IBM Security Identity Manager
Version 7.0.0.2

Configuration Topics

IBM Security Identity Manager
Version 7.0.0.2

Configuration Topics

IBM

Table of contents

Table list

Chapter 1. Virtual appliance configuration

For your virtual appliance, you can manage external entities, server settings, cluster settings, or advanced settings. The configuration settings can be for the feed file upload, database, directory server, directory integrator, mail server, server properties, external user registry, custom file, library and workflow extension, or others.

To configure the IBM® Security Identity Manager settings for the virtual appliance, log on to the **Appliance Dashboard** at `https://`*`isimva_hostname`*`.` For example: `https://isimva1.jk.example.com`.

Note: Before you make any configuration changes on the virtual appliance, take a snapshot of a working virtual appliance. See Managing the snapshots.

Do the following tasks to configure the IBM Security Identity Manager virtual appliance.

Managing the directory server configuration

Use the Directory Server Configuration page to configure the directory server in the IBM Security Identity Manager virtual appliance.

Before you begin

Complete the following tasks:

- Installation and configuration of a directory server.
- Create the directory server DN location.

About this task

Configure or reconfigure the directory server options. See Table 1.

Table 1. Directory Server configuration details

Button	Directory server options
Configure	**Host name** Specify the name of the server that hosts the directory server. The acceptable formats for the host name are IPv4, FQDN, and IPv6. For example, `isimldap.example.com`. **Port** Specify the directory service port. For example, `389`. You can select or clear the **SSL** check box to manage the secure connection. **Principal DN** Specify the principal distinguished name. For example, `cn=root`. **Password** Specify the password for the directory server. **Organization name** Specify the name of the enterprise or the organization. For example, `JK Enterprises`. **Default organization short name** Specify the abbreviation or short form of the organization name. For example, `jke`. **IBM Security Identity Manager DN Location** Specify the directory server DN location. For example, `dc=com`.

Table 1. Directory Server configuration details (continued)

Button	Directory server options
Reconfigure	**Host name** Specify the name of the server that hosts the directory server. The acceptable formats for the host name are IPv4, FQDN, and IPv6. For example, `isimldap.example.com`. **Port** Specify the directory service port. For example, `389`. You can select or clear the **SSL** check box to manage the secure connection. **Principal DN** Specify the principal distinguished name. For example, `cn=root`. **Password** Specify the password for the directory server.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage External Entities** > **Directory Server Configuration**. The Directory Server Configuration page displays the Directory Server Configuration table.
2. Click **Configure**.
3. In the Directory Server configuration details window, specify the expected variable values. For more information, see Table 1 on page 2.
4. Click **Save Configuration** to complete this task.

   A window with certificate information is displayed if you selected the **SSL** check box during configuration.
5. Click **Yes** to confirm.

   Note: The directory server reconfiguration takes some time. Do not refresh or close the page. Wait for the reconfiguration process to complete.
6. Optional: To reconfigure an existing directory server configuration, do these steps:

   Note: Before you reconfigure, create a snapshot to recover from any configuration failures. See Managing the snapshots.

   a. From the Directory Server Configuration table, select a record. For example, `IBM Security Identity Manager User Registry`.

   b. Click **Reconfigure**.

   c. In the Edit directory server configuration details window, edit the configuration variables. For more information, see Table 1 on page 2.

   d. Click **Save Configuration**. A window opens that displays the certificate information.

   e. Click **Yes** to confirm.

Note: The directory server reconfiguration takes some time. Do not refresh or close the page. Wait for the reconfiguration process to complete.

7. Optional: To unconfigure an existing directory server configuration, do these steps:
   a. From the Directory Server Configuration table, select a record.
   b. Click **Unconfigure**.
   c. Click **Yes** to confirm the deletion.

Managing the database server configuration

Use the Database Server Configuration page to configure, reconfigure, or unconfigure the database server for the IBM Security Identity Manager virtual appliance.

About this task

Configure or reconfigure the Identity data store options for the database server. See Table 2 on page 5.

Table 2. Identity data store configuration

Button	Data store options
Configure	**Database type** Select the database type from the list. To configure the database server, select **IBM DB2**. **Host name** Specify the name of the server that hosts the data store. The acceptable formats for the host name are FQDN, IPv4, or IPv6. For example: `isimidstore.example.com`. **Port** Specify the data store service port. For example: `51000`. You can select or clear the **SSL** check box to manage the secure connection. **Database name** Specify the name of the IBM Security Identity Manager database. Example: `isimdb`. **Database Administrator ID** Specify the user with database administrator privileges. For example: `isiminst`. **Note:** During the database configuration for a virtual appliance, the user must be the database owner. For example, `isiminst`. This database owner must be the same user who created the database. **Database Administrator Password** Specify the password for the user with database administrator privileges. **Database User ID** Specify the user ID for the Identity data store database that you created. **Database User Password** Specify the password for the Identity data store user ID.

Table 2. Identity data store configuration (continued)

Button	Data store options
Reconfigure	**Note:** Reconfiguration does not update the database schema. It configures only the IBM Security Identity Manager with new database details. **Host name** Specify the name of the server that hosts the data store. For example: `isimidstore1.example.com`. **Port** Specify the data store service port. For example: `60000`. You can select or clear the **SSL** check box to manage the secure connection. **Database Administrator Password** Specify the password for the user with database administrator privileges. **Database User Password** Specify the password for the Identity data store user ID.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage External Entities** > **Database Server Configuration**. The Database Server Configuration page displays the Database Server Configuration table.
2. Click **Configure**.
3. In the Database Server Configuration Details window, specify the expected variable values. For more information, see Table 2 on page 5.
4. Click **Save Configuration** to complete this task.

   A window with certificate information is displayed if you selected the **SSL** check box during configuration.
5. Click **Yes** to confirm.

   Note: The database server configuration takes some time. Do not refresh or close the page. Wait for the configuration process to complete.
6. Optional: To reconfigure an existing database server configuration, do these steps:

   Note: Before you reconfigure, create a snapshot to recover from any configuration failures. See Managing the snapshots.

   a. From the Database Server Configuration table, select a record. For example, `Identity data store`.

   b. Click **Reconfigure**.

   c. In the Edit Identity data store details window, edit the details. For more information, see Table 2 on page 5.

   d. Click **Save Configuration**. A window opens that displays the certificate information.

   e. Click **Yes** to confirm.

Note: The database server reconfiguration takes some time. Do not refresh or close the page. Wait for the reconfiguration process to complete.

7. Optional: To unconfigure an existing identity store, do these steps:
   a. From the Database Server Configuration table, select a record. For example, `Identity data store`.
   b. Click **Unconfigure**.
   c. Click **Yes** to confirm the deletion.

Managing the Oracle data store configuration

Use the Database Server Configuration page to configure, reconfigure, or unconfigure the Oracle data store for the IBM Security Identity Manager virtual appliance.

About this task

Configure or reconfigure the Identity data store options for the Oracle data store. See Table 3 on page 8.

Table 3. Identity data store configuration

Button	**Data store options**
Configure	**Database type** Select the database type from the list. To configure the Oracle data store, select **Oracle**. **Host name** Specify the name of the server that hosts the data store. The acceptable formats for the host name are FQDN, IPv4, or IPv6. For example: `isimidstore.example.com`. **Port** Specify the data store service port. For example: `1521`. **Oracle SID or Service name** Specify the Oracle System ID (SID) or the service name to identify the database. For example, `isimdb`. Select or clear the **Service name** check box to manage the following aspects: • If you select the check box, the value is treated as service name. • If you do not select the check box, the value is treated as SID. **Database Administrator ID** Specify the user with database administrator privileges. For example: `isiminst`. **Note:** During the database configuration for a virtual appliance, the user must be the database owner. For example, `isiminst`. This database owner must be the same user who created the database. **Database Administrator Password** Specify the password for the user with database administrator privileges. **Database User ID** Specify the user ID for the Identity data store database that you created. **Database User Password** Specify the password for the Identity data store user ID.

Table 3. Identity data store configuration (continued)

Button	Data store options
Reconfigure	**Note:** Reconfiguration does not update the database schema. It configures only the IBM Security Identity Manager with new database details. **Host name** Specify the name of the server that hosts the data store. For example: `isimidstore1.example.com`. **Port** Specify the data store service port. For example: `1521`. **Database Administrator Password** Specify the password for the user with database administrator privileges. **Database User Password** Specify the password for the Identity data store user ID.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage External Entities** > **Database Server Configuration**. The Database Server Configuration page displays the Database Server Configuration table.
2. Click **Configure**.
3. In the Database Server Configuration Details window, specify the expected variable values. See Table 3 on page 8.
4. Click **Save Configuration** to complete this task.
5. Optional: To reconfigure an existing Oracle data store configuration, do these steps:

   Note: Before you reconfigure, create a snapshot to recover from any configuration failures. See Managing the snapshots.

   a. From the Database Server Configuration table, select a record. For example, `Oracle data store`.
   b. Click **Reconfigure**.
   c. In the Edit Identity data store details window, edit the variable values. See Table 3 on page 8.
   d. Click **Save Configuration**.
6. Optional: To unconfigure an existing Oracle data store, do these steps:
   a. From the Database Server Configuration table, select a record. For example, `Oracle data store`.
   b. Click **Unconfigure**.
   c. Click **Yes** to confirm the deletion.

Managing the SSL certificate configuration

Use the SSL Certificate Management page to import any SSL certificate in the application server truststore of the IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage External Entities** > **SSL Certificate Management** to display the SSL Certificate Management page. The SSL Certificate Management page displays the certificate details.
2. On the SSL Certificate Management page, do one of these actions to work with certificates. See Table 4.

Table 4. SSL certificate actions

Button	SSL certificate actions
New	To import a certificate, do these steps: 1. Click **New** to open the Import Certificate window. 2. On the Import Certificate window, do these steps. a. Specify an alias name in **Certificate alias**. For example, `tdicert`. b. Click **Browse** next to the **File** field to search and select the certificate file that you want to import. 3. Click **Save Configuration**. **Note:** You can import multiple certificates. When you import a new certificate, do not specify the same alias name that exists.
Edit	To edit a certificate, do these steps: 1. From the SSL certificate table, select the certificate that you want to edit. 2. Click **Edit** to open the Import Certificate window. **Note:** The **certificate alias** field is read-only. 3. On the Import Certificate window, click **Browse** next to the **File** field to search and select the certificate file that you want to import. 4. Click **Save Configuration**.
View	To view the certificate details, do these steps: 1. From the SSL certificate table, select the certificate that you want to view. 2. Click **View** to display the certificate details window.

Managing the mail server configuration

Use the Mail Server Configuration page to configure the email notifications for the IBM Security Identity Manager virtual appliance.

About this task

Configure or reconfigure the mail server options. See Table 5.

Table 5. Mail Server Configuration

Button	Mail Server options
Configure	**Mail server** Specify the name of the server that hosts the mail server. For example, `mailserver.com`. The acceptable formats for the mail server are FQDN, IPv4, and IPv6. **Port** The service port of the mail server, which is `25`. **Mail from** Specify the email address from which the email is sent. For example, `admin@in.ibm.com`.
Reconfigure	**Mail server** Specify the name of the server that hosts the mail server. For example, `mailserver1.com`. The acceptable formats for the mail server are FQDN, IPv4, and IPv6. **Mail from** Specify the address from which the email is sent. For example, `admin1@in.ibm.com`.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Configure** > **Manage Server Setting** > **Mail Server Configuration**. The Mail Server Configuration page displays the Mail Server Configuration table.
2. Click **Configure**.
3. In the Mail Server Configuration Details window, specify the expected variable values. For information, see Table 5.
4. Click **Save Configuration** to complete this task.
5. Optional: To reconfigure an existing mail server configuration, do these steps:
   a. From the Mail Server Configuration table, select a record. For example, `Mail Configuration`.
   b. Click **Reconfigure**.
   c. In the Edit Mail Configuration Details window, edit the details. For more information, see Table 5.
   d. Click **Save Configuration**.
6. Optional: To unconfigure an existing mail server configuration, do these steps:
   a. From the Mail Server Configuration table, select a record.
   b. Click **Unconfigure**.
   c. Click **Yes** to confirm the deletion.

Managing the feed files

You can upload feed files and use them in the IBM Security Identity Manager virtual appliance as long as you put them in the prescribed location.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Configure** > **Manage Server Setting** > **Upload Feed File**.
2. On the Upload Feed File page, click **New**.
3. In the Upload Feed File window, click **Browse** to search and upload the feed file. The feed files are in `/userdata/identity/feeds`.

   The `/userdata/identity/feeds` location is mandatory while you create the feed in IBM Security Identity Manager Console.
4. Click **Save Configuration**.
5. Optional: To delete a feed file, do these steps:
   a. Select a file name.
   b. Click **Delete**.
   c. Click **Yes** to confirm.

Configuring the Identity external user registry

Use the Identity External User Registry Configuration page to configure or reconfigure the external user registry for the IBM Security Identity Manager virtual appliance.

Before you begin

Make sure to add the required users to the Identity external user registry before you work from the Identity External User Registry Configuration page.

For more information, see Adding required users to the external user registry.

About this task

Configure or reconfigure the external user registry options. See Table 6.

Table 6. Identity external user registry configuration details

Button	Identity external user registry options
Configure	**External registry type** Select an external registry type from the list: • IBM Security Directory Server • Oracle Directory Server • Microsoft Active Directory **Host name** Specify the name of the server that hosts the directory server. The acceptable formats for the host name are FQDN, IPv4, and IPv6. For example, `isimldap.example.com`. **Port** Specify the directory service port. For example, `389`. You can select or clear the **SSL** check box to manage the secure connection. **Principal DN** Specify the principal distinguished name. For example, `cn=root`. **Password** Specify the password for the principal distinguished name. **External registry DN location** Specify the location of the external registry DN. For example, `dc=com`. **Identity Manager system user** Specify the name for the IBM Security Identity Manager system user. For example, `isimsystem`. **Identity Manager system user password** Specify the password for the IBM Security Identity Manager system user. **User Filter** Filters the registry for the IBM Security Identity Manager user. Specify the LDAP filter that is based on the directory server attributes.

Table 6. Identity external user registry configuration details (continued)

Button	Identity external user registry options
Reconfigure	**External registry type** Select an external registry type from the list: • IBM Security Directory Server • Microsoft Active Directory • Oracle Directory Server **Host name** Specify the name of the server that hosts the directory server. The acceptable formats for the host name are FQDN, IPv4, and IPv6. For example, `isimldap.example.com`. **Port** Specify the directory service port. For example, `389`. You can select or clear the **SSL** check box to manage the secure connection. **Principal DN** Specify the principal distinguished name. For example, `cn=root`. **Password** Specify the password for the principal distinguished name. **External registry DN location** Specify the location of the external registry DN. For example, `dc=com`. **Identity Manager system user** Specify the name for the IBM Security Identity Manager system user. For example, `isimsystem`. **Identity Manager system user password** Specify the password for the IBM Security Identity Manager system user. **User Filter** Filters the registry for the IBM Security Identity Manager system user. Specify the LDAP filter that is based on the directory server attributes.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage Server Setting** > **Identity External User Registry Configuration**. The Identity External User Registry Configuration page displays the Identity External User Registry Configuration table.
2. Click **Configure**.
3. In the Identity External User Registry Configuration Details window, specify the expected variable values. For more information, see Table 6 on page 13.
4. Click **Save Configuration** to complete this task.

A window with certificate information is displayed if you selected the **SSL** check box during configuration.

5. Click **Yes** to confirm.

   Note: The external user registry configuration takes some time. Do not refresh or close the page. Wait for the configuration process to complete.
   A message in the **Notifications** widget indicates you to restart the IBM Security Identity Manager Server.
6. From the **Server Control** widget, do these steps.
   a. Select **Security Identity Manager server**.
   b. Click **Restart**.

   See Viewing the Server Control widget.
7. Synchronize the member nodes of the cluster with the primary node. See "Synchronizing a member node with a primary node" on page 19.
8. From the **Server Control** widget, restart the IBM Security Identity Manager Server again on the primary node.
9. Log on to the IBM Security Identity Manager Console from the primary node by using the Identity external user registry user credentials.
10. Optional: To reconfigure an existing Identity external user registry, do these steps:

    Note: Before you reconfigure, create a snapshot to recover from any configuration failures. See Managing the snapshots.
    a. From the Identity External User Registry Configuration table, select a record. For example, `IBM Security Identity Manager User Registry`.
    b. Click **Reconfigure**.
    c. In the Edit Identity External User Registry Configuration Details window, edit the configuration variables. For more information, see Table 6 on page 13.
    d. Click **Save Configuration** to complete this task. A window opens that displays the certificate information.
    e. Click **Yes** to confirm.

       Note: The external user registry reconfiguration takes some time. Do not refresh or close the page. Wait for the reconfiguration process to complete.

Managing the single sign-on configuration

Use the Single Sign-On Configuration page to configure or reconfigure the single sign-on for the IBM Security Identity Manager virtual appliance.

About this task

Configure or reconfigure the single sign-on options. See Table 7.

Table 7. Single Sign-On configuration details

Button	Single Sign-On options

Configure	**Policy server detail**
	A list of IBM Security Access Manager policy servers to which the application server can communicate. The format of this entry is host name, TCP/IP port number, and numerical rank, which is separated by colons. Multiple servers can be specified by separating them with commas.
	For example, the following 2 policy servers both use the available default TCP/IP port 7135.
	`primary.myco.com:7135:1,secondary.myco.com:7135:2`
	The host name of policy server with rank 1 is used to configure the Java™ Runtime Environment component for IBM Security Access Manager.
	Authorization server detail
	A list of IBM Security Access Manager authorization servers to which the application server can communicate. The format of this entry is host name, TCP/IP port number, and numerical rank, which is separated by colons. Multiple servers can be specified by separating them with commas.
	For example, the following 2 authorization servers both use the available default TCP/IP port 7136.
	`secazn.myco.com:7136:2,primazn.myco.com:7136:1`
	IBM Security Access Manager administrator
	An IBM Security Access Manager user with administrative privileges. This parameter is required.
	IBM Security Access Manager administrator password
	The password that is associated with the specified IBM Security Access Manager administrative user.
	IBM Security Access Manager user
	The IBM Security Access Manager user that you created from this link: http://www-01.ibm.com/support/knowledgecenter/SSRMWJ_7.0.0/com.ibm.isim.doc_7.0/securing/tsk/tsk_ic_security_sing_tai_tamuser.htm
	Account Mapping
	Single sign-on, account mapping occurs between IBM Security Access Manager and IBM Security Identity Manager during login authentication. The values are as follows:
	True No mapping is attempted. The IBM Security Access Manager user account that is passed in the `iv-user` HTTP request header must be identical to an IBM Security Identity Manager user account. This user account is defined in theIBM Security Identity Manager directory for the user to log in to IBM Security Identity Manager.
	False The IBM Security Access Manager user account that is passed in the `iv-user` HTTP request header searches the IBM Security Access Manager directory for a matching IBM Security Identity Manager user account. For more information, see: http://www-01.ibm.com/support/knowledgecenter/SSRMWJ_7.0.0/com.ibm.isim.doc_7.0/securing/cpt/cpt_ic_security_sing_tai_acctmap.htm
	Logout page
	This option is for the IBM Security Identity Manager logout page for its console and the self-service user interface. You can use the default logout page that is provided with IBM Security Identity Manager, or provide your own logout page.
	Webseal default
	This logout option is the most secure. Use it when you want the following combined behavior when you click **Logoff**:
	• End the logon session.
	• End the logon session, and the `pkmslogout` function is started.
	Single Sign-On default
	Use this logout page for the following combined behavior when you click **Logoff**:
	• End the current logon session and provide a link to return to IBM Security Identity Manager.
	• Remain logged in to IBM Security Access Manager. The `iv-user` HTTP header information is still available. For example, this action provides for continued use of a portal page or a return to IBM Security Access Manager without a logon prompt.
	Other Select this option to specify the logout page that you want to use. In **Specify**, browse to the location to specify the `.jsp` file for the logout page.

Reconfigure	**Policy server detail** Provides a list of IBM Security Access Manager policy servers to which the application server can communicate. The format of this entry is host name, TCP/IP port number, and numerical rank, which is separated by colons. Multiple servers can

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage Server Setting** > **Single Sign-On Configuration**.
2. On the Single Sign-On Configuration page, click **Configure**.
3. In the Single Sign-On Configuration Details window, specify the expected variable values. See Table 7 on page 16.
4. Click **Save Configuration** to complete this task.
5. Optional: To reconfigure a single sign-on record, do these steps:

   Note: Before you reconfigure, create a snapshot to recover from any configuration failures. See Managing the snapshots.

   a. From the Single Sign-On Configuration table, select a record. For example, `Single Sign-On`.

   b. Click **Reconfigure**.

   c. In the Edit Single Sign-On Configuration Details window, edit the configuration variables. See Table 7 on page 16.

   d. Click **Save Configuration** to complete this task.

Managing the cluster node configuration

Use the Cluster Node Configuration page to work with the cluster node. You can remove a node, reconnect a node, and synchronize between a member and primary node.

The **Configure** > **Manage Cluster** menu is displayed only in a cluster environment and not in stand-alone environment.

Removing a node from the cluster

Use the Cluster Node Configuration page to remove a node from the cluster.

About this task

You can remove a member node only from a primary node console, but you cannot remove the primary node from itself.

You might want to remove a damaged or affected node from the cluster configuration. After the node is removed, it no longer functions as part of the cluster unless you add it back to the cluster.

The **Configure** > **Manage Cluster** menu is displayed only in a cluster environment and not in stand-alone environment.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage Cluster** > **Cluster Node Configuration**.
2. Select a member node that you want to remove from the list of available nodes. For example, select `Member node1`.
3. Click **Remove Node**.
4. On the Remove Node window, click **Save Configuration**.

The selected node is temporarily removed from the IBM Security Identity Manager virtual appliance cluster. A message indicates that the selected node is temporarily disconnected from the cluster.

To reconnect the node, see "Reconnecting a node into the cluster."

Note: You must add the temporarily removed member node only to the primary node console from which it was disconnected.

5. Optional: To remove the selected node permanently from the IBM Security Identity Manager virtual appliance cluster, do these steps.
   a. Click **Remove Node**.
   b. On the Remove Node window, select the check box.
   c. Click **Save Configuration**. The selected node is removed from the cluster.
6. Optional: Click **Refresh** to display the recently updated data.

Reconnecting a node into the cluster

Use the Cluster Node Configuration page to reconnect a node into the cluster of the IBM Security Identity Manager virtual appliance.

About this task

Depending on your requirement, you can reconnect a node into the cluster for the following reasons:

- Adding a previously configured node to a cluster to increase scalability.
- A node that was shut off for maintenance is revived and must be introduced back in the cluster.
- If you see a reconnect notification on the **Appliance Dashboard** of a member node.

You can reconnect only a member node back to the cluster from the **Appliance Dashboard** of a member node. You must provide the primary node details to reconnect a node into the cluster.

Note: You must add the temporarily removed member node only to the primary node from which it was disconnected.

The **Configure** > **Manage Cluster** menu is displayed only in a cluster environment and not in a stand-alone environment.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage Cluster** > **Cluster Node Configuration**.
2. On the Cluster Node Configuration page, select the member node record. You can see only the existing member node entry on the Cluster Node Configuration page.
3. Click **Reconnect**. The Reconnect Node window is displayed.
4. On the Reconnect Node window, provide the details for the node that you want to reconnect into the cluster.

   Primary node host name
   The host name of the primary node. For example, `isimva1.jk.example.com`.

Primary node administrator
The user ID of the primary node administrator. For example, `admin`.

Primary node administrator password
The administrator password of the primary node.

5. Click **Yes** to confirm. The member node is reconnected into the cluster.

   Note: Reconnecting a permanently removed member node from the cluster is as good as setting up a new member node in the cluster.
6. Optional: Click **Refresh** to display the recently updated data.

Synchronizing a member node with a primary node

Use the Cluster Node Configuration page to synchronize a member node with a primary node in the IBM Security Identity Manager virtual appliance.

About this task

The **Configure** > **Manage Cluster** menu is displayed only in cluster environment and not in stand-alone environment.

In the primary node virtual appliance console, all nodes in the cluster are displayed in the Cluster Node Configuration table.

In the member node virtual appliance console, only the current member node is displayed in the Cluster Node Configuration table.

Synchronize the following nodes in the cluster for any configuration changes that you make in the IBM Security Identity Manager virtual appliance.

Member node
In the Cluster Node Configuration table of the Cluster Node Configuration page, select a member node for synchronization. The **Synchronize** button is not active until you select a node.

Wait for the synchronization process to complete.

Primary node
In the Cluster Node Configuration page, select one or more member nodes except the primary node for synchronization. The **Synchronize** button is not active when:

- The primary node is selected.
- The status of the selected node is displayed as `Synchronizing` in the **Synchronization State** column of the Cluster Node Configuration table.

The primary node submits the synchronization request to each of the node that was selected. You can view the synchronization status in the **Synchronization State** column of the Cluster Node Configuration table.

Note: Before you do a synchronization operation, address all the notifications on the primary node.

The **Synchronization State** column displays these synchronization states:

Table 8. Synchronization state table

Status	Description	Action
`Not Connected`	Displays when a member node cannot connect to a primary node or when a primary node cannot connect to the member node.	Connect the member node with the primary node. For a node with the `Not Connected` status, click **Reconnect Node** to connect that node into the cluster. See "Reconnecting a node into the cluster" on page 18.
`Not Synchronized`	Displays when the member node is not synchronized with the primary node.	Synchronize the member node with the primary node. See the following procedure.
`Synchronized`	Displays when the member node is synchronized with the primary node.	No action is required.
`Synchronizing`	Displays when the member node is synchronizing with the primary node.	Wait until the synchronization is complete. Click the **Refresh** icon to get the most recent status.
`Not Applicable`	Displays if the cluster node is a primary node because the primary node does not require any synchronization.	No action is required.
`Unknown`	Displays when the deployment manager is down, or when the application on the member node is down.	No action is required.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage Cluster** > **Cluster Node Configuration**.
2. Do the following actions.
   - From the member node virtual appliance console, select the current member node and click **Synchronize** to synchronize it with the primary node.

     A progress bar indicates the synchronization process. It retrieves configuration information from the primary node for any configuration changes and synchronizes within the same node.
   - From the primary node virtual appliance console, select one or more member nodes and click **Synchronize**.

     A synchronization request is submitted to each of the node that was selected.

   The member node is synchronized with the primary node.
3. Optional: Click **Refresh** to display the recently updated data.

Managing custom files

View custom files and folders that are related to the IBM Security Identity Manager virtual appliance.

About this task

Manage your files from the Custom File Management page in these ways:

- Expand or collapse the directory structure to view the different files and folders, including the recently updated files.
- Download or upload any type of file.
- Restore a selected file to the default state.

Note: The `web.xml` file is not available in IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Configure** > **Advanced Configuration** > **Custom File Management**.
2. In the Custom File Management page, do one of these actions to work with your files. See Table 9.

Table 9. File tabs and their actions

Tab	Tab Description	Actions
All Files	Displays a directory structure in the left pane. The right pane displays a list of files in a table that is based on the folder that you selected in the left pane. The right pane contains these buttons: • **Download** • **Upload** • **Refresh** You can use the search box to find a specific property name that you want to update. Type a name or a character string for the properties file in the box to help you narrow your search. Your string search is done within the context of the properties file that you selected. All property names that contain the string are displayed. If you want to return to the full list of property names, clear the search box.	To download a file, do these steps: 1. Select a folder in the left pane to display a list of files in the right pane. 2. Select a file in the table of the right pane. 3. Click **Download** to save the file.
		To upload a file, do these steps: 1. Select a folder in the left pane. 2. Click **Upload** to open the File Upload window. 3. Click **Browse** to search and select the file. 4. Click **Save Configuration**.
		To display the most recent version of the data, including changes that were made to the data since it was last refreshed, click **Refresh**.
Modified Files	Displays all the modified files in a table, including these buttons: • **Restore Default** • **Refresh**	To restore a file, do these steps: 1. Select a file from the table. 2. Click **Restore Default**. **Note:** When you click **Restore Default** for the selected file, it is deleted if it is not included with the product, or it is restored to its original included version.
		To display the most recent version of the data, including changes that were made to the data since it was last refreshed, click **Refresh**.

3. Optional: Restart the IBM Security Identity Manager Server if the **Notifications** widget indicates you to do it.

Configuring the external library

Use the External Library Configuration page to configure an external library in the IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage Server Setting** > **External Library Configuration** to display the External Library Configuration page.
2. Click **New** to open the Add External Library window.
3. Click **Browse** to search and upload the library file. The **File Name** field is populated with the library name. For example, `configuration.jar`.

   Note: You can upload various external library file formats such as `.jar`, `.war`, or others.
4. Click **Save Configuration** to complete this task. The library is added to the table.
5. Optional: To edit an existing external library, do these steps.
   1. On the External Library Configuration page, select a library name from the table. For example, `configuration.jar`.
   2. Click **Edit** to open the Edit External Library window.
   3. Click **Browse** to search and upload another library file. The **File Name** field is populated with the library name. For example, `lib_config.war`.

