDirectories = TRUE

Delete the values of the attributes that are related to the home directory. Because the value of the registry key DeleteUNCHomeDirectories is FALSE, the adapter:

- Does not delete the home directory thomas from the server H20.
- Does not remove the share homedirshare1.
- Deletes values of the Home Directory and the Home Directory Drive attributes on the Active Directory.

Example 2

A user account Thomas Daniel exists on the Active Directory with the following values in the Active Directory account form.

Table 11. Account form values

Attribute	Value
Home Directory	\\H20\shareddir\thomas
Home Directory Drive	F:
Home Directory Share	homedirshare1

The values of the registry keys are:

- ManageHomeDirectories = TRUE
- DeleteUNCHomeDirectories = TRUE
- CreateUNCHomeDirectories = TRUE

Delete the values of the attributes that are related to the home directory. Because the value of the registry key DeleteUNCHomeDirectories is TRUE, the adapter deletes the home directory thomas from the server H20.

Example 3

A user account Thomas Daniel exists on the Active Directory. This user account does not contain values of the attributes that are related to the home directory on the Active Directory account form.

The values of the registry keys are:

- ManageHomeDirectories = TRUE
- DeleteUNCHomeDirectories = TRUE
- CreateUNCHomeDirectories = FALSE

Specify values for the following attributes that are related to the home directory on the Active Directory account form.

Table 12. Account form values

Attribute	Value
Home Directory	\\H20\shareddir\thomas
Home Directory Drive	F:
Home Directory Share	homedirshare1

Because the value of the registry key CreateUNCHomeDirectories is FALSE, the adapter:

- Does not create the home directory thomas and the home directory share homedirshare1 on the server H20.
- Sets values of the attributes Home Directory and Home Directory Drive on the Active Directory.

Example 4

A user account Thomas Daniel exists on the Active Directory. This user account does not contain values of the attributes that are related to the home directory on the Active Directory account form.

The values of the registry keys are:

- ManageHomeDirectories = TRUE
- DeleteUNCHomeDirectories = TRUE
- CreateUNCHomeDirectories = TRUE

Specify values for the following attributes that are related to the home directory on the Active Directory account form.

Table 13. Account form values

Attribute	Value
Home Directory	\\H20\shareddir\thomas
Home Directory Drive	F:
Home Directory Share	homedirshare1

Because the value of the registry keys CreateUNCHomeDirectories and ManageHomeDirectories is TRUE, the adapter:

- Creates the home directory thomas on the server H20.

- Maps the home directory with the drive F.
- Assigns the share name homedirshare1 to the home directory.
- Assigns access rights to the home directory and the home directory share.

Example 5

A user account Thomas Daniel exists on the Active Directory with the following values in the Active Directory account form.

Table 14. Account form values

Attribute	Value
Home Directory	\\H20\shareddir\thomas
Home Directory Drive	F:
Home Directory Share	homedirshare1

The values of the registry keys are:

- ManageHomeDirectories = TRUE
- DeleteUNCHomeDirectories = TRUE
- CreateUNCHomeDirectories = TRUE

Change values of the attributes on the Active Directory account form to the following values.

Table 15. Changed account form values

Attribute	Value
Home Directory	\\H20\shareddir\Peter\thomas
Home Directory Drive	G:
Home Directory Share	homedirshare2

Change the value of the registry key DeleteUNCHomeDirectories to `FALSE`.

In this example, the modify operation fails because the adapter cannot create nested directories; that is, the directory thomas inside the directory Peter. The adapter ignores the other attributes that are related to the home directory.

Example 6

A user account Thomas Daniel exists on the Active Directory with the following values in the Active Directory account form.

Table 16. Account form values

Attribute	Value
Home Directory	\\H20\shareddir\thomas
Home Directory Drive	F:
Home Directory Share	homedirshare1

The values of the registry keys are:

- ManageHomeDirectories = TRUE
- CreateUNCHomeDirectories = TRUE

Change the value of the Home Directory attribute to \\H20\shareddir\thomas_daniel.

In this example, the adapter creates a home directory thomas_daniel, however, without a share because the value of registry key

CreateUNCHomeDirectories and manageHomeDirectories is TRUE. The home directory thomas remains in the shareddir directory. To create a share, you must provide the share access and NTFS access to the user account on the new home directory that is created. You must also change the values of the home directory-related attributes on the account form along with Home Directory attribute.

Note: This operation is not a directory rename operation.

Example 7

A user account Thomas Daniel exists on the Active Directory with the following values in the Active Directory account form.

Table 17. Account form values

Attribute	Value
Home Directory	\\H20\shareddir\thomas
Home Directory Drive	F:
Home Directory Share	homedirshare1

The value of the registry key is:

ManageHomeDirectories = TRUE

Change the value of Home Directory Share to newhomedirshare.

The adapter adds the share name newhomedirshare to the home directory thomas because the registry key ManageHomeDirectories is TRUE. The adapter does not remove the previous share name, that is, homedirshare1.

User password modification

You can change the password of any of the Active Directory accounts that exist on IBM Security Identity Manager.

For information about changing passwords, see the IBM Security Identity Manager product documentation.

Changing the password of a domain user from IBM Security Identity Manager, synchronizes the new password with the other accounts managed by IBM Security Identity Manager for that domain user. The Password Synchronization plug-in enables connectivity between IBM Security Identity Manager and the Windows system running the Active Directory. For more information about the Password Synchronization plug-in, see the *Password Synchronization for Active Directory Plug-in Installation and Configuration Guide*.

During the password change operation:

- If the value of the UnlockOnPasswordReset registry key is FALSE and the user account is locked, the Active Directory Adapter changes the user account password. However, the user cannot log on to the domain by using the new password.
- If the value of the UnlockOnPasswordReset registry key is TRUE, the Active Directory Adapter unlocks the user account. The user can log on to the domain by using the new password.

Note: The password change operation might fail when:

- A password policy is set on the Active Directory.
- The new password does not comply to the password policy.

Mailbox Store attribute modification

Modifying the Mailbox Store attribute means moving a user mailbox from one mailbox store to another.

You can move a mailbox either within the same Exchange server or to a different Exchange server in the same domain. For more information about moving a mailbox from one mailbox store to another, see the Microsoft Exchange server documentation.

When you modify the Mailbox Store attribute, the value of the homeMDB attribute changes because the user mailbox moves from one mailbox store to another. The following example illustrates changes in the value of the homeMDB attribute, when you modify the Mailbox Store attribute.

For example, a user account with the name Thomas Daniel exists on the Active Directory (domain name is ibm.com®). Consider Thomas Daniel has a mailbox in the First Mailbox Store of the Exchange server (ps2330) as shown in the following figure.

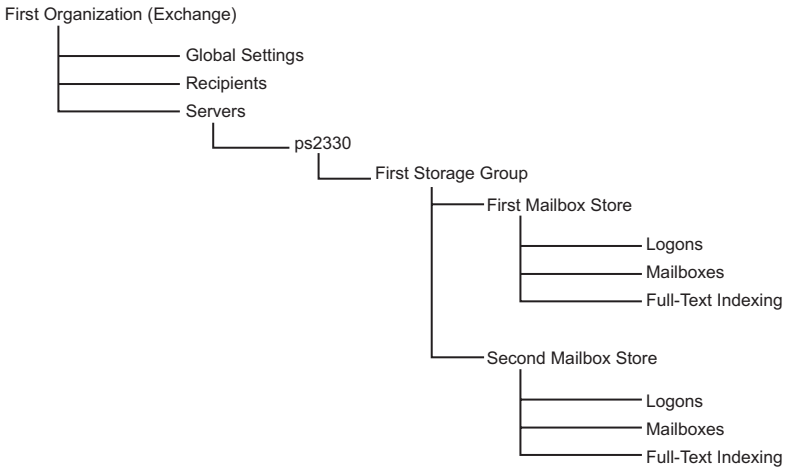

Figure 3. Exchange server organization tree

The value of the homeMDB attribute is:

```
cn=First Mailbox Store,cn=First Storage Group,cn=Information
 Store,cn=ps2330,cn=Servers,cn=First Administrative Group,
cn=Administrative Groups,cn=First Organization (Exchange),
cn=Microsoft Exchange,cn=Services,cn=Configuration,dc=ibm,dc=com
```

When you move the mailbox of Thomas Daniel from First Mailbox Store to Second Mailbox Store, the value of the homeMDB attribute changes. The value is now:

```
cn=Second Mailbox Store,cn=First Storage Group,cn=Information
Store,cn=ps2330,cn=Servers,cn=First Administrative Group,
cn=Administrative Groups,cn=First Organization (Exchange),
cn=Microsoft Exchange,cn=Services,cn=Configuration,dc=ibm,dc=com
```

Mail status modification for a user account

You can modify the mail status of a user account. The account can be either mail-enabled or mailbox-enabled.

For information about enabling a user account for mail, see "User account enablement for mail" on page 21.

Note: When you modify the mail status of a user account, you can also modify the value of the Alias attribute on the account form. If you do not modify the Alias attribute, then the adapter uses the existing value that is set on the Active Directory.

Mail status modification for a user account from Mailbox-enabled to Mail-enabled

To modify a Mailbox-enabled user account to a Mail-enabled user account, clear the value for the Mailbox Store attribute on the Active Directory account form.

You must specify a value for the Target Address attribute on the Active Directory account form.

After you successfully change the mail status, the adapter ignores the attributes that are not applicable to the Mail-enabled user account in the status change request. This behavior is true for any value and operation of that attribute.

Clearing the Exchange attributes that are applicable to the Mailbox-enabled user account

You must clear the Exchange attributes fromIBM Security Identity Manager. These attributes are ones that are applicable to Mailbox-enabled user account but, not applicable to Mail-enabled user account. To clear the Exchange attributes for a user account whose mail status is modified from Mailbox-enabled to Mail-enabled, perform one of the following steps:

- Perform a user lookup to clear the Exchange attributes that are applicable to Mailbox-enabled user account.
- Use the provisioning policy of the adapter to add attributes that are not applicable to Mail-enabled user account to the same mail status change request. For example, to clear the Mailbox-enabled attributes of a user account set the value of the attributes to NULL in the adapter provisioning policy. The adapter does not process the Exchange Mailbox-enabled attributes for a user account that is modified from Mailbox-enabled to Mail-enabled. These attributes are removed from the IBM Security Identity Manager server.

Mail status modification for a user account from Mail-enabled to Mailbox-enabled

To modify a Mail-enabled user account to a Mailbox-enabled user account, clear the value for the Target Address attribute on the Active Directory account form.

