Note

Before using this information and the product it supports, read the information in "Notices" on page 47.

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.

© Copyright IBM Corporation 2012, 2013.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Figures
# Tables

1. Checklist for configuring IBM Security Identity Manager ............................................ 3
2. Specifying the optional attributes on the account form ............................................. 8
3. Results of specifying the support data attributes on the account form ............................ 12
4. Optional attributes .................................................................................................... 18

5. Accessibility attributes ............................................................................................ 19
6. Optional attributes .................................................................................................... 22
7. Account form attributes .......................................................................................... 31
8. Service form attributes .......................................................................................... 35
9. Group form attributes ............................................................................................ 36
10. Role form attributes ............................................................................................... 37
Preface

About this book

The UNIX and Linux Adapter User Guide provides information to manage user accounts. You can use IBM® Security Identity Manager to manage accounts on various operating systems such as:

- AIX®
- HP-UX
- Linux
- Solaris

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


Online publications

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

IBM Security Identity Manager library


IBM Security Systems Documentation Central

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

IBM Publications Center


IBM Terminology website

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

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

Technical training

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

Support information

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

Appendix C, “Support information,” on page 41 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 UNIX and Linux Adapter

The UNIX and Linux Adapter provides connectivity between the IBM Security Identity Manager server and the UNIX and Linux operating systems.

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

The UNIX and Linux Adapter automates the following user account management tasks:
- Adding user accounts
- Changing user account passwords
- Modifying user account attributes
- Suspending and restoring user accounts
- Retrieving user accounts
- Deleting user accounts

The adapter also automates the following UNIX group and AIX role management tasks:
- Adding groups on the UNIX operating systems
- Modifying group attributes on the UNIX operating systems
- Deleting groups from the UNIX operating systems
- Adding roles on AIX
- Modifying role attributes on AIX
- Deleting roles from AIX

The adapter contains Tivoli® Directory Integrator assembly lines that serve one or more user account, UNIX group, and AIX role operations. When the first request is sent from IBM Security Identity Manager, the required assembly line is loaded into Tivoli Directory Integrator. The same assembly line is then cached to serve subsequent operations of the same type.

Note:
- The reconciliation and test assembly lines are not cached.
- AIX roles are not reconciled or managed by the adapter for any AIX service with a user registry that is defined as LDAP.

The UNIX and Linux Adapter uses the Secure Shell (SSH) protocol to establish communication with the UNIX and Linux operating systems. Ensure that the SSH server is running on the managed resource when you connect from IBM Security Identity Manager. The adapter runs as a service, independently of whether you are logged on to IBM Security Identity Manager. For more information about Secure Shell installation, see UNIX and Linux Adapter Installation and Configuration Guide.

Features of the UNIX and Linux Adapter

You can use the UNIX and Linux Adapter for user account reconciliation and other tasks.
- Reconciliation of user accounts and other support data from the UNIX or Linux operating system to IBM Security Identity Manager.
- User account management tasks, such as adding, modifying, changing passwords, suspending, restoring, and deleting accounts.
- UNIX group management tasks, such as adding, modifying, and deleting groups.
- AIX role management tasks, such as adding, modifying, and deleting roles.
- Assigning roles and groups to users from the account form.
- Management of multiple operating systems, such as AIX, HP-UX, Linux, and Solaris with a single Tivoli Directory Integrator connector.
- Management of the UNIX and Linux operating systems by a sudo user (also known as a super user), who can perform administrative tasks. For more information about creating a super user, see the UNIX and Linux Adapter Installation and Configuration Guide.
- Key-based authentication for managing the UNIX and Linux operating systems. This type of authentication provides a secure environment to manage your systems. For more information about key-based authentication, see the UNIX and Linux Adapter Installation and Configuration Guide.
Chapter 2. Checklist for configuring IBM Security Identity Manager to run the adapter

You must complete a series of tasks that 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

<table>
<thead>
<tr>
<th>Task</th>
<th>See this documentation:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the UNIX and Linux Adapter</td>
<td>&quot;Installing the UNIX and Linux Adapter&quot; in the UNIX and Linux Adapter Installation and Configuration Guide</td>
</tr>
<tr>
<td>Import the adapter profile into IBM Security Identity Manager</td>
<td>&quot;Importing the adapter profile into the IBM Security Identity Manager server&quot; in the UNIX and Linux Adapter Installation and Configuration Guide</td>
</tr>
<tr>
<td>Create a service for the UNIX and Linux Adapter</td>
<td>&quot;Creating the service&quot; in the UNIX and Linux Adapter Installation and Configuration Guide</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> After you create a UNIX and Linux 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 UNIX and Linux Adapter service according to the requirements of your organization. For more information, see the section about &quot;Customizing a provisioning policy&quot; in the IBM Security Identity Manager product documentation.</td>
</tr>
<tr>
<td>Configure the UNIX and Linux Adapter</td>
<td>&quot;Configuring the UNIX and Linux Adapter&quot; in the UNIX and Linux Adapter Installation and Configuration Guide</td>
</tr>
<tr>
<td>Perform a reconciliation operation to retrieve user accounts and store them in the IBM Security Identity Manager server</td>
<td>&quot;Managing reconciliation schedules&quot; in the IBM Security Identity Manager product documentation</td>
</tr>
<tr>
<td>Adopt orphan accounts on IBM Security Identity Manager</td>
<td>&quot;Assigning an orphan account to a user&quot; in the IBM Security Identity Manager product documentation</td>
</tr>
</tbody>
</table>
Chapter 3. User account management tasks

The UNIX and Linux Adapter manages user accounts for a specific person, a service instance, or specific accounts by using the search function of IBM Security Identity Manager.

The reconciliation operation retrieves the user account information from the UNIX or Linux systems and stores it in the directory server of IBM Security Identity Manager. The operation also retrieves support data such as groups and roles on AIX systems.

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

This section includes the following topics:

- “Before you begin the adapter operations”
- “Reconciling support data without reconciling user accounts”
- “Reconciling single user accounts” on page 6
- “User account additions” on page 7
- “User account modification” on page 14
- “User account deletion” on page 15

Before you begin the adapter operations

Before performing any operations with the adapter, you must verify that the adapter environment is correctly set up.

1. Perform the steps in Chapter 2, “Checklist for configuring IBM Security Identity Manager to run the adapter,” on page 3.

2. Run the Dispatcher. The Dispatcher in turn runs the UNIX and Linux Adapter. See the section about running the adapter service in the UNIX and Linux Adapter Installation and Configuration Guide.

Reconciling support data without reconciling user accounts

Perform support data reconciliation when you want an updated list of groups and roles that are available on the operating systems.

About this task

When you perform support data reconciliation, the adapter retrieves the support data information without processing the user account information from the operating system.
Support data for the UNIX or Linux user account includes the following attributes:

- Primary group
- Secondary group

**Note:** You can reconcile the following additional support data attributes from the AIX operating system. For more information about the support data attributes on the account form and the supported operating systems, see [Appendix A, "UNIX and Linux Adapter attributes," on page 31.](#)

- Groups that can use the `su` command to switch to this user
- Groups that can be managed by this user
- Administrative roles

To reconcile only the support data without reconciling user accounts:

**Procedure**

1. Log on to IBM Security Identity Manager as an administrator.
2. In the My Work pane, click **Manage Services** to display the Manage Services page.
3. Select the type of service from the **Service type** list and click **Search**. Use one of the following service types:
   - **POSIX AIX profile**
     - Select this option when you want to manage user accounts on the AIX operating system.
   - **POSIX HP-UX profile**
     - Select this option when you want to manage user accounts on the HP-UX operating system.
   - **POSIX Linux profile**
     - Select this option when you want to manage user accounts on the Linux operating system.
   - **POSIX Solaris profile**
     - Select this option when you want to manage user accounts on the Solaris operating system.
4. Select the name of the service that you created for the UNIX and Linux Adapter.
5. Click the arrow icon to view the popup menu.
6. Select **Reconcile Now** from the menu to display the Reconcile Now page.
7. Click **Define query**.
8. Select the **Reconcile supporting data only** check box and click **Submit**.