      Note: You can upload various external library file formats such as `.jar`, `.war`, or others.
   4. Click **Save Configuration** to complete this task. The edited library is listed in the table.

Managing the server properties

You can create, update, or reconfigure the custom property values, the IBM Security Identity Manager Server property values, or the application server property values from the **Appliance Dashboard** of the IBM Security Identity Manager virtual appliance.

Before you begin

You must be familiar with the property keys and values of the IBM Security Identity Manager, the custom property, or the application server supplemental property files before you do this task.

About this task

When you select a property, the **Property value** field is populated with a value. You can update a property value by overwriting its old value with the new one. For example, to use another file in the IBM Security Identity Manager virtual appliance, do these steps:

1. Upload a file that you want by using the upload function of the virtual appliance.

2. Update or edit the name of that file in the **Property value** field.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Configure** > **Advanced Configuration** > **Update Property** to display the Update Property page.
2. In the Update Property page, do these actions to work with the properties files. See Table 10 on page 24.

Table 10. Properties tabs and their actions

Tab	Tab Description	Actions
All properties	Displays this property list in the left pane: • **Custom property files** • **Identity server property files** • **Application server property files** Displays a list of properties files when you select a property. Select a properties file to display a list of the property names in the right pane. The right pane can have multiple tabbed pages, depending on the number of property names that are associated with the selected properties file. The default setting is 10 names per page. Depending on your requirement, click the tabbed page number or change the setting to view the property names. You can also go to a specific page by specifying the page number in the Go to Page window. To open this window, click the arrow, which is placed next to tabbed page number. You can use the search box to find a specific property name that you want to update. Type a name or a character string for the properties file in the box to help you narrow your search. Your string search is done within the context of the properties file that you selected. All property names that contain the string are displayed. If you want to return to the full list of property names, clear the search box. The right pane contains these buttons: • **New** • **Edit** • **Refresh** • **Upload** • **Delete File**	To add a property, do these steps: 1. Click a property files tab: • **Custom property files** • **Identity server property files** • **Application server property files** For example, click **Identity server property files**. 2. Select a property file from its list. For example, `CustomLabels.properties`. 3. Click **New** to open the Update property window. 4. Provide a value in the **Property name** field. For example, `ernamingcontexts`. 5. Provide a value in the **Property value** field. For example, `AttributesExtension`. 6. Click **Save Configuration**.
		To edit a property, do these steps: 1. Click a property files tab: • **Custom property files** • **Identity server property files** • **Application server property files** For example, click **Application server property files**. 2. Select a properties file from its list. For example, `CustomLabels.properties`. Depending on any property names and its values that are associated with the selected file, the right pane displays all of them. 3. Select a property name. For example, `com.ibm.SOAP.loginUserid`. 4. Click **Edit** to open the Update property window. 5. Edit the existing value in the **Property value** field with the new value. For example, `User1`. 6. Click **Save Configuration**.
		To display the most recent version of the data, including changes that were made to the data since it was last refreshed, click **Refresh**.
		To upload a property file, do these steps: 1. Click **Custom property files**. 2. Click **Upload** to open the File Upload window. 3. Click **Browse** to search and select the property file. 4. Click **Save Configuration**. **Note:** You can upload property files only from **Custom property files**.
		To delete a property file, do these steps: 1. Click **Custom property files**. 2. Select a properties file. For example, `demo.properties`. 3. Select a property name from the table. 4. Click **Delete File**. 5. Click **Yes** to confirm. **Note:** You can delete property files only from **Custom property files**.

Table 10. Properties tabs and their actions (continued)

Tab	Tab Description	Actions
Modified properties	Displays a segregated list of all the updated properties files under these tabs, including the **Reconfigure** button: • **Identity server** • **Application server** • **Custom** **Note:** Depending on your requirement, you can choose to reconfigure a properties file.	To reconfigure a properties file, do these steps. 1. Click a property tab that contains the properties file: • **Identity server** • **Application server** • **Custom** For example, select **Identity server**. 2. Select a properties file. For example, `ui.properties`. 3. Click **Reconfigure** to display the Update property window. 4. Edit the existing value in the **Property value** field with the new value. For example, `700`. 5. Click **Save Configuration**.
		To delete a properties file, do these steps: 1. Click **Custom**. 2. Select a property file. For example, `enRole.properties`. 3. Click **Delete**. 4. Click **Yes** to confirm. **Note:** You can delete properties files only from **Custom**.

Managing the application server certificate configuration

Use the Application Server SSL Certificate page to configure the application server SSL certificate in the IBM Security Identity Manager virtual appliance. The certificate update is for the primary node and each member node.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Advanced Configuration** > **Application Server Certificate Management** to display the Application Server SSL Certificate page. The Application Server SSL Certificate page displays the certificate details.
2. Click **Update** to open the Upload Keystore window.
3. Click **Browse** to search and select the certificate that you want to import. The **File** field is populated with the certificate name. For example, `appserver.jks`.
4. Type the password for the certificate in the **Keystore Password** field.
5. From the **Keystore Type** list, select a type that specifies the keystore.
   - **CMSKS**
   - **JCEKS**
   - **JKS**
   - **PKCS11**
   - **PKCS12**
6. Click **Save Configuration**.

   Note: The application server SSL certificate configuration takes some time. Do not refresh or close the page. Wait for the configuration process to complete.

Managing the export and import settings

Use the Export Import Settings page to export or import configuration settings from the virtual appliance. You can also download report files from the Export Import Settings page.

About this task

Export the service settings from the primary virtual appliance or the primary node. In another virtual appliance or member node, import the service settings from the primary node.

Note: Export or import operations work with same build version on the virtual appliance. They do not support between different build versions.

- The export file typically contains configuration information about custom file management, properties, custom libraries, SSL certificates, and workflow extensions from the virtual appliance.
- On the Export Import Settings page, the **Reports** tab displays a list of configuration reports. This list is displayed after an export or import operation, irrespective of whether the operation was complete or not. A separate report is generated for each export or import operation. Report names are generated by the type of operation that you run. For example:
  - `ExportReport201504280408.txt`
  - `ImportReport201504300709.txt`

  Note: The **Export** and **Import** buttons are not active after you select a report in the Imported Settings column of the **Reports** tab.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Manage** > **Manage Export Import** > **Export Import Settings**.
2. On the Export Import Settings page, do one of these actions.

Table 11. Export and import settings actions

Action	Button	Description
`Exporting a file`	**Export**	1. Click **Export** to display the Export Configuration window. 2. The Export Configuration window consists of these tabs. **Certificates** Certificates are listed under the **Certificate alias** column. **Workflow Extensions** Workflow extensions are listed under the **Name** column. **Custom Files** Custom files are listed under the **File name** column. **External Libraries** External libraries are listed under the **Library name** column. **Properties** Displays a list of the modified identity, application server, and custom properties under the **Property file name** column of the following tabs. • **Identity Properties** • **Application Server Properties** • **Custom Properties** **Note:** – If you upload a custom property file and do not modify any of its properties, the custom property file entry is listed in custom files, but the **Custom Properties** tab is empty. – If you modify any of the properties from a custom property file, the file entry is removed from custom files, and the **Custom Properties** tab displays the modified custom properties. 3. Select one or multiple configurations from one or all these tabs for your export operation. 4. Optional: To export all the configuration, select the **Export all configuration** check box. 5. Click **Save Configuration** to export the settings. **Note:** This operation downloads an export package file in an archived format. The file name format is `configuration`*`host_name`*`.export`. For example, `configurationislrpbfixv607.in.ibm.com.export`.

Table 11. Export and import settings actions (continued)

Action	Button	Description
`Importing a file`	**Import**	1. Click **Import** to display the Import Configuration window. 2. In **Administrator ID**, specify an ID value. 3. In **Administrator Password**, specify a password. 4. Click **Browse** to select a package file that you want to import. 5. Click **Save Configuration**. A message indicates that the import operation is completed. The configurations are imported to the virtual appliance.
`Downloading a report`	**Download Report**	1. From the Imported Settings column of the **Reports** tab, select a report. 2. Click **Download Report**. 3. Save a copy of the report to your local drive. **Note:** The report that you download is in `.txt` format.

Configuring the workflow extension

Use the Workflow Extension page to configure workflow extension information in the IBM Security Identity Manager virtual appliance.

About this task

Supply workflow extension values in the Workflow Extension page.

Consider these points for XML-related information in the Workflow Extension page.

- Select the **Provide XML** check box and add the entire XML information in the specified text area.
- Clear the **Provide XML** check box and create activities in the **Activities** area.

Important: If you selected or cleared the **Provide XML** option when you created a workflow extension, you cannot change it when you edit a workflow extension.

A typical XML snippet can be as follows:

```
<ACTIVITY ACTIVITYID="asynchronousChangePasswordExtension" LIMIT="600000"><IMPLEMENTATION_TYPE>
<APPLICATION CLASS_NAME="examples.workflow.AsynchronousApplicationExtension" METHOD_NAME="asynchronou
</IMPLEMENTATION_TYPE>
</ACTIVITY>

<ACTIVITY ACTIVITYID="synchronousChangePasswordExtension" LIMIT="600000"><IMPLEMENTATION_TYPE>
<APPLICATION CLASS_NAME="examples.workflow.SynchronousApplicationExtension" METHOD_NAME="synchronousC
</IMPLEMENTATION_TYPE>
</ACTIVITY>
```

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Advanced Configuration** > **Workflow Extension** to display the Workflow Extension page.
2. On the Workflow Extension page, do one of these actions.

Table 12. Workflow Extension actions

Action	Button	Description
`Create a workflow extension`	**New**	1. Click **New** to open the Create Workflow Extension window. 2. Specify a name for the extension in **Extension name**. 3. Specify a name for the servlet in **Servlet name**. 4. Specify a description for the servlet in **Servlet description**. 5. Specify a class for the servlet in **Servlet class**. 6. Specify a pattern in **URL pattern**. 7. Select or clear the **Load on startup** check box for servlet mapping. 8. Select or clear the **Provide XML** check box to provide or override XML attribute values. 9. Specify the XML attribute values in **Process Definition**. 10. In the **Activities** area, click **New** to open the Create Activity window. 11. Specify an ID value in **Activity ID**. 12. Set a limit value in **Limit**. 13. Specify a name for the class in **Class name**. 14. Specify a name for the method in **Method name**. 15. Select or clear the **Enable restriction** check box to restrict the types. 16. From the **Join** list, restrict the type with these conditions. • **AND** • **XOR** 17. From the **Split** list, restrict the type with these conditions. • **AND** • **XOR** 18. Select or clear the **Enable script** check box to provide or override the script details. 19. From the **Script event** list, assign a script event with these options. • **onCreate** • **onComplete** 20. Specify a script for the workflow extension in **Script**. 21. In the **Parameters** area, set the parameters with these options. **Add In Param** Do these steps. a. Click **Add In Param** to add an input parameter. b. In the record that you created, click and specify an ID under **Parameter ID**. c. Specify a type under **Parameter Type**. **Note:** The parameter category is specified as `IN`. **Add Out Param** Do these steps. a. Click **Add Out Param** to add an output parameter. b. In the record that you created, click and specify an ID under **Parameter ID**. c. Specify a type under **Parameter Type**. **Note:** The parameter category is specified as `OUT`.

Table 12. Workflow Extension actions (continued)

Action	Button	Description
Edit a workflow extension	**Edit**	1. Select a workflow extension from the table. 2. Click **Edit** to open the Edit Workflow Extension window. 3. Edit the extension name. 4. Edit the servlet name. 5. Edit the servlet description. 6. Edit the servlet class. 7. Edit the URL pattern. 8. Select or clear the **Load on startup** check box for servlet mapping. 9. In the **Activities** area, select an activity. 10. Click **Edit** to open the Edit Activity window. 11. Edit the ID value in **Activity ID**. 12. Edit the limit value in **Limit**. 13. Edit the class name. 14. Edit the method name. 15. Enable or disable the restriction. 16. In **Join**, change the restriction condition. 17. In **Split**, change the restriction condition. 18. Select or clear the **Enable script** check box to provide or override the script details. 19. In **Script event**, change the event. 20. Edit the workflow extension script information. 21. Edit the parameters. For more information about parameters, see Parameters. 22. Click **Save Configuration** to save the activity that you selected to edit. 23. Click **Save Configuration** to save the workflow extension that you selected to edit.
Delete a workflow extension	**Delete**	1. Select a workflow extension record from the table. 2. Click **Delete**. 3. Click **Yes** to confirm your action.
Refresh the workflow extension information	**Refresh**	Click **Refresh** to display the most recent version of the data, including changes that were made to the data since it was last refreshed.

Managing the log configuration

You can view component-specific and IBM Security Identity Manager virtual appliance log files to troubleshoot any virtual appliance issues better.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Manage** > **Maintenance** > **Log Retrieval and Configuration**.
2. Select the product from the tabs to view the available logs. For more information, see “Retrieving logs” on page 31.

3. Optional: Click **Configure** to configure the logs. For a set of configuration tasks, see "Configuring logs" on page 32.

Retrieving logs

Use the Log Retrieval and Configuration page to view, save, or clear the log files. You can also use the page to configure the server log settings for the IBM Security Identity Manager virtual appliance.

About this task

See Table 13 for a list of available logs, which can help you to diagnose or troubleshoot them from the Log Retrieval and Configuration page.

Table 13. Available logs to help you diagnose or troubleshoot

Tab	Tab description	Log file name	Log file name description
Appliance	The files assist you to debug any configuration failures that occur in the virtual appliance.	Identity data store configuration	Identity data store configuration log file.
		Directory server information	IBM Security Directory Server user registry configuration log file.
		Server System out	Appliance system output log file.
		Server Message	Appliance server message log file.
Identity	Identifies issues in the Identity applications.	Cluster manager system out and Cluster manager system error	Cluster manager system out and system error log files.
		Application server system out and Application server system error	Identity Application server system out and system error log files.
		Message server system out and Message server system error	Identity Message server system out and system error log files.
		Application message	Identity virtual appliance message log file.
		Application trace	Identity virtual appliance trace log file.
		Application access	Identity virtual appliance access log file.
	Identifies issues in the cluster manager of the Identity virtual appliance.	Cluster manager system out and Cluster manager system error	Identity cluster manager system out and system error log files.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Manage** > **Maintenance** > **Log Retrieval and Configuration**.
2. On the Log Retrieval and Configuration page, do one of the following actions.
   - Click **Appliance** to open the **Appliance** tab.
   - Click **Identity** to open the **Identity** tab.

For example, click **Appliance**.

3. From the Log Retrieval and Configuration table of the **Appliance** tab, select a log file. For more information about the **Appliance** and the **Identity** log files, see Table 13 on page 31.
4. Do one of the following actions:
   - Click **View** to display the contents of the selected log file in the **Log file** field of the Log Content window.
   - Click **Download** to save or download a copy of the log file.
   - Click **Clear**, and confirm the action to remove the contents from the selected log file.
   - Click **Refresh** to display the most recent version of the log files, including changes that were made to the data since it was last refreshed.

Configuring logs

Configure different options to manage the quantity and size of the log files.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Manage** > **Maintenance** > **Log Retrieval and Configuration**. The Log Retrieval and Configuration page consists of two tabs.
   - **Appliance**
   - **Identity**

   To work with these tabs, see "Retrieving logs" on page 31.
2. Click **Configure** to display the Logging Configuration window. The Logging Configuration window consists of these tabs.

   General

   This tab contains information about log rollover settings such as maximum log file rotation size and maximum number of historical log files.

   Provide the following details:

   Maximum size for log file rotation

   The size of the log file in megabytes that you want to assign. For example, specify `2`.

   Maximum number of historical log files

   The maximum number of historical log files that you want to assign. For example, specify `10`.

   To edit the existing log details, specify the new values.

   Identity Manager

   This tab contains information about identity-specific logging details such as date format, time format, package, and their trace levels.

   Provide the following details:

   Date Format

   Specify a format for that date that you want to assign for the logs.

   Time Format

   Specify a format for the time that you want to assign for the logs.

   New Do these steps:

a. Click **New** to add a package name.

b. In the **Package Name** column, select a package name from the list and assign it to the Identity log.

c. In the **Trace Level** column, select a trace level from the list and assign it to the Identity log.

Delete Select a record and click **Delete**.

To edit an existing package name, click it and do one or both of these steps.

a. Select another package name from the list.

b. Select another trace level from the list.

Application Server
This tab contains information about application server-specific logging properties such as package and their trace levels. Do these steps:

New Do these steps:

a. Click **New** to add a package name.

b. In the **Package Name** column, click to type a package name and assign it to the application server log.

c. In the **Tracing Level** column, select a trace level from the list and assign it to the application server log.

Delete Select a record and click **Delete**.

To edit an existing package name, click it and do one or both of these steps.

a. Type another package name.

b. Select another trace level from the list.

SDI This tab contains information about Security Directory Integrator logging properties such as package and their trace levels. Do these steps:

New Do these steps:

a. Click **New** to add a package name.

b. In the **Package Name** column, select a package name from the list and assign it to the Security Directory Integrator log.

c. In the **Trace Level** column, select a trace level from the list and assign it to the Security Directory Integrator log.

Delete Select a record and click **Delete**.

To edit an existing package name, click it and do one or both of these steps.

a. Select another package name from the list.

b. Select another trace level from the list.

3. Click **Save Configuration**.

Note: Depending on the changes that you made on any of these tabs, a message indicates to restart the server in the **Notifications** widget.

Managing the core dump files

Use the Core Dumps page to delete or download core dump files in the IBM Security Identity Manager virtual appliance.

About this task

A core dump file can be generated in the IBM Security Identity Manager virtual appliance due to many reasons. A core dump file stores a large amount of raw data for further examination. Use the core dump files to diagnose or debug errors in the IBM Security Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Manage** > **Maintenance** > **Core Dumps**.

   The Core Dumps page displays a table with a list of core dump files. The **Category** column in the table indicates the category for which the core dump file is generated. The category list is as follows.
   - Application
   - Application management
   - SDI, which is Security Directory Integrator
   - Others
2. On the Core Dumps page, do one of the following actions.

Table 14. Core dump file management actions

Action	Description
Delete	1. From the **File name** column, select a core dump file. **Note:** To delete multiple core dump files, select more files. To select all the core dump files, select the check box next to **File name**. 2. Click **Delete**. 3. Click **Yes** to confirm.
Download	1. From the **File name** column, select a core dump file. **Note:** You can select only 1 core dump file at a time for download. A message is displayed if you select multiple core dump files. 2. Click **Download** to save or download a copy of the core dump file. **Note:** The core dump file is downloaded in an archived format such as `.zip`. **Note:** To view the contents of a core dump file, open the downloaded file.

Reconfiguring the data store connection

Reconfigure the data store if the data store configuration changes.

Procedure

1. Make a backup of the database. On the database server that runs DB2 Universal Database™ for IBM Security Identity Manager, complete the following steps:
   a. Log on as the instance owner. For example: `db2admin`.

b. Close all connections to the IBM Security Identity Manager database. Stop DB2 Universal Database or any other tools. If necessary, run the following command to force all connections to close:

```
db2 force application all
```

c. Back up the data store database:

```
db2 backup database IDM_DB to OLD_DB2_BACKUP_DIR
```

Where:

- `IDB_DB` is the name of the IBM Security Identity Manager data store database. For example: `idmdb`
- `OLD_DB2_BACKUP_DIR` is a directory path to store the backup. For example:

Linux or UNIX systems
`/tmp/db2`

Windows systems
`c:\temp\db2`

2. Restore the backup of the database.

Install the new version of DB2 Universal Database. For this reconfiguration, ensure that you create the database instance and database with the same name. Users must have the same rights and privileges as setup on the previous system.

To create a database instance and a database, see Database installation and configuration.

Copy the contents of the IBM Security Identity Manager data store backup directory to the target server. For example: `tmp/db2`.

Ensure that the database instance owner you create has permission to read the target directory and files within.

To restore the DB2 Universal Database data on the target database server, complete the following steps:

a. Launch DB2® command line.

Windows

1) Start the Windows command prompt.

2) Run the following command:

`set DB2INSTANCE=isiminst` where `isiminst` is the database instance.

3) Run **`db2cmd`** to start the DB2 command line.

Linux Run the command `su - isiminst` where `isiminst` is the database instance.

b. In the DB2 command line, enter the following commands to restore the database by using the migrated DB2 data:`restore db idmdb from OLD_DB2_TEMP_DATA`

Where:

- `idmdb` is the IBM Security Identity Manager data store database name.
- `OLD_DB2_TEMP_DATA` is the location of the migrated DB2 data that you copied over from the previous version. For example: `c:\temp\db2`

c. Stop and start the DB2 server to reset the configuration.

After you create the IBM Security Identity Manager data store database, stop, and start the DB2 server to allow the changes to take effect.

Enter the following commands:

- `db2stop`

- db2start

Note: If the db2stop fails and the database remains active, enter the following command to deactivate the database:

- db2 force application all
- Then, enter the db2stop command again.

3. For the Identity data store, clear the **Service Integration Bus**.

   For reconfiguration of the Identity data store, you must clear out the Service Integration Bus (SIB) from the restored database.

   To clear out the**Service Integration Bus** on the target DB2 server, complete the following steps:

   a. Ensure that theIBM Security Identity Manager database is running (IDMDB).

   b. Start the DB2 command line.

      Windows

      1) Start the Windows command prompt.

      2) Run the following command:

         set DB2INSTANCE=isiminst where isiminst is the database instance.

      3) Run **db2cmd** to start the DB2 command line.

      Linux Run the command su - isiminst where isiminst is the database instance.

   c. In the DB2 command line, enter the DELETE SQL statements that you require to delete all data from the tables in the Service Integration Bus schemas.

      Enter the following commands for each of the Service Integration Bus schema in your environment:

      ```
      db2 delete from schema_name.SIB000
      db2 delete from schema_name.SIB001
      db2 delete from schema_name.SIB002
      db2 delete from schema_name.SIBCLASSMAP
      db2 delete from schema_name.SIBKEYS
      db2 delete from schema_name.SIBLISTING
      db2 delete from schema_name.SIBXACTS
      db2 delete from schema_name.SIBOWNER
      db2 delete from schema_name.SIBOWNERO
      ```

      Where the Service Integration Bus schema, schema_name is ITIML000 for a single server, and ITIML000, ITIML0001, ITIML002, ITIML003, and ITIMS000 are for a cluster environment. For a cluster, the number of schemas such as ITIML0001, ITIML0002, or other schemas vary depending on the number of nodes in the cluster. ITIMS000 is also one of the schema names for the cluster.

      Note: The SIMOWNER0 might not exist in all Identity data store environments. If it does not exist and the delete statement fails, you can ignore the failure.

4. Reconfigure the data store.

   a. From the IBM Security Identity Manager administrative console, click **Menu** > **Database Configuration**.

   b. Select the existing data store that you want to set up and click **Reconfigure**. Provide the details and click **Save Configuration**.

   c. Restart the server to complete the process.

Reconfiguring the directory server connection

Reconfigure the directory server if the directory server configuration changes.

Procedure

1. Make a backup of the directory server.

   On the server running IBM Security Directory Server for IBM Security Identity Manager, complete the following steps:

   a. Log on as an Administrator with root privileges.

   b. Open a command window.

   c. Go to the *TDS_HOME*/sbin directory and type the following command:

   ```
   db2ldif -s ldap_suffix -o ldap_output_file -I ldap_instance_name
   ```

   where:

   ldap_suffix is the name of the suffix. For example: dc=com.

   ldap_output_file is the name of the ldif output file. For example: old_ldif_data.ldif.

   ldap_instance_name is the name of the LDAP server instance, which can be obtained through theIBM Security Directory Server Instance Administration tool.

   d. Use the backup of the schema file V3.modifiedschema from the OLD_ITDS_INSTANCE_HOME\etc directory of the IBM Security Directory Server instance home directory.

2. Restore the backup of the database.

   Install a version of IBM Security Directory Server that IBM Security Identity Manager supports. For this reconfiguration, ensure that you take the following actions:

   - Create and use the same root suffix.
   - Use the same encryption seed value as the old directory server instance. If not, you must export the data from the old directory server instance to use the seed and salt keys from the new instance.

   Copy the contents of the IBM Security Identity Manager directory server backup ldif file and schema file to the target server.

   To restore the directory server data on the target directory server, complete the following steps:

   a. Log on as an Administrator with root privileges.

   b. Stop the LDAP server.

   c. Copy the schema file V3.modifiedschema that you copied over from the previous server to the NEW_ITDS_INSTANCE_HOME\etc directory of the IBM Security Directory Server instance.

   Note: If you customized or modified the schema files, manually merge the changes into the new schema files.

   d. From TDS_HOME/sbin, run the command:

   ```
   bulkload -i OLD_ITDS_TEMP_DATA\ldif_output_file -I ldap_instance_name
   ```

   where:

   OLD_ITDS_TEMP_DATA is the temporary directory location of the IBM Security Directory Server data you copied over from the previous server. For example, C:\temp\51data\ids\.

   ldif_output_file is the name of the file that you exported in a previous task. For example, old_ldif_data.ldif `ldap_instance_name` is the name of the LDAP server instance. For example, `itimldap`. You can obtain use the IBM Security Directory Server Instance Administration tool to obtain the instance name.

For more information, see Bulkload command errors.

e. Stop and start the IBM Security Directory Server to activate the changes.

3. Reconfigure the IBM Security Directory Server.
   a. From the IBM Security Identity Manager administrative console, go to **Menu** > **Directory Server Configuration**.
   b. Select the directory server and click **Reconfigure**. Provide the details and click **Save Configuration**.
   c. Restart the Identity server to complete the process.

IBM Security Identity Manager Mobile App

You can use IBM Security Identity Manager Mobile App to manage accounts by using a mobile phone to communicate your requests.

Install or configure the IBM Security Identity Manager Mobile App to enable connectivity between the IBM Security Identity Manager Server and the mobile device.

Installing the iOS application

You must install the iOS application on your mobile device before you can use IBM Security Identity Manager.

About this task

This task is performed with either an iPhone or iPad.

Procedure

1. Download and install the app from the Apple iPhone App Store. The application is listed under: **IBM Security Services** > **IBM Security Identity Mobile**.
2. Review and follow the “Getting Started” section from the app details on the App Store.

Installing the Android application

You must install the Android application on your mobile device before you can use IBM Security Identity Manager

Before you begin the installation task for Android application, extract the content of the IBM Security Identity Manager Mobile App solution package into a temporary directory.

Note: The extracted file name is in the form `mobile.android.isimm-release.apk`.

Three options to install the Android application exist.

- You can email the `mobile.android.isimm-release.apk` file and access the email from your phone.
- You can physically copy the `mobile.android.isimm-release.apk` file to your phone. From your phone, go to the file location.

- Make the `mobile.android.isimm-release.apk` file available to install through a URL from your phone.

Create an account for the Android application. See “Creating an account for the Android application.”

Creating an account for the Android application

Before you can use the Mobile App, you must create an account that is associated with the application.

About this task

When you install the Mobile App, a login screen is displayed. Use the screen to create your Android application account.

Note: You can also create an account by using the local Android account management option and selecting the **IBM Security Identity Mobile Manager** option.

Procedure

1. Type the information for the following fields.

   Server Address

   Specify the URL for the Mobile App URL. For example, `http://`*`ip-address`*`:`*`port`*`/isimm`. If SSL is configured, specify `https`, where:

   ip-address

   Specifies the application server IP.

   port Specifies the port number for the application server.

   Username

   Specify an IBM Security Identity Manager user ID.

   Password

   Specify the password for the user ID.

   Notification Sync Interval (minutes)

   Accept the default setting of 10 minutes.

   Allow untrusted security certificate

   Accept the default setting that allows untrusted security certificates. Clear the check box if you do not want to allow untrusted security certificates from the Mobile App application.
2. Click **Sign-in**.
3. Accept the default setting for the **Save Details** check box. If you clear this check box, you are prompted for the login details every time that you start the application. You are also not notified of any new IBM Security Identity Manager approval activities.

   After you create an account, make sure that you log in to the IBM Security Identity Manager Console by clicking the **Identity Administration Console** link in the **Quick Links** widget of the **Appliance Dashboard**.

IBM Security Identity Manager access control item configuration for approvers

The Mobile App provides an option that enables the approver to make a telephone call to the IBM Security Identity Manager Account requester and requestee. These calls are made directly from the Request Details screen of the mobile application.

The phone number is displayed as a hyperlink. The approver must be able to retrieve the telephone number values from the requester and requestee details that are stored in the IBM Security Identity Manager server.

The account approver must have the appropriate access control items (ACIs) set in IBM Security Identity Manager to retrieve the phone number of the requestee and requester. To display the phone numbers on the Request Details screen, the account approver must have:

- The ability to search for the IBM Security Identity Manager person.
- At a minimum, the read ACI set for the **`telephonenumber`** attribute of the IBM Security Identity Manager person.