You must specify a value for the Mailbox Store attribute on the Active Directory account form.

When you modify the mail status of a user account from Mail-enabled to Mailbox enabled, the Active Directory adds the Mailbox-related attributes to that user account. Perform a user lookup to add these attributes to the IBM Security Identity Manager server for that account.

Mail status clearing for a user account

Enabling a user account for mail sets the Exchange attributes on the Active Directory. When you disable a user account for mail, the Active Directory clears the Exchange attributes for that user account.

To disable a user account for mail, clear the value that is set for one of the following attributes on the user account form:

Mailbox Store
Clear this attribute value if the user account is Mailbox-enabled.

Target Address
Clear this attribute value if the user account is Mail-enabled.

To clear the Exchange attributes on IBM Security Identity Manager, perform one of the following steps:

- Perform a filter reconciliation.
- Use the provisioning policy of the adapter to add all the Exchange attributes to mail status clear request. For example, to clear the Exchange attributes of a user account set the value of the Exchange attributes to NULL in the adapter provisioning policy.

When the mailbox for a user account is deleted, creating another mailbox for the same user account with the same alias creates a mailbox. The adapter does not permanently delete the mailbox from the Exchange server. A deleted mailbox is flagged as disconnected by the Exchange server.

By default, the Exchange server preserves the deleted mailbox for a specific duration. An administrator can configure this duration.

You can connect the disconnected mailbox to a user account. The name of the mailbox is changed according to the user account name. For more information about connecting a disconnected mailbox to a user account, see the Microsoft Exchange server documentation.

Mailbox support modification for Exchange 2010

The adapter is enhanced to support disabling (disconnecting) mailboxes when user accounts are suspended. The adapter also supports connecting a user account to a disabled mailbox.

The following new registry keys are introduced to the set of adapter registry keys:

Table 18. New registry keys

Registry key name	Default value
DisableMailboxOnSuspend	FALSE
ReconDisconnectedMailbox	FALSE

A disabled user mailbox

Disabling a mailbox means disconnecting a mailbox-enabled user account in Active Directory from its mailbox.

When the mailbox is disabled, all the exchange attributes of the user account are removed from Active Directory. The user account associated with the mailbox remains in Active Directory, but is no longer associated with a mailbox.

The adapter uses the registry key **DisableMailboxOnSuspend** to decide whether to disable the mailbox during a suspend operation.

Table 19. DisableMailboxOnSuspend registry key actions

Value of **DisableMailboxOnSuspend**	Action
TRUE	The mailbox of the user is disabled.

Table 19. DisableMailboxOnSuspend registry key actions (continued)

Value of DisableMailboxOnSuspend	Action
FALSE	The mailbox of the user is not disabled

The mailbox of a user can also be disabled by clearing the value of Mailbox Store attribute on account form. The adapter does not depend on the value of the **DisableMailboxOnSuspend** registry key.

When a user mailbox is disabled all the exchange properties of the mailbox are removed from the user account on Active Directory. The mailbox is marked in the database for removal. When a mailbox-enabled user account is removed from Active Directory, the mailbox is marked in exchange database for removal.

A disabled mailbox that is deleted remains in exchange database for configured number of days before it is deleted. The default is 30 days. This configuration can be changed through the Exchange Admin Console. When you create a mailbox for a new or existing user, the exchange attributes that are required for a mailbox are added to the user object in Active Directory. When a disabled mailbox is connected to an existing Active Directory user account, that user account becomes the owner of the mailbox. The account has full access to any content within the mailbox

User account connection to a disabled mailbox

A disconnected mailbox is a mailbox object in the Microsoft Exchange store that is not associated with an Active Directory user account.

To connect a user account to a disabled mailbox, the adapter needs information about the disabled mailbox and the user account for which to connect. The Exchange server can have many disabled mailboxes on an exchange store to which user account can be connected. The user account to which user disabled mailbox is connecting must be logon-enabled.

The adapter uses the registry key **ReconDisconnectedMailbox** during reconciliation operation. If this feature is enabled the adapter performance for the reconciliation operation might be slower.

The adapter uses the registry key **ReconDisconnectedMailbox** to decide whether to return information about disabled mailboxes during a reconciliation operation.

Table 20. ReconDisconnectedMailbox registry key actions during reconciliation

Value of ReconDisconnectedMailbox	Action
TRUE	The adapter returns information about all the disabled mailboxes from configured exchange servers to IBM Security Identity Manager.
FALSE	The adapter does not reconcile disconnected mailboxes to IBM Security Identity Manager.

A new support data object class **erADDisabledMB** is added to Windows Active Directory profile schema. The object class **erADDisabledMB** is supported for adapter-based Filtering but not for adapter-based event notification.

The **erADAccount** class has a new attribute **erADEConnectToMailbox** to connect a user account to a disabled mailbox. Use this attribute to select one of the disabled

mailboxes from the list of disabled mailboxes returned by the adapter in a reconciliation operation. This attribute is used only to provide the information required by the adapter to connect the user account to the disabled mailbox.

A full reconciliation or a support data reconciliation must be performed to get information about all the disabled mailboxes from each Exchange Server in the organization.

After connecting to a disabled mailbox, when a reconciliation or a user lookup is performed, the value of this attribute is cleared from the account form.

After connecting the mailbox, reapply mailbox folder policy and other mailbox-related attributes. These attributes were removed from Active Directory when the mailbox was disabled.

Note: A disabled mailbox can be either a user mailbox or a resource mailbox on the exchange server. To differentiate between the two types of disabled mailboxes, a new attribute **erADEMailboxType** of object class **erADDisabledMB** is added. Customize the filter value used by attribute **erADEConnectToMailbox** to display only disabled user mailboxes on account form. If you connect a user account to a disabled resource mailbox, the adapter connects mailbox and converts it to a user mailbox.

Primary Group attribute modification

The default value of the Primary Group attribute on the IBM Security Identity Manager is `Domain Users`.

To specify a primary group for a user account, the user must be a member of that group.

User account suspension

When you suspend a user account, the status of the user account on IBM Security Identity Manager becomes inactive, and the user account becomes unavailable for use.

Suspending a user account does not remove the user account from IBM Security Identity Manager. For more information about suspending user accounts, see the IBM Security Identity Manager Information Center.

When you suspend a user account from IBM Security Identity Manager, the Active Directory Adapter sets the property flag ACCOUNTDISABLE of the userAccountControl attribute on the Active Directory. For more information about property flags of the userAccountControl attribute, see the Microsoft Windows Server documentation.

When you suspend a user account from IBM Security Identity Manager, the adapter suspends the user's access to the Mailbox on the Active Directory. The adapter suspends the user's access to the Mailbox on the Active Directory by setting the value of the exchange attribute msExchUserAccountControl to 2. However, the adapter does not explicitly suspend the user's access to the Mailbox when the Recipient Update Service (RUS) is running. In this case, the adapter lets the RUS replicate the information and suspend user's access to the mailbox.

User account restoration

The restore operation reinstates the suspended user accounts to IBM Security Identity Manager.

After restoring a user account, the status of the user account on IBM Security Identity Manager becomes active. For more information about restoring user accounts, see the IBM Security Identity Manager product documentation.

When you restore a user account from IBM Security Identity Manager, the Active Directory Adapter modifies the property flag ACCOUNTDISABLE of the userAccountControl attribute on the Active Directory. For more information about property flags of the userAccountControl attribute, see the Microsoft Windows Server documentation.

When you restore a user account from IBM Security Identity Manager, the adapter enables the user's access to the Mailbox on the Active Directory. The adapter enables the user's access to the Mailbox on the Active Directory by setting the value of the exchange attribute msExchUserAccountControl to 0. However, the adapter does not explicitly restore the user's access to the Mailbox when the Recipient Update Service (RUS) is running. In this case, the adapter lets the RUS to replicate the information and enables user's access to the mailbox.

Note: You can configure the restore operation to prompt you for a password. For information about enabling password prompt for restore operation, see "Managing passwords when restoring accounts" in the *Active Directory Adapter Installation and Configuration Guide*. When a user account is locked and suspended on the Active Directory and the registry key UnlockOnPasswordReset is set to TRUE, the adapter unlocks the user account on the Active Directory when you perform the restore operation with a new password.

User account deletion

Use the deprovision feature of IBM Security Identity Manager to delete user accounts.

For more information about deleting user accounts, see the IBM Security Identity Manager Information Center.

When you deprovision a user account from IBM Security Identity Manager, the Active Directory Adapter:

- Deletes the user account from the Active Directory .
- Deletes the mailbox of the user account from the Exchange server, if the user account is enabled for a mailbox.
- Removes the membership of the user account from the groups that the user account is a member of.
- Deletes the home directory of the user account, if the value of the delUNCHomeDirOnDeprovision registry is `TRUE`.
- Deletes the profile of the user account, if the value of the delRoamingProfileOnDeprovision is `TRUE`.
- Deletes the WTS home directory of the user account, if the values of the delUNCHomeDirOnDeprovision and the WtsEnabled registry keys are `TRUE`.
- Deletes the WTS profile of the user account, if the values of the delRoamingProfileOnDeprovision and the WtsEnabled registry keys are `TRUE`.

Note: The Active Directory Adapter does not support the deletion of local home directories and user mailboxes.

Enabling and disabling unified messaging

The Active Directory Adapter can manage the Exchange Unified Messaging setup on Active Directory account with the Exchange 2010 environment.

Before you begin

The following components of unified messaging must exist:

- A UM dial plan. If you need information about creating a dial plan, go to the Microsoft TechNet website. Search on UM dial plan.
- A UM mailbox policy. If you need information about creating a mailbox policy, go to the Microsoft TechNet website. Search on UM mailbox policy.

Note: Creating and modifying a dial plan, or a UM mailbox policy is beyond the scope of the Active Directory Adapter.

The Active Directory Adapter service must be running under and administrator account.

About this task

Only a MailBox enabled user is able to use the feature of Unified Messaging. When you enable a user for Unified Messaging (UM), a default set of UM properties is applied to the user. The user can then use the Unified Messaging features.

Procedure

1. Log on to IBM Security Identity Manager.
2. Click **Manage Users**.
3. Click **Search**.
4. Select the user you want to enable unified messaging for and expand the menu.
5. Click **Request accounts**.
6. Select Active Directory Profile as the **Service type** and click **Search**.
7. Select as service name and click **Continue**.
8. Click **Mailbox**.
9. At the **Unified Messaging Mailbox Policy** field, click **Search** and select a mailbox policy. This example represents a typical mailbox policy.