---

**Reconciling single user accounts**

Reconciling a single user account means performing a *filter reconciliation*.

**About this task**

Filter reconciliation takes less time than reconciling all the user accounts. Perform filter reconciliation when you want to:

- Modify a specific user account
- Obtain information about a specific user account
Procedure
1. Log on to IBM Security Identity Manager as an administrator.
2. In the My Work pane, click Manage Services to display the Manage Services page.
3. Select the type of service from the Service type list and click Search. Use one of the following service types:
   - POSIX AIX profile
     Select this option when you want to manage user accounts on the AIX operating system.
   - POSIX HP-UX profile
     Select this option when you want to manage user accounts on the HP-UX operating system.
   - POSIX Linux profile
     Select this option when you want to manage user accounts on the Linux operating system.
   - POSIX Solaris profile
     Select this option when you want to manage user accounts on the Solaris operating system.
4. Select the name of the service that you created for the UNIX and Linux Adapter.
5. Click the arrow icon to view View popup menu.
6. Select Reconcile Now from the menu to display the Reconcile Now page.
7. Click Define query.
8. In the Reconcile accounts that match this filter field, type the following syntax.
   (eruid=UserID)
   UserID is the name of the user account that you want to reconcile.
9. Click Submit.

User account additions
You can add user accounts at any time for either an existing person or a new person in the organization. You can change the adapter attributes that define the accounts on the account form.

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

This section includes the following topics:
- “Required attribute” on page 8
- “Optional attributes on the account form” on page 8
- “Password lifespan for a user account” on page 10
- “Determining the lifespan of a user account” on page 10
- “Group assignment to users” on page 11
- “Role assignment to users” on page 11
- “Support data attributes” on page 11
- “Discovery of sudo privileges” on page 13
**Required attribute**

The **User ID** attribute is the only required attribute on the account form. This attribute on the account form is mapped to the **Login Name** attribute on the UNIX and Linux operating systems.

**Note:** The account forms for the UNIX and Linux operating systems (AIX, HP-UX, Linux, and Solaris) are different. For more information about the attributes on the account form and the supported operating systems, see “UNIX and Linux Adapter account form attributes” on page 31.

You can also specify optional attributes on the account forms.

**Optional attributes on the account form**

In addition to the required attributes, you can create more fields on the account form. You can use **Design Forms** in IBM Security Identity Manager to customize the account form.

The Force a password change, Allow at jobs, and Allow cron jobs attributes are examples of the optional attributes on the account form. For more information about account attributes, see “UNIX and Linux Adapter account form attributes” on page 31 and the documentation for your operating system.

**Note:** The Allow at jobs and Allow cron jobs attributes affect the contents of these files:
- at.allow
- at.deny
- cron.allow
- cron.deny

In some cases, platform-specific configuration might be required to enable the user to perform at or cron jobs. For example, on the AIX operating system the user’s daemon attribute must be set to true to enable the user to run at or cron jobs.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Supported operating system</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force a password change</td>
<td>AIX HP-UX Linux Solaris</td>
<td>Selecting the <strong>Force a password change</strong> check box forces you to change your password the next time you log on to the operating system.</td>
</tr>
</tbody>
</table>
Table 2. Specifying the optional attributes on the account form (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Supported operating system</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AIX HP-UX Linux Solaris</td>
<td>Specifying the Allow at jobs attribute grants permissions to users to submit jobs with the <code>at</code> command. You can run the <code>at</code> command once, at a particular time in the future.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When you select the <strong>Allow at jobs</strong> check box from IBM Security Identity Manager, the adapter:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Creates the user account on the operating system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Adds the user to the <code>at.allow</code> file. If the file does not exist, then the adapter creates the <code>at.allow</code> file on the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Removes the user from the <code>at.deny</code> file if the file exists on the operating system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specifying the Allow cron jobs attribute grants permissions to users to use the cron utility to schedule repetitive tasks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When you select the <strong>Allow cron jobs</strong> check box from IBM Security Identity Manager, the adapter:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Creates the user account on the operating system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Adds the user to the <code>cron.allow</code> file. If the file does not exist, then the adapter creates the <code>cron.allow</code> file on the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Removes the user from the <code>cron.deny</code> file if the file exists on the operating system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Selecting the <strong>Delete user account even when it is in use</strong> check box ends the active processes that a user has when you delete the user account.</td>
</tr>
</tbody>
</table>

Chapter 3. User account management tasks 9
Table 2. Specifying the optional attributes on the account form (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>AIX</th>
<th>HP-UX</th>
<th>Linux</th>
<th>Solaris</th>
<th>Result</th>
</tr>
</thead>
</table>
| Execute user profile? | | ✓ | | | Specifying the Execute user profile? attribute causes the adapter user profile to be run before the IBM Security Identity Manager task. This attribute enables special terminal control characters such as @ or # on HP-UX services. If the profile remaps these characters and you enable this attribute, you can use these characters in passwords when you add or modify accounts. Do not change the default owner, group, or permissions of the /etc/profile and .profile of the adapter user. Doing so might cause the adapter to fail. Running the profile has some limitations:  
• Do not call another shell from profile scripts, it can cause the adapter to hang.  
• Do not echo anything when the profile traps a logout signal, it can cause the echo output to be merged with command results. |

Password lifespan for a user account

The password lifespan attributes specify the time before the password of a user account expires.

Use the following attributes:

**Password maximum age**
Specifies the maximum number of days the password is valid. If you specify this attribute, then after the specified number of days, the password expires. You must then change the password to continue accessing the UNIX or Linux operating system.

**Password minimum age**
Specifies the minimum number of days you cannot change your existing password. If you do not specify a value for this attribute, you can change the password anytime.

**Password warning age**
Specifies the number of days before the password expires from which you start receiving a warning to change the existing password.

Determining the lifespan of a user account
The lifespan of a user account is the time before it expires.
About this task

The Account Expiration Date attribute specifies the date on which the account becomes inactive and unavailable. The default value for this attribute is Never. If you do not specify a date, the user account is valid indefinitely. Follow these steps to specify a date value:

Procedure
1. Clear the Never check box.
2. Click the View Calendar icon and select the date.
3. Click OK. The status of a user account becomes inactive and unavailable for use when the following situations occur:
   • The account expiration date elapses.
   • The value of the Account Expiration Date attribute is same as the current date.

   In both the situations, the user account is created on the UNIX or Linux operating system, however the user cannot log on to the system.

Group assignment to users

You can assign groups to users on the UNIX and Linux operating systems.

To assign groups to a user, select the groups that are listed on the account form. You can associate a user to the following groups:
• Primary group
• Secondary group

You can assign only one primary group to a user, however you can assign multiple secondary groups to a user. When you assign groups to a user from IBM Security Identity Manager, the adapter creates the user account and associates the user to the group.

Role assignment to users

To assign administrative roles to a user, select the roles that are listed on the account form of the AIX operating system.

You can assign multiple administrative roles to a user. When you assign an administrative role to a user, you provide permissions to the user to perform the administrative actions defined for that role. Ensure that you assign roles that grant enough permissions to the user to accomplish administrative tasks.