Chapter 2. User interface customization overview

Many customers want a simple user interface for their employees to interact with IBM Security Identity Manager to do basic management and provisioning functions. IBM Security Identity Manager provides multiple user interfaces that are customizable and provide the basic IBM Security Identity Manager functions that are needed by both users and administrators.

Interface customization options that IBM Security Identity Manager provides give customers the control and flexibility to manage how IBM Security Identity Manager functions are presented to their employees. With these options, customers can integrate a service center interface and an administrative console interface into their intranet website and maintain a common corporate appearance.

Self-service user interface customization

The IBM Security Identity Manager self-service user interface is highly customizable. You can integrate a common corporate appearance while they maintain the flexibility to do self-care identity management tasks integral to their roles and responsibilities.

You can define and customize the self-service interface in two ways, by using the built-in console framework and by directly modifying files that are installed within IBM Security Identity Manager:

- Built-in console features:
  - Access control items (ACIs)
  - Views
- Modifiable files:
  - Properties files
  - Cascading style sheet (CSS) files
  - A subset of Java server pages (JSP) files
  - Image files

Back up any modifiable files for recovery purposes before you make customization changes to IBM Security Identity Manager.

Configuration files and descriptions

Configuration files define the appearance of the IBM Security Identity Manager self-service user interface.

The following tables list the file names and describe their roles in the customization of IBM Security Identity Manager.

Table 15. Property configuration files and descriptions

File Name	File Description
SelfServiceUI.properties	• Controls the layout of the user interface (banner, footer, navigation bar, toolbar), the number of pages that display, and the number of search results returned. • Configures the items available in the "Search By" box for user search in the self-service interface. • Enables direct access to the Expired Password change screen and bypass the self-service login page under certain conditions. The property key that allows these actions is ui.directExpiredChangePasswordEnabled.
SelfServiceScreenText.properties	Provides the text on the self-service user interface.
SelfServiceScreenText_*language* .properties	Provides the language-specific text on the self-service user interface. By default this file is `SelfServiceScreenText_en.properties`, which contains the English language bundle.
SelfServiceHomePage.properties	Defines the sections of the self-service user interface home page and the order in which they occur.
SelfServiceHelp.properties	Defines the links to html help pages on the self-service user interface. The html files are in the `WAS_PROFILE_HOME\installedApps\node_name\ ITIM.ear\itim_self_service_help.war` directory. You can redirect help by modifying the information in this file.
SelfServiceScreenTextKeys .properties	Provides label keys on the self-service user interface. This file can be used to assist with customization of screen text by providing a template to develop labels and instructions. The file contains labels that are set to the key name. For instance, password_title=password_title. For customization and development purposes. you can copy this file to `SelfServiceScreenText_language.properties`, where *language* is a language suffix that is not installed. You can then switch your browser locale from your current language to the unused language. Restart the web application to navigate through the pages and see the label keys instead of the value text. By switching your browser locale, you can then toggle between keys and values. When customization is complete, you can then copy and rename the file to the language suffix you want to use, for example SelfServiceScreenText_en.properties, to finalize changes.

Table 16. Java server pages (JSP) configuration files and descriptions

File Name	File Description
loginBanner.jsp	Contains the content of the banner on the self-service login page.
loginFooter.jsp	Contains the content of the footer on the self-service login page.

Table 16. Java server pages (JSP) configuration files and descriptions (continued)

File Name	File Description
loginToolbar.jsp	Contains the content of the toolbar on the self-service login page.
Home.jsp	Contains the content of the self-service home page.
banner.jsp	Contains the content of the self-service banner.
footer.jsp	Contains the content of the self-service footer.
nav.jsp	Contains the content of the self-service navigation bar.
toolbar.jsp	Contains the content of the self-service toolbar.

Table 17. Cascading style sheet (CSS) configuration files and descriptions

File Name	File Description
calendar.css	CSS file that contains the styles that are used for calendar widgets.
customForm.css	CSS file that contains the styles that are used to lay out custom forms for left to right language orientation.
customForm_rtl.css	CSS file that contains the styles that are used to lay out custom forms for right to left language orientation.
dateWidget_ltr.css	CSS file that contains the styles that are used for date widgets for left to right language orientation.
dateWidget_rtl.css	CSS file that contains the styles that are used for date widgets for right to left language orientation.
enduser.css	CSS file that contains main CSS styles for left to right language orientation.
enduser_rtl.css	CSS file that contains main CSS styles for right to left language orientation.
time.css	CSS file that contains the styles that are used for time widgets.
widgets.css	CSS file that contains the styles that are used for other widgets for left to right language orientation.
widgets_rtl.css	CSS file that contains the styles that are used for other widgets for right to left language orientation.

Backing up and restoring self-service user interface configuration files

Before you begin customization of the self-service user interface, back up all configuration files in IBM Security Identity Manager for later recovery purposes.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Log in to each computer that is running Security Identity Manager. Back up the following files:

- In the `directories\itim_self_service.war\custom` directory:
  - banner.jsp
  - calendar.css

  - customForm.css
  - customForm_rtl.css
  - dateWidget_ltr.css
  - dateWidget_rtl.css
  - enduser.css
  - enduser_rtl.css
  - footer.jsp
  - Home.jsp
  - loginBanner.jsp
  - loginFooter.jsp
  - loginToolbar.jsp
  - nav.jsp
  - time.css
  - toolbar.jsp
  - widgets.css
  - widgets_rtl.css
- In the `directories\data` directory:
  - SelfServiceHelp.properties
  - SelfServiceHomePage.properties
  - SelfServiceScreenText.properties
  - SelfServiceUI.properties
  - SelfServiceScreenTextKeys.properties

About this task

Any changes made to properties files require you restart the Security Identity Manager application. For instance, upon recovering any properties files, complete these steps:

Procedure

1. From the **Server Control** widget, do these steps.
   a. Select **Security Identity Manager server**.
   b. Click **Restart**.

   See Viewing the Server Control widget.
2. Verify that the recovery is complete by logging in to the self-service user interface.

User interface elements affected by view definitions

Defined views affect the visibility of task panels and other elements within the self-service interface.

View definition elements

View definitions can have the following effects on the self-service user interface:

Home page
Adapts to the user's views by showing only the tasks and task panels on

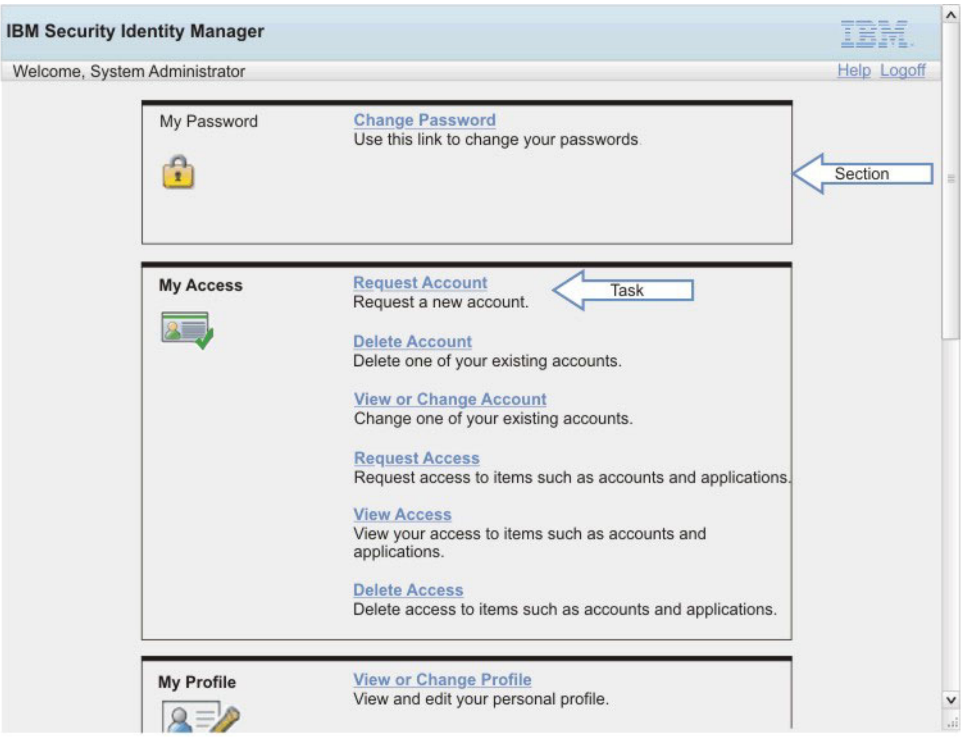
the home page that the user is granted. If the user is not allowed to view any tasks in a section, then the task panel also does not appear on the home page.

Some task views, such as the Request Account task, have advanced views. To clarify, Request Account is a single task. If the **Request Account Advanced** view is granted, or if both the **Request Account** and **Request Account Advanced** views are granted, the user has a single **Request Account** task on the home page. The main Request Account page displays a search page in which the user can search for a service on which they can request an account. If only the standard Request Account view is granted, and not the advanced view, then the **Request Account** task appears on the home page. The main Request Account page displays a table that lists the services that the user can request an account on, instead of a search page.

If the user can do both Change and View tasks for an account or profile, it combines them into a single task. For example, the task appears as **View or Change Account**.

Some tasks might not appear if they are not enabled by the system administrator. For example, **Change Forgotten Password Information**requires the enablement of challenge response.

The **Action Needed** task is only available if there are pending to-do items or challenge response information is not configured.



IBM Security Identity Manager

Welcome, System Administrator

My Password

Change Password
Use this link to change your passwords

My Access

Request Account
Request a new account.

Delete Account
Delete one of your existing accounts.

View or Change Account
Change one of your existing accounts.

Request Access
Request access to items such as accounts and applications.

View Access
View your access to items such as accounts and applications.

Delete Access
Delete access to items such as accounts and applications.

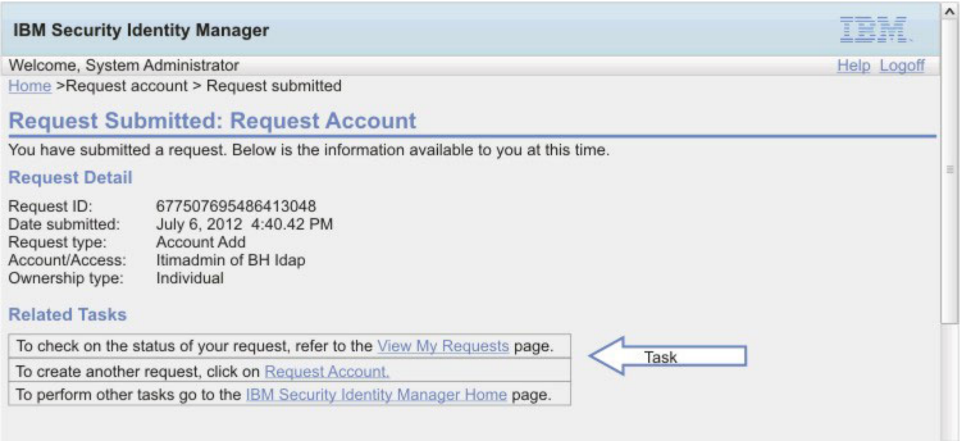
My Profile

View or Change Profile
View and edit your personal profile.

Figure 1. Home page elements

Related tasks

Related task sections are displayed in many areas of the self-service application, for example when a request is submitted. View definitions can filter some or all of the sections from being shown based on the view definition permissions. For example, if the user does not have regular access to **View My Requests**, then it is filtered from the **Related Tasks** task panel.



IBM Security Identity Manager

Welcome, System Administrator

Help Logoff

Home >Request account > Request submitted

Request Submitted: Request Account

You have submitted a request. Below is the information available to you at this time.

Request Detail

Request ID:	677507695486413048
Date submitted:	July 6, 2012 4:40.42 PM
Request type:	Account Add
Account/Access:	Itimadmin of BH ldap
Ownership type:	Individual

Related Tasks

To check on the status of your request, refer to the View My Requests page.

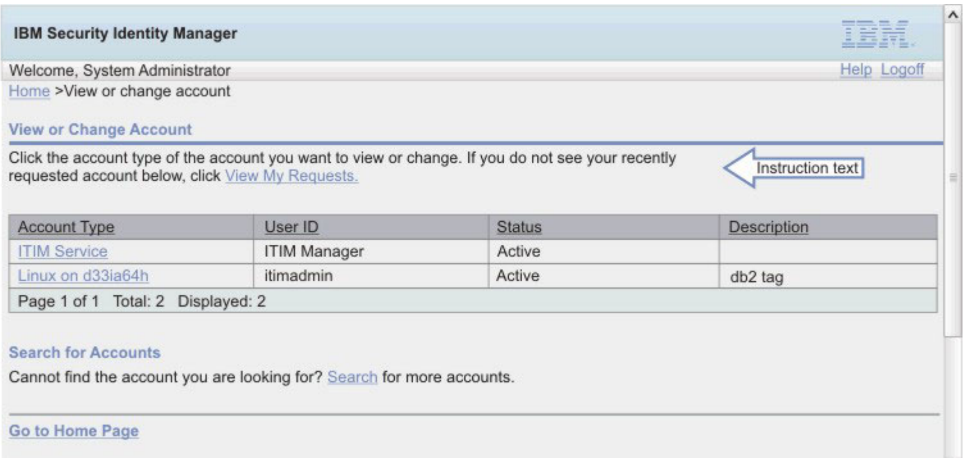
To create another request, click on Request Account.

To perform other tasks go to the IBM Security Identity Manager Home page.

Figure 2. Related task panel element

Panel instruction text

The instruction text on certain screens can contain links to the **View My Requests** task. A different instruction message is displayed without the task link if the user is not granted the **View My Requests** task in a view definition.



IBM Security Identity Manager

Welcome, System Administrator

Help Logoff

Home >View or change account

View or Change Account

Click the account type of the account you want to view or change. If you do not see your recently requested account below, click View My Requests.

Account Type	User ID	Status	Description
ITIM Service	ITIM Manager	Active	
Linux on d33ia64h	itimadmin	Active	db2 tag

Page 1 of 1 Total: 2 Displayed: 2

Search for Accounts

Cannot find the account you are looking for? Search for more accounts.

Go to Home Page

Figure 3. Instruction text panel element

Customizing labels, description, and other screen text

You can change the majority of the text displayed in the self-service user interface with customization.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

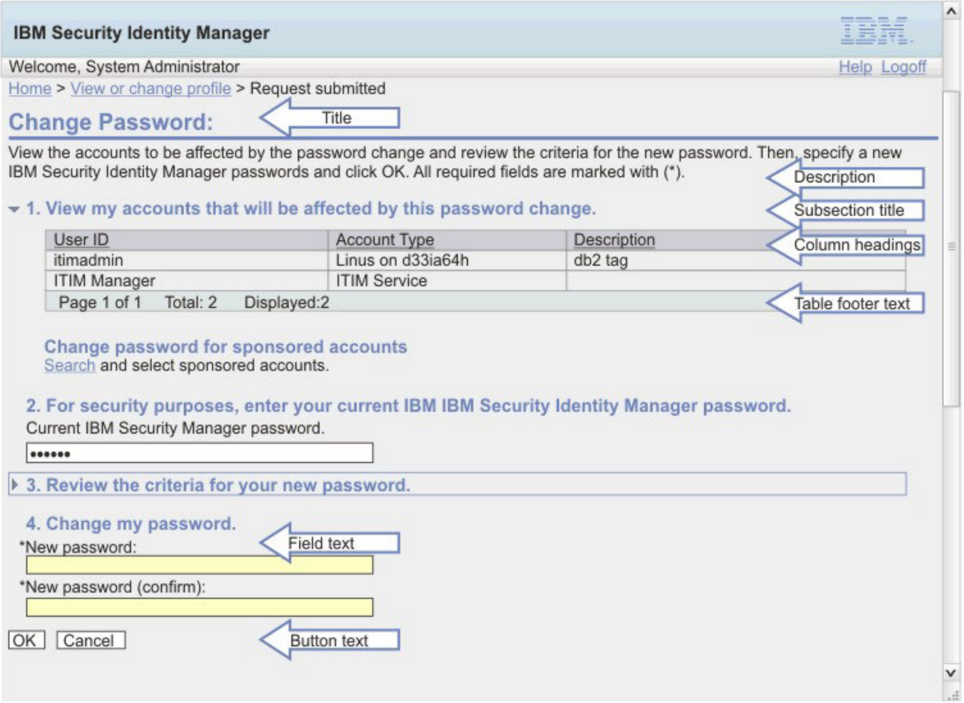
About this task

Not every label can be customized by the user. Only the labels that have an entry present in the SelfServiceScreenTextKeys.properties file can be customized.

The following screen text items can be customized:

- Titles
- Subsection titles
- Subsection descriptions
- Field labels
- Table column headers and footers
- Button text

The following figure shows the visual representation of these screen text items.



IBM Security Identity Manager

Welcome, System Administrator

Help Logoff

Home > View or change profile > Request submitted

Change Password:

View the accounts to be affected by the password change and review the criteria for the new password. Then, specify a new IBM Security Identity Manager passwords and click OK. All required fields are marked with (*).

1. View my accounts that will be affected by this password change.

User ID	Account Type	Description
itimadmin	Linus on d33ia64h	db2 tag
ITIM Manager	ITIM Service	
Page 1 of 1 Total: 2 Displayed:2		

Change password for sponsored accounts

Search and select sponsored accounts.

2. For security purposes, enter your current IBM IBM Security Identity Manager password.

Current IBM Security Manager password.

••••••

3. Review the criteria for your new password.

4. Change my password.

*New password:

*New password (confirm):

OK Cancel

Figure 4. Screen text

Text that cannot be replaced includes error messages and text in the help content that you access by clicking on the help link. However, it is possible to redirect help requests to a different URL.

To customize screen text, complete the following steps:

Procedure

1. Make a backup copy of the `SelfServiceScreenText.properties` and `SelfServiceScreenTextKeys.properties` files. If you have installed a language pack, back up any other language pack files you plan to modify, including the `SelfServiceScreenText_en.properties` file. `SelfServiceScreenText.properties` is the default file used if no other matching language is found.
2. Edit the properties files. Modify the values of the screen text fields and save the files. Note that any changes you make to the `SelfServiceScreenText.properties` file should also be made to the `SelfServiceScreenText_en.properties` files to maintain consistency.
3. Restart the IBM Security Identity Manager application to make the changes effective.

Customizing website layout

You can change the layout in the self-service user interface with customization.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

High-level layout elements can be enabled and disabled from display in the self-service user interface with settings in the `SelfServiceUI.properties` file. The default layout contains a banner, toolbar, and footer.

Turning on and off page elements can give various layout options. The only required page element is the content element, which contains the tasks and task pages.

To show or hide a page element, change the ui.layout.show*name* property in the `SelfServiceUI.properties` file. For instance, ui.layout.showBanner controls the display of the banner section. Setting a property to true indicates that the element is included in the page. A setting of false indicates that the element is not included in the page.

Any change to the `SelfServiceUI.properties` file requires a restart of the IBM Security Identity Manager application in the IBM Security Identity Manager virtual appliance to make the change effective.

The following figures show a visual representation of different layout elements and options.

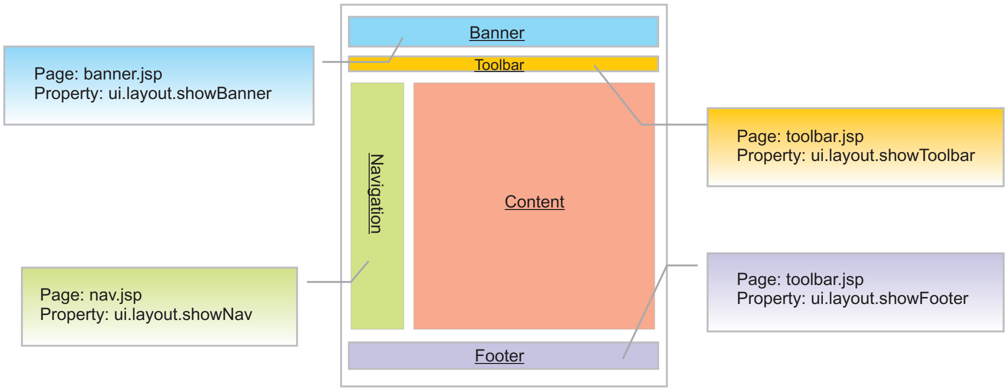

Banner
Toolbar
Page: banner.jsp
Property: ui.layout.showBanner
Page: toolbar.jsp
Property: ui.layout.showToolbar
Navigation
Content
Page: nav.jsp
Property: ui.layout.showNav
Page: toolbar.jsp
Property: ui.layout.showFooter
Footer

Figure 5. Layout elements

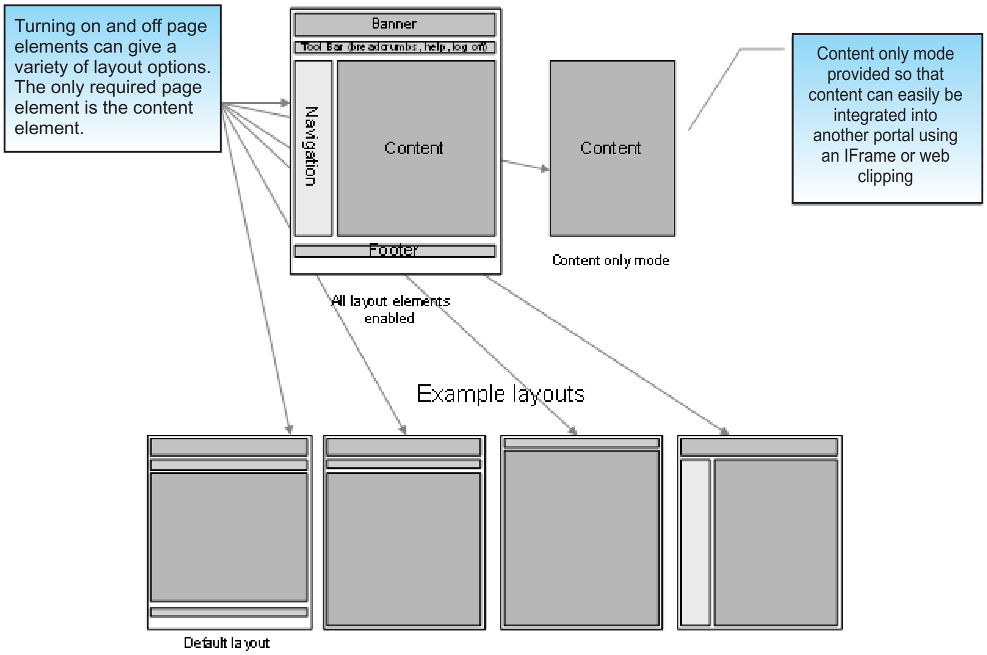

Turning on and off page elements can give a variety of layout options. The only required page element is the content element.
Banner
Tool Bar (breadcrumbs, help, log off)
Navigation
Content
Footer
All layout elements enabled
Content
Content only mode
Content only mode provided so that content can easily be integrated into another portal using an IFrame or web clipping
Example layouts
Default layout

Figure 6. Layout options

The following table displays a list of properties and their details.

Table 18. Layout properties and details

Property	Description
ui.layout.showBanner	Controls the banner section. The default banner contains IBM and product images.
ui.layout.showFooter	Controls the footer section. The default footer contains the product copyright.
ui.layout.showToolbar	Controls the toolbar section. The default toolbar contains the welcome message, help link, logoff link, and breadcrumbs.
ui.layout.showNav	Controls the Navigation bar. **Note:** No default content is included for the navigation bar.

To customize the layout, complete the following steps:

Procedure

1. Make a backup copy of the `SelfServiceUI.properties` file in your local computer.
2. Edit the `SelfServiceUI.properties` file. Modify the values of the screen text fields and save the file. See "Managing the server properties" on page 22.
3. Restart the Security Identity Manager application to make the changes effective.

Customizing banner, footer, toolbar, and navigation bar content

You can change the appearance of the self-service user interface by customizing the banner, footer, toolbar, and navigation bar.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Content in the `directories\itim_self_service.war\custom` directory can be replaced or modified to alter the appearance of the self-service user interface. You can replace or modify the banner, footer, toolbar, and navigation bar.

The layout elements are JSP fragments that are included in the layout of the web page when the JSP is rendered.

The following table displays a list of layout elements and their corresponding files, which are in the `directories\itim_self_service.war\custom` directory.

Table 19. Layout elements and file names

Layout element	File name
Banner	banner.jsp
Footer	footer.jsp
Toolbar	toolbar.jsp
Navigation bar	nav.jsp

To modify these files, complete these steps:

Procedure

1. Make backup copies of the files and store the files you want to modify in a temporary directory.
2. Edit the files in the temporary directory and copy the updated files back into the deployed WebSphere® directory. No restart of the IBM Security Identity Manager application is required for these changes to take effect.

What to do next

The default version of these files is shipped with the product archive. Be sure to back up the custom version of the files you created so that your changes are not lost.

Request parameters and content examples for use in customizing user interface content

This section describes the request parameters that you can use in JSP files to customize content.

Request parameter values

To support dynamic content such as `breadcrumbs`, help links and user IDs, a few request parameters are available. The following table shows these properties, their possible values, and a description.

Table 20. Request parameters, values, and descriptions

Property name	Value	Description
loggedIn	true or false	Flag that indicates whether the user is logged in.
usercn	The common name of the owner of the logged in account	**Note:** This value is only set if the user is logged in.
langOrientation	ltr or rtl	Indicates the language direction of the current locale, either left to right, or right to left.
helpUrl	/itim/self/ Help.do?helpId=*example_url*	URL to the help web page with the *helpId* parameter set for the current page.
helpLink	Example: home_help_url	The *helpId* for the current page. The value *home_help_url* maps to the corresponding key in the `SelfServiceHelp.properties` file.
breadcrumbs	*example_message_key1* *example_message_key2* *example_message_key3*	A list of message keys that correspond to entries in the `SelfServiceScreenText.properties` file.
breadcrumbLinks	*pathname1* *pathname2* *empty_string*	A list of links that is the same length as the breadcrumbs list.

Examples of request parameters in toolbar.jsp

The default file `toolbar.jsp` contains the logic to display the welcome message and help links. This logic can be moved into the other layout elements; for example, the welcome message might be provided in the banner.

Displaying the welcome message

The following code checks to see whether the user's common name is set. If so, it translates the welcome message and substitutes the name into the message.

Note: The self-service user interface message labels and keys are defined in the `SelfServiceScreenText.properties` file.

```
<%-- If the Users Common Name is not empty display it. Note this value is not
     set until the user is logged in --%>

<c:if test="${!empty usercn and loggedIn == true}">
    <%--Translate the Welcome, Common Name message passing in the name --%>
    <fmt:message key="toolbar_username" >
        <fmt:param><c:out value="${usercn}"/></fmt:param>
    </fmt:message>
</c:if>
</div>
<%-- end user info -- %>
```

Displaying help links

The following code adds the Help link to the page. The helpUrl is retrieved from help attributes, and the help label is translated for display.

```
<%-- Add Help Link to the page --%>

<a id="helpLink" href="javascript:launchHelp('<c:out value='${helpUrl}')">
      <fmt:message key="toolbar_help"/></a>
```

Supporting logoff

The Logoff link can only be displayed if the user is logged in. The following code tests to see whether the **loggedIn** request parameter is true. If so, the code translates the label for the logoff link and includes the link in the page.

```
<%-- If the user is logged in display the logoff link --%>
<c:if test="${loggedIn == true}">
   <a id="logofflink" href="/itim/self/Login/Logoff.do">
       <fmt:message key="toolbar_logoff"/></a>
</c:if>
```

Displaying breadcrumbs

The following code adds the breadcrumbs attribute to the page. The breadcrumbs attribute contains the list of label keys for the breadcrumbs attribute. The breadcrumbLinks contain URL information for each breadcrumb label. A value of null or empty for the breadcrumbLinks indicates that the breadcrumb is not linkable.

```
<%-- If the breadcrumbs label keys are not empty then display --%>

<c:if test="${!empty breadcrumbs}">
    <c:forEach items="${breadcrumbs}" var="breadcrumb" varStatus="status">

        <c:if test="${status.index > 0}">
            &nbsp;&gt;&nbsp;
        </c:if>

        <c:choose>
            <%-- If the action link is not empty for the current label then
                 create a link for the breadcrumb --%>

           <c:when test="${!empty breadcrumbLinks{status.index}}">
               <html:link action="${breadcrumbLinks{status.index}}">
               <fmt:message key="${breadcrumb}"/></html:link>
           </c:when>
           <%-- If the action link is empty then just translate the
                label for the breadcrumb --%>
           <c:otherwise>
               <fmt:message key="${breadcrumb}"/>
           </c:otherwise>
        <c:choose>

    </c:forEach>

</c:if>
```

Customizing the self-service home page

You can change the home page in the self-service user interface with customization.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

The home page refers to the main page that gets loaded in the content layout element after a user logs in to the self-service user interface.

Section and task definitions tie defined views to tasks, and group tasks into sections, also called task pages. These section and task definitions are defined in the `SelfServiceHomePage.properties` file in the `directories\data` directory.