   ```
   "CN=TestPolicy,CN=UM Mailbox Policies,CN=Exchange First Organization,
   CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=orion,DC=com"
   ```

   Note: To disable unified messaging, clear this field.
10. In the UM Addresses (Extensions) field, type the UM address that was created for the user. It must contain the same number of digits that is specified in the mailbox dial plan. Special characters cannot be used in the address.
11. Click **Add**.
12. Click **Continue**.
13. Select password and schedule options that you want to change and click **Submit**.
14. Click **Close**.

What to do next

If you disabled unified messaging for the mailbox of a user, you must reconcile the user. For information about service reconciliation, see the IBM Security Identity Manager product documentation.

Modifying unified messaging

You can change the UM mailbox policy or the UM address or both for a user account.

Before you begin

Unified messaging must be enabled for the user account. The Active Directory Adapter service must be running under and administrator account.

About this task

The Unified Messaging Policy can be changed only if the selected new policy belongs to the same dial plan.

To modify UM Addresses (Extensions) value you must provide the value in following format that the API requires.

`eum:`*`extension number`*`;phone-context:`*`dial plan name for the given extension number`*

In this example `eum` indicates the secondary UM address and `EUM` indicates the primary UM address.

```
eum:12345;phone-context:Mydialplan.newport.cm.ibm.com
EUM:67890;phone-context:Mydialplan.newport.cm.ibm.com
```

Procedure

1. Log on to IBM Security Identity Manager.
2. Click **Manage Users**.
3. Click **Search**.
4. Select the user you want to modify unified messaging for and expand the menu.
5. Click **Accounts**.
6. Click **Search**.
7. Expand the menu by the service name and click **Change**.
8. Click **Mailbox**.
9. At the **Unified Messaging Mailbox Policy** field, click **Search** and select a mailbox policy. This example represents a typical mailbox policy.

   ```
   "CN=TestPolicy,CN=UM Mailbox Policies,CN=Exchange First Organization,
   CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=orion,DC=com"
   ```
10. In the UM Addresses (Extensions) field, type the new UM address. It must contain the same number of digits that is specified in the mailbox dial plan. Special characters cannot be used in the address.
11. Click **Add**.
12. Click **Continue**.
13. Select password and schedule options that you want to change and click **Submit**.
14. Click **Close**.

Chapter 4. Group management tasks

The Active Directory Adapter manages groups on Active Directory.

You can add, modify, and delete groups directly from IBM Security Identity Manager.

Managing groups include the following tasks:

- Adding groups on the managed resource
- Modifying the attributes of groups
- Deleting groups

Adding groups on Active Directory

You can add groups to grant specific permissions to a set of users in an organization. When you do so, only the members of the group are authorized to do the tasks for which the group has permissions. You can use the group form to directly add Active Directory users to a group at any time.

About this task

The Group Unique Name attribute is the only required attribute on the group form. The attribute can contain:

- Alphabetic characters
- Unicode characters
- Numbers
- Special characters, such as _ ` ' # - $ % ^ @ ( ) ! ~. { }

You cannot include control characters or any other special characters except those characters mentioned in the previous list. The Group Unique Name attribute is mapped to the sAMAccountName attribute on the Active Directory.

To add groups to the Active Directory:

Procedure

1. Log on to IBM Security Identity Manager as an administrator.
2. In the My Work pane, click **Manage Groups** to display the Manage Groups page.
3. Select the **Active Directory Profile** option from the **Service type** list and click **Search**.
4. Select the name of the service that you created for the Active Directory Adapter and click **OK**.
5. Click **Create** to display the group form.
6. Specify a name for the group in the **Group Unique Name** field.
7. Click **Finish** to add the group to the Active Directory.

Support data attribute specification on the group form

You can specify support data attributes on the group form when you want to assign a group.

You can assign groups to:

- A container
- Another group on the Active Directory

Note: Perform the reconciliation operation before you specify the support data attributes on the group form. The operation provides an updated list of containers and groups that are available on the Active Directory. For information about reconciling user accounts and support data attributes, see "User account reconciliation" on page 5.

The following attributes are the support data attributes on the group form:

Container attribute

Specify this attribute to associate the group with a container that is selected from the list on the group form of the Active Directory profile. Specifying the container decides the location of the group in an organization hierarchy. For more information about the Container attribute, see "Container attribute modification on the group form" on page 41.

When you do not specify the container attribute on the group form, the group is created on Active Directory under the Groups Base Point DN. The value of the Groups Base Point DN is specified on the service form. If no Groups Base Point DN is specified on the service form, the group is created under CN=USERS container on the Active Directory.

Member of attribute

Specify this attribute to add a group to another group that is selected from the list on the group from of the Active Directory profile. When you do so, one group becomes a member of another group. You can select multiple groups to specify the Member of attribute.

The Active Directory restricts the groups that can or cannot be a member of a specified group. The following table lists the group types, scope, and the groups that can or cannot be a member of the specified group.

Table 21. Group membership details

Group type	Group scope	Type and scope of the group that this group can be a member of	Type and scope of the group that this group cannot be member of
Distribution	Universal	• Security Group - Domain Local • Security Group - Universal • Distribution Group - Domain Local • Distribution Group - Universal	• Security Group – Global • Distribution Group – Global
Distribution	Global	All group types can be members of this group type.	

Table 21. Group membership details (continued)

Group type	Group scope	Type and scope of the group that this group can be a member of	Type and scope of the group that this group cannot be member of
Distribution	Domain Local	• Security Group - Domain Local • Distribution Group - Domain Local	- • Security Group - Global • Security Group - Universal • Distribution Group - Global • Distribution Group - Universal
Security	Universal	• Security Group - Domain Local • Security Group - Universal • Distribution Group - Domain Local • Distribution Group - Universal	• Security Group – Global • Distribution Group – Global
Security	Global	All group types are allowed as members of this group.	
Security	Domain Local	• Security Group - Domain Local • Distribution Group - Domain Local	- • Security Group - Global • Security Group - Universal • Distribution Group - Global • Distribution Group - Universal

Note: When you add a group member to a group that does not accept a group member of a specified type and scope, the Active Active Directory Adapter fails the request. The adapter generates the message `0x80072035 - The server is unwilling to process the request`.

Accessibility attribute specification on the group form

You can specify accessibility attributes on the group form to grant defined access to users. When you do so, you can limit the access to a group, which is based on the access type.

Select the Define an access check box on the IBM Security Identity Manager group form to activate access fields. Clearing this check box deactivates the access fields. The information contained in the fields is cleared only when the operation is completed or canceled.

Table 22. Accessibility attributes

Attribute	Description
Access status	Specify this attribute to set the access status for the user. You can select one of the following statuses: • Enable Access • Enable Common Access • Disable Access
Access name	Specify a name for the access that you want to grant the user.

Table 22. Accessibility attributes (continued)

Attribute	Description
Access type	Select the type of access from the drop-down list that you want to grant the user. You can select one of the following types: **Application** Select this option when you want to grant an application-based access to the user. **E-mail group** Select this option when you want to restrict the network resource access to an email group of users on the operating system. **Role** Select this option when you want to grant role-based access to the user. **Shared folder** Select this option when you want to grant folder-based access to the user.
Access description	Provide a short description for the access that you are defining.
Access owner	Select the name of the access owner from the list.
Approval workflow	Specify whether no approval or specific approval is required to grant access.
Notify users when access is provisioned and available for use	Select this check box when you want to send an auto-notification email to users who are granted the defined access. Users who are granted the access are authorized to perform the tasks that are defined for that access.
Notify users when access is de-provisioned	Select this check box when you want to send an auto-notification email to users about the de-provisioning of the access.

Modifying group attributes

You can modify attributes of a group at any time on IBM Security Identity Manager.

About this task

Modify only those groups that are under the group base point. You can perform the modify attributes of the group operation from IBM Security Identity Manager .

To modify the attributes of a group on the Active Directory:

Procedure

1. Log on to IBM Security Identity Manager as an administrator.
2. In the My Work pane, click **Manage Groups** to display the Manage Groups page.
3. Select the **Active Directory Profile** option from the **Service type** list and click **Search**.
4. Select the name of the service that you created for the Active Directory Adapter and click **OK**.
5. On the Select Group page, click **Refresh** to display all the groups created for that service.

6. From the Groups table, select the group whose attributes you want to modify and click **Change**.

   Note: The Group Unique Name attribute is the only non-modifiable attribute on the group form. You can modify all the other attributes of a group.
7. After you modify the group attributes, click **OK**.

Container attribute modification on the group form

Modifying the Container attribute means moving a group from one container to another in an organization.

You can move a group between:

- Containers that are stored at the specified base point
- All containers, if no base point is specified.

Note: If no group base point is specified when creating an Active Directory service, the Active Directory Adapter creates groups in the Users container of the Active Directory.

When you modify the Container attribute, the distinguished name of a group changes because the user moves to a different position in the Active Directory hierarchy. The following example illustrates changes in the distinguished name of a user, when you modify the Container attribute.

For example, a group with the name Administrator Group exists on the Active Directory. The Active Directory has the following structure.

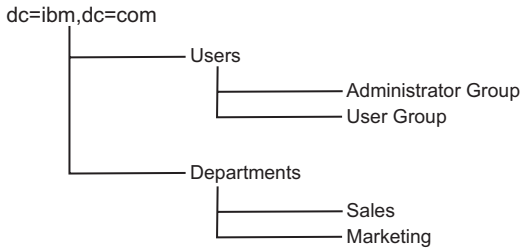

Figure 4. Example of an Active Directory container structure

The distinguished name of Administrator Group is:

```
cn=Administrator Group,cn=Users,dc=ibm,dc=com
```

Modify the Container attribute on the group form from ou=Users to ou=Marketing. After this change, the distinguished name of Administrator Group changes to the following value:

```
cn=Administrator Group,ou=Marketing,ou=Departments,dc=ibm,dc=com
```

Scope modification for the group

The Active Directory checks the group members of a group before it changes the scope of the group.

Depending on the type of group members of the group, the Active Directory provides or denies the scope of the group.

Note:

- You cannot change the scope of the group to Universal if both of these conditions exist:
  - The scope of a group is Local.
  - The group has other Local groups as members.
- You cannot change the scope of the group from Local to Global or Local to Global.
- When the scope of the group is Universal and has other Universal groups as members, you cannot change the scope of the group to Global. However, you can change the scope of the group from Universal to Local.
- When you attempt to perform listed cases, the Active Directory Adapter generates the following

  ```
  message:0x80072035 - The server is unwilling to process the request.
  ```

Creating a group

You can use IBM Security Identity Manager to create a group.