When you assign administrative roles to a user from IBM Security Identity Manager, the adapter creates the user account. The adapter also sets the value of the administrative roles attribute on the AIX operating system.

Support data attributes

Specifying the support data attributes assign groups and roles to the users on the operating system.

The following table lists:
• The support data attributes on the account form
• The supported operating systems

Chapter 3. User account management tasks  11
• The result of specifying the support data attributes

**Table 3. Results of specifying the support data attributes on the account form**

<table>
<thead>
<tr>
<th>Support data attribute</th>
<th>Supported operating system</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AIX</td>
<td>HP-UX</td>
</tr>
</tbody>
</table>
| Primary group          | ✓   | ✓     | ✓     | ✓       | The adapter associates a user to a primary group that is selected from the list on the account form. When you assign a user to a primary group:  
  • The users gain privileges that are available to that group.  
  • The adapter creates the user account on the operating system and sets the value of the `primary group` attribute on the operating system.  
  You can associate a user only to one primary group. |
| Secondary group        | ✓   | ✓     | ✓     | ✓       | The adapter associates a user to secondary groups that are selected from the list on the account form. When you assign a user to a secondary group:  
  • The user gains privileges that are available to that group.  
  • The adapter creates the user account on the operating system and makes the user a member of each of the selected secondary groups.  
  You can associate a user to multiple secondary groups. |
| Groups that can use the `su` command to switch to this user | ✓   |       |        |         | The adapter enables the users in the selected groups to use the `su` command to switch to the specified user account. When you set the value of this attribute:  
  • The adapter creates the user account on the AIX operating system.  
  • The member users of the selected groups gain permissions to use the `su` command to switch to the specified user account. |
Table 3. Results of specifying the support data attributes on the account form (continued)

<table>
<thead>
<tr>
<th>Support data attribute</th>
<th>Supported operating systems</th>
<th>Result</th>
</tr>
</thead>
</table>
| Groups to be administered | AIX ✓ HP-UX Linux Solaris | The adapter enables a user to administer the groups that are selected from the list on the account form of the AIX operating system. When you set the value of this attribute:  
• The adapter creates the user account.  
• The adapter enables the user to administer the selected groups. |

| Administrative roles | ✓ | The adapter enables a user to perform administrative tasks by assigning roles on the AIX operating system. An administrative role defines the permissions granted to a user for administrative tasks. When you assign administrative roles to a user, the adapter creates the user account. It sets the value of the user’s roles attribute on the AIX operating system. |

Discovery of sudo privileges

The sudo privileges granted to users and groups on a system can be returned during account reconciliation. The privileges are read from the sudoers file on the resource where the reconciliation occurs.

To discover sudo privileges, enable the feature by selecting the check box Return sudo privileges? on the service form. Also specify the path to the sudoers file, if it is not in the default location /etc/sudoers on the resource. The sudoers file on the resource must be readable by the ID that IBM Security Identity Manager uses to administer the system. The UNIX and Linux Adapter does not validate the sudoers file. Use only the visudo command to modify the sudoers file because it validates the file.

The sudo privileges that are discovered are displayed on the account and group forms in read-only lists. The format of the sudo privileges is the same as the specification in the sudoers file. However, alias names are replaced with the alias member values. Currently no functionality exists to provision changes in sudo privileges in IBM Security Identity Manager to the sudoers file on services.

The sudo privileges displayed for user accounts do not include privileges that are defined for groups. The user might inherit sudo privileges from group membership, but they are not displayed.

The sudo privileges that are returned from the resource might not be in the same order that they are in the sudoers file. The order of privileges displayed in IBM Security Identity Manager does not imply the order of precedence for privileges on the system.
Restrictions on what the adapter reads from the sudoers file

Because **sudo** command capabilities might vary widely between releases, the UNIX and Linux Adapter does limited processing of the sudoers file. Limiting the processing enables the adapter to support the most common usage across a wide range of sudo versions.

The adapter discovers sudo privileges for an account by reading the sudoers file and searching for user specifications that match the account on the host computer. For the adapter to match accounts to user specifications, the accounts in the sudoers file must be specified by one of the following identifiers:

- User name
- Group ID
- The keyword ALL

For the adapter to match the host computer to a user specification, one of the following conditions must be met:

- The host name must equal the value returned by the `hostname` command on the workstation.
- The IP address of the computer must match.
- The keyword ALL must be specified.
- A matching IP network is used.

Aliases can be used for users and hosts, but they must resolve to values that the adapter can match.

If the `#include` directive is used in the sudoers file, the adapter searches for privileges in the specified file as well. However, advanced features such as the `%h` escape and the `#includedir` directives are not currently supported.

If aliases are used in the sudoers file, the adapter processes these aliases:

- Cmd_Alias
- User_Alias
- Runas_Alias
- Host_Alias

Other features of the sudoers file such as defaults, parameters, options, and wildcard characters are not processed by the adapter.

User account modification

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

This section describes some typical adapter attributes that you can use to modify the user accounts. For more attributes and specific procedures, see the IBM Security Identity Manager product documentation.

This section includes the following topics:

- "User unassignment from groups" on page 15
- "Role removal on AIX" on page 15
- "Password changes for user accounts" on page 15
- "User account suspension" on page 15
- "User account restoration" on page 15
User unassignment from groups
When you use IBM Security Identity Manager to unassign a user from a group, the adapter modifies the user account on the operating system.

The adapter also removes the value of that group from the user account.

Role removal on AIX
You can unassign roles on AIX.

You can unassign an administrative role by deleting it from IBM Security Identity Manager. Users assigned to that role can no longer perform the administrative tasks that are defined for that role on the AIX operating system.

When you use IBM Security Identity Manager to unassign a user from any administrative role, the adapter modifies the user account. The adapter removes the value of that role from the roles attribute of that user account.

Password changes for user accounts
You can change the password of any of the UNIX or Linux accounts that exist on IBM Security Identity Manager.

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

User account suspension
When you suspend a user account, the status of the user account on IBM Security Identity Manager becomes inactive.

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 product documentation.

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.

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 product documentation.

When you delete a user account from IBM Security Identity Manager, the adapter removes the user from the /etc/passwd file. You can no longer manage the user account.
Note: On Linux systems, you cannot delete account if the account user has running processes. To delete a user with running processes, add the `erPosixDelUsrInUse` attribute as a check box to the Linux account form. Then, select the check box when you delete the account. See "Optional attributes on the account form" on page 8.
Chapter 4. UNIX group and AIX role management tasks

The UNIX and Linux Adapter manages UNIX groups and AIX roles. You can add, modify, and delete UNIX groups and AIX roles directly from IBM Security Identity Manager.

This section includes the following topics:
- “Defining UNIX groups”
- “Modifying UNIX group attributes” on page 19
- “Deleting UNIX groups” on page 20
- “Defining AIX roles” on page 21
- “Modifying AIX role attributes” on page 22
- “Deleting AIX roles” on page 23

Defining UNIX groups

You can add groups at any time to define specific accesses to a set of users in an organization.

About this task

When you add a group, the members of the group have access rights to perform the tasks for which the group has access. You can use the group form to directly add UNIX or Linux operating system users to a group at any time.

The Group name attribute is the only required attribute on the group form. The permissible character limit for this attribute is 8.

Note: The group forms for the UNIX and Linux operating systems (AIX, HP-UX, Linux, and Solaris) are different. For more information about the attributes on the group form and the supported operating systems, see "UNIX and Linux Adapter group form attributes" on page 36.