The home page layout element is a JSP fragment that is included in the layout of the web page. This layout information is stored in the `Home.jsp` file in the `directories\itim_self_service.war\custom` directory.

You can add tasks and sections to the home page by updating the `SelfServiceHomePage.properties` file. The comments in the file explain the file format. You can alter the content without modifying the jsp file.

To customize the home page, complete these steps:

Procedure

1. Download a copy of the `SelfServiceHomePage.properties` file from `directories\data`. See “Managing custom files” on page 20.
2. Download a copy of the `Home.jsp` file from `directories\itim_self_service.war\custom`. See “Managing custom files” on page 20.
3. Edit the `SelfServiceHomePage.properties` file. Modify the values and save the file.
4. Upload the `Home.jsp` file to another directory, then modify the file in that directory and upload the updated file back into `directories\itim_self_service.war\custom`. The default version of these files is shipped with the product archive. Be sure to back up the custom version of the files you created so your customizations are not lost.
5. Restart the IBM Security Identity Manager application in the IBM Security Identity Manager virtual appliance to make the changes effective.

Request parameters and content examples for use in customizing the home page content

This section describes the request parameters that you can use in JSP files to customize home page content.

Home page form parameters

To support dynamic home page content such as sections, action-needed sections, tasks, a Java bean is available as a request parameter called **HomePageForm**. The home page Java bean contains a handful of methods that can be used to access information about sections and tasks.

Table 21. Home page request parameters, values, and descriptions

Property name	Value	Description
sections	List of Section Java beans	A list of sections the current user can view.
sectionToTaskMap	Map of sections to their corresponding tasks	A map that links a specified section Java bean to a task Java bean.
actionNeededSection	Section Java bean, or null	A section Java bean that contains the pending actions for the current user. A null is used if no pending actions exist for the current user.

The following properties are available for the section Java bean:

Table 22. Section Java bean request parameters, values, and descriptions

Property name	Value	Description
titleKey	Title message key for the section	The message key for the section title.
iconUrl	Icon URL, or null	The URL path for the icon to be used for the section. A null is used to indicate that no icon is used.
iconAltTextKey	Text key	Text key to be used as the alternate text for the icon of the section.
tasks	List of task Java beans	A list of tasks that can be displayed in the section

The following properties are available for the task Java bean:

Table 23. Task Java bean request parameters, values, and descriptions

Property name	Value	Description
urlPath	URL	A URL path to this task.
urlKey	Text key	The text key to be used for the link to this task.
descriptionKey	Text key	Text key to be used as the description of this task.

Examples of request parameters in home.jsp

The following code obtains the **HomePageForm** Java bean and iterates through the available sections and tasks and creates links to each available task.

```
<c:set var="pageConfig" value="${HomePageForm}" scope="page" />
<c:forEach items="${pageConfig.sections}" var="section">
      <%-- Process each section here --%>
      <c:forEach items="${pageConfig.sectionToTaskMap[section]}" var="task">
      <%-- Process each section here --%>
            <a href="/itim/self/<c:out value="${task.urlPath}"/>"
               title="<fmt:message key="${task.urlKey}" />">
               <fmt:message key="${task.urlKey}" />
            </a>
            <fmt:message key="${task.descriptionKey}" />
        </c:forEach>
</c:forEach>
```

Customizing style sheets

You can change the appearance of the self-service user interface by customizing Cascading Style Sheets (CSS).

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Cascading Style Sheets (CSS) are used to style the appearance of the self-service user interface. You can edit the style sheets to modify the fonts, colors, and other styles associated with the self-service user interface. This section describes the location of the style sheets, and key styles to edit to customize the user interface to match the look and feel of your website.

The default deployed CSS files are compressed and optimized with bandwidth in mind for scalability. The non-optimized versions (with whitespace/formatting intact) can be found in the `directories\defaults\custom` directory. The CSS files stored in the `directories\itim_self_service.war\custom` directory are unsuitable for editing. Copy the default files stored in the `directories\defaults\custom` directory to another directory. Edit the style sheets and then copy your changed files to the `directories\itim_self_service.war\custom` directory.

The following table shows the CSS files that can be modified to adjust the self-service user interface.

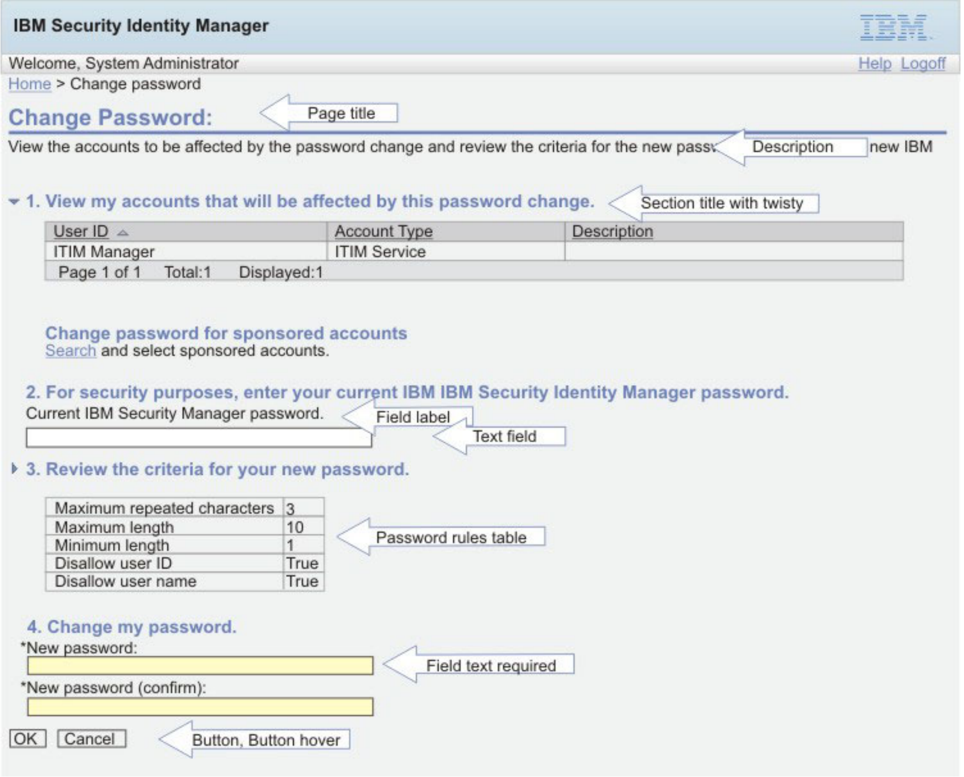
Table 24. Cascading Style Sheet file names

CSS file name	Description
end_user.css	CSS file that contains main CSS styles for left to right language orientation.
end_user_rtl.css	CSS file that contains main CSS styles for right to left language orientation.
widgets.css	CSS file that contains styles used for widgets, such as those contained in Profile, Account, and RFI forms, for left to right language orientation. **Note:** Editing this file takes more advanced CSS skills.
widgets_rtl.css	CSS file that contains styles used for widgets, such as those contained in Profile, Account, and RFI forms, for right to left language orientation. **Note:** Editing this file takes more advanced CSS skills.

Table 24. Cascading Style Sheet file names (continued)

CSS file name	Description
dateWidget_ltr.css	CSS file that contains styles used for date widgets, such as those contained in Profile, Account, and RFI forms, for left to right language orientation. **Note:** Editing this file takes more advanced CSS skills.
dateWidget_rtl.css	CSS file that contains styles used for date widgets, such as those contained in Profile, Account, and RFI forms, for right to left language orientation. **Note:** Editing this file takes more advanced CSS skills.
time.css	CSS file that contains styles used for time widgets, such as those contained in Profile, Account, and RFI forms. **Note:** Editing this file takes more advanced CSS skills.
customForm.css	CSS file that contains styles used for layout forms, such as those contained in Profile, Account, and RFI forms, for left to right language orientation. **Note:** Editing this file takes more advanced CSS skills.
customForms_rtl.css	CSS file that contains styles used for layout forms, such as those contained in Profile, Account, and RFI forms, for right to left language orientation. **Note:** Editing this file takes more advanced CSS skills.

The following figures provide a visual representation of page elements for which style changes can apply.



IBM Security Identity Manager

Welcome, System Administrator Help Logoff

Home > Change password

Change Password:

View the accounts to be affected by the password change and review the criteria for the new passw new IBM

1. View my accounts that will be affected by this password change.

User ID	Account Type	Description
ITIM Manager	ITIM Service	
Page 1 of 1 Total:1 Displayed:1		

Change password for sponsored accounts
Search and select sponsored accounts.

2. For security purposes, enter your current IBM IBM Security Identity Manager password.

Current IBM Security Manager password.

3. Review the criteria for your new password.

Maximum repeated characters	3
Maximum length	10
Minimum length	1
Disallow user ID	True
Disallow user name	True

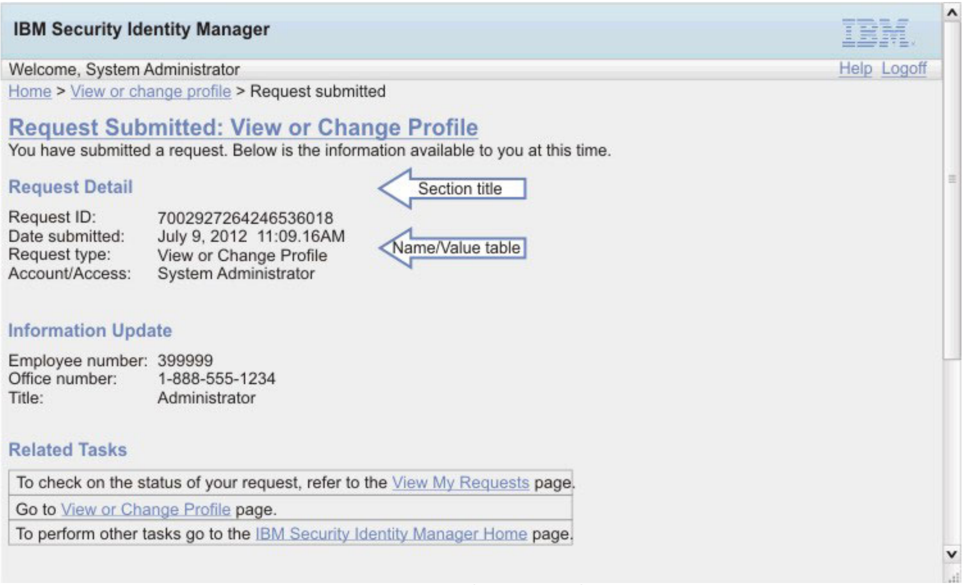
4. Change my password.

*New password:

*New password (confirm):

OK Cancel

Figure 7. Page elements for style changes



IBM Security Identity Manager

Welcome, System Administrator Help Logoff

Home > View or change profile > Request submitted

Request Submitted: View or Change Profile

You have submitted a request. Below is the information available to you at this time.

Request Detail

Request ID:	7002927264246536018
Date submitted:	July 9, 2012 11:09.16AM
Request type:	View or Change Profile
Account/Access:	System Administrator

Information Update

Employee number:	399999
Office number:	1-888-555-1234
Title:	Administrator

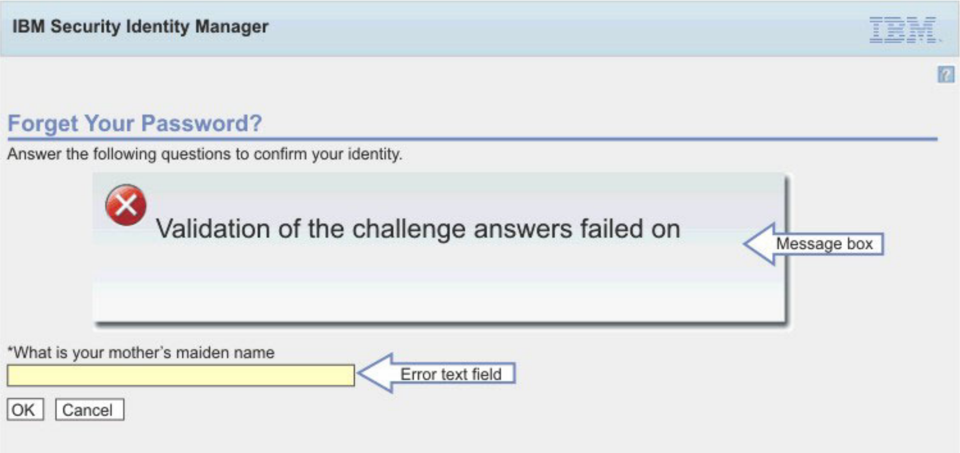
Related Tasks

To check on the status of your request, refer to the View My Requests page.

Go to View or Change Profile page.

To perform other tasks go to the IBM Security Identity Manager Home page.

Figure 8. Page elements for style changes (continued)



IBM Security Identity Manager

Forget Your Password?

Answer the following questions to confirm your identity.

Validation of the challenge answers failed on

*What is your mother's maiden name

Figure 9. Page elements for style changes

The following table provides a reference for the main CSS styles.

Table 25. CSS styles reference

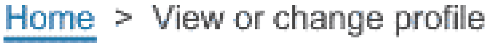
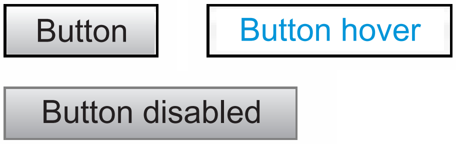
Element	**Example**	**Main style selector**	**Description**
Page Title	**Page Title**	Type selector: h1	Element used for all page titles.
Section title	**Subsection Title**	Type selector: h2	Section titles for pages that do not contain a twisty.
Section title (twisty)	**Twisty Title**	Type selector: h3	Section titles on pages which contain twisty sections. The titles are intended to allow space for the twisty image.
Breadcrumbs	 Home > View or change profile	Type selector: #breadcrumbs	The breadcrumbs navigation trail shown on the top left above the page title.
Button, Button Hover, Disabled Button		Class selectors: • .button • .button_hover • .button_disabled	These button styles cover the majority of buttons in the user interface. The hover style is used when a mouse hovers over the button

Table 25. CSS styles reference (continued)

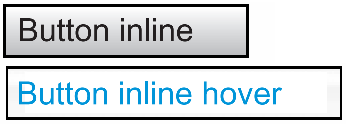
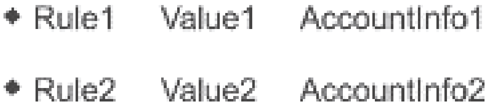
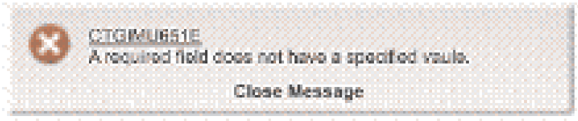
Element	Example	Main style selector	Description
Inline button, Inline button hover		Class selectors: • .button_inline • .button_inline_hover	Used for a subset of buttons with special layout requirements.
Page/section descriptions	This is a description.	Class selector: .description	Page and section descriptions. The description is contained in a <div> block. Therefore, you could add borders, colors, etc. if desired.
Field labels	Field label	Type selector: label	Field labels on forms.
Text field	Text field (white field background default)	Class selector: input.textField_std	Standard text fields.
Required text field	Required text field (yellow field background default)	Class selector: input.textField_required	Required text fields.
Error text field	Error text field (red field border default)	Class selector: input.textField_error	Text fields in an error state.
Warning text field	Warning text field (yellow field border default)	Class selector: input.textField_warning	Text fields in a warning state.

Table 25. CSS styles reference (continued)

Element	Example	Main style selector	Description
Field/value tables	Field Name1 Field value1 Field Name2 Field value2 Multi-valued Field3 Item 1 Item 2 Item 3 Item 4 Multi-valued Field3 Item 1 Item 2	Class selector: table.nameValueTable	Field value tables are used through out the user interface to display a field name and one or more corresponding values. For example, the Information section of the request submitted pages use name value tables. The selector is shown for the table. Additional selectors exist that style the rows, cells, multi-value lists, and name columns for this table.
Password rules table	 ◆ Rule1 Value1 AccountInfo1 ◆ Rule2 Value2 AccountInfo2	Class selectors: • .pwRulesTable • .pwRulesTable .ruleCol • .pwRulesTable .valueCol • .pwRulesTable .accountInfoCol • .button_inline_hover	The password rules table is used to style the password rules sections through out the user interface. The table consists of three columns; a rule column, a value column, and an account information column.
Message box	 CTGIMU651E A required field does not have a specified vaule. 	div.messageBoxComposite	The message box composite is the main CSS selector for the message box. Additional selectors exist to specify the image / link / and message layout.

To customize the style sheets, complete these steps:

Procedure

1. Download copy of the CSS files in the `directories\itim_self_service.war\custom` directory. See "Managing custom files" on page 20.
2. Upload the CSS files from the `directories\defaults\custom` directory to another directory, then modify the files in that directory and upload the updated files to the `directories\itim_self_service.war\custom` directory. Be sure to back up the custom version of the files you created so your customizations are not lost.

   See "Managing custom files" on page 20.

Merging style sheet customization from a previous version

After upgrading from a previous version of IBM Tivoli® Identity Manager, you must reapply any customizations you made to the cascading style sheet for the self-service user interface.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

You need access to the file system on which IBM Tivoli Identity Manager is deployed.

You must have a working knowledge of Security Identity Manager and cascading style sheets (CSS).

About this task

Customizations, including view definitions, that are defined through the administrative console are preserved during an upgrade. Updates to SelfServiceScreenText.properties are automatically merged as well.

However, after the upgrade program completes, the deployed self-service cascading style sheet (CSS) is restored to factory defaults. First merge the updated CSS values into your customized CSS skin created for your previous version of the product. Then reapply your customized files to the deployed self-service war.

Note: During the upgrade, `ITIM.ear` file is backed up from WebSphere application server to `*ISIM_HOME*/data/backup/ITIM.ear` directory. You can view the `itim_self_service.war/custom` directory for a copy of the CSS skin that was deployed before the upgrade.

To merge CSS customizations, make the following additions and modifications to your original IBM Tivoli Identity Manager CSS files.

Note: If modifications for right-to-left (RTL) CSS files (for example, `enduser_rtl.css`) were made, merge the modifications by using a text comparison tool. Make the equivalent changes to the `enduser_rtl.css` file as the `enduser.css` file, but adjust for the right-to-left layout.

Procedure

1. Open your existing CSS file with an editor.

   This file can be found in the directory *ISIM_HOME*/data/backup/ITIM.ear

   Note: For a separate system upgrade, copy the files from the deployed ITIM.ear file.
2. Add the appropriate changes based on your migration path. See "CSS updates."

   For migration from Version 5.0 to Version 6.0, add the CSS changes made in both Version 5.1 and Version 6.0.

   For migration from Version 5.1 to Version 6.0, add the CSS changes made in Version 6.0 only.
3. Copy the updated CSS files to the Self Service user interface custom directory itim_self_service.war/custom.

Results

These modifications take effect immediately, and no restart of the Security Identity Manager application is required.

CSS updates

CSS changes added in 5.1:

enduser.css

Description: Added twistie for h2 headings.

Add the following text:

```
a.twistie_open h2{
 margin-left:0px;
 background-repeat: no-repeat;
 background-position: left;
 padding-left: 15px;
 background-image: url("/itim/self/images/twistie_open.gif");
}

a.twistie_closed h2{
 margin-left:0px;
 background-repeat: no-repeat;
 background-position: left;
 padding-left: 15px;
 background-image: url("/itim/self/images/twistie_closed.gif");
}
```

Description: Changed Review Activities instructions to be a twistie.

Add the following text:

```
/* Review Activity Styles */
#instructionDetailTwistieDiv {
 white-space: expression("pre"); /* IE */
 white-space: -moz-pre-wrap; /* Firefox */
 word-wrap: break-word;
}
/* End Review Activity Styles */
```

Description: Added CSS Styles for User Recertification.

Add the following text:

```
/* Recertification items table styles */
table.recertItemsTable {
 width: auto;
}

table.recertItemsTable th {
 padding: .2em 1em .2em 1em;
 background-color: #C0C0C0;
 white-space: nowrap;
 text-align: left;
}

table.recertItemsTable td {
 padding: .2em 1em .2em 1em;
 border: 1px solid #C0C0C0;
}

table.recertItemsTable tr.recertItemRow td {
 border-bottom-style: none;
}

table.recertItemsTable tr.recertSubItemRow td {
 border-top-style: none;
 border-bottom-style: none;
}

table.recertItemsTable tr.altRow {
 background-color: #F6F6F6;
}

table.recertItemsTable .selectAllOptions {
 display: inline;
 padding: 0 .5em 0 .5em;
 font-weight: normal;
}

table.recertItemsTable .selectAllOptions a {
 padding: 0 .3em 0 .3em;
 color:#1375D7;
 font-weight: normal;
}

table.recertItemsTable .recertItemSelectAllOptions {
 display: inline;
 padding: 0 .5em 0 .5em;
 font-weight: normal;
 font-size: .8em;
}

table.recertItemsTable .recertItemSelectAllOptions a {
 padding: 0 .3em 0 .3em;
}

table.recertItemsTable a.recertExpandCollapseLink {
 margin-right: .2em;
}

table.recertItemsTable a.recertExpandCollapseLink img {
 border: none;
 vertical-align: bottom;
}

table.recertItemsTable div.recertItem {
 display: inline;
 margin-bottom: 2px;
}
```

```
table.recertItemsTable td.recertItemImpact {
 text-align: center;
}

table.recertItemsTable div.recertItemDescription {
 max-width: 300px;
 font-size: .8em;
}

table.recertItemsTable div.recertItemImpactedBy {
 display: inline;
 margin-bottom: 2px;
}

table.recertItemsTable td.recertItemActionRecertify {
 width: expression("0%"); /* IE */
 width: 1px; /* Firefox */
 white-space: nowrap;
 padding-right: 0;
 border-right: none;
}

table.recertItemsTable td.recertItemActionRecertifyErrorNone {
 width: expression("0%"); /* IE */
 width: 1px; /* Firefox */
 white-space: nowrap;
 padding: .2em 0 .2em 13px;
 border-right: none;
}

table.recertItemsTable td.recertItemActionRecertifyErrorExists {
 width: expression("0%"); /* IE */
 width: 1px; /* Firefox */
 white-space: nowrap;
 padding: .2em 0 .2em 5px;
 border-right: none;
}

table.recertItemsTable td.recertItemActionReject {
 width: 0%;
 white-space: nowrap;
 padding-left: 0;
 border-left: none;
 border-right: none;
}

table.recertItemsTable td.recertItemActionBlank {
 height: 24px;
}

table.recertItemsTable label.recertItemAction {
 display: inline;
}

table.recertItemsTable td.recertItemSelectAll {
 width: 0%;
 white-space: nowrap;
 padding-left: 0;
 border-left: none;
}

table.recertItemsTable .recertSubItem {
    font-size: 1em;
    margin: 0 0 0 1em;
}

table.recertItemsTable div.recertItemDecision {
 display: block;
 margin-bottom: 2px;
 margin-top: 5px;
}
/* End recertification items table styles */

.simpleLink:link, .simpleLink:visited {
 font-weight: normal;
}


.requiredInstruction {
 font-size: .8em;
 margin: 1em 0 0 1em;
 background-image: url("/itim/self/images/required_field.gif");
 background-repeat: no-repeat;
 background-position: center left;
 padding-left: 12px;
}
```

CSS changes added in 6.0:

enduser_extra.css

Import enduser_extra.css

Add the following text:

```
@import "enduser_extra.css";
```

Description : Background color of self console has been changed to whitesmoke color.

Add the following style in body tag selector

```
background-color: #F5F5F5;
```

Description : Background color of banner has been changed to light blue.

Update the following style in banner id selector:

```
background-color: black;
```

to

```
background-color: #c8e0f8;
```

Description : Various changes in login screen.

Update the loginContainer id selector using the following style:

```
#loginContainer{
  width:619px;
  margin:20px auto;
  margin-left: auto ;
  margin-right: auto ;
    background-position:left top;
   background-repeat:no-repeat;
  background-color:#FFF;
  padding:0;
  border: solid 1px #bbbbbb;
  font-family:Arial,Verdana,Helvetica,Tahoma,sans-serif;
  font-size:12px;
  color:#555555;
  overflow: hidden;
  text-align: left;
  }
```

Description : Layout changes for product login image

Add the following style in loginImage id selector:

```
margin-left: 40px;
margin-top: -30px;
```

Description : Layout changes and font size changes for product version

Update content in loginVersion id selector:

```
margin-left: 110px;
font-size:10px;
```

Description : Layout changes and font size changes for login content

Update content in loginContent id selector

```
margin-left: 40px ;
margin-right: 20px ;
font-size:14px;
```

Description : Styling for new help link in login screen

Add the following style:

```
#loginToolbar {
  margin-right: 20px ;
  }
```

Description : Styling for message box

Add the following style:

```
#messageBox {
  margin-right:80px;
  font-size:14px;
  }
```

Description : Add an extra tag selector h2i to the existing group selector declaration box for h1, h2, h3. Also, add corresponding style for h2i tag selector.

Add the following style:

```
h2i {
  font-size:120%;
  border-bottom-style: none;
  border-bottom-width: 2px;
  margin-bottom: 0px;
  margin-left: 15px;
  }
```

Description : Added hand cursor for anchor.

Add the following style in pseudo class a:LINK, a:VISITED:

```
cursor: hand;
```

Description : Added a new class **descriptioni**.

Add the following style:

```
.descriptioni {
  display: block;
    margin-bottom: 20px;
  margin-left: 15px;
  }
```

Description : Added new style for tables.

Add the following style:

```
span.tableLayout {
  display:inline-block;
  min-width:80%;
  margin : 10px 10px 10px 0 ;
  }
```

Description : Updated width for table column header.

Add the following style in **thead th** selector:

```
width: auto;
```

Description : Added a new class dataTable

Add the following style:

```
.dataTable {
  width:100%;
  margin: 0px;
  }
```

Description : Added a new class customHeader

Add the following style:

```
customHeader {
  text-align: left;
  border-style: solid;
  background-color: #E6E6E6;
   border-width:1px 1px 1px 1px;
  border-color:#C8C8C8 #C8C8C8 #737373 #C8C8C8;
  width: auto;
  }
```

Description : Added a new class customHeaderTable

Add the following style:

```
.customHeaderTable {
  border-top-style:hidden;
  }
```

Description : Updated the width of anchors in column header

Add the following style in **thead th a:LINK, thead th a:VISITED** selector:

```
width: auto;
```

Description : Added style for account tables

Add the following style:

```
table #global_table_accounttype {
   width: 20%;
  }
  table #global_table_userid_10 {
    width: 10%;
    }

  table #global_table_description_30 {
  width: 30%;
  }
```

Description : Added a new class viewRequestsCustomHeaderStyle

Add the following style:

```
.viewRequestsCustomHeaderStyle{
  text-align: left;
  padding: 5px;
  vertical-align: middle;
  }
```

Description : Added style for custom header labels

Add the following style:

```
div.viewRequestsCustomHeaderStyle label{
  display: inline;
  font-weight:bold;
  }
```

Description : Added new style for recertItemOwnershipType

Add the following style:

```
table.recertItemsTable div.recertItemOwnershipType {
   max-width: 300px;
  font-size: 1em;
  }
```

Description : Added styles for table cells

Add the following style:

```
div.tableCellContent {
  white-space:nowrap;
  overflow:hidden;
  width:25em;
  text-overflow:ellipsis;"
  }
```

Add an extra tag class tfootTd to the existing group selector declaration box for tfoot th selector. Also, add an extra tag class label to the existing group selector declaration box for label selector.

Description : Removed following styles that are not used anymore.

Remove the following styles:

```
th.reviewActivitiesCustomHeader {
  text-align: left;
  border-style: solid;
  border-width:1px 1px 1px 1px;
  background-color: #E6E6E6;
  border-color:#FFFFFF #C8C8C8 #737373 #FFFFFF;
  }

.simpleLink:link, .simpleLink:visited {
  font-weight: normal;
  }
```

```
    .label_accessibility {
     display: none;
    }

  .requiredInstruction {
     font-size: .8em;
     margin: 1em 0 0 1em;
     background-image: url("/itim/self/images/required_field.gif");
     background-repeat: no-repeat;
     background-position: center left;
     padding-left: 12px;
    }
```

What to do next

These modifications take effect immediately. A restart of the Security Identity Manager application is not required.

Redirecting help content

You can redirect help requests to your own website to deliver custom help content.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Editing the out-of-the box help content shipped with the self-service user interface is not supported. But it is possible to redirect help requests to your own website to deliver custom help content in line with your corporate appearance.

The SelfServiceHelp.properties file specifies the base URL that help requests are sent to. See "Managing the server properties" on page 22.

The following table shows the property and property description for self-service help.

Table 26. Self-service help properties and description

Property	Description
helpBaseUrl	Specifies the base URL to send help requests to. A blank value indicates that help goes to the default URL for the self-service user interface.
Help Id mappings: helpId = relative page URL	The help mappings section maps IDs from specific pages to a relative URL sent to the help server.