About this task

You can use the Create Group wizard to create additional groups.

To create a group, complete these steps:

Procedure

1. Log on to IBM Security Identity Manager as an administrator.
2. In the My Work pane, click **Manage Groups** to display the Manage Groups page.
3. Select the **Active Directory Profile** option from the **Service type** list and click **Search**.
4. Select the name of the service that you created for the Active Directory Adapter and click **OK**.
5. On the Select Group page, click **Create**. The Create Group wizard is displayed.
6. In the Create Group wizard, complete these steps:
   a. On the Select Type page, click the radio button next to the type of group that you want to create, and then click **Next**. This page is displayed only if the service supports more than one type of group.
   b. On the General Information page, complete the required fields. Then click **Next** to display the Access Information page, or click **Finish** to complete the operation without adding access information or any members to the group.
   c. Optional: On the Access Information page, select the **Define an Access** check box to activate the access definition fields. Click the radio button for the type of access you want to enable. Specify the required access information and any other optional information such as access type, description, access owner, approval workflow, or notification options. Click **Next** to display the Group Membership page, or click **Finish** to complete the operation without adding any members to the group.
   d. Optional: On the Group Membership page, add members to the group, and then click **Next** to display the Schedule Add Member Operation page.
   e. On the Schedule Add Member Operation page, specify when to add the members to the group, and then click **Finish**. This page is displayed only if you chose to add members to the group on the Group Membership page.

Adding users to groups

You can use IBM Security Identity Manager to add users to a group.

About this task

Note:

- You cannot add orphan user accounts as members to a group.
- You cannot add member user accounts from another service.
- When you add user accounts as members, IBM Security Identity Manager submits the user modify request for the selected user account.

Procedure

1. Log on to IBM Security Identity Manager as an administrator.
2. In the My Work pane, click **Manage Groups** to display the Manage Groups page.
3. Select the **Active Directory Profile** option from the **Service type** list and click **Search**.
4. Select the name of the service that you created for the Active Directory Adapter and click **OK**.
5. On the Select Group page, click **Refresh** to display all the groups created for that service.
6. From the groups listed on the Select Group page, click the right-arrow key and select **Add members**.
7. On the Add Members page, click **Search** to display all the user accounts created for that service.
8. Select check box for the user accounts that you want to add to the group and click **OK**. You can select more than one user account check box.

Viewing information about members of a group

You can use IBM Security Identity Manager to view information about the members of a group.

About this task

All the fields on the information pages are read-only.

Procedure

1. Log on to IBM Security Identity Manager as an administrator.
2. In the My Work pane, click **Manage Groups** to display the Manage Groups page.
3. Select the **Active Directory Profile** option from the **Service type** list and click **Search**.
4. Select the name of the service that you created for the Active Directory Adapter and click **OK**.
5. On the Select Group page, click **Refresh** to display all the groups created for that service.
6. From the groups listed on the Select Group page, click the right-arrow key and select **Manage members**.
7. On the Manage Group Members page, click **Refresh** to display all the members of that group.

8. Click the User ID link of the member to view the user information.
9. When you are finished, click **Close**.

Removing users from a group

You can use IBM Security Identity Manager to remove users from a group.

About this task

Note:

- You cannot remove membership of orphan accounts.
- You cannot add member user accounts from another service.
- When you remove membership of user accounts from a group, IBM Security Identity Manager submits the user modify request for the selected user account.

Procedure

1. Log on to IBM Security Identity Manager as an administrator.
2. In the My Work pane, click **Manage Groups** to display the Manage Groups page.
3. Select the **Active Directory Profile** option from the **Service type** list and click **Search**.
4. Select the name of the service that you created for the Active Directory Adapter and click **OK**.
5. On the Select Group page, click **Refresh** to display all the groups created for that service.
6. From the groups listed on the Select Group page, click the right-arrow key and select **Manage members**.
7. On the Manage Group Members page, click **Refresh** to display all the members of that group.
8. Select check box for the user accounts that you want to remove from the group and click **Remove**. You can select more than one user account check box.

Deleting groups from Active Directory

Use the delete feature of IBM Security Identity Manager to delete groups at any time from the Active Directory. You can delete only those groups that are under the group base point.

About this task

When you delete a group from Tivoli Identity Manager, the adapter removes the group from the Active Directory and you can no longer manage the group. You can also use the group form to directly remove users from a group at any time. When you do so, users are removed from the group on Active Directory.

To delete groups from the Active Directory:

Procedure

1. Log on to IBM Security Identity Manager as an administrator.
2. In the My Work pane, click **Manage Groups** to display the Manage Groups page.
3. Select the **Active Directory Profile** option from the **Service type** list and click **Search**.

4. Select the name of the service that you created for the Active Directory Adapter and click **OK**.
5. On the Select Group page, click **Refresh** to display all the groups created for that service.
6. From the groups listed on the Select Group page, select one or more groups that you want to delete and click **Delete** to display the confirmation page.
7. On the Confirm page, again click **Delete**.

Results

When you delete a group from IBM Security Identity Manager, the adapter clears the group membership from other groups

Chapter 5. Troubleshooting the Active Directory Adapter errors

Troubleshooting can help you determine why a product does not function properly. Use this information and techniques to identify and resolve problems with the Active Directory Adapter.

This section also describes the format in which the adapter logs are stored in the log file.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem.

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

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

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

What are the symptoms of the problem?

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

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

Where does the problem occur?

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

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

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

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

When does the problem occur?

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

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

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

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to happen for the problem to occur?
- Do any other applications fail at the same time?

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

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of

tools or procedures at your disposal to help you investigate. Consequently, problems that you can reproduce are often easier to debug and solve.

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

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

For information about obtaining support, see Appendix F, "Support information," on page 79.

Active Directory Adapter errors

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

Whenever an operation fails, the corresponding error messages are logged in the WinADAgent.log file that you can find in the `Agents` installation directory. The log file contains error messages with corresponding error codes. For information about error codes and their description, see the Microsoft Windows Server documentation and search for "ADSI Error Codes."

Table 23. Troubleshooting the Active Directory Adapter errors

Error message	Corrective action
Unable to bind to base point	Ensure that: • The Users Base Point is correctly specified on the adapter service form. • The target servers are up and reachable when they are specified in the base point. • The user ID is correctly specified on the adapter service form. • The password is correctly specified on the adapter service form. • The Active Directory is reachable from the workstation where the adapter is installed.
Unable to bind to group base point.	Ensure that: • The Groups Base Point is correctly specified on the adapter service form. • The user ID is correctly specified on the adapter service form. • The password is correctly specified on the adapter service form. • The target servers are up and reachable when they are specified in the base point. • The Active Directory is reachable from the workstation where the adapter is installed.

Table 23. Troubleshooting the Active Directory Adapter errors (continued)

Error message	Corrective action
Unable to determine default domain	This error occurs when the Active Directory Adapter fails to: • Bind to root DSE • Get the default naming context Ensure that: • The Users Base Point is correctly specified on the adapter service form. • The user ID is correctly specified on the adapter service form. • The password is correctly specified on the adapter service form. • The Active Directory is reachable from the workstation where the adapter is installed.
Error binding to DN: *DN String*	This error occurs when the Active Directory Adapter fails to bind to a user object of the Active Directory for processing. Ensure that the user being processed in the Active Directory is not deleted by any other process simultaneously.
Extended attribute *attribute name* has unsupported syntax	The Active Directory Adapter does not support the data type used for the extended attribute. Use one of the following data types: • Boolean • Integer • Case-sensitive string • Case-insensitive string • Numerical string • Unicode string • Distinguished name • UTC coded time • Octet string For more information about customizing the adapter to use the extended attributes, see the *Active Directory Adapter Installation and Configuration Guide* and search for the section "Customizing the Active Directory Adapter".
Extended attribute *attribute name* not found in Active Directory schema	The extended attribute specified in the exschema.txt file does not exist on the Active Directory Either remove the attribute name from the exschema.txt file or add the attribute to the Active Directory.

Table 23. Troubleshooting the Active Directory Adapter errors (continued)

Error message	Corrective action
Error binding to schema container error code. Loading of extended schema attribute *attribute name* failed.	These errors occur when the Active Directory Adapter fails to extract the schema of the extended attributes. • Ensure that the Active Directory is reachable from the workstation where the adapter is installed. • Verify that the extended attribute is correctly defined and added to the user class.
Error getting parent of schema error code. Loading of extended schema attribute *attribute name* failed.	
Error binding to DN of schema error code. Loading of extended schema attribute *attribute name* failed.	
Unable to connect to default domain. Loading of extended schema attribute *attribute name* failed.	
Extended schema file not found. No extensions loaded.	This information message occurs when the Active Directory Adapter fails to find the extended schema file (exschema.txt) or fails to open the file.
Unable to bind to user *user name*	This error occurs when the Active Directory Adapter fails to connect to a user object in the Active Directory for processing. Ensure that the user *user name* exists on the Active Directory.
Error determining RAS server name	Check the value of the registry key ForceRASServerLookup. If the value of the key is `TRUE`, the Active Directory Adapter determines the RAS server regardless of whether you specify the server name on the adapter service form. This error could be because the domain does not exist or the domain controller is not available for the specified domain. Ensure that the Active Directory is reachable from the workstation where the adapter is installed.
Unable to get domain name. Terminal and RAS servers cannot be determined.	This error occurs when the Active Directory Adapter fails to get the domain name from the specified base point or from the default domain. Ensure that a base point is specified with a correct domain name.
Invalid domain name syntax	Use one of the following formats to specify the domain name: • `Server name/ou=org1,dc=ibm,dc=com` • `ou=org1,dc=ibm,dc=com`
User not found	Ensure that the user exists on the Active Directory and is not directly deleted or modified on the Active Directory.
Group not found.	Ensure that the group exists on the Active Directory and is not directly deleted or modified on the Active Directory.
Error setting attributes *country*. Unknown country code.	The country code specified for the user is invalid. Specify a valid country code and submit the request again. For information about valid country codes, see Appendix A, “Country and region codes,” on page 57.
Could not modify the attribute-msExchUserAccountControl	This warning occurs when the user mailbox is not disabled on suspending a user account.