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 type of service from the Service type list and click Search. Use one of the following service types:
   - POSIX AIX profile
     Select this option when you want to manage groups on the AIX operating system.
   - POSIX HP-UX profile
     Select this option when you want to manage groups on the HP-UX operating system.
   - POSIX Linux profile
     Select this option when you want to manage groups on the Linux operating system.
**POSIX Solaris profile**
Select this option when you want to manage groups on the Solaris operating system.

4. Select the name of the service that you created for the UNIX and Linux Adapter and click **Continue**.

5. Click **Create** to display the group form.

6. Specify the name for the group in the Group name field.

7. Click **Finish**. The group is added to the operating system.

**Optional attributes on the group form**
You can also specify the optional attributes to define a group on IBM Security Identity Manager.

The following table lists the optional attributes that you can specify on the group form.

*Table 4. Optional attributes*

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Supported operating system</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ID number</td>
<td>AIX HP-UX Linux Solaris</td>
<td>Specify a group ID number that identifies each group on the operating system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If you do not specify the Group ID number on the group form and perform the add operation, the operating system generates the ID number for that group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Avoid modifying the Group ID number on the UNIX and Linux operating systems because that might affect system security.</td>
</tr>
<tr>
<td>Administrator group</td>
<td>AIX</td>
<td>Select this check box to add the group as an administrative group.</td>
</tr>
<tr>
<td>Group administrators</td>
<td>AIX</td>
<td>Add the users who can perform administrative tasks for the group.</td>
</tr>
<tr>
<td>Group projects</td>
<td>AIX</td>
<td>Lists the projects that you can assign to the user’s processes. The project names must be valid project names as defined on the operating system.</td>
</tr>
<tr>
<td>Allow duplicate group IDs</td>
<td>AIX HP-UX Linux Solaris</td>
<td>Specifies that the group ID number can be non-unique.</td>
</tr>
<tr>
<td>sudo privileges</td>
<td>AIX HP-UX Linux Solaris</td>
<td>Display the sudo privileges granted to the group. This attribute is read-only.</td>
</tr>
</tbody>
</table>

**Accessibility attributes on the group form**
You can limit the access to a group based on the access type.

You can specify accessibility attributes on the group form to grant defined access to users. Select the **Define an access** check box to enable the listed accessibility attributes on the group form. Clearing this check box clears the access.
Table 5. Accessibility attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access status</td>
<td>Specify this attribute to set the access status for the user. You can select one of the following statuses:</td>
</tr>
<tr>
<td></td>
<td>• Enable status</td>
</tr>
<tr>
<td></td>
<td>• Enable common status</td>
</tr>
<tr>
<td></td>
<td>• Disable status</td>
</tr>
<tr>
<td>Access name</td>
<td>Specify a name for the access that you want to grant the user.</td>
</tr>
<tr>
<td>Access type</td>
<td>Select the type of access to be granted to the user from the drop-down list. You can select one of the following types:</td>
</tr>
<tr>
<td></td>
<td>Application</td>
</tr>
<tr>
<td></td>
<td>Select this option to grant an application-based access to the user.</td>
</tr>
<tr>
<td></td>
<td>Email group</td>
</tr>
<tr>
<td></td>
<td>Select this option to restrict the network resource access to an email group of users on the operating system.</td>
</tr>
<tr>
<td></td>
<td>Role</td>
</tr>
<tr>
<td></td>
<td>Select this option to grant role-based access to the user.</td>
</tr>
<tr>
<td></td>
<td>Shared folder</td>
</tr>
<tr>
<td></td>
<td>Select this option to grant folder-based access to the user.</td>
</tr>
<tr>
<td>Access description</td>
<td>Provide a short description for the access that you are defining.</td>
</tr>
<tr>
<td>Access owner</td>
<td>Select the name of the access owner from the list.</td>
</tr>
<tr>
<td>Notify users when access is provisioned and available for use</td>
<td>Select this check box to send an auto-notification email to users who gained the defined access. Users who gained access are authorized to perform the tasks that are defined for that access.</td>
</tr>
<tr>
<td>Notify users when access is de-provisioned</td>
<td>Select this check box to send an auto-notification email to users about the de-provisioning of the access.</td>
</tr>
</tbody>
</table>

Modifying UNIX group attributes

You can modify groups at any time on IBM Security Identity Manager.

About this task

You can perform the following modify operation:

• Add users to a group
• Remove users from a group
• Modify the attributes of the group

Note: The Group name attribute is the only non-modifiable attribute on the group form. You can modify all the other attributes of a group.

To modify groups to the operating system:

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 type of service from the Service type list and click Search. Use one of the following service types:

- **POSIX AIX profile**
  Select this option when you want to manage groups on the AIX operating system.

- **POSIX HP-UX profile**
  Select this option when you want to manage groups on the HP-UX operating system.

- **POSIX Linux profile**
  Select this option when you want to manage groups on the Linux operating system.

- **POSIX Solaris profile**
  Select this option when you want to manage groups on the Solaris operating system.

4. Select the name of the service that you created for the UNIX and Linux Adapter and click Continue.

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 that you want to modify and click Change.

7. After you modify the group attributes, click OK.

---

**Deleting UNIX groups**

You can delete groups at any time on IBM Security Identity Manager.

**About this task**

When you delete a group from IBM Security Identity Manager, the adapter removes the group from the /etc/group file. You can no longer manage the group.

To delete groups on the operating system:

**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 type of service from the Service type list and click Search. Use one of the following service types:

   - **POSIX AIX profile**
     Select this option when you want to manage groups on the AIX operating system.

   - **POSIX HP-UX profile**
     Select this option when you want to manage groups on the HP-UX operating system.

   - **POSIX Linux profile**
     Select this option when you want to manage groups on the Linux operating system.
POSIX Solaris profile
Select this option when you want to manage groups on the Solaris operating system.

4. Select the name of the service that you created for the UNIX and Linux Adapter and click Continue.

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 that you want to delete and click Delete. The confirmation page is displayed.

7. On the Confirm page, click Delete.

---

Defining AIX roles
You can add roles at any time to grant administrative permissions to users in an organization.

About this task
The users assigned to the role are authorized to perform the administrative tasks that are defined for the role.

Note: Only the AIX operating system supports role management.

The AIX role name attribute is the only required attribute on the role form. The attribute can contain letters and numbers. The permissible character limit for this attribute is 8.

To add roles to the operating system:

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 POSIX AIX profile from the Service type list and click Search.
4. Select the name of the service that you created for the UNIX and Linux Adapter and click Continue.

   Note: AIX roles are not reconciled or managed by the adapter for any AIX service with a user registry that is defined as LDAP.

5. Click Create to display the group type.
6. Select AIX roles and click Next to display the form.
7. Specify the name for the role in the AIX role name field.
8. Click Finish. The role is added to the AIX operating system.

Optional attributes on the role form
You can also specify the optional attributes to define a role on IBM Security Identity Manager.