The Help URL is the combination of the helpBaseUrl + locale + relativeHelppageURL

For example:

```
helpBaseUrl=http://myserver:80
locale = en_US
```

Locale is determined by resolving the SelfServiceScreenText.properties resource bundle for the current logged in user and with the associated locale.

```
loginId/relativeURL = login_help_url=ui/ui_eui_login.html
```

Therefore, the final URL = http://myserver:80/en_US/ui/ui_eui_login.html.

To redirect help, complete these steps:

Procedure

1. Make a backup copy of the `SelfServiceHelp.properties` file in your local computer.
2. Change the helpBaseUrl property in the `SelfServiceHelp.properties` file.
3. Update helpId mappings to use the relative URLs for your server.
4. Add pages to your server for the appropriate locales.
5. Restart the IBM Security Identity Manager application to make the changes effective.

Configuration of direct access to self-service tasks

Many pages in the interface can be directly accessed from other HTML pages or integrated with a company intranet portal.

The user must first authenticate by either logging in through the Login page or through a single sign-on. When a user attempts to access a page for which direct access is supported, the following occur:

- If the page is defined by a configured view, the page is displayed.
- If the page is not in a configured view, an error page is displayed instead of the requested page.

Note: Direct access to the **Approve and Review Requests** task is supported even if it is not enabled in a configured view. Also, depending on group membership, more than one view configuration might apply. If at least one view configuration that applies to a user includes the task that the user is attempting to access, the page is displayed.

The following table displays tasks and URLs that are supported for direct access, and that you can link to from your company intranet portal.

Table 27. Direct-access tasks and URLs

Task	URL
Logon Page	http://*server_name*/itim/self
Change Password	http://*server_name*/itim/self/PasswordChange.do
Change Forgotten Password Information	http://*server_name*/itim/self/changeForgottenPasswordInformation.do
Expired Password (bypass the Login page)	http://*server_name*/itim/self/Login/DirectExpiredPasswordChange.do?expiredUserId=*userID* **Note:** This solution works only if single sign-on is not enabled and the ui.directExpiredChangePasswordEnabled property is set to true in SelfServiceUI.properties file.
Request Access	http://*server_name*/itim/self/RequestAccess.do
Request Access (for a specific access request)	http://*server_name*/itim/self/RequestAccess.do?accessDN=*accessDN*

Table 27. Direct-access tasks and URLs (continued)

Task	**URL**
View Access	http://*server_name*/itim/self/ViewAccess.do
Delete Access	http://*server_name*/itim/self/DeleteAccess.do
Delete Access Confirmation (for a specific access deletion)	http://*server_name*/itim/self/DeleteAccess.do?accessDN=*accessDN*
Request Account	http://*server_name*/itim/self/RequestAccounts.do
Request Account (directly access the request account form for a specific service)	http://*server_name*/itim/self/RequestAccounts.do?serviceDN=*serviceDN*
View Account	• http://*server_name*/itim/self/ViewAccount.do (multiple accounts view) • http://*server_name*/itim/self/ViewAccount.do?userID=*userID*&serviceDN=*serviceDN* (specific service account)
View or Change Account	http://*server_name*/itim/self/ViewChangeAccount.do
Change Account	• http://*server_name*/itim/self/ChangeAccount.do (multiple accounts view) • http://*server_name*/itim/self/ChangeAccount.do?userID=*userID*&serviceDN=*serviceDN* (specific service account)
Delete Account	http://*server_name*/itim/self/DeleteAccount.do
Delete Account Confirmation	http://*server_name*/itim/self/DeleteAccount.do?userID=*userID*&serviceDN=*serviceDN* (specific service account)
View Profile	http://*server_name*/itim/self/ViewProfile.do
Change Profile	http://*server_name*/itim/self/ChangeProfile.do
View or Change Profile	http://*server_name*/itim/self/ViewChangeProfile.do
View My Requests	• http://*server_name*/itim/self/ViewRequests.do (multiple requests view) • http://*server_name*/itim/self/ViewRequests.do?request=*requestID* (specific request view)
Approve and Review Requests	• http://*server_name*/itim/self/ReviewActivities.do (multiple activity view) • http://*server_name*/itim/self/ReviewActivities.do?activity=*activityID* (specific activity view)
Delegate Activities	http://*server_name*/itim/self/delegateActivities.do
Check out Credential (available only if shared access module is installed and configured)	http://*server_name*/itim/self/CheckoutSharedAccount.do
Check in Credential (available only if shared access module is installed and configured)	http://*server_name*/itim/self/CheckinSharedAccount.do

Table 27. Direct-access tasks and URLs (continued)

Task	URL
View Password (available only if shared access module is installed and configured)	http://*server_name*/itim/self/ViewPassword.do

Customizing person search capability

You can enable person search capability in the self-service user interface.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Person search capability is a powerful feature that you can use to select only people that match certain search criteria. Person search filters a wide range of search attributes.

The names of attributes take the form of `ui.usersearch.attr.`*attribute_name=attribute_name* in cases where *attribute_name* is common to all person and business partner person profiles. The *attribute_name* is a value that maps to that profile attribute. For example, `ui.usersearch.attr.cn=cn` searches by common name.

Some single attributes can map to multiple attributes if the profiles vary. In this case, the names of attributes take the form of `ui.usersearch.attr.`*attribute_name=profile1.attribute_name1*`,`*profile2.attribute_name1*

For example, `ui.usersearch.attr.telephone=Person.mobile,BPPerson.telephonenumber` would map the mobile number for the person profile and the telephone number for the business partner person profile.

The translated value of the attribute name is displayed in the search by attribute box. Do not specify attributes that cannot be searched by using plain text. For example, audio, photo, and other similar items.

To enable person search capability for the self-service user interface, complete these tasks:

Procedure

1. Make a backup copy of the `SelfServiceUI.properties` file in your local computer.
2. Add or remove attributes in the `SelfServiceUI.properties` file under the **User Search** configuration section.
3. Restart the IBM Security Identity Manager application to make the changes effective.

Administrative console user interface customization

This section describes how to customize the administrative console user interface.

The IBM Security Identity Manager administrative console user interface is customizable. Customers can integrate a common corporate appearance while maintaining the flexibility to do administrative identity tasks integral to their roles and responsibilities.

You can define and customize the administrative console interface in two ways, by using the built-in console framework and by directly modifying files installed within IBM Security Identity Manager:

- Built-in console features:
  - Access control items (ACIs)
  - Views
- Modifiable files:
  - Properties files
  - Image files

Back up any modifiable files for recovery purposes before making customization changes to IBM Security Identity Manager.

Configuration files and their descriptions

Configuration files define the appearance of the IBM Security Identity Manager administrative console user interface.

The following table lists the file names and describe their roles in the customization of IBM Security Identity Manager.

Table 28. Configuration property files and descriptions

File Name	File Description
ui.properties	Controls the appearance of the header, footer, and home page, and configures the title, number of pages that are displayed, and the number of search results returned.
helpmapping.properties	Controls the redirection and mapping of administrative console html help.

Backing up and restoring administrative console user interface configuration files

Before you begin customization of the administrative console user interface, back up all configuration files in IBM Security Identity Manager for later recovery purposes.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Create a directory named `custom` in the `directories\itim_console.war` directory and store any new customization files in that custom directory. See “Managing custom files” on page 20.

Log in to each computer that is running Security Identity Manager and back up the following files:

- In the `directories\data` directory:
  - `ui.properties`
  - `helpmappings.properties`

About this task

Any changes made to properties files require you restart the Security Identity Manager application. For instance, upon recovering any properties files, complete these steps:

Procedure

1. From the **Server Control** widget, do these steps.
   a. Select **Security Identity Manager server**.
   b. Click **Restart**.

   See Viewing the Server Control widget.
2. Verify that the recovery is complete by logging in to the administrative console user interface.

Customizing banner content

You can change the appearance of the administrative console user interface by customizing the banner.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

You can add or modify banner content to alter the appearance of the administrative console user interface.

The default banner area is defined in two files, a JSP file named `banner.jsp` and a properties file named `ui.properties`. The banner area consists of four parts:

- Banner launch link
- Banner launch logo
- Banner logo
- Banner background image

When customizing the banner, adjust the dimensions (width and height) of the components in the banner.jsp. Adjust these dimensions so that the custom logo image is sized properly without any distortion. Also ensure that the entire banner frame is not distorted.

You can change the banner launch link and logo by modifying the `ui.properties` file. If you want to modify the background image and banner logo, you must create a file to display your banner. This file can be either an HTML or a JSP banner file.

The following property keys in the `ui.properties` file define the banner launch link and banner launch logo. They also define the URL to the banner background image and logo.

Table 29. Banner property keys

Property key	Default value	Description
enrole.ui.customerLogo.image	ibm_banner.gif	Launch link logo, located in the `directories\itim_console.war\html\images` directory. You can also specify a URL pointing to the image file or put this file in the `directories\itim_console.war\custom` directory. If this directory does not exist, you must create it. Prefix the path name with `/itim/console/custom` in the `ui.properties` file. Specifying no value results in the default ibm_banner.gif file being displayed.
enrole.ui.customerLogo.url	www.ibm.com	Launch link URL. This value can be specified with or without the HTTP prefix. For instance, you can use `www.ibm.com` or `http://www.ibm.com` to specify the launch link URL.
ui.banner.URL	This value is left blank by default and displays the default banner area.	The HTML or JSP file that provides the banner logo, background image, and launch link and logo. You can enter either a URL or put this file in the `directories\itim_console.war\custom` directory If this directory does not exist, you must create it. Prefix the path name with `/itim/console/custom` in the `ui.properties` file.
ui.banner.height	48	Enter the pixel height of the banner.

To modify these files, complete these steps:

Procedure

1. Edit the files in the temporary directory and upload the updated file. See “Managing the server properties” on page 22.
2. Restart the IBM Security Identity Manager application for these changes to take effect.
   a. From the **Server Control** widget, do these steps.
      1) Select **Security Identity Manager server**.
      2) Click **Restart**.

      See Viewing the Server Control widget.

What to do next

Be sure to back up the custom version of the files you have created so your customizations are not lost.

Customizing footer content

You can change the appearance of the administrative console user interface by customizing the footer.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

You can add or modify footer content to alter the appearance of the administrative console user interface.

The default footer area is defined in the `ui.properties` file.

The following property keys in the `ui.properties` file define the footer and specify its visibility and height.

Table 30. Footer property keys

Property key	Default value	Description
ui.footer.isVisible	no	Specifies whether the footer is visible. By default the footer is disabled.
ui.footer.URL	This value is left blank by default.	Specifies the location of the HTML or JSP file that provides the footer. You can enter a URL. Alternatively, put this file in the `directories\itim_console.war\custom` directory (if this directory does not exist, you must create it), and prefix the path name with `/itim/console/custom` in the `ui.properties` file.
ui.footer.height	50	Enter the pixel height of the footer.

To modify these files, complete these steps:

Procedure

1. Edit the files in the temporary directory and upload the updated file. See “Managing the server properties” on page 22.
2. Restart the IBM Security Identity Manager application for these changes to take effect.
   a. From the **Server Control** widget, do these steps.

1) Select **Security Identity Manager server**.

2) Click **Restart**.

See Viewing the Server Control widget.

What to do next

Be sure to back up the custom version of the file you created so your customizations are not lost.

Customizing the administrative console home page

You can change the home page in the administrative console user interface with customization.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

The home page refers to the main page that gets loaded after a user logs in to the administrative console user interface.

Section and task definitions tie defined views to tasks, and group tasks into sections, also called task pages. These section and task definitions are defined in a properties file in the `directories\data` directory. See "Managing the server properties" on page 22

You can code direct links to tasks from the home page to administrative functions. Use JSP to generate dynamic HTML so administrative functions are limited to users with the appropriate authority.

To customize the home page, complete these steps:

Procedure

1. Edit the `ui.properties` file. Modify the `ui.homepage.path` key, and save the file. See "Managing the server properties" on page 22.
2. Enter a URL of the HTML or JSP file that you are using for a home page. Alternatively, put this file in the `directories\itim_console.war\custom` directory (if this directory does not exist, you must create it), and prefix the file name with `/itim/console/custom`. See "Managing custom files" on page 20.
3. Restart the IBM Security Identity Manager application for these changes to take effect.
   a. From the **Server Control** widget, do these steps.
      1) Select **Security Identity Manager server**.
      2) Click **Restart**.

      See Viewing the Server Control widget.

Direct-access URL links to administrative console tasks

This section provides the direct URL access links to tasks in the administrative console user interface.

The following table displays the links to tasks that are supported for direct access, and that you can link to from the home page.

Table 31. Direct access tasks and links

Task	URL
Change Password	<a href="/itim/console/home/task/chopass">Change Password</a>
Manage Roles	<a href="/itim/console/home/task/manage_orgroles">Manage Roles</a>
Manage Organization Structure	<a href="/itim/console/home/task/manage_org_structure">Manage Organization Structure</a>
Manage Users	<a href="/itim/console/home/task/manage_people">Manage Users</a>
Manage Services	<a href="/itim/console/home/task/manage_services">Manage Services</a>
Manage Identity Policies	<a href="/itim/console/home/task/manage_identity_policies">Manage Identity Policies</a>
Manage Password Policies	<a href="/itim/console/home/task/manage_password_policies">Manage Password Policies</a>
Manage Adoption Rules	<a href="/itim/console/home/task/manage_adoption_rules">Manage Adoption Rules</a>
Manage Recertification Policies	<a href="/itim/console/home/task/manage_recertification_policies">Manage Recertification Policies</a>
Manage Provisioning Policies	<a href="/itim/console/home/task/manageProvisioningPolicyTaskLauncher">Manage Provisioning Policies</a>
Manage Service Selection Policies	<a href="/itim/console/home/task/manageServiceSelectionPolicies">Manage Service Selection Policies</a>
Manage Account Request Workflows	<a href="/itim/console/home/task/manageAccountRequestWorkflows">Manage Account Request Workflows</a>
Manage Access Request Workflows	<a href="/itim/console/home/task/manageAccessRequestWorkflows">Manage Access Request Workflows</a>
Manage Groups	<a href="/itim/console/home/task/manage_groups">Manage Groups</a>
Manage Access Control Items	<a href="/itim/console/home/task/manage_acis">Manage Access Control Items</a>
Manage Views	<a href="/itim/console/home/task/defineViewFilter">Manage Views</a>
Set Security Properties	<a href="/itim/console/home/task/sysprops">Set Security Properties</a>
Configure Forgotten Password Settings	<a href="/itim/console/home/task/set_challenge_response">Configure Forgotten Password Settings</a>
Request Reports	<a href="/itim/console/home/task/reports_requests">Request Reports</a>
Service Reports	<a href="/itim/console/home/task/reports_services">Service Reports</a>

Table 31. Direct access tasks and links (continued)

Task	URL
Audit and Security Reports	<a href="/itim/console/home/task/reports_audit_and_security">Audit and Security Reports</a>
Custom Reports	<a href="/itim/console/home/task/reports_custom">Custom Reports</a>
Report Properties	<a href="/itim/console/home/task/reports_properties">Report Properties</a>
Configure Replication Schema	<a href="/itim/console/home/task/reports_schema">Configure Replication Schema</a>
Design Reports	<a href="/itim/console/home/task/designReports">Design Reports</a>
Manage Service Types	<a href="/itim/console/home/task/manservicetype">Manage Service Types</a>
Design Forms	<a href="/itim/console/home/task/designfrms">Design Forms</a>
Set Workflow Notification Properties	<a href="/itim/console/home/task/workflowNotificationProperties">Set Workflow Notification Properties</a>
Configure Post Office	<a href="/itim/console/home/task/post_office_configuration">Configure Post Office</a>
Manage Entities	<a href="/itim/console/home/task/manageEntities">Manage Entities</a>
Manage Operations	<a href="/itim/console/home/task/manageOperations">Manage Operations</a>
Manage Lifecycle Rules	<a href="/itim/console/home/task/manageLifecycleRules">Manage Lifecycle Rules</a>
Manage Access Types	<a href="/itim/console/home/task/manageAccessCategory">Manage Access Types</a>
Configure Policy Join Behaviors	<a href="/itim/console/home/task/config_policy_join">Configure Policy Join Behaviors</a>
Configure Global Policy Enforcement	<a href="/itim/console/home/task/global_policy_enforcement_configuration">Configure Global Policy Enforcement</a>
Import Data	<a href="/itim/console/home/task/import">Import Data</a>
Export Data	<a href="/itim/console/home/task/export">Export Data</a>
View Pending Requests by User	<a href="/itim/console/home/task/viewOthersPendingRequest">View Pending Requests by User</a>
View All Requests by User	<a href="/itim/console/home/task/viewAllOthersRequests">View All Requests by User</a>
View Pending Requests by Service	<a href="/itim/console/home/task/viewPendingServiceRequests">View Pending Requests by Service</a>
View All Requests by Service	<a href="/itim/console/home/task/viewRequestService">View All Requests by Service</a>

Table 31. Direct access tasks and links (continued)

Task	URL
View All Requests	<a href="/itim/console/home/task/viewAllRequests">View All Requests</a>
View Activities	<a href="/itim/console/home/task/view_todo_list">View Activities</a>
View Activities by User	<a href="/itim/console/home/task/viewtodosforothers">View Activities by User</a>
Manage Delegation Schedules	<a href="/itim/console/home/task/multiDelegateMyActivities">Manage Delegation Schedules</a>
About	<a href="/itim/console/home/task/about">About</a>
Define Forgotten Password Questions	<a href="/itim/console/home/task/defchallenges">Define Forgotten Password Questions</a>

Customizing the title bar

You can change the title bar shown in the web browser when you log in to the IBM Security Identity Manager administrative console.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

To customize the title bar, complete these steps:

Procedure

1. Make a backup copy of the `ui.properties` file and store the file in a temporary directory.
2. Edit the `ui.titlebar.text` property with the title you want to use, and save the file. The default value is blank and displays the text IBM Security Identity Manager. See "Managing the server properties" on page 22.
3. Upload the updated file. See "Managing custom files" on page 20.
4. Restart the IBM Security Identity Manager application for these changes to take effect.
   a. From the **Server Control** widget, do these steps.
      1) Select **Security Identity Manager server**.
      2) Click **Restart**.

      See Viewing the Server Control widget.

What to do next

Be sure to back up the custom version of the files you created so your customizations are not lost.

Redirecting help content

You can redirect help requests to your own website to deliver custom help content for the administrative console user interface.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Editing the out-of-the box help content shipped with the administrative console user interface is not supported. But it is possible to redirect help requests to your own website to deliver custom help content.

The `helpmappings.properties` file specifies the base URL that help requests are sent to. These files are in the `directories\data` directory.

The following table shows the property and property description for help.

Table 32. Administrative help properties and description

Property	Description
helpBaseUrl	Specifies the base URL to send help requests to. A blank value indicates that help goes to the default URL for the administrative console user interface.
Help ID mappings: helpID = relative page URL	The help mappings section maps IDs from specific pages to a relative URL sent to the help server.

The Help URL is the combination of the helpBaseUrl + locale + relativeHelppageURL

For example:

```
helpBaseUrl=http://myserver:80
locale = en_US
```

Note: Locale is determined by matching the current logged in user's browser settings with the currently installed IBM Security Identity Manager language packs.

```
loginID/relativeURL = login_help_url=ui/ui_eui_login.html
```

Therefore, the final URL is http://myserver:80/en_US/ui/ui_eui_login.html.

To redirect help, complete these steps:

Procedure

1. Make a backup copy of the `helpmappings.properties` file in the `directories\data` directory.
2. Change the `helpBaseUrl` property in the `helpmappings.properties` file. It is important that customers do not change the helpIDs. They are what the Security Identity Manager user interface panels use to find the appropriate help.

3. Update helpID mappings to use the relative URLs for your server.
4. Add pages to your server for the appropriate locales.
5. Restart the IBM Security Identity Manager application for these changes to take effect.
   a. From the **Server Control** widget, do these steps.
      1) Select **Security Identity Manager server**.
      2) Click **Restart**.

      See Viewing the Server Control widget.

Customizing the number of items displayed on pages

You can change the number of items displayed on pages.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

The following table shows the properties, default values, and description of these page parameters.

Table 33. Panel parameters, default values, and descriptions

Property	Default value	Description
enrole.ui.pageSize	50	Specifies the number of list items displayed on a page.
enrole.ui.maxSearchResults	1000	Specifies the maximum number of search items returned.

Note: These changes can affect memory usage if set to excessive values.

To change page parameters, complete these steps:

Procedure

1. Make a backup copy of the `ui.properties` file in the `directories\data` directory.
2. Edit the file in a temporary directory and copy the updated file back into the directory. See “Managing the server properties” on page 22.
3. Restart the IBM Security Identity Manager application for these changes to take effect.
   a. From the **Server Control** widget, do these steps.
      1) Select **Security Identity Manager server**.
      2) Click **Restart**.

      See Viewing the Server Control widget.

What to do next

Be sure to back up the custom version of the file so your customizations are not lost.

Configuring the Justification field in the user interface

You can add the **Justification** field to the user interface. You can also configure the **Justification** field to be a required field.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

By default, the **Justification** field is not displayed in the user interface. You can configure the properties so that the **Justification** field is displayed in the user interface. You can also configure the **Justification** field to be a required field.

The following table shows the properties, default values, and description of the parameters that are related to the **Justification** field. These properties settings are global and affect all user interface pages that contain the **Justification** field.

Table 34. Properties, default values, and descriptions

Property	Properties File	Default Value	Description
`ui.displayJustification`	`ui.properties`	`false`	Specifies whether the **Justification** field is displayed in the user interface.
`enrole.justificationRequired`	`enRole.properties`	`false`	Specifies whether the **Justification** field is displayed in the user interface as a required field.

To change the properties for the **Justification** field, complete these steps:

Procedure

1. Edit the files in a temporary directory and copy the updated file back into the `directories\data` directory:

Option	Description
To configure the Justification field to be displayed but not required	In the `ui.properties` file, set `ui.displayJustification=true`.

Option	Description
To configure the Justification field to be displayed *and* to be required, you modify the	In the `enRole.properties` file, set `enrole.justificationRequired=true`. **Note:** You do not need to modify the `ui.properties` file. If the `enrole.justificationRequired` property is set to `true`, then the **Justification** field is displayed as a required field regardless of the setting for the `ui.displayJustification` property in the `ui.properties` file.

2. Refresh the IBM Security Identity Manager application in your web browser. The **Justification** field is displayed in the user interface pages for which it applies.

What to do next

Be sure to back up the custom version of the files so that your changes are not lost.

Related reference:

Required field properties
These properties are used to configure whether fields in the user interface are required to be completed by the user.

ui.properties
The `ui.properties` file specifies attributes that affect the operation and display of the Security Identity Manager graphical user interface.

Identity Service Center user interface customization

The Identity Service Center user interface is highly customizable. You can change most of the screen text, icons, graphics, help file content, and layout. You can also change the contents of many user interface elements, such as the home page, user cards, and access cards.

You can customize the Identity Service Center user interface in the following ways:

- Copying and modifying the customizable files that are installed with IBM Security Identity Manager.
- Replacing the icons and graphics.

When the customized files are placed in the appropriate location, the IBM Security Identity Manager server can find and use them.

Without customization, you can use the Identity Service Center user interface to achieve goals such as these:

- Request access to applications
- View your requests

Location of Identity Service Center customizable files

As an administrator, if you want to customize the Identity Service Center, you must know where to find the files that IBM provides. You must also know where to put the customized versions of those files.

Customizable files are maintained in folders under the `\directories` directory. See “Managing custom files” on page 20.

The exact location depends on the use of a managed-clustered application server configuration. For a managed-cluster configuration, the customizable files are under the profile for the deployment manager. The files are pushed to application servers during synchronization.

Note: During the installation or maintenance upgrade, the customizable files that are provided by IBM are copied to an `original` folder under the `.../itim/custom/ui` folder. These files can be copied or used as a reference during the customization process. The files in the `original` folder are for reference only and are installed as Read-Only files. These files are only copies of the files that are used at run time. Changes to these files do not affect the Identity Service Center user interface.

See "Customizing Identity Service Center files" on page 87 for information about how to customize these files that IBM provides.

Maintenance upgrades to IBM Security Identity Manager add or replace files in the `original` folder so that the files are always the most recent versions.

The customizable files that are provided by IBM are organized into folders under the `.../itim/custom/ui/original` folder. By convention:

- Translatable files that contain screen text are under the `.../itim/custom/ui/original/nls` folder.
- Configuration files that contain non-translatable configuration properties are in the `.../itim/custom/ui/original/config` folder.
- Icons, graphics and other image files are under the `.../itim/custom/ui/original/images` folder.
- HTML templates that contain no translatable text are in the `.../itim/custom/ui/original/template` folder.

To work with these files from the IBM Security Identity Manager virtual appliance, see these sections:

- "Managing custom files" on page 20
- "Managing the server properties" on page 22

The following table lists the customizable files that are provided by IBM.

Table 35. Types and locations of customizable files

Locations of customizable files	Descriptions
nls/AdditionalInformation.properties nls/advanceSearchDialog.properties nls/BigCard.properties nls/CardCustomValue.properties nls/CardGrid.properties nls/Category Display.properties nls/common.properties nls/CriteriaTextBox.properties nls/DateTimeWidget.properties nls/DesignatedMaeesgeArea.properties nls/DualList.properties nls/ExpiredPassword.properties nls/filteringCardSelect.properties nls/HCard.properties nls/headerLabel.properties nls/LoginHour.properties nls/LoginPageCopyrightContent.properties nls/LoginPageInfoContent.properties nls/logMessages.properties nls/operators.properties nls/Picker.properties nls/PickerPage.properties nls/RequestAccess.properties nls/RequestListCard.properties nls/RequestStatusDetails.properties nls/RequestStatusList.properties nls/SearchCustomAttributes.properties nls/SearchCustomValue.properties nls/tmsMessagesUI.properties nls/UILanguages.properties nls/UMask.properties nls/validatorMessage.properties	These files contain screen text that is translated into multiple languages to support globalization. There are versions of each of these files for all of the supported locales. If you customize any of these files, you must also customize the locale-specific versions of the files. You must customize the files for all of the languages that you plan to support in your environment.
config/Access.json config/ActionDefinition.json config/HeaderMenu.json config/Homepage.json config/Person.json config/Search.json config/UIconfig.properties config/UIHelp.properties	These files contain configuration information that does not require language translation.

Table 35. Types and locations of customizable files (continued)

Locations of customizable files	Descriptions
images/approved.png images/companyLogo.gif images/favicon.ico images/getDetailsButton.png images/getDetailsButton_rtl.png images/identity.png images/more.png images/notprovisioned.png images/pending.png images/provisioned.png images/rejected.png images/access/iconAccessRoleAccess.gif images/access/iconAccessServiceAccess.gif images/access/iconApplicationAccess.gif images/access/iconDefaultAccess.gif images/access/iconMailGroup.gif images/access/iconProvideAccountInfo.png images/access/iconProvideAccountInfoRtl.png images/access/iconServiceAccess.gif images/access/iconSharedFolderAccess.gif images/homepage/network_nav.png images/homepage/RequestAccess.png images/homepage/ViewRequests.png images/status/request/fulfilled.png images/status/request/notfulfilled.png images/status/requests/partiallyfulfilled.png images/status/requests/pending.png	These files are the icons, images, and graphics that are displayed throughout the user interface. Subfolders are used to group related images together.
html/Login.html	This file is an HTML template that does not contain any text that requires language translation.
nls/html/LoginPageCopyrightContent.html nls/html/LoginPageInfoContent.html	These files are HTML files that might contain text that is translated into multiple languages to support globalization. There are versions of each of these files for all of the supported locales. If you customize any of these files, you must also customize the locale-specific versions of the files. You must customize the files for all of the languages that you plan to support in your environment.

Customizing Identity Service Center files

As a site administrator, you might want to customize Identity Service Center to meet your specific business needs. Customization involves either copying and modifying files that are provided by IBM or creating your own custom files to use in place of the IBM files. You must ensure that your new and modified custom files are placed in the correct location. Otherwise, the files cannot be found and used by Identity Service Center.

Before you begin

Customizing the Identity Service Center user interface requires access to files and folders under the WebSphere Application Server configuration folder of your IBM Security Identity Manager runtime environment. See “Location of Identity Service Center customizable files” on page 84 for the exact location of the files and folders to which you need access. To obtain access to the necessary files and folders, contact your system administrator.

About this task

The Identity Service Center can be customized in many ways. To customize a particular aspect of the Identity Service Center such as the login page, or the home page, see the appropriate customization instructions. Most customization tasks involve changing or providing replacements for one or more of the customizable files that are provided by IBM. This procedure describes how to create a custom file and where to place the custom file so that it can be used by the IBM Security Identity Manager server.

Many of the customizable files contain text that is translated into multiple languages for globalization. For customizable globalization files, a default file exists that is not locale-specific, such as `common.properties`. There are also locale-specific files for each supported language such as `common_fr.properties` for French and `common_ar.properties` for Arabic. The instructions in the following sections describe how to customize the default version of a globalization file only. If you choose to customize globalization files, follow the same instructions to customize the locale-specific versions of the files. You must customize the files for each language that you intend to support in your environment.