Table 23. Troubleshooting the Active Directory Adapter errors (continued)

Error message	Corrective action
Error removing membership from group *group name*	The Active Directory Adapter failed to remove the membership of a user or group from the group *group name*. Ensure that: • The user or group exists on the Active Directory. • The user or group is a member of the group group name. • The group specified exist on the Active Directory.
Error adding membership to group *group name*	The Active Directory Adapter failed to add membership of the user or group to the group *group name*. Ensure that: • The user or group exists on the Active Directory. • The user or group is not already a member of the group *group name*. • The group specified exists on the Active Directory.
Unable to get info on share *share name*	This error occurs when the Active Directory Adapter fails to retrieve share information from the home directory of the user. Ensure that: • The user account under which the adapter is running has access to the home directory. • The share name exists on the workstation where the home directory is created.
Invalid home directory path *path name*	The Active Directory Adapter supports creation and deletion of only UNC home directories. Specify the UNC home directory path in the following format: `\\servername\sharename\foldername` **Note:** • NTFS security and Shares can be set only on the Home Directories that are UNC paths. • Share Access can be set only on the Home Directories that are UNC paths that have a share created.
Unable to delete home directory *home directory name*	The Active Directory Adapter is not able to delete the specified home directory. If the adapter is unable to delete the UNC home directory, ensure that: • The value of the registry key DeleteUNCHomeDirectories is `TRUE`. • The user account under which the adapter is running has permissions to delete the directory.
Home directory deletion is not enabled. Home directory will not be deleted.	To enable home directory deletion, set the values of DeleteUNCHomeDirectories and ManageHomeDirectories registry keys to `TRUE`. Resend the modify request from IBM Security Identity Manager.
Home directory creation not enabled. Directory will not be created.	To enable home directory creation, set the values of CreateUNCHomeDirectories and ManageHomeDirectories registry keys to `TRUE`. Resend the modify request from IBM Security Identity Manager.

Table 23. Troubleshooting the Active Directory Adapter errors (continued)

Error message	Corrective action
Error creating home directory *home directory name*	The Active Directory Adapter is not able to create home directory. Ensure that: • A directory with the same name does not exist. • The user account under which the adapter is running has permissions to create home directory. • Intermediate directories exist. The adapter creates only the final directory in the specified path.
Unable to set Home Directory Drive. Failed to create Home Directory.	
Unable to set Home Directory NTFS security. Failed to create Home Directory.	
Unable to set Home Directory Share. Failed to create Home Directory.	
Unable to set Home Directory Share Access. Failed to create Home Directory.	
Error deleting share *share name*	The Active Directory Adapter is not able to delete the share when you clear value of the share-related attributes from the Active Directory account form. Ensure that: • The user account has access to the specified share. • The specified share name exists. • The user account under which the adapter is running has permissions to create home directory.
Search failed. Unable to retrieve additional data after 3 retries.	The Active Directory Adapter retrieves data from the Active Directory in a paged manner. The adapter reconciles users, groups, and containers and attempts to retrieve data in a maximum of three attempts. If all three attempts fail, the adapter abandons the search. The adapter cannot retrieve data because of one of the following reasons: • The network response is slow. • The Active Directory server is busy. • The Active Directory Adapter installed on the Active Directory server is overloading the server. For information about configuring the Active Directory, see http://support.microsoft.com/.
User search failed	
Group search failed. Error code: *error code* - error *description*. Provider: *provider name*.	
Container search failed. *error code* - error *description*. Provider: *provider name*.	
Error performing User Lookup	
errorMessage="Unsupported filter"	The adapter does not support the attribute specified in the filter. For the list of supported attributes, see Table 2 on page 10.
Error setting attribute eradprimarygroup. ADSI Result code: 0x80072035 - The server is unwilling to process the request.	Ensure that: • The user is a member of the specified group. • The specified group is either a universal security group or a global security group.

Table 23. Troubleshooting the Active Directory Adapter errors (continued)

Error message	Corrective action
ADSI Result code: 0x80072014 - The requested operation did not satisfy one or more constraints associated with the class of the object. ADSI Result code: 0x8007202f - A constraint violation occurred.	These errors occur when the specified value for the attribute violates any constraint associated with that attribute. For example, a constraint might be: • Minimum or maximum length of characters the attribute can store • Minimum or maximum value the attribute can accept Ensure that the specified value for the attribute does not violate these constraints. **Note:** If any one of the attribute specified in the request violates a constraint, the adapter gives the same error for all the subsequent attributes. The error is given even though the subsequent attributes do not violate any constraints. For example, the Title attribute on the Active Directory can store a description of maximum of 64 characters. If you specify description of length more than 64 characters, the adapter gives these errors: • For the Title attribute • For all the other attributes specified in the request.
Unable to load XML transformation buffer from *adapter installation directory*\data\xforms.xml.	The Active Directory Adapter does not use the xforms.xml file. Therefore, you can safely ignore the xforms-related errors that are recorded in the WinADAgent.log file.
Request for proxy email types should contain at least one primary SMTP address	Verify that the request for proxy email types contains a primary SMTP address.
Unable to bind to group E-mail Addresses.	This error occurs when the Active Directory Adapter fails to connect to a group object in the Active Directory for processing. Ensure that the group E-mail Addresses exists on the Active Directory.
Error while fetching the group interface for group DN.	This error occurs when the Active Directory Adapter fails to bind to a group object on the Active Directory for processing. Ensure that the group that is being processed in the Active Directory is not deleted by any other process simultaneously.
Unable to bind to the container object in move operation.	This error occurs when the Active Directory Adapter binds to the requested container when a user or group object is moved in the Active Directory hierarchy. Ensure that the container exists on the Active Directory.
Cannot set Fixed Callback without Callback number. Callback number not found in the request.	When you select Callback Settings as Fixed Callback, you must specify the Callback Number.
Error setting the RAS attribute RAS attribute name. Error reading RAS info.	Ensure that: • The user account under which the adapter is running has administrator rights to the Active Directory. • The RAS service is running on the Domain Controller.
Not a valid IPv4 address.	The IP address specified for the Static IPv4 Address is in an incorrect format. Specify the IP address in the IPv4 format.

Table 23. Troubleshooting the Active Directory Adapter errors (continued)

Error message	Corrective action
0x80072035 - The server is unwilling to process the request.	This error occurs from the Active Directory when an attempt is made to perform an operation that is not supported on the Active Directory. Ensure that: • You provided the correct value for the attributes in the request. For example, clear the value of the Country or region attribute. • The requested operation is supported for the attribute, user account, or group on the Active Directory.
Home Directory will not be created. Home directory management is disabled.	Set the adapter registry keys CreateUNCHomeDirectories and ManageHomeDirectories to `TRUE`: • To create a home directory. • To create home directory share. • To set share access. • To set home directory NTFS access for a user account. For more information, see "Creating a home directory for a user account" on page 19 and "Home Directory attribute modification" on page 24.
Cannot create share *share name*. Home directory management is disabled.	
Cannot set share access. Home directory management is disabled.	
Cannot set NTFS access. Home directory management is disabled.	
Value specified is not in the proper format.	Ensure that the value format of extended attribute of type DNWithBinary is `B:char count:binary value:object DN`
Value specified for the attribute does not start with character 'B'.	Ensure that value specified for extended attribute of type DNWithBinary is start with the character 'B' only.
Value given after 'B:' is not correct. Expected value is the total number of Hexadecimal Digit count	For extended attribute of type DNWithBinary, verify that value given for the *char count* is the total number of Hexadecimal Digit count. Ensure that it does not contain any alphabetical characters or any special characters.
Hexadecimal value does not contain the number of characters specified in the character count.	For extended attribute of type DNWithBinary, verify that total hexadecimal digit count specified in the *char count* is equal to number of hexadecimal characters.
Wrong Digit in Hex String.	For extended attribute of type DNWithBinary, verify that value given in the *binary value* contains only hexadecimal character. Valid characters are numerals 0 through 9 and letters A through F. The value can be a combination of valid numerals and letters.
Value is not set on resource due to invalid constraint.	This error occurs when the specified value for the extended attribute of type DNWithBinary violates any constraint associated with that attribute. For example, some constraints might be: • The *object DN* in the value must be a distinguished name of existing user object. • The maximum or minimum number of bits in the hexadecimal value. Ensure that the specified value for the attribute does not violate any constraints.
Hexadecimal value should always contain even number of characters.	For extended attribute of type DNWithBinary, verify that value given in the *binary value* contains an even number of hexadecimal characters.

Table 23. Troubleshooting the Active Directory Adapter errors (continued)

Error message	Corrective action
Attribute can be set only if Mailbox is enabled for Unified Messaging. To enable Unified Messaging both values UMMailbox Policy and UM Addresses(Extensions) are required.	Ensure that valid values of both UMMailbox Policy and UM Addresses(Extensions) are specified in the request to enable the user for Unified Messaging.
Attribute Operation Type is not supported.	Ensure that the value specified for UM Addresses (Extensions) is not of operation type, MODIFY.
Attribute cannot be set. Mailbox is Disabled for Unified Messaging.	Ensure that the request does not contain Unified Messaging attributes with operation ADD or MODIFY when the MailBox of the user is disabled for Unified Messaging.
Attribute cannot be set. Error occurred while trying to Disable MailBox for Unified Messaging.	This error occurs if disable Unified Messaging is failed and if request contains UM Addresses (Extensions) attribute with operation types ADD or MODIFY.
Attribute cannot be delete. Error occurred while trying to Disable MailBox for Unified Messaging.	This error occurs if disable Unified Messaging is failed and if the request contains UM Addresses (Extensions) attribute with operation type DELETE.

Log information format

The Active Directory Adapter logs are stored in specific formats in the `WinADAgent.log` file.

Each log entry contains a logging level, a timestamp, an optional thread ID, and the message text. The Active Directory Adapter records the following three logging levels:

- Base (BSE)
- Detail (DTL)
- Debug (DBG)

Log format

The following example shows the format of a log entry:

```
BSE:08/03/24 16:41:08 Thread:001132 Received PayLoad Message
```

where,

- BSE is the base logging level
- 08/03/24 16:41:08 is the date and time when the log entry is created
- Thread:001132 is the thread ID that uniquely identifies the thread
- Received PayLoad Message is the message text

Similarly, the following examples show log entries that record the detail and the debug logging levels:

```
DTL:08/03/24 16:41:08 Thread:001132 New callback thread. Operation is Modify.
Thread count: 1
```

```
DBG:08/03/24 16:41:08 Thread:001132 The RUS service is found running on the
resource & it has been correctly indicated by the registry key also.
So, agent is not managing RUS related attributes.
```

Appendix A. Country and region codes

The Active Directory Adapter uses a code to modify the countryCode attribute on the Active Directory.

Countries and regions and their corresponding codes are listed in the following table.