The following table lists the optional attributes that you can specify on the group form.
Table 6. Optional attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorizations</td>
<td>Specify this attribute to list the additional authorizations that are required for the role beyond the default authorizations.</td>
</tr>
<tr>
<td>Roles implied</td>
<td>Specify this attribute to list additional roles that users can perform in an organization.</td>
</tr>
<tr>
<td>List of groups</td>
<td>Specify this attribute to list the groups to which a user must belong to for effectively performing the defined role. Note: This attribute is for information only and does not automatically make the user a member of the listed groups.</td>
</tr>
<tr>
<td>Visibility</td>
<td>Specify the visibility status of the role. You can select one of the following options on the role form:</td>
</tr>
<tr>
<td></td>
<td><strong>Enabled and selectable</strong> Select this option to enable, display, and select the role on the AIX operating system. Authorizations contained in this role are applied to the user.</td>
</tr>
<tr>
<td></td>
<td><strong>Enabled but not selectable</strong> Select this option to enable and display the role as existing, however, you cannot select the role. Authorizations contained in this role are applied to the user.</td>
</tr>
<tr>
<td></td>
<td><strong>Disabled</strong> Select this option to disable the role on the AIX operating system. Authorizations contained in this role are not applied to the user.</td>
</tr>
</tbody>
</table>

Modifying AIX role attributes

You can modify the AIX role attributes at any time on IBM Security Identity Manager.

About this task

To modify roles to the operating system:

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 POSIX AIX profile from the Service type list and click Search.
4. Select the name of the service that you created for the UNIX and Linux Adapter and click Continue.
5. On the Select Group page, click Refresh to display all the groups and roles created for that service.
6. From the Groups table, select the role that you want to modify and click Change.

Note: The AIX role name attribute is the only non-modifiable attribute on the role form. You can modify all the other attributes of a role.
7. After you modify the role attributes, click OK.
Deleting AIX roles

You can delete roles at any time on IBM Security Identity Manager.

About this task

When you delete a role from IBM Security Identity Manager, the adapter removes the role from the /etc/security/roles file. You can no longer manage the role.

To delete roles on the operating system:

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 POSIX AIX profile from the Service type list and click Search.
4. Select the name of the service that you created for the UNIX and Linux Adapter and click Continue.
5. On the Select Group page, click Refresh to display all the groups and roles created for that service.
6. From the Groups table, select the role that you want to delete and click Delete. The confirmation page is displayed.
7. On the Confirm page, click Delete.
Chapter 5. Troubleshooting

Use the UNIX and Linux Adapter error messages and warnings to resolve errors.

The UNIX and Linux Adapter operation might fail if:

- A change is made in the structure of standard files, such as /etc/passwd.
- The UNIX and Linux operating system version is not supported by the adapter. For information about the supported versions of the UNIX and Linux operating systems, see the UNIX and Linux Adapter Installation and Configuration Guide.
- The Secure Shell (SSH) configuration settings are incorrect. Ensure that the value of the UsePrivilegeSeparation attribute in the sshd_config file is set to yes. The sshd_config file is located in the /etc/ssh/ directory.
- The managed resources are configured to send Client-keep-alive messages. The adapter does not acknowledge client-keep-alive messages. If the managed resource sends such messages, the connection is ended as a result. You must set ClientAliveInterval value in the /etc/ssh/sshd_config configuration file to the default value 0. This setting disables the ClientAliveInterval attribute. Then restart the SSHD server.

Techniques for troubleshooting problems

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

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

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

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

What are the symptoms of the problem?

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

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

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

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

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

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

When does the problem occur?

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

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

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

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

Under which conditions does the problem occur?

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

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to happen for the problem to occur?
- Do any other applications fail at the same time?
Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.

**Can the problem be reproduced?**

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

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

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

For information about obtaining support, see Appendix C, “Support information,” on page 41.

**Error log access**

When an operation fails, the corresponding error messages and warnings are logged in the `ibmdi.log` file. This file is in the `adapter solution/logs` directory.

You can display the error logs in the user interface by running the Dispatcher from the command prompt. You can also configure logging information for the adapter. For more information about displaying logs in the user interface and configuring logging information, see *UNIX and Linux Adapter Installation and Configuration Guide*.

**Error messages and warnings**

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

This table lists the error messages and warnings that might occur while performing the UNIX and Linux Adapter user, group, or role tasks. The table also provides the corrective actions to resolve those errors.
<table>
<thead>
<tr>
<th>Error message</th>
<th>Corrective action</th>
</tr>
</thead>
</table>
| The login credential is missing or incorrect. | Specify the values of the login attributes correctly. Ensure that:  
  - The managed resource (AIX, HP-UX, Solaris, or Linux) is functioning and that you are connected to the correct resource.  
  - The value of the Managed resource location attribute on the service form is specified correctly.  
  - The name in the Administrator name field on the service form is specified correctly.  
  - The value of the Password attribute on the service form is specified correctly.  
  - The Secure Shell (SSH) is enabled and running on the managed resource. For information about installing and enabling the SSH, see the UNIX and Linux Adapter Installation and Configuration Guide. |
| The account exists. | This error might occur when:  
  - A request is made to add a user that exists. Create a user account with another user ID.  
  - The UNIX and Linux operating system and IBM Security Identity Manager are not synchronized. Schedule a reconciliation between the managed resource and IBM Security Identity Manager. For more information about scheduling a reconciliation, see the IBM Security Identity Manager product documentation. |
| - The adapter does not have permission to add an account.  
- The adapter does not have permission to modify an account.  
- The adapter does not have permission to delete an account. | The user specified in the Administrator name field on the service form does not have the permissions to add, modify, or delete the account. Perform one of the following actions:  
  - Assign the appropriate privileges to the user whose name is specified in the Administrator name field.  
  - Change the name in the Administrator name field to a name that has the appropriate privileges. For example, root.  
  **Note:** The Administrator name attribute is a required attribute on the service form. |
| - The required attributes are missing from the request.  
- There were no attributes passed to the adapter in the request.  
- One or more required attributes are missing in the request. | One or more required attributes were not provided when a request was made to add, modify, delete, or search for a user. Ensure that the required User ID attribute is specified on the account form. |
<table>
<thead>
<tr>
<th>Error message</th>
<th>Corrective action</th>
</tr>
</thead>
</table>
| • A system error occurred while adding an account. The account was not added.  
• A system error occurred while modifying an account. The account was not changed.  
• A system error occurred while deleting an account. The account was not deleted.  
• The search failed due to a system error. | This error might occur for several reasons. Ensure that:  
• The name in the Administrator name field on the service form is specified correctly.  
• The value of the Password attribute on the service form is specified correctly.  
• The name in the Administrator name field has the appropriate privileges to add, modify, or delete a user account. |
| • The account was added but some attributes failed.  
• The account was modified but some attributes failed.  
• The account was deleted successfully, but additional steps failed. | The account was created, modified, or deleted, however some of the specified attributes in the request were not set. See the list of attributes that failed and the error message that explains why the attribute failed. Correct the errors associated with each attribute and perform the action again.  
**Note:** You might need to review the documentation on the UNIX or Linux operating system to determine the correct values for some attributes. |
| The account is already suspended. | This error occurs if an attempt is made to suspend an already suspended account. |
| The account was not suspended. | The request to suspend the account failed. Ensure that:  
• The name in the Administrator name field on the service form is specified correctly.  
• The value of the Password attribute on the service form is specified correctly.  
• The name in the Administrator name field has the necessary privileges to suspend an account.  
• The user exists on the specified managed resource.  
See the `ibmdi.log` file in the `adapter solutions` directory of the Tivoli Directory Integrator server for specific details about the error. |
| The account is already restored. | This error occurs if an attempt is made to restore an already restored account. |
| The account was not restored. | The request to restore the account failed. Ensure that:  
• The name in the Administrator name field on the service form is specified correctly.  
• The value of the Password attribute on the service form is specified correctly.  
• The name in the Administrator name field has the necessary privileges to restore an account.  
• The user exists on the specified managed resource.  
See the `ibmdi.log` file in the `adapter solutions` directory of the Tivoli Directory Integrator server for specific details about the error. |
<table>
<thead>
<tr>
<th>Error message</th>
<th>Corrective action</th>
</tr>
</thead>
</table>
| The reconciliation is successful, but no accounts were added to your service. | Check the ibmdi.log file to ensure that the usage of the shadow file is correct.  
**Note:** If you want the adapter to perform the reconciliation operation by using the shadow file, select the Use Shadow File check box on the service form.  
Shadow files are available on the Linux and HP-UX operating systems. |
| The application could not establish a connection to hostname.                  | Ensure that:  
• The SSH is enabled on the managed resource.  
• The managed resource is operational and connected to the network. |
| The group cannot be added because it exists.                                 | This error occurs when a request is made to add a group that exists. Create a group with another group name. |
| The group cannot be added because group with the GID Group ID number exists.  | This error occurs when a request is made to add a group with a group ID number that exists. Do either of the following:  
• Do not specify a group ID number.  
• Clear the Allow duplicate group IDs? checkbox if that option is supported for the managed resource. |
| The group Group name cannot be modified or deleted because it does not exist. | This error occurs when a request is made to modify or delete a group that does not exist on the managed resource. Perform a reconciliation operation to ensure that the group exists on the managed resource. |
| An error occurred while creating, modifying, or deleting the Group name group. | Ensure the following on the service form:  
• The name in the Administrator name field on the service form is specified correctly.  
• The value of the Password attribute on the service form is specified correctly.  
• The managed resource is operational and connected to the network. |
| The IBM Tivoli Directory Integrator detected the following error. Error: Connector parameter executeUserProfile has a value that is not valid: true. | Clear the Execute user profile? check box for the service used in the operation. |
Appendix A. UNIX and Linux Adapter attributes