Use the following sections to work with customizing Identity Service Center files from the IBM Security Identity Manager virtual appliance console:

- To edit any custom files, see “Managing custom files” on page 20.
- To edit properties or other files, see “Managing the server properties” on page 22.
- To start, stop, or restart servers, see Viewing the Server Control widget.

Procedure

1. To replace an image file that IBM provides such as an icon or other graphic, complete the following steps.
   a. In the `.../itim/custom/ui/original/` folder, locate the image that you want to replace. For example, `.../itim/custom/ui/original/images/identity.png`.
   b. Create your custom image. Use the same file name and type as the file that IBM provides. For example, `identity.png`.
   c. Copy the custom image to the `.../itim/custom/ui` folder. Use the same relative path and file name as the file that IBM provides in the `.../itim/custom/ui/original/` folder. For example, `.../itim/custom/ui/images/identity.png`
2. To create a custom version of an IBM text file, complete the following steps.

a. In the `.../itim/custom/ui/original/` folder, identify the text file that you want to customize. For example, `.../itim/custom/ui/original/config/UIconfig.properties`.
b. Copy the file to the `.../itim/custom/ui/` folder. Ensure that you keep the same relative path and file name. For example, `.../itim/custom/ui/config/UIconfig.properties`.
c. Change the file permissions on the copied file so that it can be modified. The files that IBM provides are installed with Read-Only file permissions.
d. Modify the copied file for your customization requirements.

Merging new and existing customized configuration files

To work with new features after you upgrade, you must merge the content of new configuration files with any existing, customized Identity Service Center configuration files. If you do not merge the new and existing customized configuration files, you get errors when you work with the upgraded version of Identity Service Center.

Before you begin

- See “Location of Identity Service Center customizable files” on page 84 and “Customizing Identity Service Center files” on page 87 for the location of the Identity Service Center customizable files and how to customize the files.
- If you did not previously customize the tertiary attribute in the `config/Access.Json`, you can see that the tertiary attribute values are modified from `"tertiary": [ "accessCategory", "entityProfile" ]` to new default value `"tertiary": [ "additionalInformation" ]`.
- If you did not previously customize the `config/HeaderMenu.json`, you can see that the new attribute `menuIconItem` is introduced. The tasks **View Access**, **Request Access**, and **Edit and Delete Access** are grouped under the **Manage Access** toolbar menu.

About this task

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To edit any custom files, see “Managing custom files” on page 20.
- To edit properties or other files, see “Managing the server properties” on page 22.

If you previously customized the configuration files that contain non-translatable configuration properties, complete the following steps.

Procedure

1. Merge the content of the new configuration files into the existing customized configuration files. For example, if you previously customized the file `.../itim/custom/ui/config/Person.json`, then merge it to the new`.../itim/custom/ui/original/config/Person.json` file.
2. Replace the existing customized configuration files in the directory `.../itim/custom/ui/config` with the merged files.

Results

You can now work with the new features by restoring the previous customization that you made.

User interface elements that are affected by view definitions

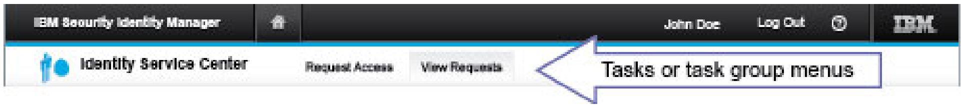
Defined views affect the visibility of the tasks that are displayed in the page header menus and on the home page of the Identity Service Center.

Page header menus

The page header menus of the Identity Service Center adapt to the user's views by showing only the tasks that are granted to the user. These tasks can be arranged in groups, with each group displayed as a drop-down menu on the page header. If the user is not granted any tasks in a group, the menu for that task group is not displayed on the page header. In the following scenarios, a task itself is displayed on the page header instead of a drop-down menu.

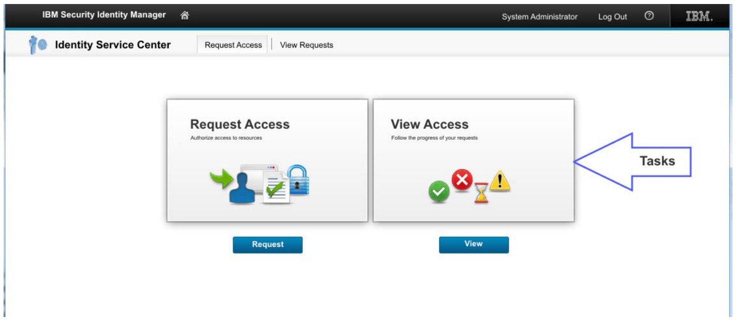
- If there is only one task in the group.
- If the user is granted only one task in the group.

Some tasks might not be displayed in the page header menus. The system administrator can choose not to include tasks in the header menus.



Home page

The content on the home page of the Identity Service Center user interface adapts to the user's views. The home page displays only the tasks that are granted to the user. Some tasks might not be displayed on the home page. The system administrator can choose not to display tasks on the home page.



Note: If the user is not granted any tasks, the home page does not display after the user logs in to the Identity Service Center. An error message is displayed and the user must log out.

Enabling Identity Service Center as the default user interface

To enable the Identity Service Center as the default user interface, you must complete the configuration steps. The configuration steps provide the mechanism to hide the view of the self-service user interface.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To edit any custom files, see “Managing custom files” on page 20.
- To edit properties or other files, see “Managing the server properties” on page 22.

Procedure

1. In the `ui.properties` file, set the property `ui.defaultui.redirectSelfToISC` to true. See “Managing the server properties” on page 22.
2. Optional: Set the language at these two locations because the languages set in both the Identity Service Center and self-service user interfaces might be different at few occasions.
   - On the **Language** menu in the Identity Service Center login page
   - In the browser
3. Optional: To ensure that users have access to the same functions in the Identity Service Center that they have in self-service user interface, manually configure the views. Configuring the view is applicable for each view that provides access to self-service function. See View management.
4. Optional: Customize the self-service user interface to hide the headers so that a user does not have both an Identity Service Center header and a self-service interface header. See “Self-service user interface customization” on page 41.
5. Optional: Configure to enable the forgotten password link on Identity Service Center login page.
   a. Log on to IBM Security Identity Manager administrative console.
   b. Select **Set System Security** > **Configure Forgotten Password Settings**.
   c. Select **Enable forgotten password authentication**.

   Note: A user must set answers for the security questions in the self-service user interface. If the forgotten password link is enabled, you must create a custom task for the forgotten password challenge behavior so that a user can update the forgotten password information.
   For more information about the forgotten password, see Forgotten password settings.
6. Optional: If you want to view the status of the requests that are placed through custom tasks that launch the self-service user interface, you must create a new custom task that points to the relevant view request status.

Login page customization

Users can enter their user names and passwords in the Login page to authenticate with the IBM Security Identity Manager Server and access the Identity Service Center.

The Login page can be customized in various ways to meet the needs of your business. They are as follows:

- Change the logo to your company or product image. The image dimensions are resized to fit the allocated space.
- Modify or replace the site information on the right side of the Login page.
- Modify the text for the **Help?** and **Learn More** hyperlinks or remove the hyperlinks from the Login page.

- Change the copyright information at the bottom of the Login page.
- Customize the validation messages for the Login page.

Customizing the Login page

You can customize the authentication Login page to meet the requirements of your organization. For example, you can customize your company or product logo. You can also define more details, or change the labels of fields on the page.

Before you begin

You must have read or write access to the customizable files and the directories where they are maintained. See "Location of Identity Service Center customizable files" on page 84 and "Customizing Identity Service Center files" on page 87 for specific details about where these files are located. Contact your system administrator if you do not have the necessary permissions.

About this task

You can customize the appearance and content of the Login page to meet your needs.

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To edit any custom files, see "Managing custom files" on page 20.
- To edit properties or other files, see "Managing the server properties" on page 22.

Procedure

1. Optional: Edit the `nls/LoginText.properties` file to customize the various fields on the Login page. The `nls/LoginText.properties` file contains a set of properties that define the text strings that are displayed in the various fields of the Login page. You can customize the Login page text by changing the text that is associated with these properties, as follows:

   `LOGO_ALT_TEXT`
   Specify custom text to display if the logo image is missing.

   `HELP_TAG`
   Specify a custom label for the **Help** hyperlink.

   `LEARN_MORE`
   Specify custom text for the **Learn More** hyperlink.

   `LOG_IN` Specify a custom label for the **Log in** button.

   `PASSWORD`
   Specify a custom label for the **Password** field.

   `PRODUCT_NAME`
   Specify a custom title for the product name.

   `USER_ID`
   Specify a custom label for the **User ID** field.

   `INVALID_USERNAME`
   Specify a custom message that is displayed when an invalid user name is entered.

INVALID_PASSWORD
: Specify a custom message that is displayed when an invalid password is entered.

LANGUAGE_LABEL
: Specify the label for the language selection field.

2. Optional: Customize the company or product image on the Login page. You can customize the image on the login page by using either of the following ways:
   - Create a custom image file in GIF format with the file name companyLogo.gif. Place the image file in the /images folder of your customizable files.
   - Create a custom image file with any file name, such as someImage.jpg. Place the image file in the /images folder of your customizable files. Then, create a custom copy of the config/UIconfig.properties file and modify the LOGO_IMAGE property to specify the name of the image file such as someImage.png.
3. Optional: Modify the copyright information at the bottom of the Login page. The copyright information that is provided by IBM is delivered as an HTML template, nls/html/LoginPageCopyrightContent.html, and a properties file, nls/LoginPageCopyrightContent.properties. The properties file contains the text that is substituted into the HTML template. To customize the copyright information on the Login page, you can take one of the following actions:
   - Continue to use the HTML template that is provided by IBM. Create a custom copy of the template substitutions nls/LoginPageCopyrightContent.properties file. Then, modify the FOOTER_TEXT property in the nls/LoginPageCopyrightContent.properties file to the text you want to be displayed at the bottom of the Login page.
   - Create a custom version of the nls/html/LoginPageCopyrightContent.html template and modify it to use whatever HTML formatting and template substitutions that you want. Then, create a custom copy of the nls/LoginPageCopyrightContent.properties file and add or modify the properties in it to provide the necessary substitutions for your custom HTML template.
   - If you do not want to use an HTML template with substitutions, you can create a custom copy of the nls/html/LoginPageCopyrightContent.html template file. Then, replace the template substitution references with the actual copyright text that you want to display.
4. Optional: Modify the site information on the right side of the Login page. The site information that is provided by IBM is delivered as an HTML template, nls/html/LoginPageInfoContent.html, and a properties file, nls/LoginPageInfoContent.properties. The properties file contains text that is substituted into the HTML template. To customize the site information on the Login page, you can take one of the following actions:
   - Continue to use the HTML template that is provided by IBM. Create a custom copy of the template substitutions nls/LoginPageInfoContent.properties file. Then, modify the properties in the nls/LoginPageInfoContent.properties file to provide the text that you want to be displayed on the right side of the Login page.
   - Create a custom version of the nls/html/LoginPageInfoContent.html template and modify it to use whatever HTML formatting and template substitutions that you want. Then, create a custom copy of the nls/LoginPageInfoContent.properties file and modify or replace the properties in it to provide the necessary substitutions for your custom HTML template.

- If you do not want to use an HTML template with substitutions, you can create a custom copy of the `nls/html/LoginPageInfoContent.html` template file. Then, replace the template substitution references with the actual site information text that you want to display.

5. Save and close each of the custom files when you are finished customizing for the Login page.
6. Start the Login page again.

Results

The Login page now displays the customization that you made.

Customizing the page header

The Identity Service Center user interface has a header at the top of the page. The header provides menus that are used to navigate to tasks that the user is authorized to perform. The page header can be customized in various ways to meet the needs of your organization.

Before you begin

You must have read and write access to the customizable files and the directories where they are maintained. See “Location of Identity Service Center customizable files” on page 84 and “Customizing Identity Service Center files” on page 87 for specific details about where these files are located. Contact your system administrator if you do not have the necessary permissions.

About this task

The Identity Service Center page header is divided into two areas. The upper portion is the primary header. It displays the product name and the current user, as well as the **Home** and **Log Out** shortcuts, the header logo, and the **Help** menu. The lower portion is the secondary header. It displays a product image, the name of the active task, and menus of tasks the user is authorized to perform. You can customize the appearance of the page header to suit your needs.

The task menus on the page header adapt to the user's authorized views so that only tasks the user is allowed to perform are shown. You can customize the organization of tasks in the page header menus.

The IBM Security Identity Manager administrator console is used to manage view definitions by:

- Assigning tasks to views.
- Associating groups with those views.
- Managing the members of the groups.

IBM provides a set of ready-to-use Service Center tasks. You can also create custom tasks to launch your own web applications from the Identity Service Center user interface. Both the tasks that are provided by IBM and your custom tasks can be displayed in the page header menus. However, the method of customizing the appearance and organization of tasks is different for each of these types of tasks.

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To edit, download or upload, a custom file, see "Managing custom files" on page 20.
- To edit or upload a property file, see "Managing the server properties" on page 22.

Procedure

1. Optional: Customize the product name in the primary area of the page header or the home page name in the secondary area of the page header:
   a. If you did not already do so, make a custom copy of the `nls/headerLabel.properties` file.
   b. Open the custom copy of the `nls/headerLabel.properties` file in a text editor.
   c. Modify these properties to suit your needs.

      identityManager
         Specify the custom text to display for the product name field.

      SVCENTER_HOMEPAGE
         Specify the custom text to display for the home page name.
2. Optional: You can customize the logo that is displayed in the primary area of the page header by using either of these methods.
   - Create a custom image file in PNG format with the same name as the image provided by IBM, `headerLogo.png`. Place the image file in the `images` folder of your customizable files. The custom image is used in place of the `headerLogo.png` image that is provided by IBM.
   - If you did not already do so, make a custom copy of the `config/UIconfig.properties` file. Create a custom image in any image format with any file name, for example `customLogo.jpg`. Place the image file in the `images` folder of your customizable files. Edit the custom copy of the `config/UIconfig.properties` file. Change the value of the **`HEADER_LOGO_IMAGE`** property to specify the name of your custom image, such as `customLogo.jpg`. Save the file.
3. Optional: You can customize the alternate text for the header logo in the primary area of the page header. The alternate text is displayed when the user's browser is set to not show images. Screen readers for visually impaired users also read the alternate text to indicate what the image represents.
   a. If you did not already do so, make a custom copy of the `nls/headerLabel.properties` file.
   b. Open the custom copy of the `nls/headerLabel.properties` file in a text editor.
   c. Modify the value of the **`headerLogoAltText`** property to define the alternate text for the header logo.
4. Optional: You can customize the image that is displayed in the secondary area of the page header, by using either of the following ways:
   - Create a custom image file in PNG format with the same name as the image provided by IBM, `identity.png`. Place the image file in the `images` folder of your customizable files. The custom image is used in place of the `identity.png` image that is provided by IBM.
   - If you did not already do so, make a custom copy of the `config/HeaderMenu.json` file. Create a custom image file in any image format and with any file name, for example `customIcon.jpg`. Place the image file in the `images` folder of your customizable files. Edit the custom copy of the `config/HeaderMenu.json` file. Change the value of the **`secondaryIcon`** field to

specify the location and name of your custom image, such as custom/ui/images/customIcon.jpg. Save the file.

5. Optional: Customize the appearance and organization of the tasks that are provided by IBM in the page header menus.

   The config/HeaderMenu.json file defines the appearance and organization of the page header menus. The contents of this file are maintained in JavaScript Object Notation (JSON) format, which is a way of representing structured data. The text labels for the drop-down menus and the task names in the menus are defined in the nls/headerLabel.properties file.

   The **secondaryNavigation** section of the config/HeaderMenu.json file contains a **menus** subsection.

   ```
    "secondaryNavigation": {
           . . .
           "menus": [
               . . .
           ]
       }
   ```

   Each area in this **menus** subsection describes one of the menus in the secondary area of the page header.

   ```
   {
     "labelKey": "manageAccess",
     "icon": "custom/ui/images/header/tab_RequestAccess.png",
     "menuItemIcon":"/itim/ui/custom/ui/images/header/dd_requestAccess.png",
     "menuItems": [
           {
               "actionId": "SVCENTER_REQUEST_ACCESS"
           }
       ]
   },
   ```

   labelKey
   Specifies the name of the property in the nls/headerLabel.properties file whose value is displayed for the menu. To customize the labels for the menus and tasks, if you did not previously complete this task, make a custom copy of the nls/headerLabel.properties file. Find the corresponding property from the config/HeaderMenu.json, such as **manageAccess**, in the custom nls/headerLabel.properties file. Change the value.

   Note: If a menu contains only a single task, the **labelKey** for the menu is not used. That task is displayed on the page header instead of a drop-down menu with a single menu item.

   icon Specifies an icon that is displayed at the left corner of the task header.

   menuItemIcon
   Specifies an icon that is displayed for each of the tasks in the menu.

   menuItems
   Defines the list of tasks that are displayed in the menu.

   actionId
   Specifies the name of the property in the nls/headerLabel.properties file whose value is displayed for the task. To customize the label for a task, if you did not previously complete this task, make a custom copy of the nls/headerLabel.properties file. Find the corresponding property from the config/HeaderMenu.json, such as **SVCENTER_REQUEST_ACCESS**, in the custom nls/headerLabel.properties file. Change the value.

To change the organization of the menus and the tasks in each menu:

a. If you did not previously complete this task, make a custom copy of the `config/HeaderMenu.json` file.

b. Open the custom copy of the `config/HeaderMenu.json` file in a text editor.

c. Edit the **`menus`** subsection of the **`secondaryNavigation`** section of the file.

d. Move the menu sections so that they are in the order that you want them to be displayed on the page header.

e. Add or move tasks in the **`menuItems`** subsection so that they are in the order that you want them to be displayed in the drop-down menu.

f. Save the file.

6. Optional: Customize the appearance and organization of custom tasks in the page header menus. The IBM Security Identity Manager administration console can be used to create custom tasks to launch your own web applications. To create these custom tasks, the administrator specifies parameters that define the appearance of the task, such as:
   - Label
   - Description
   - Page header menu in which the custom task is displayed

   For information about creating custom tasks, see View management.

Results

The appearance of the page header is changed to reflect your customizations.

What to do next

In a managed-cluster environment, you must wait until after the configuration is synchronized to the application servers in the cluster. For information about synchronizing, see “Synchronizing a member node with a primary node” on page 19. Log in to the Identity Service Center and verify that the home page reflects the customizations that you made.

Customizing the home page

The home page of the Identity Service Center displays a list of tasks that the user is permitted to perform. The home page can be customized in various ways to meet the needs of your organization.

Before you begin

You must have read and write access to the customizable files and the directories where they are maintained. See “Location of Identity Service Center customizable files” on page 84 and “Customizing Identity Service Center files” on page 87 for specific details of where these files are located. Contact your system administrator if you do not have the necessary permissions.

About this task

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To edit, download or upload, a custom file, see “Managing custom files” on page 20.

- To edit or upload a property file, see "Managing the server properties" on page 22.

The IBM Security Identity Manager administrator console is used to manage view definitions by:

- Assigning tasks to views.
- Associating groups with those views.
- Managing the members of the groups.

IBM provides an initial set of ready-to-use Service Center tasks. You can also create custom tasks to launch your own web applications from the Identity Service Center user interface. Both the tasks that are provided by IBM and your custom tasks can be displayed on the home page. However, the method of customizing of the appearance and organization of tasks is different for each of these types of tasks. For information about adding custom tasks, see View management.

Each task on the home page is represented by a card. The card provides information about the task, such as a task name, a description, and an image. You can customize the appearance and organization of these tasks on the home page to suit your needs.

The tasks on the home page adapt to the user's authorized views so that only tasks the user is allowed to perform are shown.

The `config/Homepage.json` file defines the appearance and organization of the tasks that IBM provides on the home page. The contents of this file are maintained in JavaScript Object Notation (JSON) format, which is a way of representing structured data. Each section in the `config/Homepage.json` file is enclosed in braces and defines the appearance of one task on the home page. For example, the following section of the `config/Homepage.json` file defines the **Request Access** task.

```
{
        "actionId":"SVCENTER_REQUEST_ACCESS",
        "btnLabel": "SVCENTER_REQUEST_ACCESS_BUTTON",
        "desc":  "SVCENTER_REQUEST_ACCESS_DESC",
        "img": "./custom/ui/images/homepage/requestOthersAccess.png"
    },
    {
        "actionId":"SVCENTER_REQUEST_ACCESS_FOR_MYSELF",
        "btnLabel": "SVCENTER_REQUEST_ACCESS_BUTTON",
        "desc":  "SVCENTER_REQUEST_ACCESS_FOR_MYSELF_DESC",
        "img": "./custom/ui/images/homepage/requestMyAccess.png"
    },
```

actionId
Specifies the name of the property in the `nls/headerLabel.properties` file whose value is displayed for the task name.

btnLabel
Specifies the name of the property in the `nls/headerLabel.properties` file whose value is displayed for the label of the button for the task.

desc Specifies the name of the property in the `nls/headerLabel.properties` file whose value is displayed for the description of the task.

img Specifies the location of the image that is displayed for the task.

The steps in this procedure use the **Request Access** section of the `config/Homepage.json` file as an example. The actual property names in the `nls/headerLabel.properties` file depend on the section of the config/Homepage.json file that you are customizing.

Procedure

1. Optional: Customize the text for a task that IBM provides on the home page.
   a. If you have not previously completed this task, make a custom copy of the nls/headerLabel.properties file.
   b. Open the custom copy of the nls/headerLabel.properties file in a text editor.
   c. Optional: To customize the text for the task name, find the property that matches **actionId** field, such as **SVCENTER_REQUEST_ACCESS**. Change the value.
   d. Optional: To customize the text for the task button, find the property that matches **btnLabel**field, such as **SVCENTER_REQUEST_ACCESS_BUTTON**. Change the value.
   e. Optional: To customize the text for the task description, find the property that matches **desc** field, such as **SVCENTER_REQUEST_ACCESS_DESC**. Change the value.
   f. Save the file.
2. Optional: Customize the image that is displayed for the task that IBM provides. You can use either of two methods.
   - Create a custom image file in PNG format with the same name as the image provided by IBM, such as requestAccess.png in the previous example. Place the image file in the images/homepage folder of your customizable files. The custom image is used in place of the requestAccess.png image that is provided by IBM.
   - If you have not previously completed this task, make a custom copy of the config/Homepage.json file. Create a custom image file in any image format and with any file name, for example customImage.jpg. Place the image file in the images/homepage folder of your customizable files. Edit the custom copy of the config/Homepage.json file. Change the value of the **img** field for the task to specify the location and name of your custom image custom/ui/images/homepage/customImage.jpg. Save the file.
3. Optional: Change the organization of the tasks that IBM provides on the home page.
   a. If you have not previously completed this task, make a custom copy of the config/Homepage.json file.
   b. Open the custom copy of the config/Homepage.json file in a text editor.
   c. Move the sections so that they are in the order that you want them to be displayed on the home page.
   d. Save the file.
4. Optional: Customize the appearance and organization of custom tasks on the page header menus. The IBM Security Identity Manager administration console can be used to create custom tasks to launch your own web applications. To create these custom tasks, the administrator specifies parameters that define the appearance of the task, such as:
   - Label
   - Description
   - Icon

   For information about creating custom tasks, see View management.

Results

The appearance of the home page is changed to reflect your customizations.

What to do next

In a managed-cluster environment, you must wait until after the configuration is synchronized to the application servers in the cluster. For information about synchronizing, see “Synchronizing a member node with a primary node” on page 19. Log in to the Identity Service Center and verify that the home page reflects the customizations that you made.

Customizing the scope of user lists for tasks

You can customize the definition of a task to limit the list of users that are displayed in the task. The definition can limit the list to include only the users that are relevant for the current Identity Service Center user.

Before you begin

You must have read and write access to the customizable files and the directories where they are maintained. See “Location of Identity Service Center customizable files” on page 84 and “Customizing Identity Service Center files” on page 87 for specific details of where these files are located. Contact your system administrator if you do not have the necessary permissions.

About this task

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To edit, download or upload, a custom file, see “Managing custom files” on page 20.
- To edit or upload a property file, see “Managing the server properties” on page 22.

The home page and page header menus of the Identity Service Center display tasks that the user is allowed to perform. Some tasks, such as the Request Access task, involve the selection of one or more users from a list. For some organizations, this list of users can be large.

You can customize the definition of tasks so that the user list shows only the users that are relevant for the current Identity Service Center user. For example, you might want the list of users to be restricted to only those users in the department that is managed by the current user.

The `config/ActionDefinition.json` file defines how tasks are launched when the user selects them. The contents of this file are maintained in JavaScript Object Notation (JSON) format, which is a way of representing structured data. Each section in this file defines the launch information for one task, as shown here for the Request Access task.

```
"SVCENTER_REQUEST_ACCESS": {
   "actionType": "CreateFlow",
   "urlHash":"requestAccess",
   "properties": {
       "widgetPath":
            "com/ibm/isim/ui/util/uiflow/requestaccess/RequestAccessFlow",
        "widgetArgs": { "personFilterId": "" }
    }
},
```

The **properties** section contains a **widgetArgs** field that defines a list of JavaScript variables that are passed to the task when it is launched. The value of the **personFilterId** variable specifies the `filterId`. The `filterId` is configured in the `custom/rest/searchfilter.json` file. This filter is used by the task when it looks for users that are relevant to the current Identity Service Center user. The value can be customized to suit the needs of your organization by modifying the attribute **baseFilter** for the configured `filterId` in the `custom/rest/searchfilter.json` file. For example, see Filter configuration for REST search services.

Procedure

1. Download a copy of the `ActionDefinition.json` file. See "Managing custom files" on page 20.
2. Locate the section of this file that describes the launch information for the task to be customized, such as **SVCENTER_REQUEST_ACCESS**.
3. Modify the value of the **personFilterId** variable of the **widgetArgs** field in the properties section to specify the `filterId` for the user list in the task. See Filter configuration for REST search services.
4. Save and close the file.

Results

When the task with the customized user scope is launched, the list of users is restricted to only those users that match the specified filter. Only those users are displayed on the Select user page.

What to do next

In a managed-cluster environment, you must wait until after the configuration is synchronized to the application servers in the cluster. For information about synchronizing, see "Synchronizing a member node with a primary node" on page 19. Log in to the Identity Service Center and verify that the scope reflects the customizations that you made.

Request Access wizard

You can customize the user interface characteristics of the Request Access wizard to suit your needs.

The following items in the Request Access wizard can be changed or customized:

- The appearance and content of the user cards
- The appearance and content of the access cards
- The text and styling of badges on access cards
- The access card selection limit
- The search control properties

Customizing a user card in the Request Access wizard

The first step in the Request Access wizard is used to select the user for whom access is being requested. The set of users to choose from is displayed as a collection of user cards that are arranged in a grid. You can customize the information that is displayed in the user cards, and also how the user cards in the grid can be sorted.

Before you begin

You must have read or write access to the customizable files and the directories where they are maintained. See "Location of Identity Service Center customizable files" on page 84 and "Customizing Identity Service Center files" on page 87 for specific details about where these files are located. Contact your system administrator if you do not have the necessary permissions.

About this task

A *user card* is like a business card for people in your organization. The information that is displayed on a user card is arranged into several areas. You can customize which user attributes are displayed in each of the areas to meet your needs.

The `primary` area of the user card displays the most important user attribute, such as the user name. The information in this area displays at the top of the card and in the largest font. Only one user attribute can be assigned to the `primary` area, but you can choose a different attribute for each of the user profiles that are defined in your environment.

The `secondary` area of the user card displays the next most important user attribute, such as the user email address. The information in this area is displayed just under the `primary` area and in a smaller font than the `primary` area. Only one user attribute can be assigned to the `secondary` area, but you can choose a different attribute for each of the user profiles that are defined in your environment.

The `tertiary` area of the user card displays extra information about the user, such as the user title, department name, or sponsor name. The information in this area is displayed just under the `secondary` area and in a smaller font than the `secondary` area. Multiple user attributes can be assigned to the `tertiary` area. You can choose different sets of attributes for each of the user profiles that are defined in your environment. Each assigned attribute is given a label, such as **Title** or **Sponsor** that is displayed on the user card with the attribute value. The label is to help the user understand the information that is displayed on the card.

The *icon* area of the user card displays an image that is associated with the user, such as the user picture from your organization directory.

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To go to a custom file and edit, download, upload, or search it, see "Managing custom files" on page 20.
- To go to a property file and edit, upload, or search it see "Managing the server properties" on page 22.

Procedure

1. Optional: Customize the user attributes that are displayed in the different areas of user cards and whether sorting on the information in those areas is supported. Make a custom copy of the `Person.json` file and open the file with a text editor. The contents of this file are maintained in *JavaScript Object Notation* (JSON) format, which is a way of representing structured data.