Table 24. Countries and regions and their corresponding codes

Country or region	Code
Aaland Islands	248
Afghanistan	004
Albania	008
Algeria	012
American Samoa	016
Andorra	020
Angola	024
Anguilla	660
Antarctica	010
Antigua	028
Argentina	032
Armenia	051
Aruba	533
Australia	036
Austria	040
Azerbaijan	031
Bahamas	044
Bahrain	048
Bangladesh	050
Barbados	052
Belarus	112
Belgium	056
Belize	084
Benin	204
Bermuda	060
Bhutan	064
Bolivia	068
Bosnia	070
Botswana	072
Bouvet	074
Brazil	076
British Indian Ocean Territory	086

Table 24. Countries and regions and their corresponding codes (continued)

Country or region	Code
Brunei	096
Bulgaria	100
Burkina Faso	854
Burundi	108
Cambodia	116
Cameroon	120
Canada	124
Cape Verde	132
Cayman Islands	136
Central African Republic	140
Chad	148
Chile	152
China	156
Christmas Island	162
Cocos (Keeling) Islands	166
Colombia	170
Comoros	174
Congo	178
Congo Democratic Republic Of	180
Cook Islands	184
Costa Rica	188
Côte d'Ivoire	384
Croatia	191
Cuba	192
Cyprus	196
Czech Republic	203
Denmark	208
Djibouti	262
Dominica	212
Dominican Republic	214
East Timor	626
Ecuador	218
Egypt	818
El Salvador	222
Equatorial Guinea	226
Eritrea	232
Estonia	233
Ethiopia	231
Falkland Islands	238
Faroe Islands	234

Table 24. Countries and regions and their corresponding codes (continued)

Country or region	Code
Fiji	242
Finland	246
France	250
France Metropolitan	249
French Guiana	254
French Polynesia	258
French Southern Lands	260
Gabon	266
Gambia	270
Georgia	268
Germany	276
Ghana	288
Gibraltar	292
Great Britain	826
Greece	300
Greenland	304
Grenada	308
Guadeloupe	312
Guam	316
Guatemala	320
Guinea	324
Guinea-Bissau	624
Guyana	328
Haiti	332
Heard and McDonald Islands	334
Holysee	336
Honduras	340
Hong Kong S.A.R. of the P.R.C.	344
Hungary	348
Iceland	352
India	356
Indonesia	360
Iran	364
Iraq	368
Ireland	372
Israel	376
Italy	380
Jamaica	388
Japan	392
Jordan	400

Table 24. Countries and regions and their corresponding codes (continued)

Country or region	Code
Kazakhstan	398
Kenya	404
Kiribati	296
Kuwait	414
Kyrgyzstan	417
Lao People's Democratic Republic	418
Latvia	428
Lebanon	422
Lesotho	426
Liberia	430
Libyan Arab Jamahiriya	434
Liechtenstein	438
Lithuania	440
Luxembourg	442
Macao S.A.R. of the P.R.C.	446
Macedonia	807
Madagascar	450
Malawi	454
Malaysia	458
Maldives	462
Mali	466
Malta	470
Marshall Islands	584
Martinique	474
Mauritania	478
Mauritius	480
Mayotte	175
Mexico	484
Micronesia	583
Moldova	498
Monaco	492
Mongolia	496
Montserrat	500
Morocco	504
Mozambique	508
Myanmar	104
Namibia	516
Nauru	520
Nepal	524
Netherlands	528

Table 24. Countries and regions and their corresponding codes (continued)

Country or region	Code
Netherlands Antilles	530
New Caledonia	540
New Zealand	554
Nicaragua	558
Niger	562
Nigeria	566
Niue	570
Norfolk Island	574
Northern Mariana Islands	580
North Korea	408
Norway	578
No Value	0
Oman	512
Pakistan	586
Palau	585
Palestinian Territory	275
Panama	591
Papua New Guinea	598
Paraguay	600
Peru	604
Philippines	608
Pitcairn	612
Poland	616
Portugal	620
Puerto Rico	630
Qatar	634
Reunion	638
Romania	642
Russian Federation	643
Rwanda	646
Saint Kitts and Nevis	659
Saint Lucia	662
Saint Vincent and the Grenadines	670
Samoa	882
San Marino	674
Sao Tome and Principe	678
Saudi Arabia	682
Senegal	686
Serbia	688
Seychelles	690

Table 24. Countries and regions and their corresponding codes (continued)

Country or region	Code
Sierra Leone	694
Singapore	702
Slovakia	703
Slovenia	705
Solomon Islands	090
Somalia	706
South Africa	710
South Georgia	239
South Korea	410
Spain	724
Sri Lanka	144
St. Helena	654
St. Pierre and Miquelon	666
Sudan	736
Suriname	740
Svalbard	744
Swaziland	748
Sweden	752
Switzerland	756
Syrian Arab Republic	760
Taiwan	158
Tajikistan	762
Tanzania	834
Thailand	764
Togo	768
Tokelau	772
Tonga	776
Trinidad and Tobago	780
Tunisia	788
Turkey	792
Turkmenistan	795
Turks and Caicos Islands	796
Tuvalu	798
Uganda	800
Ukraine	804
United Arab Emirates	784
United States	840
United States Minor Outlying Islands	581
Uruguay	858
Uzbekistan	860

Table 24. Countries and regions and their corresponding codes (continued)

Country or region	**Code**
Vanuatu	548
Venezuela	862
Vietnam	704
Virgin Islands, British	092
Virgin Islands, U.S.	850
Wallis and Futuna Islands	876
Western Sahara	732
Yemen	887
Yugoslavia	891
Zambia	894
Zimbabwe	716

Appendix B. Active Directory Adapter attributes

IBM Security Identity Manager communicates with the Active Directory with attributes included in transmission packets that are sent over a network.

The combination of attributes included in the packets depends on the type of action the Active Directory requests from the Active Directory Adapter.

Active Directory account form attributes

The following table lists the mapping of the user account form attributes on IBM Security Identity Manager to the attributes on the Active Directory.

Table 25. Mapping of attributes on IBM Security Identity Manager to the attributes on the Active Directory

Attribute on IBM Security Identity Manager	**Attribute on the Active Directory**
• cn • erADFullName **Note:** At a particular time only one of the listed attributes is used. For more information, see "cn attribute reconciliation" on page 9 and "CN attribute specification" on page 15.	cn
description	description
erADAllowEncryptedPassword	userAccountControl
erADBadLoginCount	badPwdCount
erADCallbackNumber	msRADIUSCallbackNumber
erADCannotBeDelegated	userAccountControl
erADContainer	User is located in the specified container.
erADCountryCode	countryCode
erADDialinCallback	msRADIUSServiceType
erADDisplayName	displayName
erADDistinguishedName	distinguishedName
erADEAlias	mailNickname
erADEAllowPermTo1Level	msExchMailboxSecurityDescriptor
erADEApplyOntoAllow	msExchMailboxSecurityDescriptor
erADEApplyOntoDeny	msExchMailboxSecurityDescriptor
erADEAssociatedExtAcc	msExchMailboxSecurityDescriptor
erADEAutoGenEmailAddrs	msExchPoliciesExcluded
erADEChgPermissions	msExchMailboxSecurityDescriptor
erADEDaysBeforeGarbage	garbageCollPeriod
erADEDelegates	publicDelegates
erADEDelMailboxStorage	msExchMailboxSecurityDescriptor
erADEDenyPermTo1Level	msExchMailboxSecurityDescriptor

Table 25. Mapping of attributes on IBM Security Identity Manager to the attributes on the Active Directory (continued)

Attribute on IBM Security Identity Manager	Attribute on the Active Directory
erADEEnableStoreDeflts	mDBUseDefaults
erADEExtension1	extensionAttribute1
erADEExtension10	extensionAttribute10
erADEExtension11	extensionAttribute11
erADEExtension12	extensionAttribute12
erADEExtension13	extensionAttribute13
erADEExtension14	extensionAttribute14
erADEExtension15	extensionAttribute15
erADEExtension2	extensionAttribute2
erADEExtension3	extensionAttribute3
erADEExtension4	extensionAttribute4
erADEExtension5	extensionAttribute5
erADEExtension6	extensionAttribute6
erADEExtension7	extensionAttribute7
erADEExtension8	extensionAttribute8
erADEExtension9	extensionAttribute9
erADEForwardingStyle	deliverAndRedirect
erADEForwardTo	altRecipient
erADEFullMailboxAccess	msExchMailboxSecurityDescriptor
erADEGarbageAfterBckp	deletedItemFlags
erADEHardLimit	mDBOverHardQuotaLimit
erADEHideFromAddrsBk	msExchHideFromAddressLists
erADEHomeMDB	homeMDB
erADEIncomingLimit	delivContLength
erADELanguages	language
erADEMailboxStore	homeMDB
erADEmployeeID	employeeID
erADEOutgoingLimit	submissionContLength
erADEOverQuotaLimit	mDBOverQuotaLimit
erADEOverrideGarbage	deletedItemFlags
erADEProxyAddresses	proxyAddresses
erADEReadPermissions	msExchMailboxSecurityDescriptor
erADERecipientLimit	msExchRecipLimit
erADERstrctAdrsFg	*Null*
erADERstrctAdrsLs	authOrig/unauthOrig
erADEServerName	*Null*
erADEShowInAddrBook	showInAddressBook
erADESMTPEmail	mail

Table 25. Mapping of attributes on IBM Security Identity Manager to the attributes on the Active Directory (continued)

Attribute on IBM Security Identity Manager	**Attribute on the Active Directory**
erADEStoreQuota	mDBStorageQuota
erADETakeOwnership	msExchMailboxSecurityDescriptor
erADETargetAddress	targetAddress
erADEX400Email	textEncodedORAddress
erADExpirationDate	accountExpires
erADfax	facsimileTelephoneNumber
erADHomeDir	homeDirectory
erADHomeDirAccessShare	*Null*
erADHomeDirDrive	homeDrive
erADHomeDirNtfsAccess	*Null*
erADHomeDirShare	*Null*
erADHomePage	wWWHomePage
erADInitial	initials
erADIsAccountLocked	lockoutTime
erADLastFailedLogin	badPasswordTime
erADLastLogoff	lastLogoff
erADLastLogon	lastLogon
erADLoginScript	scriptPath
erADLoginWorkstations	userWorkstations
erADManager	manager
erADNamePrefix	personalTitle
erADNameSuffix	generationQualifier
erADNoChangePassword	*Null*
erADOfficeLocations	physicalDeliveryOfficeName
erADOtherName	middleName
erADPasswordForceChange	pwdLastSet
erADPasswordLastChange	pwdLastSet
erADPasswordMinimumLength	*Null*
erADPasswordNeverExpires	userAccountControl
erADPasswordRequired	userAccountControl
erADPrimaryGroup	primaryGroupID
erADRequireUniquePassword	*Null*
erADSmartCardRequired	userAccountControl
erADTrustedForDelegation	userAccountControl
erADUPN	userPrincipalName
erADWTSAllowLogon	userParameters
erADWTSBrokenTimeout	userParameters
erADWTSCallbackNumber	userParameters