You can manage the adapter attributes that are on the various adapter forms.

These topics include:
- Account form attributes
- Service form attributes
- UNIX group form attributes
- AIX role form attributes

UNIX and Linux Adapter account form attributes

You can manage user accounts from IBM Security Identity Manager.

The following table lists:
- The attributes that are displayed on the UNIX and Linux operating system account form on IBM Security Identity Manager.
- The corresponding names on the IBM Tivoli Directory Server.
- The supported operating systems.

Table 7. Account form attributes

<table>
<thead>
<tr>
<th>Attribute name on the UNIX and Linux operating system account form on IBM Security Identity Manager</th>
<th>Attribute name on the IBM Tivoli Directory Server</th>
<th>Supported operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>erUid</td>
<td>AIX</td>
</tr>
<tr>
<td>Gecos (comments)</td>
<td>erPosixGecos</td>
<td>✓</td>
</tr>
<tr>
<td>UID number</td>
<td>erPosixUid</td>
<td>✓</td>
</tr>
<tr>
<td>UNIX shell</td>
<td>erPosixShell</td>
<td>✓</td>
</tr>
<tr>
<td>Account expiration date</td>
<td>erPosixExpireDate</td>
<td>✓</td>
</tr>
<tr>
<td>Force a password change</td>
<td>erPosixForcePwdChange</td>
<td>✓</td>
</tr>
<tr>
<td>Primary group</td>
<td>erPosixPrimaryGroup</td>
<td>✓</td>
</tr>
<tr>
<td>Secondary group</td>
<td>erPosixSecondGroup</td>
<td>✓</td>
</tr>
<tr>
<td>Groups that can use the su command on this user</td>
<td>erPosixSuGroup</td>
<td>✓</td>
</tr>
<tr>
<td>Groups to be administered</td>
<td>erPosixAdmGroups</td>
<td>✓</td>
</tr>
<tr>
<td>Home directory</td>
<td>erPosixHomeDir</td>
<td>✓</td>
</tr>
<tr>
<td>Password maximum age</td>
<td>erPosixMaxPwdAge</td>
<td>✓</td>
</tr>
<tr>
<td>Password minimum age</td>
<td>erPosixMinPwdAge</td>
<td>✓</td>
</tr>
</tbody>
</table>
### Table 7. Account form attributes (continued)

<table>
<thead>
<tr>
<th>Attribute name on the UNIX and Linux operating system account form on IBM Security Identity Manager</th>
<th>Attribute name on the IBM Tivoli Directory Server</th>
<th>Supported operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password warning age</td>
<td>erPosixPwdWarnAge</td>
<td>AIX</td>
</tr>
<tr>
<td>Administrative roles</td>
<td>erPosixRoles</td>
<td>✓</td>
</tr>
<tr>
<td>Additional mandatory methods for authenticating the user</td>
<td>erPosixAuth1</td>
<td>✓</td>
</tr>
<tr>
<td>Additional optional methods for authenticating the user</td>
<td>erPosixAuth2</td>
<td>✓</td>
</tr>
<tr>
<td>Allow at jobs</td>
<td>erPosixAT</td>
<td>✓</td>
</tr>
<tr>
<td>Allow cron jobs</td>
<td>erPosixCron</td>
<td>✓</td>
</tr>
<tr>
<td>Audit class</td>
<td>erPosixAuditClasses</td>
<td>✓</td>
</tr>
<tr>
<td>Allow user to execute daemon process</td>
<td>erPosixDaemonAllowed</td>
<td>✓</td>
</tr>
<tr>
<td>Allow user to log in to the system</td>
<td>erPosixLoginAllowed</td>
<td>✓</td>
</tr>
<tr>
<td>Can another user switch user to this user</td>
<td>erPosixSuGroup</td>
<td>✓</td>
</tr>
<tr>
<td>Is this user an administrator</td>
<td>erPosixAdminUser</td>
<td>✓</td>
</tr>
<tr>
<td>Soft limit for the largest core size</td>
<td>erPosixSoftCore</td>
<td>✓</td>
</tr>
<tr>
<td>Soft limit for the maximum amount of CPU utilization</td>
<td>erPosixSoftCPU</td>
<td>✓</td>
</tr>
<tr>
<td>Soft limit for largest data segment</td>
<td>erPosixSoftData</td>
<td>✓</td>
</tr>
<tr>
<td>Soft limit for the largest file size</td>
<td>erPosixSoftFileSize</td>
<td>✓</td>
</tr>
<tr>
<td>Soft limit for the largest stack segment</td>
<td>erPosixSoftStack</td>
<td>✓</td>
</tr>
<tr>
<td>Largest core size</td>
<td>erPosixHardCore</td>
<td>✓</td>
</tr>
<tr>
<td>Maximum CPU utilization</td>
<td>erPosixHardCPU</td>
<td>✓</td>
</tr>
<tr>
<td>Largest data segment</td>
<td>erPosixHardData</td>
<td>✓</td>
</tr>
<tr>
<td>Largest file size</td>
<td>erPosixHardFileSize</td>
<td>✓</td>
</tr>
<tr>
<td>Largest stack segment</td>
<td>erPosixHardStack</td>
<td>✓</td>
</tr>
<tr>
<td>Allowed login time</td>
<td>erPosixLoginTimes</td>
<td>✓</td>
</tr>
</tbody>
</table>
Table 7. Account form attributes (continued)