The primary section of this file contains attribute and sort subsections. For example:

```
"primary": {
     "attribute": {
         "default": "name",
         "Person" : "CN",
         "BPPerson" : "CN"
     },
     "sort": {
         "enabled": true,
         "labelKey" : "name"
     }
 },
```

In the attribute section, define the user attribute to display in the primary area of the user card. You can choose a different user attribute for each user profile that is defined in your environment. You must always set a default user attribute to use for any user profiles that are not explicitly defined. In the earlier example, the default user attribute is "name", but the attribute for users in the "Person" and "BPPerson" user profiles is "CN".

Note: Ensure that the primary section is defined with a valid LDAP attribute for the specified profiles or for a default attribute that is common across all profiles.

In the sort section, you can enable or disable sorting of the user card that is based on the information in the primary area of the card. If you enable sorting, "enabled": true, the uppercase value of the **labelKey** field is used to look up the display string for this sort option in the customizable nls/Picker.properties file. In this example, the **labelKey** value NAME is looked up as a property in the nls/Picker.properties file to find the sort option string to display.

The secondary section of this file is identical to the primary section. For example:

```
"secondary": {
     "attribute": {
         "default": "mail",
         "Person": "manager.name"
     },
     "sort": {
         "enabled": true,
         "labelKey" : "contactInfo"
     }
 },
```

In the attribute section, define the user attribute to display in the secondary area of the user card. You can choose a different user attribute for each user profile that is defined in your environment. You must always set a default user attribute to use for any user profiles not explicitly defined. In the earlier example, the default user attribute is "name", but the attribute for users in the "Person" user profile is "manager.name".

In the sort section, you can enable or disable sorting of the user card that is based on the information in the secondary area of the card. If you enable sorting, "enabled": true, the uppercase value of the **labelKey** field is used to look up the display string for this sort option in the customizable nls/Picker.properties file. In this example, the **labelKey** value CONTACTINFO is looked up as a property in the nls/Picker.properties file to find the sort option string to display.

The `tertiary` section of this file contains an `attributes` section. The `attributes` section is used to define the list of user attributes to be displayed in the `tertiary` area of the user card. For example:

```
"tertiary": {
     "attributes": {
         "default": [ "title", "department" ],
         "BPPerson":[ "ersponsor.name" ]
     }
 },
```

The attributes to be displayed are separated by commas and enclosed in square brackets. You can choose a different set of user attributes for each user profile that is defined in your environment. You must always set a default list of user attributes to use for any user profiles that are not explicitly defined. In the earlier example, the default list of user attributes is `[ "title", "department" ]`, but the attribute list for users in the `"BPPerson"` user profile is `[ "ersponsor.name" ]`.

Sometimes the attribute that you want to display is not an attribute of the user, but it might be an attribute of an object that is related to the user. For example, a user might have attributes that are called `"manager"` or `"ersponsor"` that are actually references to related users, namely the manager or sponsor of this user. To display an attribute like `"name"` from the related user in this user card, you can use the dotted notation that is shown in the earlier examples:

```
  "manager.name"
  "ersponsor.name"
```

2. Optional: Customize the labels that are displayed with the user attributes in the `tertiary` area of the user card. Make a custom copy of the `nls/Picker.properties` file and open the file with a text editor. The properties in this file define the text that displays in various parts of the user selection step of the Request Access wizard.

   User attributes assigned to the `tertiary` area of the user card are displayed with a label to help the user understand what information they see. For example, if the `config/Person.json` file contains this definition for the `tertiary` section:

   ```
   "tertiary": {
        "attributes": {
            "default": [ "title", "department" ],
            "BPPerson":[ "ersponsor.name" ]
        }
    },
   ```

   Then, for the users in the `BPPerson` user profile, the `tertiary` field of the user card might be displayed as follows:

   ```
   Sponsor: John Doe
   ```

   To customize the label for a user attribute in the `tertiary` area of the user card, look for a property in the `nls/Picker.properties` file. The property must match the uppercase form of the user attribute name that is specified in the `tertiary` section of the `config/Person.json` file. For example, `ERSPONSOR.NAME`. If this property does not exist in the file, add a property with this name. Customize this property value to specify the string that you want to display as the user attribute label in the `tertiary` area of the card.

3. Customize the text that is displayed in the sort option list for the `primary` or `secondary` areas of the user card. Make a custom copy of the `nls/Picker.properties` file and open the file with a text editor. The properties in this file define the text that is displayed in various parts of the user selection step of the Request Access wizard.

You can enable sorting of the user cards that are based on information in the primary and secondary areas of the user card. For example, if the config/Person.json file contains the following definition for the primary and secondary sections.

```
"primary": {
     "attribute": {
         "default": "name",
         "Person" : "CN",
         "BPPerson" : "CN"
     },
     "sort": {
         "enabled": true,
         "labelKey" : "name"
     }
 },
 "secondary": {
     "attribute": {
         "default": "mail",
         "Person": "manager.name"
     },
     "sort": {
         "enabled": true,
         "labelKey" : "contactInfo"
     }
 },
```

Then, sorting of user cards is enabled for both the primary and secondary areas of the user card. The set of user cards has a sort control at the top that displays as follows:

```
Sort By: Name, Contact Information
```

Note: Sorting is not supported for attributes from objects that are related to the user, such as "manager.name". If any attributes that are specified in the primary section are from related objects, then the sort control does not include an option to sort on the primary area of the user card. Similarly, if any attributes that are specified in the secondary section are from related objects, then the sort control does not include an option to sort on the secondary area of the user card.

You can customize the text to display in the list of sort options for the primary or secondary areas of the user card. To customize the text, look for a property in the nls/Picker.properties file. The property must match the uppercase value of the **labelKey** of the corresponding section of the config/Person.json file. For example, NAME or CONTACTINFO in the earlier example. If this property does not exist in the file, add a property with this name. Customize the value of this property to specify the string that you want to display in the list of sort options.

4. Optional: Customize the icon area of the user card to display an image for the associated user. Make a custom copy of the config/Person.json file and open the file with a text editor. The contents of this file are maintained in *JavaScript Object Notation* (JSON) format, which is a way of representing structured data.

   The icon section of this file contains an attribute subsection. For example:

```
"icon": {
     "attribute": {
         "default": "erimageuri",
         "BPPerson": null
     }
 }
```

   In the attribute section, define the user attribute that contains the location of the icon or image to display on the user card. You can choose a different user attribute for each user profile that is defined in your environment. You must always set a default user attribute to use for any user profiles that are not explicitly defined. If some user profiles do not have an image attribute, you can specify null to indicate no image to be displayed for users in that profile. In the earlier example, the default user attribute is erimageuri, but no image is displayed for users in the BPPerson user profile.

See "Customizing the server to generate user image URIs" for information about how to configure a plug-in for the IBM Security Identity Manager Server that can dynamically generate the location of an image for the erimageuri attribute by using the values of attributes that are associated with users.

5. Customize the display value for user attributes with values that are not intuitive.

   You might want to display some user attributes on a user card, but the value of these user attributes is not intuitive to the user. For example, there might be a user attribute name such as employeeType whose value is encoded as "a" for active employees, "r" for retired employees or "p t" for part-time employees. Displaying the actual value of this attribute on the user card might not be intuitive to the user.

   To customize the displayed values for some user attributes, make a custom copy of the nls/CardCustomValue.properties file and open the file with a text editor. The properties in this file define the custom text that is displayed in place of the actual values for various user attribute and value combinations. For example, to define the display text for the values of the employeeType user attribute, you can add or modify the properties in this file as follows:

   ```
   employeeType.a=Active
   employeeType.r=Retired
   employeeType.p__DELIMITER__t=Part-time
   ```

   With these assigned values, the user card displays Active when the *employeeType* value is "a", Retired when the *employeeType* value is "r", and "Part-time" when the *employeeType* value is "p t".

   Note: The property names in this file cannot contain spaces. If any of the possible user attribute values contain a space, you must replace it with the special character sequence __DELIMITER__. See the earlier example for reference. The employeeType value of "p t" is represented by a property name of employeeType.p__DELIMITER__t.

Results

The appearance of the user cards on the user selection step of the Request Access wizard is changed to reflect the customization that you made.

What to do next

In a managed-cluster environment, you must wait until after the configuration is synchronized to the application servers in the cluster. For information about synchronizing, see "Synchronizing a member node with a primary node" on page 19. Log in to the Identity Service Center. Start the Request Access wizard and verify that the appearance of the user cards reflects the customization that you made.

Customizing the server to generate user image URIs

The IBM Security Identity Manager Server can be customized to dynamically generate the location (URI) for the user images that are shown on user cards.

Before you begin

Depending on your system customization, you might not have access to this task. Contact your system administrator to obtain access to this task, or to have someone complete it for you.

About this task

The user cards that are shown in the request access wizard can be configured to show an image that is associated with each user. The IBM Security Identity Manager Server provides a plug-in that can be used to dynamically generate the location (URI) of a user image. It is based on one or more attributes of the user.

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To go to a custom file and edit, download or upload it, see "Managing custom files" on page 20.
- To go to a property file and edit, or upload, see "Managing the server properties" on page 22.

Procedure

1. Open the `enroleExtensionAttributes.properties` file in the `directories/data` directory.
2. Add the following line in the file to enable the default plug-in.

```
person.extension.classname = com.ibm.itim.dataservices.extensions.plugins.PersonExtensionPlugin
```

   See "Managing the server properties" on page 22.
3. Set a value for the URI of the picture of each user. For example, if all your people images are stored on the web server, `images.myserver.com` under the `/uid` directory, then the configuration is as shown in the following example.

   ```
   plugin.person.erImageURI=http://images.myserver.com/uid/${uid}.jpg
   ```

   Note: Variables that refer to other attributes can be included in the URI, for example, **`${uid}`**. The variables are replaced with the real attribute values of the user at run time.
4. Optional: Set a value for the default URI in case you cannot do any substitution. For example, if the **`uid`** attribute is not set for the user, then you cannot substitute any other values. As a result, the default URI is returned.

   ```
   plugin.person.erImageURI.default=http://images.myserver.com/default.jpg
   ```
5. When you finish your customization, save and close the property file.
6. Log in to the Identity Service Center user interface.
7. From the Home page, click **Request Access** to open the Select user page.

Results

Your customization updates are shown in the user card in the Select user page with the associated picture.

What to do next

You can also write a custom plug-in that generates the picture URI for each person. See the `Readme.html` in the `extensions.zip` file at `directories/utilities` for instructions about compiling the supplied example plug-in.

Customizing an access card in the Request Access wizard

The second step in the Request Access wizard is used to select the accesses that are requested for a user. The set of access items to choose from is displayed as a collection of access cards that are arranged in a grid. You can customize the information that is displayed in these access cards.

Before you begin

You must have read or write access to the customizable files and the directories where they are maintained. See "Location of Identity Service Center customizable files" on page 84 and "Customizing Identity Service Center files" on page 87 for specific details about where these files are located. Contact your system administrator if you do not have the necessary permissions.

About this task

An *access card* is like a brochure for the access items in your organization. The information that is displayed on an access card is arranged into several areas. You can customize which access attributes to display in each of these areas to meet your needs.

The following access attributes are available to be displayed on the access card:

- `accessName`
- `description`
- `additionalInformation`
- `tags`

Note: The `tags` attribute refers to the `Search terms` that are defined for the access item.

The `primary` area of the access card displays the most important access attribute, such as the access name. The information in this area is displayed at the top of the card and in the largest font. Only one access attribute can be assigned to the `primary` area.

The `secondary` area of the access card displays the next most important access attribute, such as the access description. The information in this area is displayed just under the `primary` area and in a smaller font than the `primary` area. Only one access attribute can be assigned to the `secondary` area.

The `tertiary` area of the access card displays extra information about the access item, such as the additional information. The information in this area is displayed just under the `secondary` area and in a smaller font than the `secondary` area. The `tertiary` area of the access cards displays the additional information about the attributes.

The `image` area of the access card displays an icon that is associated with the access item.

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To go to a custom file and edit, download, upload, or search it, see "Managing custom files" on page 20.

- To go to a property file and edit, upload, or search it see "Managing the server properties" on page 22.

Procedure

1. Optional: Customize the access attributes that are displayed in the different areas of access cards. Make a custom copy of the `config/Access.json` file and open the file with a text editor. The contents of this file are maintained in *JavaScript Object Notation* (JSON) format, which is way of representing structured data.

   The `primary` field specifies the name of the access attribute to display in the `primary` area of the access card. For example:

   ```
   "primary" :"accessName",
   ```

   You can specify a different attribute to display in the `primary` area to meet your needs.

   The `secondary` field specifies the name of the access attribute to display in the `secondary` area of the access card. For example:

   ```
   "secondary": "description",
   ```

   You can specify a different attribute to display in the `secondary` area to meet your needs.

   The `tertiary` field specifies the access attribute to display in the `tertiary` area of the access card. For example:

   ```
   "tertiary": [ "additionalInformation" ],
   ```

   You can choose a different set of access attributes to display in the tertiary area to meet your needs. The attributes to be displayed are separated by commas and enclosed in square brackets.
2. Optional: Customize the labels that are displayed with the access attributes in the `tertiary` area of the user card. Make a custom copy of the `nls/Picker.properties` file and open the file with a text editor. The properties in this file define the text that is displayed in various parts of the access selection step of the Request Access wizard.

   Access attributes assigned to the `tertiary` area of the access card are displayed with a label to help the user understand what information is displayed. For example, the `config/Access.json` file contains the following definition for the `tertiary` section:

   ```
   "tertiary": [ "additionalInformation" ],
   ```

   To customize the label for an access attribute in the `tertiary` area of the access card, search for a property in the `nls/Picker.properties` file. The property must match the uppercase form of the access attribute name that is specified in the `tertiary` section of the `config/Access.json` file. For example, `additionalInformation`. If this property does not exist in the file, then add a property with this name. Customize this property value to specify the string that you want to display as the label of the access attribute in the `tertiary` area of the card.
3. Customize the text that is displayed in the sort option list for the `primary`, `secondary`, or `tertiary` areas of the access card. Make a custom copy of the `nls/Picker.properties` file and open the file with a text editor. The properties in this file define the text that is displayed in various parts of the access selection step of the Request Access wizard.

   Sorting of access cards is only supported for the `accessName`, `description`, and `additionalInformation` attributes. If the attribute in the `primary` area is supported for sorting, then it is displayed as the first choice in the sort option list. If the attribute in the `secondary` area is supported for sorting, then it is displayed as the next choice in the sort option list. If any of the attributes in the `tertiary` area are supported for sorting, then they are displayed next in the sort option list. The support is only up to a maximum of three sort options. For example, the `config/Access.json` file contains the following definition:

```
"primary": "accessName",
"secondary": "description",
"tertiary": ["additionalInformation"],
```

Then, sorting on the access name, description, and additional information attributes is supported. The set of access cards has sort control at the top that is represented as follows:

```
Sort By: Name, Description, Additional Information
```

To customize the text that is displayed in the list of sort options, search for a property in the `nls/Picker.properties` file. This property must match the uppercase form of the corresponding attribute name. For example, `accessName`, `description`, or `additionalInformation`. If this property does not exist in the file, add a property with this name. Customize this property value to specify the string that you want to display in the list of sort options.

4. Customize the image area of the access card to display an icon for the associated access item. Make a custom copy of the `config/Access.json` file and open the file with a text editor. The contents of this file are maintained in *JavaScript Object Notation* (JSON) format, which is a way of representing structured data.

   The `image` field specifies whether an image is to be displayed with each access item. For example:

   ```
   "image": "icon"
   ```

   This condition specifies that access icons must be displayed on access cards, when the appropriate image file can be found. If you do not want to display images on access cards, remove the `"image": "icon"` from the `config/Access.json` file.

   Images for access items can be defined for each individual access item, or for access categories. When you configure an access category image, then it displays for any access items in the category that do not have their own image explicitly defined. IBM Security Identity Manager includes default images for the predefined access categories, but you can provide custom images for these access categories, and custom images for individual access items. By convention, images for access items are maintained in the `directories/itim_self_service.war/images/access` folder of your customizable files. For example, the image for the `Application` access category is `directories/itim_self_service.war/images/access/iconApplicationAccess.gif`.

   - To define a custom image for one of the predefined access category images, create the image in GIF format by using the naming convention `icon<`*`access-Category`*`>Access.gif`. <*access-Category*> is the access category to which the image is applicable. For example, `iconApplicationAccess.gif`. Place the custom image in the `directories/itim_self_service.war/images/access` folder of your customizable files.
   - To define a custom image for a customer-defined access category, create the image in GIF format by using the naming convention `icon<`*`access~category~hierarchy`*`>Access.gif`. Place the custom image in the `directories/itim_self_service.war/images/access` folder of your customizable files. If your site administrator defined access categories in a

hierarchy, then the GIF name must reflect that hierarchy by using "~" characters. For example, if a Finance category is defined as a child of the Application category, then the image file must be called iconApplication~FinanceAccess.gif.

- To define a custom image for a specific access item, create the new image file in any image format. Use any file name that you choose for the image file. Place the image file in the directories/itim_self_service.war/images/access folder of your customizable files. Your site administrator can then specify this image file location in the Access Information page of the service that is associated with the access item. For example, if you create an image that is called iconMyApplicationAccess.jpg, the image location is specified in the **Access icon** > **Icon URL** field as: /itim/ui/custom/ui/images/access/iconMyApplicationAccess.jpgdirectories/itim_self_service.war/images/access/iconMyApplicationAccess.jpg

Results

The appearance of the access cards on the access selection step of the Request Access wizard is changed to reflect the customization that you made.

What to do next

In a managed-cluster environment, you must wait until after the configuration is synchronized to the application servers in the cluster. For information about synchronizing, see "Synchronizing a member node with a primary node" on page 19. Log in to the Identity Service Center. Start the Request Access wizard and verify that the appearance of the access cards reflects the customization that you made.

Customizing badges on access cards in the Request Access wizard

The second step in the Request Access wizard is used to select the accesses being requested for a user. The set of access items to choose from is displayed as a collection of access cards that are arranged in a grid. Access cards can be annotated with highlighted text called *badges*. Badges are used to alert the user to special considerations that are associated with the access, such as risk, data sensitivity, or regulatory compliance requirements. You can customize the text that is displayed for badges on access cards, and the style of the badges.

Before you begin

Depending on your system customization, you might not have access to this task. Contact your system administrator to obtain access to this task, or to have someone complete it for you.

About this task

A site administrator or a service owner uses the IBM Security Identity Manager Console to create badges and associate those badges with access items.

The badge text is defined as either a fixed string such as High Risk or the name of a property in the CustomLabels.properties file such as $highrisk. If a fixed string was defined as the badge text, then it cannot be customized. But if a property name was defined, you can customize the text that is displayed on the badge by modifying the value of the property.

The badge class is selected from one of the *Cascading Style Sheets* (CSS) style classes that are defined in the `Badge.css` file.

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To go to a custom file and edit, download, upload, or search it, see "Managing custom files" on page 20.
- To go to a property file and edit, upload, or search it see "Managing the server properties" on page 22.

Procedure

1. Optional: Customize the text that is displayed for a badge on an access card. Consult your site administrator or service owner to determine the property name that is defined as the text for the badge that you want to customize. For this example, assume that the badge text was specified as `$highrisk`. So the property name is `highrisk`.

   Locate the property name that is associated with the badge you want to customize, such as `highrisk`. If the property does not exist in the `CustomLabels.properties` file, then create a new property for the property name.

   Change the value of the property to the text that you want to display for the badge.
2. Optional: Customize the style for a badge on an access card. Changing the style for badges is an advanced topic that requires a working knowledge of *Hypertext Markup Language* (HTML) and *Cascading Style Sheets* (CSS). IBM Security Identity Manager contains several predefined CSS classes for badges. These classes might be suitable for your organization, but you can change these predefined classes or add new classes to meet your needs.

   To change the badge style for an existing CSS class, open the `Badge.css` file. Locate the CSS class definition for the badge that you want to change. Modify the style attributes that are associated with the CSS class to suit your needs. For example, to change the style of a badge that is associated with the `green` badge class, you can do the following actions:

   - Find the `.badge.green` CSS selector in the `Badge.css` file.
   - Modify the style attributes that are associated with it.

   To create a new badge class that can be assigned to access entities, open the `Badge.css` file. Create a CSS selector or copy an existing CSS selector for the new badge class. CSS selectors for badges must always be in the form, `.badge.`*`customName`*, where *customName* is the name of the new badge class. The IBM Security Identity Manager Console displays this *customName* in the drop-down list of badge classes when the site administrator or service owner assigns badges to access entities. Modify the style attributes associated with the new CSS class to suit your needs.

   If you want to define more complex styles for badges, you can also create custom CSS selectors that include dynamic pseudo-classes. For example, `.badge.customName:after`.

Results

The badges that are displayed on access cards are changed to reflect the customization that you made in the `CustomLabels.properties` and `Badge.css` files.

What to do next

Select one or more accesses for a user that is based on your request access requirements.

Customizing the access card selection limit in the Request Access wizard

The second step in the Request Access wizard is used to select the accesses that are being requested for a user. There is a limit to the number of accesses that can be requested at one time. You can change this limit to meet your needs.

Before you begin

You must have read or write access to the customizable files and the directories where they are maintained. See "Location of Identity Service Center customizable files" on page 84 and "Customizing Identity Service Center files" on page 87 for specific details about where these files are located. Contact your system administrator if you do not have the necessary permissions.

About this task

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To go to a custom file and edit, download, upload, or search it, see "Managing custom files" on page 20.
- To go to a property file and edit, upload, or search it see "Managing the server properties" on page 22.

The Select accesses page of the Request Access wizard is used to select the accesses that are being requested for a user. By default, the number of accesses that can be selected on the Select accesses page is limited to `25`. But you can change this limit to meet your needs by modifying the `UIconfig.properties` file.

Procedure

1. Select the `UIconfig.properties` file. See "Managing the server properties" on page 22.
2. Click **Edit** and locate the `access.selection.maximum.number` property.
3. Change the value to the expected access limit for your organization. For example, `20`.

Results

The Select accesses page of the Request Access wizard restricts the number of accesses that the user can select to the specified limit in the `UIconfig.properties` file.

What to do next

In a managed-cluster environment, you must wait until after the configuration is synchronized to the application servers in the cluster. For information about synchronizing, see "Synchronizing a member node with a primary node" on page 19. Log in to the Identity Service Center. Start the Request Access wizard and confirm that the number of accesses selected is restricted to the specified limit.

Customizing the search controls in the Request Access wizard

The third step in the Request Access wizard is used to provide required information for accesses that are being requested. The forms for this required information might contain fields that are defined as `Search Control` or `Search Match Control`. You can customize the appearance of the search controls to meet your organizational requirements.

Before you begin

You must have read and write access to the customizable files and the directories where they are maintained. See "Location of Identity Service Center customizable files" on page 84 and "Customizing Identity Service Center files" on page 87 for specific details about where these files are located. Contact your system administrator if you do not have the necessary permissions.

About this task

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To go to a custom file and edit, download, upload, or search it, see "Managing custom files" on page 20.
- To go to a property file and edit, upload, or search it see "Managing the server properties" on page 22.

For some access requests, the user provides required information by completing fields of the form that is associated with the access. Some fields of the form might have a search control that enables the user to search the IBM Security Identity Manager Server for the appropriate value.

Each search field on a form is configured to search for a specific category of object, such as a `Person`, `Account`, or `Organizational Unit`. Search controls on forms can be used in two modes:

- The basic search mode allows the user to type some search text into the form field. The objects that match the search text are displayed as a drop-down list of cards under the form field.
- The Advanced Search mode is displayed as a dialog box. You can do the following actions:
  - Specify the search text.
  - Select the specific attribute to compare.
  - Select a comparison operator such as **Equals** or **Contains**.

  The objects that match the search criteria are displayed in rows of a table.

The object attributes in the drop-down list of cards and in the columns of the Advanced Search table can be customized to suit your needs. The information is arranged into several areas, and you can choose which object attribute is displayed in each area.

The `primary` area of the card displays the most important attribute, such as the object name. The information in this area is displayed at the top of the card and in the largest font. Only one attribute can be assigned to the `primary` area. But you can choose a different attribute for each of the object profiles that are defined in your environment. The attribute that is assigned to this area of the card is displayed as the first column in the Advanced Search table.

The secondary area of the card displays the next most important attribute, such as the object description. The information in this area is displayed just under the primary area and in a smaller font than the primary area. Only one attribute can be assigned to the secondary area. But you can choose a different attribute for each of the object profiles that are defined in your environment. The attribute that is assigned to this area of the card is displayed as the second column in the Advanced Search table.

The tertiary area of the card displays extra information about the object, such as the user title. The information in this area is displayed just under the secondary area and in a smaller font than the secondary area. Only one attribute can be assigned to the tertiary area. But you can choose a different attribute for each of the object profiles that are defined in your environment. The attribute that is assigned to this area of the card is displayed as the third column in the Advanced Search table.

The icon area of the card displays an image that is associated with the object. The icon is displayed at the side of the card, next to the primary, secondary, and tertiary areas. The attribute that is assigned to this area must provide the location (URI) of the image to display. You can choose a different attribute for each of the object profiles that are defined in your environment. The attribute that is assigned to this area of the card is not displayed in the Advanced Search table.

Sometimes the attribute that you want to display is not an attribute of the object, but it might be the attribute of a related object. For example, a user might have attributes that are called "manager" or "ersponsor" that are actually references to related users, namely the manager or sponsor of this user. To display an attribute like "name" from the related user in the card or the Advanced Search table, you can specify the attribute by using dotted notation. For example, "manager.name" or "ersponsor.name".

Note: Some types of attributes, such as mapped attributes and attributes from related objects, can be selected and displayed in search results. But they cannot be used as the search criteria.

Procedure

1. Optional: Customize the attributes that are displayed in the different areas of search cards and the Advanced Search table. Make a custom copy of the Search.json file and open the file with a text editor. The contents of this file are maintained in *JavaScript Object Notation* (JSON) format, which is a way of representing structured data.

   The Search.json file has sections for each object category, such as Person or ACCOUNT. You can use this file to select different display attributes for each type of object. There are sections within each object category that define the attributes to display for that object type.

   The primary section contains an attribute subsection. For example:

   ```
   "primary": {
        "attribute": {
            "default": "name",
            "Person" : "CN"
        },
        . . .
    },
   ```

   In the attribute section, define the object attribute to display in the primary area of the search card and in the first column of the Advanced Search table. You can choose a different attribute for each profile that is defined in your environment. You must always set a default attribute to use for any profiles not explicitly defined. In the preceding example, the default attribute is "name", but the attribute for objects in the "Person" profile is "CN".

The secondary section is identical to the primary section. For example:

```
"secondary": {
     "attribute": {
         "default": "mail"
     },
     . . .
 },
```

In the attribute section, define the object attribute to display in the secondary area of the search card and in the second column of the Advanced Search table. You can choose a different attribute for each profile that is defined in your environment. You must always set a default attribute to use for any profiles that are not explicitly defined. In the previous example, the default attribute is "mail", and no other attributes are defined for specific profiles.

The tertiary section of this file is identical to the primary and secondary sections. For example:

```
"tertiary": {
     "attribute": {
         "default": "title"
     },
     . . .
 },
```

In the attribute section, define the object attribute to display in the tertiary area of the search card and in the third column of the Advanced Search table. You can choose a different attribute for each profile that is defined in your environment. You must always set a default attribute to use for any profiles not explicitly defined. In the previous example, the default attribute is "title", and no other attributes are defined for specific profiles.

2. Optional: Customize the labels that are displayed for the column headings in the Advanced Search table. Make a custom copy of the SearchCustomAttributes.properties file and open the file with a text editor. The properties in this file define the text that is displayed in the column headings of the Advanced Search table.

   The primary, secondary, and tertiary sections of each object category in the Search.json file contain a **labelKey** field. For example:

```
 "primary": {
     . . .
     "labelKey": "name"
 },
 "secondary": {
     . . .
     "labelKey": "contactInfo"
 },
 "tertiary": {
     . . .
     "labelKey": "title"
 },
```

   The uppercase value of these **labelKey** fields is used to look up the display strings for the column headings of the Advanced Search table in the SearchCustomAttributes.properties file. In this example, the **labelKey** value NAME is looked up as a property to find the column heading to display for the primary attribute. It is the first column in the Advanced Search table. If any properties are not found, then the value of the **labelKey** field is used as the column heading.

3. Customize the icon area of the search card to display an image for the associated object. Make a custom copy of the Search.json file and open the file with a text editor. The contents of this file are maintained in *JavaScript Object Notation* (JSON) format, which is a way of representing structured data.

   The icon section of each object category of this file contains an attribute subsection. For example:

   ```
   "icon": {
        "attribute": {
            "default": "erimageuri"
        }
    }
   ```

   In the attribute section, define the attribute that contains the location of the icon or image to display on the search card. You can choose a different attribute for each profile that is defined in your environment. You must always set a default attribute to use for any profiles that are not explicitly defined. If some profiles do not have an image attribute, you can specify null to indicate that no image must be displayed for objects in that profile. In the earlier example, the default attribute is "erimageuri", and no other attributes are defined for specific profiles.