Table 25. Mapping of attributes on IBM Security Identity Manager to the attributes on the Active Directory (continued)

Attribute on IBM Security Identity Manager	Attribute on the Active Directory
erADWTSCallbackSettings	userParameters
erADWTSClientDefaultPrinter	userParameters
erADWTSClientDrives	userParameters
erADWTSClientPrinters	userParameters
erADWTSHomeDir	userParameters
erADWTSHomeDirAccessShare	userParameters
erADWTSHomeDirDrive	userParameters
erADWTSHomeDirNtfsAccess	userParameters
erADWTSHomeDirShare	userParameters
erADWTSInheritInitialProg	userParameters
erADWTSInitialProgram	userParameters
erADWTSProfilePath	userParameters
erADWTSReconnectSettings	userParameters
erADWTSRemoteHomeDir	userParameters
erADWTSShadowSettings	userParameters
erADWTSTimeoutConnections	userParameters
erADWTSTimeoutDisconnections	userParameters
erADWTSTimeoutIdle	userParameters
erADWTSWorkingDir	userParameters
erCompany	company
erDepartment	department
erDivision	division
erGroup	memberOf
erLogonTimes	logonHours
erMaxStorage	maxStorage
erPassword	*Null*
erProfile	profilePath
eruid	sAMAccountName
givenName	givenName
homePhone	homePhone
l	l
mail	mail
mobile	mobile
pager	pager
postalCode	postalCode
postOfficeBox	postOfficeBox
sn	sn
st	st

Table 25. Mapping of attributes on IBM Security Identity Manager to the attributes on the Active Directory (continued)

Attribute on IBM Security Identity Manager	Attribute on the Active Directory
street	streetAddress
telephoneNumber	telephoneNumber
title	title
erADEAllowedAddressList	authOrig
erADEOutlookWebAccessEnabled	protocolSettings
erADEActiveSyncEnabled	msExchOmaAdminWirelessEnable
erADEMAPIEnabled	protocolSettings
erADEEnableRetentionHold	msExchELCMailboxFlags
erADEStartRetentionHold	msExchELCExpirySuspensionStart
erADEEndRetentionHold	msExchELCExpirySuspensionEnd

Active Directory group form attributes

You can manage Active Directory groups from IBM Security Identity Manager.

The following table maps the attributes on the Active Directory group form on IBM Security Identity Manager, corresponding names on IBM Security Identity Manager server, and their names on the Active Directory.

Table 26. Group form attributes

Attribute name on the Active Directory group form on IBM Security Identity Manager	Attribute name on the IBM Security Identity Manager server	Attribute name on the Active Directory
Group unique name	erADGroupSamAccountName	samAccountName
Common Name	erADGroupCN	cn
Container	erADContainer	Group is located in the specified container
Group Type	erADGroupType	groupType
Group Scope	erADGroupScope	groupType
Member of	erADGroupIsMemberOf	memberOf
Description	erADGroupDescription	description
Managed by	erADGrpManagedBy	managedBy

Customizable attributes on the Active Directory group form

You can customize the attributes on the Active Directory group form to meet the requirements of your organization.

The following table maps:

- The customizable attributes on the Active Directory group form on IBM Security Identity Manager
- The corresponding names on IBM Security Identity Manager server
- The corresponding names on the Active Directory.

Table 27. Customizable group form attributes

Customizable attribute name on the Active Directory group form on IBM Security Identity Manager	Attribute name on the IBM Security Identity Manager server	Attribute name on the Active Directory
Distinguished Name	erADGroupDN	distinguishedName
Group GUID	erADGroupGUID	objectGUID
Group Token	erADPrimaryGrpTkn	primaryGroupToken
Distribution List e-mail	erADGroupDlEmail	mail

Mapping extended attributes

The adapter supports mapping of attribute names for extended attributes.

About this task

A different attribute name can be used on IBM Security Identity Manager than the attribute name on Active Directory.

To use a different attribute name for IBM Security Identity Manager, you must follow the attribute name rules that are defined by the directory server. The attribute name must not have a pipe (|) in it. Ensure that you specify each attribute on a separate line.

Note: The adapter supports Octet String as an extended attribute type. The attribute is passed as a string value and must have an even number of characters. No adapter-specific errors exist for these attributes, but the attributes might return Active Directory error codes.

Procedure

1. Go to the *adapter home*/data directory and edit the exschema.txt file.
2. Specify the attribute name in the following format: *attribute name* on IBM Security Identity Manager|*attribute name* on Active Directory. For example:
   ```
   erADUserInfo|Info
   ```
   Note: To use the Active Directory attribute name on IBM Security Identity Manager, specify either:
   - `Info|Info`
   - Just the Active Directory attribute name. For example,
     ```
     Info
     ```
3. Save the file.

Appendix C. APIs used by the adapter

This section lists the APIs that are used by the Active Directory Adapter.

ADSI interfaces and the corresponding APIs used by the adapter

The following table lists the ADSI interfaces and the corresponding APIs used by the adapter.

For more information about an API, go to http://msdn2.microsoft.com and search for the API together with its corresponding ADSI interface.

For example, to search information about get_AccountDisabled, see http://msdn2.microsoft.com and in the **Search** field, type `get_AccountDisabled and IADsUser`

Table 28. ADSI Interfaces and the corresponding APIs used by the Active Directory Adapter

ADSI interfaces	**APIs**
IADs	Get
IDirectorySearch	ExecuteSearch
IDirectorySearch	GetFirstRow
IDirectorySearch	GetColumn
IDirectorySearch	FreeColumn
IDirectorySearch	GetNextRow
IDirectorySearch	CloseSearchHandle
IDirectorySearch	SetSearchPreference
IADsUser	GetEx
IADsUser	PutEx
IADsUser	get_AccountDisabled put_AccountDisabled
IADsUser	get_LoginHours put_LoginHours
IADsUser	get_LoginWorkstations put_LoginWorkstations
IADsUser	get_PasswordRequired put_PasswordRequired
IADsUser	get_ADsPath
IADsUser	get_BadLoginCount
IADsUser	get_PasswordMinimumLength
IADsUser	get_RequireUniquePassword
IADsUser	SetPassword
IADsUser	SetInfo
IADsUser	put_IsAccountLocked

Table 28. ADSI Interfaces and the corresponding APIs used by the Active Directory Adapter (continued)

ADSI interfaces	APIs
IADsUser	put_MaxStorage
IADsUser	Groups
IADsUser	put_AccountExpirationDate
IADsUser	get_Parent
IADsGroup	get_GUID
IADsGroup	Remove
IADsGroup	Add
IDirectoryObject	CreateDSObject
IDirectoryObject	DeleteDSObject
IADsProperty	get_Syntax
IADsProperty	get_MaxRange
IADsProperty	get_MinRange
IADsProperty	get_MultiValued
IADsContainer	GetObject
IADsContainer	MoveHere
IADsTSUserEx	get_TerminalServicesProfilePath put_TerminalServicesProfilePath
IADsTSUserEx	get_TerminalServicesHomeDirectory put_TerminalServicesHomeDirectory
IADsTSUserEx	get_TerminalServicesHomeDrive put_TerminalServicesHomeDrive
IADsTSUserEx	get_AllowLogon put_AllowLogon
IADsTSUserEx	get_MaxDisconnectionTime put_MaxDisconnectionTime
IADsTSUserEx	get_MaxConnectionTime put_MaxConnectionTime
IADsTSUserEx	get_MaxIdleTime put_MaxIdleTime
IADsTSUserEx	get_ReconnectionAction put_ReconnectionAction
IADsTSUserEx	get_BrokenConnectionAction put_BrokenConnectionAction
IADsTSUserEx	get_ConnectClientDrivesAtLogon put_ConnectClientDrivesAtLogon
IADsTSUserEx	get_ConnectClientPrintersAtLogon put_ConnectClientPrintersAtLogon

Table 28. ADSI Interfaces and the corresponding APIs used by the Active Directory Adapter (continued)

ADSI interfaces	APIs
IADsTSUserEx	get_DefaultToMainPrinter put_DefaultToMainPrinter
IADsTSUserEx	get_TerminalServicesWorkDirectory put_TerminalServicesWorkDirectory
IADsTSUserEx	get_TerminalServicesInitialProgram put_TerminalServicesInitialProgram
IADsTSUserEx	get_EnableRemoteControl put_EnableRemoteControl
IADsGroup	Get
IADsGroup	Put
IADsGroup	PutEx
IADsGroup	GetInfo
IADsGroup	SetInfo
IADsGroup	get_ADsPath
IADsGroup	Release
IADsGroup	get_Parent

Windows APIs used by the adapter

The following table lists the Windows APIs used by the adapter.

For more information about an API, go to http://msdn2.microsoft.com and search for the API together with its corresponding ADSI interface.

For example, to search information about MprAdminUserGetInfo, see http://msdn2.microsoft.com and in the **Search** field, type `MprAdminUserGetInfo`

Table 29. Windows APIs used by the Active Directory Adapter

- ADsGetObject
- ADsOpenObject
- BuildSecurityDescriptor
- CreateDirectory
- CryptAcquireContext
- CryptCreateHash
- CryptDestroyHash
- CryptGetHashParam
- CryptHashData
- CryptReleaseContext
- EqualSid
- GetAce
- GetAclInformation
- GetFileSecurity
- GetNamedSecurityInfo
- AuthzInitializeResourceManager
- AuthzInitializeContextFromSid
- AuthzAccessCheck
- GetNamedSecurityInfoW
- GetSecurityDescriptorDacl
- InitializeAcl
- IsValidSecurityDescriptor
- MprAdminGetPDCServer
- MprAdminUserGetInfo
- MprAdminUserSetInfo
- NetApiBufferFree
- NetShareAdd
- NetShareDel
- NetShareEnum
- NetShareGetInfo
- NetShareSetInfo
- RegCreateKeyExW
- RegCreateKeyExA
- RegQueryValueExW
- RegQueryValueExA
- RegSetValueExW
- SetFileSecurity
- WTSQueryUserConfig
- WTSSetUserConfig

Appendix D. PowerShell command-line functions used by the adapter

The Active Directory Adapter uses PowerShell command-line functions (cmdlets) for managing Exchange 2010.