<table>
<thead>
<tr>
<th>Attribute name on the UNIX and Linux operating system account form on IBM Security Identity Manager</th>
<th>Attribute name on the IBM Tivoli Directory Server</th>
<th>Supported operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed number of login retries before locking the account</td>
<td>erPosixLoginRetries</td>
<td>✓  ✓  ✓</td>
</tr>
<tr>
<td>Maximum number of days (weeks for AIX) the account can remain valid after the password expires</td>
<td>erPosixPwdMaxAge</td>
<td>✓  ✓</td>
</tr>
<tr>
<td>Minimum number of alphabetic characters in password</td>
<td>erPosixPwdMinAlphaChar</td>
<td></td>
</tr>
<tr>
<td>Minimum difference between the current and last password</td>
<td>erPosixPwdMinDiff</td>
<td>✓</td>
</tr>
<tr>
<td>Maximum number of characters that can be repeated in a password</td>
<td>erPosixPwdMaxRepeats</td>
<td></td>
</tr>
<tr>
<td>Minimum length of the password</td>
<td>erPosixPwdMinLen</td>
<td>✓</td>
</tr>
<tr>
<td>Password restriction methods</td>
<td>erPosixPwdCheck</td>
<td>✓</td>
</tr>
<tr>
<td>Password dictionaries used to restrict passwords</td>
<td>erPosixPwdDiction</td>
<td></td>
</tr>
<tr>
<td>Number of previous passwords that cannot be reused</td>
<td>erPosixPwdHistory</td>
<td>✓</td>
</tr>
<tr>
<td>Time for which a user cannot reuse passwords</td>
<td>erPosixPwdHistoryExpire</td>
<td>✓</td>
</tr>
<tr>
<td>Account last accessed on</td>
<td>erPosixLastAccessDate</td>
<td>✓  ✓  ✓  ✓</td>
</tr>
<tr>
<td>Valid terminals allowed to access the account</td>
<td>erPosixValidTtys</td>
<td>✓</td>
</tr>
<tr>
<td>System authentication mechanism for the user</td>
<td>erPosixRegistry</td>
<td></td>
</tr>
<tr>
<td>Number of days the account can remain idle</td>
<td>erPosixIdleDays</td>
<td>✓</td>
</tr>
<tr>
<td>sudo privileges</td>
<td>erPosixSudoPrivileges</td>
<td>✓  ✓  ✓  ✓</td>
</tr>
<tr>
<td>Allow duplicate UIDs</td>
<td>erPosixDupUid</td>
<td>✓  ✓  ✓  ✓</td>
</tr>
</tbody>
</table>
**Table 7. Account form attributes (continued)**

<table>
<thead>
<tr>
<th>Attribute name on the UNIX and Linux operating system account form on IBM Security Identity Manager</th>
<th>Attribute name on the IBM Tivoli Directory Server</th>
<th>Supported operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is No Password Account?</td>
<td>erPosixNpAccount</td>
<td>✓</td>
</tr>
<tr>
<td>Do Not Create User Private Group</td>
<td>erPosixPrivateGroup</td>
<td>✓</td>
</tr>
<tr>
<td>Hosts on which user will be able to login</td>
<td>erPosixHostsAllowedLogin</td>
<td>✓</td>
</tr>
<tr>
<td>Hosts on which user will not be able to login</td>
<td>erPosixHostsDeniedLogin</td>
<td>✓</td>
</tr>
<tr>
<td>Create home directory while creating the account</td>
<td>erPosixDefaultHomedir</td>
<td>✓</td>
</tr>
<tr>
<td>Minimum number of non-alphabetic characters in password</td>
<td>erPosixPwdMinOtherChar</td>
<td>✓</td>
</tr>
<tr>
<td>Command used to query failed logins</td>
<td>erPosixFailedLoginCmd</td>
<td>✓</td>
</tr>
<tr>
<td>File or directory where failed login records are found</td>
<td>erPosixFailedLoginTallyLoc</td>
<td>✓</td>
</tr>
<tr>
<td>Maximum failed logins allowed</td>
<td>erPosixMaxFailedLogins</td>
<td>✓</td>
</tr>
<tr>
<td>Delete user account even when it is in use</td>
<td>erPosixDelUserInUse</td>
<td>✓</td>
</tr>
</tbody>
</table>

**UNIX and Linux Adapter service form attributes**

You must create a service for the UNIX and Linux Adapter before the IBM Security Identity Manager server can use the adapter.

IBM Security Identity Manager uses the adapter to communicate with the managed resource. The following table lists:

- The attributes that are displayed on the UNIX or Linux operating system service form on IBM Security Identity Manager.
- The corresponding names on the IBM Tivoli Directory Server.
- The supported operating systems.
<table>
<thead>
<tr>
<th>Attribute name on the UNIX and Linux operating systems service form on IBM Security Identity Manager</th>
<th>Attribute name on the IBM Tivoli Directory Server</th>
<th>Supported operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service name</td>
<td>erServiceName</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Description</td>
<td>description</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Tivoli Directory Integrator location</td>
<td>erITDIurl</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Managed resource location</td>
<td>erURL</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>User registry</td>
<td>erPosixRegistry</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Delete home directory when the account is deleted?</td>
<td>erPosixHomeDirRemove</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Owner</td>
<td>owner</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Service prerequisite</td>
<td>erPre requisite</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Administrator name</td>
<td>erServiceUid</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Is sudo user?</td>
<td>erPosixUseSudo</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Return sudo privileges?</td>
<td>erPosixReturnSudoPrivileges</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Path to the sudoers file</td>
<td>erPosixSudoersPath</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Authentication method</td>
<td>erPosixAuthMethod</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Password</td>
<td>erPassword</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Passphrase (Required for key based authentication)</td>
<td>erPosixPassphrase</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Private key file (Required for key based authentication)</td>
<td>erPosixPKFile</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Use a shadow file?</td>
<td>erPosixUseShadow</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Disable AL Caching</td>
<td>erPosixDisableALCache</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>AL File System Path</td>
<td>erPosixALFileSystemPath</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Max Connection Count</td>
<td>erPosixMaxConnectionCnt</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Case Insensitive filter</td>
<td>erLdapCaseInsensitiveFilter</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Execute user profile?</td>
<td>erPosixExecuteUserProfile</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Command used to query failed logins</td>
<td>erPosixFailedLoginCmd</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td></td>
<td>erPosixFailedLoginTallyLoc</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td></td>
<td>erPosixMaxFailedLogins</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
</tbody>
</table>
UNIX and Linux Adapter group form attributes

You can manage UNIX groups from IBM Security Identity Manager.

The following table lists:

- The attributes that are displayed on the UNIX and Linux operating system group form on IBM Security Identity Manager.
- The corresponding names on the IBM Tivoli Directory Server.
- The supported operating systems.