Results

The appearance of the search controls on form fields of the Request Access wizard is changed to reflect the customization that you made.

What to do next

In a managed-cluster environment, you must wait until after the configuration is synchronized to the application servers in the cluster. For information about synchronizing, see “Synchronizing a member node with a primary node” on page 19.

Log in to the Identity Service Center. Start the Request Access wizard, and verify that the appearance of the search control reflects the customization that you made.

Customizing the hint and help text for form fields in the Request Access wizard

The third step of the Request Access wizard is used to provide required information for the accesses that are being requested. For some access requests, the user provides the required information by completing fields of the form that is associated with the access. These forms can be customized by the site administrator. For more information, see the “Form customization” section in the IBM Security Identity Manager product documentation. The hint text and help text that are associated with the fields on a form can be customized to suit your needs.

Before you begin

Depending on your system customization, you might not have access to this task. Contact your system administrator to obtain access to this task, or to have someone complete it for you.

About this task

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To go to a custom file and edit, download, upload, or search it, see "Managing custom files" on page 20.
- To go to a property file and edit, upload, or search it see "Managing the server properties" on page 22.

The site administrator can set properties for form fields to define hint text and help text. A user can view the hint text and help text in the Identity Service Center to understand what values are needed or are appropriate for the fields.

- If the administrator sets the `Hint text` property for a form field, the text is displayed inside the input field as a hint to the user. The hint text is replaced by the field data that is entered by the user.
- If the administrator sets the `Help text` property for a form field, a help icon is displayed next to the label for the form field. If the user selects or hovers over the help icon, the help text is displayed to provide more information about the form field.

The hint text and help text are specified as either a fixed string such as `Select a primary group` or the name of a property in the `CustomLabels.properties` file such as `$PrimaryGroupHintText`. If a fixed string was defined as the hint text or help text, then it cannot be customized. But if a property name was defined, you can customize the hint text or help text by modifying the value of the property.

Procedure

1. Consult with the site administrator to determine the property names that were defined as the values of the `Hint text` and `Help text` for the form fields that you want to customize.
2. Open the `CustomLabels.properties` file See "Managing the server properties" on page 22.
3. Optional: Find the property names that are defined for the `Hint text` in the `CustomLabels.properties` file. For each of the form fields that you want to customize, modify the values to the hint text that you want to display.
4. Optional: Find the property names that are defined for the `Help text` in the `CustomLabels.properties` file. For each of the form fields that you want to customize, modify the values to the help text that you want to display.
5. Save and close the `CustomLabels.properties` file.

Results

The fields on the Provide account information form of the Request Access wizard that have the `Hint text` property defined now display the customized hint text in the input area. The fields that have the `Help text` property defined now display a help icon next to the field label, and selecting or hovering over the help icon displays the customized help text.

What to do next

Log in to the Identity Service Center. Start the Request Access wizard, and verify that the Provide account information form fields reflect the customization that you made.

View Access wizard

You can customize the user interface of the View Access wizard to suit your needs.

You can change or customize the following items:

- The display of user ID to make the user ID sortable
- The display of the account status and compliance information on the access cards

Customizing an account attribute in the View Access wizard

You can customize an account attribute to display or sort on the access cards.

Before you begin

- You must have read or write access to the customizable files and the directories where they are maintained. See “Location of Identity Service Center customizable files” on page 84 and “Customizing Identity Service Center files” on page 87 for specific details about where these files are located. Contact your system administrator if you do not have the necessary permissions.
- By default, the user ID is displayed on the access cards and sorting is enabled for the user ID.

About this task

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To go to a custom file and edit, download, upload, or search it, see “Managing custom files” on page 20.
- To go to a property file and edit, upload, or search it see “Managing the server properties” on page 22.

The file `Access.json` contains the access attributes that are customizable. The access attributes can be in the following categories:

- Standard attributes that are in the primary, secondary, or tertiary areas of the access cards. See “Customizing an access card in the Request Access wizard” on page 108.
- Account attributes that are customized for user-specific views. For example, `account.eruid`.

Procedure

1. Optional: Customize an account attribute that is displayed on the access cards.
   a. Download a copy of the `Access.json` file. See “Managing the server properties” on page 22.
   b. Edit the file. The contents of this file are maintained in *JavaScript Object Notation* (JSON) format, which is way of representing structured data.

      The `userAccessView` section contains the `userId` subsection. For example:

      ```
      "userAccessView": {
         "userId": {
         "attribute": "account.eruid" "display": true,
          .....
          }
         }
      ```

   c. If you do not want to display an account attribute on the access cards, set `"display": false`.
2. Optional: Customize an account attribute for the sort functionality.

a. Download a copy of the Access.json file. See "Managing the server properties" on page 22.

b. Edit the file. The contents of this file are maintained in *JavaScript Object Notation* (JSON) format, which is way of representing structured data.

   The uerId section contains the sort subsection. For example:

```
"userAccessView": {
   "userId": {
   "attribute": "account.eruid" "display": true,
    "sort": {
     "enabled": true,
     "labelKey": "userId"
    }
   }.....
}
```

c. To disable the sort on an account attribute, set "enabled": false.

   Note: If you enable the sort functionality, an account attribute is the third sort attribute in the grid sortable attributes.

Results

An account attribute that is displayed on access cards reflects the customization that you made in the Access.json file.

Customizing account status and compliance information in the View Access wizard

You can customize the account status and compliance information that is displayed on the access cards in the View Access wizard.

Before you begin

- Depending on your system customization, you might not have access to this task. Contact your system administrator to obtain access to this task, or to have someone complete it for you. See "Location of Identity Service Center customizable files" on page 84 and "Customizing Identity Service Center files" on page 87 for specific details about where these files are located.
- By default, the account status and compliance information is displayed on the access cards. Account status is displayed for the suspended and disallowed accounts. The compliance information is displayed for the accounts that are non-compliant. You might see the following compliance messages on the access cards:

  Compliance evaluation is pending
  Indicates that the access was returned from a reconciliation, which means it was not checked against the existing policies.

  Access is not compliant with the policy
  Indicates that the access can exist for the user, but that one or more of the underlying account attributes do not comply with the existing provisioning policies.

  Access is not allowed by the policy
  Indicates either that the access is not supposed to exist because the user is not allowed to have access to the specified resource, or that a provisioning policy is not defined for the resource.

  No message
  Indicates that the access is compliant.

About this task

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To go to a custom file and edit, download, upload, or search it, see "Managing custom files" on page 20.
- To go to a property file and edit, upload, or search it see "Managing the server properties" on page 22.

The file `Access.json` contains the access attributes that are customizable. The access attributes can be in the following categories:

- Standard attributes that are in the primary, secondary, tertiary, or image areas of the access cards. For more information about customizing the standard attributes, see "Customizing an access card in the Request Access wizard" on page 108.
- Attributes that are customized for the user-specific views. For example, account status and compliance information.

Procedure

1. Optional: Customize the account status that is displayed on the access cards.
   a. Download a copy of the `Access.json` file. See "Managing the server properties" on page 22.
   b. Edit the file. The contents of this file are maintained in *JavaScript Object Notation* (JSON) format, which is way of representing structured data.

      For example:

      ```
      "userAccessView": {
         "userId": {
          "attribute": "account.eruid",
          "display": true,
          "sort": {
           "enabled": true,
           "labelKey": "userId"
          }
         },
         "showCompliance": true,
                  "showAccountStatus": true
        }
      ```
   c. If you do not want to display the account status on the access cards, set the value for `showAccountStatus` to `false`. For example, `"showAccountStatus": false`.
2. Optional: Customize the compliance information that is displayed on the access cards.
   a. Download a copy of the `Access.json` file. See "Managing the server properties" on page 22.
   b. Edit the file. The contents of this file are maintained in *JavaScript Object Notation* (JSON) format, which is way of representing structured data.

      For example:

      ```
      "userAccessView": {
         "userId": {
          "attribute": "account.eruid",
          "display": true,
          "sort": {
           "enabled": true,
           "labelKey": "userId"
          }
      ```

```
         },
         "showCompliance": true,
                  "showAccountStatus": true
        }
```

c. If you do not want to display the compliance information on the access cards, set the value for `showCompliance` to `false`. For example, `"showCompliance": false`.

Results

The account status and compliance information that are displayed on access cards are changed to reflect the customization that you made in the `Access.json` file.

View pending accesses on access cards

Access cards display the information about the pending accesses that are requested from the IBM Security Identity Manager.

You can view the pending accesses that are requested from the following IBM® Security Identity Manager user interfaces:

- Administrative console
- Self-service user interface
- Identity Service Center

You can also view the accesses requests that are originated from public APIs or web services.

Manage Activities wizard

You can view and act on the activities that are assigned to you. You can also review activities that you completed.

View approval details

Before you act on the requests, you can view the details about the requests.

You can view the operation that triggers an approval request. You can configure the following entities and operations for approval activities:

Access
Includes the roles and groups in the system. You can configure these operations for approval activities: `Add`, `Modify`, and `Delete`.

Note: On the Approval Details page, the **View Details** link is not visible in the Identity Service Center user interface for access entity.

Account
Includes the accounts on a service. You can configure these operations for approval activities: `Add`, `Modify`, `Delete`, `Restore`, and `Suspend`.

Person
Includes any user in the system. You can configure these operations for approval activities: `Add`, `Modify`, `Delete`, `Restore`, `SelfRegister`, `Suspend`, and `Transfer`.

Dependent access overview:

Dependent accesses are provisioned to a user upon approval of the access request. The dependent accesses are evaluated based on the provisioning policy that is configured with the service access.

The following cases explain what can be considered as dependent accesses.

Provisioning policy membership

The provisioning policy membership is one of the criteria that governs the calculation of the dependent accesses. For a provisioning policy with a membership type as role and the provisioning option as automatic, the entitlements that are added are considered as dependent accesses. The following target type options are available for a provisioning policy:

- Specific service
- Service type
- Service selection policy

Group-based access requests

When a group membership is requested and if there is no account for a user on the service, a new account is created. This new account is considered as dependent access.

Customizing the due date notification period

You can customize the default due date notification period (24 hours) to suit your business needs.

Before you begin

You must have read or write access to the customizable files and their directories. See “Location of Identity Service Center customizable files” on page 84 and “Customizing Identity Service Center files” on page 87. Contact your system administrator if you do not have the necessary permissions.

About this task

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To go to a custom file and edit, download, upload, or search it, see “Managing custom files” on page 20.
- To go to a property file and edit, upload, or search it see “Managing the server properties” on page 22.

Procedure

1. Edit the `UIconfig.properties` file. See “Managing the server properties” on page 22.
2. Search for the `activity.duedate.threshold` property.
3. Set the value for the property `activity.duedate.threshold` in hours. For example, `activity.duedate.threshold=48`.

Results

The due date notification period changes.

Customizing the labels

You can rename the labels to suit your business needs.

Before you begin

You must have read or write access to the customizable files and their directories. See “Location of Identity Service Center customizable files” on page 84 and

"Customizing Identity Service Center files" on page 87. Contact your system administrator if you do not have the necessary permissions.

About this task

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To go to a custom file and edit, download, upload, or search it, see "Managing custom files" on page 20.
- To go to a property file and edit, upload, or search it see "Managing the server properties" on page 22.

AA and AR are the default approval activity result codes that are used by workflows in IBM Security Identity Manager. The user interface displays labels from the CustomLabels.properties file that are based on the property names. These property names are derived from the approval activity result codes. If you customize workflows to use customized approval activity result codes, you must add the appropriate properties to the CustomLabels.properties file. You customize the labels for the interface when you define these properties. For example, if you use the customized result code XYZ to represent approval, you must add properties with the names XYZ, XYZ_inProgress, and XYZ_complete to CustomLabels.properties file.

Note: If you do not add the values to the CustomLabels.properties file, the actual key names are displayed in the user interface. For example, XYZ_inProgress is displayed instead of "Processing".

Procedure

1. Optional: Rename any of the following labels in the CustomLabels.properties file by changing the property value to the text that you want to display:

Label	Property value
Approve	AA
Reject	AR
Approving	AA_inProgress
Rejecting	AR_inProgress

   a. Edit the CustomLabels.properties file. See "Managing the server properties" on page 22.
   b. Change the value of the property to the text that you want to display for the label.
2. Optional: Rename the either Approved or Rejected labels or both.
   a. Edit the ActivityListCard_en.properties file. See "Managing the server properties" on page 22.
   b. Change the value of the property AA_Complete or AR_Complete to the text that you want to display for the label.

Results

The labels change to reflect the customization that you made in the CustomLabel.properties and ActivityListCard_en.properties files.

Redirecting help content

You can redirect help requests to your own website to deliver custom help content.

Before you begin

You must have read and write access to the customizable files and the directories where they are maintained. See "Location of Identity Service Center customizable files" on page 84 and "Customizing Identity Service Center files" on page 87 for specific details of where these files are located. Contact your system administrator if you do not have the necessary permissions.

About this task

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To go to a custom file and edit, download, upload, or search it, see "Managing custom files" on page 20.
- To go to a property file and edit, upload, or search it see "Managing the server properties" on page 22.

Editing the help content that is shipped with the Identity Service Center user interface is not supported. But you can redirect help requests to your own website to deliver custom help content in line with your corporate appearance.

The `UIHelp.properties` file specifies properties that control the redirection of help file requests. The following table shows the property and property description for Identity Service Center help.

Table 36. Identity Service Center help properties and description

Property	Description
helpBaseUrl	Specifies the base URL to which to send help requests. A blank or null value indicates that help goes to the default URL for the help files in the Identity Service Center.
helpLocales	Restricts the locales for which help is supported. For example, **`helpLocales=en,fr`** restricts help support to English and French regardless of the number of available locales. If the attribute is not specified or null, the supported help locales are the same as the supported locales for the Identity Service Center user interface. These locales are specified by the **`isim.ui.supportedLocales`** property in the `UIconfig.properties` file.
Help Id mappings: helpId = relativeHelppageURL	The help mappings section maps IDs from specific pages to a relative URL sent to the help server.

The Help URL is the combination of the helpBaseUrl + locale + relativeHelppageURL

For example, if your custom `config/UIHelp.properties` file contains:

```
helpBaseUrl=http://myserver:80/helpfiles
login_help_url=ui/ref_ui_login.html
```

Then for a user who selects the English (en) locale, the request for the Login help page is redirected to `http://myserver:80/helpfiles/en/ui/ref_ui_login.html`.

Procedure

1. Edit the `config/UIHelp.properties` file. See "Managing the server properties" on page 22.
2. Change the **`helpBaseUrl`** property in the file.
3. Update **`helpId`** mappings to use the relative URLs for your server.
4. Optional: If you want to restrict the list of supported help locales, uncomment the **`helpLocales`** property. Modify it to specify the list of locales for which help is supported in your environment.
5. Add pages to your server for the appropriate locales.

Results

The help requests are now redirected to your customized help files.

What to do next

In a managed-cluster environment, you must wait until after the configuration is synchronized to the application servers in the cluster. For information about synchronizing, see "Synchronizing a member node with a primary node" on page 19. Log in to the Identity Service Center. Start the Identity Service Center in a browser to verify that the customized file is being used.

Supporting more languages

You can extend the Identity Service Center to support more languages by providing your own translations for all of the IBM-provided globalization files.

Before you begin

You must have read and write access to the customizable files and the directories where they are maintained. See "Location of Identity Service Center customizable files" on page 84 and "Customizing Identity Service Center files" on page 87 for specific details of where these files are located. Contact your system administrator if you do not have the necessary permissions.

Determine the value of the locale identifier for the language (`xx`) or language and country (`xx_YY`) associated with the translation you want to provide. For example: `da` (Danish) or `ro_MO` (Romanian, Moldova).

About this task

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To go to a custom file and edit, download, upload, or search it, see "Managing custom files" on page 20.
- To go to a property file and edit, upload, or search it see "Managing the server properties" on page 22.

Procedure

1. Create a custom version of the `common.properties` file for the new language.

   For example, create the `common_xx_YY.properties` file.

   You must create the properties file in the new locale. The server determines the list of available locales by searching for all variants of the `common.properties` file. You must also translate all of the properties in the `common_xx_YY.properties` file to the new language.
2. If you previously restricted the locales that you support, you must modify your customized copy of the `UIconfig.properties` file to include the new language. Update the **`isim.ui.supportedLocales`** property in your custom version of this file to include the new locale, `xx_YY`. If all locales are supported, no change is required to the `UIconfig.properties` file because the default is to support all available locales.
3. The new language might be a language that is read from right-to-left. In this case, you must modify your customized copy of the `UIconfig.properties` file to include the new language in the list of right-to-left locales. Update the **`isim.ui.rtlLocales`** property in your custom version of this file to include the new locale, `xx_YY`.
4. Create custom versions of all supported language variants of the `UILanguages*.properties` files.

   Add a line to each file that specifies the display name for the new locale. This file is used to build the language selection control of the Login page. For example: `xx_YY=`*`New language name`*
5. Create custom versions of all of the other files under `custom/ui/nls` for the new locale.
6. Translate the text in all of the `*_xx_YY.properties` files into the new language.
7. You can add a language for page help files only if you already provided custom help files, as described in “Redirecting help content” on page 125. Take these steps:
   a. Create a directory for the `xx_YY` locale at the same level as the directory that contains the existing `en` (English) and other locales.
   b. Copy the custom help files for an existing language into the new `xx_YY` directory with the same directory structure.
   c. Translate the help files in the `xx_YY` directory to the new language.
   d. Update the `<html>` element in each of the help files to specify the locale of the new language, such as `<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="`**`xx-yy`**`" lang="`**`xx-yy`**`">`. If the new language is read from right-to-left, you must also modify the `<html>` element in each of the help files to specify the direction as `"rtl"`. For example: `<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="xx-yy" lang="xx-yy" dir="`**`rtl`**`">`
8. If you previously restricted the help locales that you support, you must modify your customized copy of the `UIHelp.properties` file to include the new language. Update the **`helpLocales`** property in your custom version of this file to include the new locale, `xx_YY`. If all help locales are supported, no change is required to the `UIHelp.properties` file because the default is to support all available locales.

Results

The Identity Service Center user interface is available to users in the new language translation. If you translated the help files, the Identity Service Center page help is also available to users in the new language translation.

What to do next

In a managed-cluster environment, you must wait until after the configuration is synchronized to the application servers in the cluster. For information about synchronizing, see “Synchronizing a member node with a primary node” on page 19.

To view the new language translation, select the new language from the dropdown list of languages on the Identity Service Center Login page. Alternatively, configure your browser preferences to use the new language.

Chapter 3. Modifying the sample email content

You can modify the content of the sample email notifications that are used for testing.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

A post office email aggregation template must already be configured.

About this task

Use the following sections to work with the configuration files or the configuration properties from the IBM Security Identity Manager virtual appliance console:

- To go to a custom file and edit, download, upload, or search it, see “Managing custom files” on page 20.
- To go to a property file and edit, upload, or search it, see “Managing the server properties” on page 22.

Modify the content of the sample email notification.

Procedure

1. Edit the `enRole.properties` file. See “Managing the server properties” on page 22.
2. Specify the new `enrole.postoffice` values, and then save the `enRole.properties` file. `enRole.properties` is the name of the properties file, and `enrole.postoffice` is the name of the key for which you specify a value. This key-value pair resides in the properties file.
3. Restart your application server for the new values to take effect.

Results

The results of this task can be seen only after you test the aggregation template that you created or modified. The new sample email notifications are aggregated and sent to the test email address.

Example

The `enRole.properties` file contains the following default values:

```
##############################################################
## Post Office Template Test Configuration
##############################################################
# These are the contents of the emails that will be used
# when the "test" button is used on the Post Office
# configuration page. These 3 emails will be used as the
# content to which the template will be applied.
enrole.postoffice.test.subject1=This is subject 1
enrole.postoffice.test.textbody1=This is the text body 1
enrole.postoffice.test.xhtmlbody1=This is the xhtml body 1

enrole.postoffice.test.subject2=This is subject 2
enrole.postoffice.test.textbody2=This is the text body 2
enrole.postoffice.test.xhtmlbody2=This is the xhtml body 2

enrole.postoffice.test.subject3=This is subject 3
enrole.postoffice.test.textbody3=This is the text body 3
enrole.postoffice.test.xhtmlbody3=This is the xhtml body 3

# The topic to use for the test emails above
enrole.postoffice.test.topic=topic1

# The locale to use for the test emails above
enrole.postoffice.test.locale=en_US
```

What to do next

Test the new aggregate template by sending it to a test email address.

Chapter 4. Comma-Separated Value (CSV) identity feed

The Comma-Separated Value (CSV) identity feed provides capability for reading comma-separated value (CSV) file to add users to IBM Security Identity Manager.

CSV service type

This identity feed service type parses identity feeds with CSV file formats that comply with RFC 4180 grammar. The IBM Security Identity Manager parser has the following RFC enhancements:

- Trims leading and trailing white space from unquoted text in a field. In contrast, RFC 4180 regards all space to be significant, whether inside or outside of quotation mark delimiters.
- Allows quoted and unquoted text to be in the same field. In contrast, RFC 4180 does not allow both text types in the same field.
- Does not enforce the RFC 4180 restriction that all records have the same number of fields. However, the code that calls the CSV parser reports an error if a record has more fields than the CSV header has.
- Allows record termination to use carriage return (CR) or to use carriage return/line feed (CR/LF) to be compatible with both UNIX and DOS base files. In contrast, RFC 4180 terminates all records with carriage return/line feed (CR/LF).

Services that use CSV files

IBM Security Identity Manager has the following types of services that use CSV files as input:

- CSV identity feed
- Custom services that use the Manual Service Provider type. These custom services use a CSV file format for the reconciliation upload file. This service type can be used for both identity and account feeds.

  By default, all accounts defined in a CSV file for reconciliation of a manual service are marked as active in Security Identity Manager. To suspend a person or account using a manual service reconciliation, add the `erpersonstatus` or the `eraccountstatus` attribute to the CSV file (depending on whether the feed is for identities or accounts). A value of `0` (zero) indicates active. A value of 1 indicates inactive.
- Custom services that use the Directory Integrator Adapter Provider type that use the IBM Security Directory Integrator CSV connector. This service type can be used for both identity and account feeds.

CSV file format

A CSV file contains a set of records separated by a carriage return/line feed (CR/LF) pair (\r\n), or by a line feed (LF) character. Each record contains a set of fields separated by a comma. If the field contains either a comma or a CR/LF, the comma must be escaped with double quotation marks as the delimiter. The first record in the CSV source file defines the attributes provided in each of the following records. For example:

```
uid,sn,cn,givenname,mail,initials,employeenumber,erroles
```

The `sn` and `cn` attributes are required by the object classes used by IBM Security Identity Manager to represent a person. The identity feed process uses all objects in the file. The CSV file cannot contain binary attributes.

You might use a multi-valued attribute to specify a user who has membership in multiple groups. Groups might include Service Owner, Windows Local Management (a self-defined group), and Manager. If you include multi-valued attributes, they must be represented by using multiple columns with the same attribute name.

To specify multi-valued attributes, repeat the column the required number of times. For example:

```
cn, erroles, erroles, erroles, sn
cn1,role1, role2, role3, sn1
cn2,rolea,,,sn2
```

The record that you feed into IBM Security Identity Manager might not have an email address for the user. That user does not receive a notification email that contains the password for a new account, and must call the help desk or contact the manager.

CSV connector for IBM Security Directory Integrator

Information about the CSV connector for IBM Security Directory Integrator is available in the following product directory:

```
/extensions/versionNumber/examples/idi_integration/HRFeedCSV/ITDIFeedExpress
```

(For example, `directories/utilities/extensions.zip/6.0/examples/idi_integration/HRFeedCSV/ITDIFeedExpress`)

Complete these steps:

1. See “Managing custom files” on page 20.
2. From the **Custom File Management** menu in the **Appliance Dashboard**, go to `directories/utilities`.
3. Download the `extensions.zip` file.
4. Extract the file and go to the `6.0/examples/idi_integration/HRFeedCSV/ITDIFeedExpress`.

UTF-8 encoding in an identity feed file

Your identity feed file must be in UTF-8 format. You must use an editor that supports UTF-8 encoding.

- Windows

  The following are UTF-8 capable: Microsoft Word 97 or later, or the Notepad editor that is included with the Windows 2003 Server or Windows XP operating systems.

  To save a file in UTF-8 format using Notepad, click **File** > **Save As**. Then, expand the list of choices for the **Encoding** field and select `UTF-8`.
- Linux

  The Vim text editor (a version of the classic vi editor) is UTF-8 capable. To work with files in UTF-8 format using the Vim text editor, specify the following:

  ```
  :set encoding=utf-8
  :set guifont=-misc-fixed-medium-r-normal--18-120-100-100-c-90-iso10646-1
  ```

If your version of UNIX does not include this text editor, access this Web site:

http://www.vim.org

Note: For the 7-bit ASCII code subset, the UTF-8 encoded Unicode format is identical to 7-bit ASCII format. For input files that contain 7-bit ASCII (ASCII character values between hex 20 to hex 7e), you can use a normal text editor to create the file. For files containing any other character values (including extended European characters), you must save the file in UTF-8 format.

For an exact list of the 7-bit ASCII characters as supported by UTF-8, access this Web site and click the **Basic Latin** link in the first column:

http://www.unicode.org/charts

Chapter 5. Directory Services Markup Language (DSML) identity feed

The Directory Services Markup Language (DSML) identity feed provides capability for reading a DSML file to add users to IBM Security Identity Manager.

DSML service type

The IBM Security Identity Manager Server allows for integration of various human resource (HR) type data feeds. You can add large numbers of individuals to the IBM Security Identity Manager Server without manually adding each individual. An identity record in HR data becomes an instance of a person object in IBM Security Identity Manager. One type of HR type data feed is the DSML Identity Feed service. The service can receive the information in one of two ways: a reconciliation or an unsolicited event notification through an event notification program.

The mechanisms that handle HR data in IBM Security Identity Manager requires that the HR data be in an XML format. The format uses the standard schema defined by the Directory Services Markup Language (DSML version 1). See the DSML website at http://www.oasis-open.org for DSMLv1. When sending asynchronous notifications, an XML message format defined by the Directory Access Markup Language (DAML version 1) is used. DAML is an XML specification defined by IBM that allows specification of add, modify, and delete operations.

DSML file format

DSML is an XML format that describes directory information. A *DSML file* represents directory structure information in an XML file format. The DSML file must contain only valid attributes of the IBM Security Identity Manager profile. The identity feed process uses all objects in the file.

The `erPersonPassword` attribute is used in an identity feed only during a Person create process, not in a Person modify process. If the value of the `erPersonPassword` attribute is set, then the IBM Security Identity Manager account password is set to that value when the person and account are created. The following statement sets a value for the `erPersonPassword` attribute:

```
<attr name="erpersonpassword"><value>panther2</value></attr>
```

If you select a DSML file format for an identity feed, specify a DSML file similar to this one:

```
<entry dn="uid=sparker">
<objectclass><oc-value>inetOrgPerson</oc-value></objectclass>
<attr name="givenname"><value>Scott</value></attr>
<attr name="initials"><value>SVP</value></attr>
<attr name="sn"><value>Parker</value></attr>
<attr name="cn"><value>Scott Parker</value></attr>
<attr name="telephonenumber"><value>(919) 321-4666</value></attr>
<attr name="postaladdress"><value>222 E. First Street Durham, NC  27788</value></attr>
</entry>
```

UTF-8 encoding in an identity feed file

Your identity feed file must be in UTF-8 format. You must use an editor that supports UTF-8 encoding.

- Windows

  The following are UTF-8 capable: Microsoft Word 97 or later, or the Notepad editor that is included with the Windows 2003 Server or Windows XP operating systems.

  To save a file in UTF-8 format using Notepad, click **File** > **Save As**. Then, expand the list of choices for the **Encoding** field and select `UTF-8`.
- Linux

  The Vim text editor (a version of the classic vi editor) is UTF-8 capable. To work with files in UTF-8 format using the Vim text editor, specify the following:

  ```
  :set encoding=utf-8
  :set guifont=-misc-fixed-medium-r-normal--18-120-100-100-c-90-iso10646-1
  ```

  If your version of UNIX does not include this text editor, access this Web site:

  http://www.vim.org

Note: For the 7-bit ASCII code subset, the UTF-8 encoded Unicode format is identical to 7-bit ASCII format. For input files that contain 7-bit ASCII (ASCII character values between hex 20 to hex 7e), you can use a normal text editor to create the file. For files containing any other character values (including extended European characters), you must save the file in UTF-8 format.

For an exact list of the 7-bit ASCII characters as supported by UTF-8, access this Web site and click the **Basic Latin** link in the first column:

http://www.unicode.org/charts

Chapter 6. Integrating withIBM Security Identity Governance

Use a special connector to integrate Security Identity Manager with IBM Security Identity Governance

Instructions for setting up the integration are provided in technote 1688802.

Index

Printed in USA