PowerShell is a scripting language that is developed by Microsoft to perform administrative tasks more efficiently with applications running on Windows. The adapter establishes a remote PowerShell session with one of the Exchange 2010 servers. In the remote Exchange 2010 PowerShell session, cmdlets are provided for Exchange-specific management tasks.

All cmdlets in the Exchange 2010 Management Shell are presented in verb-noun pairs. The verb-noun pair is always separated by a hyphen without spaces, and the cmdlet nouns are always singular. Verbs refer to the action that the cmdlet takes. Nouns refer to the object on which the cmdlet acts. For example, in the Enable-Mailbox cmdlet, the verb is Enable and the noun is Mailbox.

The following table gives PowerShell cmdlets that are used by the adapter for managing Exchange 2010, and their description.

Table 30. PowerShell cmdlets used by the Active Directory Adapterand their description

PowerShell cmdlets	Description
Enable-Mailbox	Enables an existing Active Directory user account for mailbox
Enable-MailUser	Enables an existing Active Directory user account for mail
Disable-Mailbox	Deletes an existing mailbox
Disable-MailUser	Deletes an existing mail-enabled user account
Set-Mailbox	Modifies an existing mailbox-enabled user account
Set-MailUser	Modifies an existing mail-enabled user account
Set-CASMailbox	Sets Client-Access-Server-related (CAS-related) mailbox attributes
Move-Mailbox	Moves an existing mailbox to a different mailbox store
Add-MailboxPermission	Adds mailbox permissions
Remove-MailboxPermission	Removes mailbox permissions
Get-Mailbox	Gets the attributes of a mailbox.
Get-MailUser	Gets the mail-related attributes.

Appendix E. Conventions used in this publication

This publication uses several conventions for special terms and actions, operating system-dependent commands and paths, and margin graphics.

Typeface conventions

This publication uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:**, and **Operating system considerations**:)
- Keywords and parameters in text

Italic

- Citations (examples: titles of publications, diskettes, and CDs
- Words defined in text (example: a nonswitched line is called a *point-to-point line*)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data.
- Variables and values you must provide: ... where *myname* represents....

`Monospace`

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Operating system-dependent variables and paths

This guide uses the Windows convention for specifying environment variables and for directory notation.

When using the Unix command line, replace %variable% with $variable for environment variables and replace each backslash (\) with a forward slash (/) in directory paths. The names of environment variables are not always the same in Windows and UNIX. For example, %TEMP% in the Windows operating system is equivalent to $tmp in a UNIX operating system.

Note: If you are using the bash shell on a Windows system, you can use the UNIX conventions.

Appendix F. Support information

You have several options to obtain support for IBM products.

- "Searching knowledge bases"
- "Obtaining a product fix" on page 80
- "Contacting IBM Support" on page 80

Searching knowledge bases

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

About this task

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

Procedure

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

1. Search for content by using the IBM Support Assistant (ISA).

   ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the ISA website.
2. Find the content that you need by using the IBM Support Portal.

   The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.
3. Search for content about IBM Security Identity Manager by using one of the following additional technical resources:
   - IBM Security Identity Manager version 6.0 technotes and APARs (problem reports).
   - IBM Security Identity Manager Support website.
   - IBM Redbooks®.
   - IBM support communities (forums and newsgroups).
4. Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the Search field at the top of any ibm.com® page.
5. Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to

include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

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

Obtaining a product fix

A product fix might be available to resolve your problem.

About this task

You can get fixes by following these steps:

Procedure

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

Contacting IBM Support

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

Before you begin

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

Procedure

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support topic in the *Software Support Handbook*.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA):

     Any data that has been collected can be attached to the service request. Using ISA in this way can expedite the analysis and reduce the time to resolution.

     a. Download and install the ISA tool from the ISA website. See http://www.ibm.com/software/support/isa/.
     b. Open ISA.

c. Click **Collection and Send Data**.
d. Click the **Service Requests** tab.
e. Click **Open a New Service Request**.

- Online through the IBM Support Portal: You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.
- By telephone for critical, system down, or severity 1 issues: For the telephone number to call in your region, see the Directory of worldwide contacts web page.

Results

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

Appendix G. Accessibility features for IBM Security Identity Manager

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

Accessibility features

The following list includes the major accessibility features in IBM Security Identity Manager.

- Support for the Freedom Scientific JAWS screen reader application
- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

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

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

Related accessibility information

The following keyboard navigation and accessibility features are available in the form designer:

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

IBM and accessibility

See the IBM Human Ability and Accessibility Center For more information about the commitment that IBM has to accessibility.

Notices

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

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

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

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

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

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

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

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

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

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

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

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both: http://www.ibm.com/legal/copytrade.shtml

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

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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

The Oracle Outside In Technology included herein is subject to a restricted use license and can only be used in conjunction with this application.

Index

A

access attributes, group form 39
accessibility x, 83
accounts
  adding to groups 43
  attributes, for adding 14
  changing passwords 27
  clearing mail status 29
  creating home directories 19
  deleting 33
  enabling email 21
  form attributes 65
  information, viewing groups 43
  modifying mail status 28
  proxy addresses 22
  removing from groups 44
  restoring 33
  suspending 32
adapter
  APIs 71
  attributes 65
  errors
    troubleshooting 47
    warnings 47
  features 1
  group management tasks 37
  overview 1
  registry key settings 5
  starting 5
  user account management tasks 5
  using, preliminary tasks 5
adding user accounts 14
ADSI interface, APIs 71
APIs
  Active Directory Adapter 71
  ADSI interface 71
  Windows 73
attributes
  account form 65
  adapter 65
  adding accounts 14
  cn 15
  customizable on group form 69
  dn 16
  for adding accounts 14
  for filter reconciling 10
  for groups 38
  group form 69
  groups 40
  groups access 39
  home directory security 6
  mapping 70
  not reconciled 8
  not supported for filter reconciling 12
  primary group 32
  RAS 21
  rdn 16
  reconciled 6
  user principal name, adding accounts 17
attributes *(continued)*
  Windows Terminal services 6
automated tasks 1

C

changing
  mail status 28
  mailbox support 30
  passwords of user accounts 27
checklists
  configuration 3
  process overview 3
cn
  adding accounts 15
  attribute, reconciling 9
codes
  country and region 57
  countryCode attribute 57
common name
  attribute 15
configuration
  checklist 3
  process overview 3
connecting to a disabled mailbox 31
containers
  modifying for groups 41
  modifying for user accounts 23
controls for user accounts 18
conventions
  typeface 77
country codes 57
customizable group form attributes 69

D

deleting accounts 33
directory names, notation 77
disabled
  mailbox 31
  mailbox registry keys 30
disabling unified messaging 34
distinguished name
  attribute 16
  filter reconciliation 12
dn
  adding accounts 16
  relative distinguished name 16

E

education x
email, enabling for accounts 21
enabling unified messaging 34
environment variable notation 77
error messages 49
extended attributes, mapping 70

F

filters
  for reconciliation 9
  reconciliation, non-supported attributes 12
  reconciliation, supported attributes 10
format, log files 56
forms
  attributes for accounts 65
  attributes for groups 69
  customizable attributes for groups 69

G

group form
  access attributes 39
  attributes 69
  support data 38
group operations
  adding 37
  modifying attributes 40
groups
  adding 37
  adding users 43
  creating 42
  deleting 44
  modifying attributes 40
  modifying scope 41
  removing users 44
  under the group base point 44
  viewing member information 43
Groups Base Point DN 5

H

home directory
  modifying 24
  security attributes 6
  user accounts 19

I

IBM
  Software Support x
  Support Assistant x
IBM Support Assistant 80
ISA 80

K

knowledge bases 79

L

log
  format 56
  levels 56

M

mail status
  changing 28
  changing to mail-enabled 29
  changing to mailbox-enabled 29
  clearing 29
mailbox
  connecting to user accounts 31
  disabled, connecting to user accounts 31
  disabling 30
  enabling 21
  registry keys 30
  support, changing 30
  support, modifying 30
  user account 21
mailbox store
  modifying 28
  same or different Exchange server 28
management tasks
  groups 37
  user accounts 5
mapping extended attributes 70
messages
  error 49
  warning 49
modifying
  attributes
    home directory 24
    mailbox store 28
  mailbox support 30
  unified messaging 35
  unified messaging addresses 35
  unified messaging mailbox policy 35
  user accounts 23
  user passwords 27
modifying containers for groups 41
modifying containers for users 23
modifying mail status 28

N

non-supported attributes, for filter reconciling 12
notation, environment variables
  path names 77
  typeface 77
notices 85

O

online
  publications ix
  terminology ix
operations
  adding 14
  modifying 23

P

path names, notation 77
problem-determination x
proxy address
  primary assigned by server 22
  user accounts 22
publications
  accessing online ix
  list of ix

R

RAS Saved IPv4 Address attribute 8
rdn, adding accounts 16
reconciling
  by filters 9
  cn attribute 9
  support data 8
  user accounts 5
  userAccountControl attribute 9
region codes 57
registry keys
  disabling mailboxes 30
  Groups Base Point DN 5
  settings 5
  Users Base Point DN 5
relative distinguished name
  attribute 16
remote access service attributes 21
restoring accounts 33

S

scope, modifying for groups 41
support contact information 80
support data
  group form 38
  reconciling 8
supported attributes, filter reconciling 10
suspending accounts 32
System Call attribute 8

T

tasks
  automation 1
  preliminary 5
terminology ix
training x
troubleshooting
  adapter errors 47
  contacting support 80
  error messages 49
  getting fixes 80
  identifying problems 47
  searching knowledge bases 79
  support website x
  techniques 47
  warning messages 49
typeface conventions 77

U

unified messaging
  disabling 34
  enabling 34
  modifying
    addresses 35
    mailbox policy 35
user accounts
  adding 14
  changing passwords 27
  clearing mail status 29
  controls 18
  deleting 33
  enabling email 21
  home directory 19
  modifying 23
  modifying mail status 28
  proxy addresses 22
  reconciling 5
  restoring 33
  suspending 32
User password attribute 8
user principal name, attribute 17
userAccountControl attribute, reconciling 9
users
  adding to groups 43
  removing from groups 44
  viewing from groups 43
Users Base Point DN 5

V

variables, notation for 77

W

warning messages 49
Windows
  APIs 73
  Terminal services attributes 6
WTS Server Name attribute 8

Printed in USA

SC27-4385-02