Table 9. Group form attributes

<table>
<thead>
<tr>
<th>Attribute name on the UNIX and Linux operating systems group form on IBM Security Identity Manager</th>
<th>Attribute name on the IBM Tivoli Directory Server</th>
<th>Supported operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group name</td>
<td>erPosixGroupName</td>
<td>✓ AIX ✓ HP-UX ✓ Linux ✓ Solaris</td>
</tr>
<tr>
<td>Group ID number</td>
<td>erPosixGroupId</td>
<td>✓ AIX ✓ HP-UX ✓ Linux ✓ Solaris</td>
</tr>
<tr>
<td>Administrator group</td>
<td>erPosixGroupIsAdmGrp</td>
<td>✓ AIX ✓ HP-UX ✓ Linux ✓ Solaris</td>
</tr>
<tr>
<td>Group administrators</td>
<td>erPosixGroupAdmin</td>
<td>✓ AIX ✓ HP-UX ✓ Linux ✓ Solaris</td>
</tr>
<tr>
<td>Group projects</td>
<td>erPosixGroupProjects</td>
<td>✓ AIX ✓ HP-UX ✓ Linux ✓ Solaris</td>
</tr>
<tr>
<td>Define an Access</td>
<td>No LDAP attribute exists. However, these other access attributes can be set:</td>
<td>✓ AIX ✓ HP-UX ✓ Linux ✓ Solaris</td>
</tr>
<tr>
<td>Enable Access</td>
<td>erAccessOption = 2</td>
<td>✓ AIX ✓ HP-UX ✓ Linux ✓ Solaris</td>
</tr>
<tr>
<td>Enable Common Access</td>
<td>erAccessOption = 3</td>
<td>✓ AIX ✓ HP-UX ✓ Linux ✓ Solaris</td>
</tr>
<tr>
<td>Disable Access</td>
<td>erAccessOption = 1</td>
<td>✓ AIX ✓ HP-UX ✓ Linux ✓ Solaris</td>
</tr>
<tr>
<td>Access name</td>
<td>erAccessName</td>
<td>✓ AIX ✓ HP-UX ✓ Linux ✓ Solaris</td>
</tr>
<tr>
<td>Access type</td>
<td>erObjectProfileName</td>
<td>✓ AIX ✓ HP-UX ✓ Linux ✓ Solaris</td>
</tr>
<tr>
<td>Access description</td>
<td>erAccessDescription</td>
<td>✓ AIX ✓ HP-UX ✓ Linux ✓ Solaris</td>
</tr>
<tr>
<td>Access owner</td>
<td>owner</td>
<td>✓ AIX ✓ HP-UX ✓ Linux ✓ Solaris</td>
</tr>
<tr>
<td>Approval workflow</td>
<td>erApprovalProcessID</td>
<td>✓ AIX ✓ HP-UX ✓ Linux ✓ Solaris</td>
</tr>
<tr>
<td>Notify users when access is provisioned and available for use</td>
<td>erNotifyAccessProvision</td>
<td>✓ AIX ✓ HP-UX ✓ Linux ✓ Solaris</td>
</tr>
</tbody>
</table>
Table 9. Group form attributes (continued)

<table>
<thead>
<tr>
<th>Attribute name on the UNIX and Linux operating systems group form on IBM Security Identity Manager</th>
<th>Attribute name on the IBM Tivoli Directory Server</th>
<th>Supported operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify users when access is de-provisioned</td>
<td>erNotifyAccessDeprovision</td>
<td>✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Allow duplicate group IDs</td>
<td>erPosixGroupDupGid</td>
<td>✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>sudo privileges</td>
<td>erPosixSudoPrivileges</td>
<td>✓ ✓ ✓ ✓</td>
</tr>
</tbody>
</table>

UNIX and Linux Adapter role form attributes

You can manage AIX roles from IBM Security Identity Manager.

The following table lists:

- The attributes that are displayed on the UNIX and Linux operating system group form on IBM Security Identity Manager.
- The corresponding names on the IBM Tivoli Directory Server.
- The supported operating systems.

Table 10. Role form attributes

<table>
<thead>
<tr>
<th>Attribute name on the UNIX and Linux operating systems group form on IBM Security Identity Manager</th>
<th>Attribute name on the IBM Tivoli Directory Server</th>
<th>Supported operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX role name</td>
<td>erPosixRoleName</td>
<td>✓</td>
</tr>
<tr>
<td>Authorizations</td>
<td>erPosixRoleAuthorizations</td>
<td>✓</td>
</tr>
<tr>
<td>Roles implied</td>
<td>erPosixRolelist</td>
<td>✓</td>
</tr>
<tr>
<td>List of groups</td>
<td>erPosixRoleGroups</td>
<td>✓</td>
</tr>
<tr>
<td>Visibility</td>
<td>erPosixRoleVisibility</td>
<td>✓</td>
</tr>
<tr>
<td>Define an Access</td>
<td>No LDAP attribute exists. However, you can set the erAccessOption access attribute.</td>
<td>✓</td>
</tr>
<tr>
<td>Access name</td>
<td>No LDAP attribute exists. However, you can set the erAccessName access attribute.</td>
<td>✓</td>
</tr>
<tr>
<td>Access type</td>
<td>No LDAP attribute exists. However, you can set the erObjectProfileName access attribute.</td>
<td>✓</td>
</tr>
</tbody>
</table>
Table 10. Role form attributes (continued)

<table>
<thead>
<tr>
<th>Attribute name on the UNIX and Linux operating systems group form on IBM Security Identity Manager</th>
<th>Attribute name on the IBM Tivoli Directory Server</th>
<th>Supported operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>AIX</td>
</tr>
<tr>
<td>Access description</td>
<td>No LDAP attribute exists. However, you can set the erAccessDescription access attribute.</td>
<td>✓</td>
</tr>
<tr>
<td>Access owner</td>
<td>No LDAP attribute exists. However, you can set the owner access attribute.</td>
<td>✓</td>
</tr>
<tr>
<td>Approval workflow</td>
<td>No LDAP attribute exists. However, you can set the erApprovalProcessID access attribute.</td>
<td>✓</td>
</tr>
<tr>
<td>Notify users when access is provisioned and available for use</td>
<td>No LDAP attribute exists. However, you can set the erNotifyAccessProvision access attribute.</td>
<td>✓</td>
</tr>
<tr>
<td>Notify users when access is de-provisioned</td>
<td>No LDAP attribute exists. However, you can set the erNotifyAccessDeprovision access attribute.</td>
<td>✓</td>
</tr>
</tbody>
</table>
Appendix B. Definitions for ITDI_HOME and ISIM_HOME directories

**ITDI_HOME** is the directory where Tivoli Directory Integrator is installed. **ISIM_HOME** is the directory where IBM Security Identity Manager is installed.

**ITDI_HOME**

This directory contains the jars/connectors subdirectory that contains files for the adapters.

**Windows**

`drive\Program Files\IBM\TDI\ITDI_VERSION`

For example the path for version 7.1:

`C:\Program Files\IBM\TDI\V7.1`

**UNIX**

`/opt/IBM/TDI/ITDI_VERSION`

For example the path for version 7.1:

`/opt/IBM/TDI/V7.1`

**ISIM_HOME**

This directory is the base directory that contains the IBM Security Identity Manager code, configuration, and documentation.

**Windows**

`path\IBM\isim`

**UNIX**

`path/IBM/isim`
Appendix C. Support information

You have several options to obtain support for IBM products.

- “Searching knowledge bases”
- “Obtaining a product fix” on page 42
- “Contacting IBM Support” on page 42

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 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
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/](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 technote, 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.
     - b. Open ISA.
c. Click Collection and Send Data.
d. Click the Service Requests tab.
e. Click Open a New Service Request.

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

**Results**

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

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

Accessibility features

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

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

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

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

Related accessibility information

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

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

IBM and accessibility

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

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

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

**Trademarks**

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

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

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

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

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

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

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

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

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

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

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

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

roles  (continued)
deleting  23
management tasks  17
modifying  22
optional attributes  21
unassigning users  15

S
service form attributes  31, 34
su command
groups  11
su command, groups  11
sudo
restrictions  14
user privileges  13
support contact information  42
support data
attributes
primary group  11
secondary group  11
reconciliation  5
retrieval by adapter  5
suspending user accounts  15

T
terminology ix
training x
troubleshooting  25
contacting support  42
error messages  27
getting fixes  42
identifying problems  25
searching knowledge bases  41
support website x
techniques  25
techniques for  25
warning messages  27

U
unassigning
users from groups  15
users from roles  15
UNIX
account form attributes  31
group form attributes  31, 36
service form attributes  34
user accounts
adding  7
changing passwords  15
deleting  15
lifespan  11
modifying  14
reconciling  6
restoring  15
suspending  15
users
assigning groups  11
roles  11
unassigning from groups  15
unassigning from roles  15