

IBM Cloud Identity Portal

Administration Guide



Cloud Identity Portal Administration Guide

© **Copyright International Business Machines Corporation 2015, 2017.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. IBM Cloud Identity Portal.....	1
Chapter 2. Service requirements.....	3
Browsers.....	3
Chapter 3. Overview.....	5
Features and functions.....	5
Chapter 4. Company profile.....	7
Overview.....	7
Adding account management users.....	7
Managing API keys.....	7
Chapter 5. People.....	9
People management overview.....	9
Managing users.....	10
Users overview.....	10
Searching for users.....	10
Adding user records.....	10
Resetting user passwords.....	16
Managing groups.....	17
Groups overview.....	17
Searching for groups.....	17
Creating groups.....	17
Managing the membership of a group statically.....	18
Managing the membership of groups dynamically.....	18
Managing Classifiers.....	26
Adding classifiers.....	27
Searching for classifiers.....	28
Managing custom attributes.....	28
Attributes overview.....	28
Searching for attributes.....	28
Creating custom attributes.....	28
Managing the bulk import of users.....	29
SCIM files.....	30
Importing users.....	32
Chapter 6. Self Service.....	33
Configuring Self Service applications.....	33
Configuration overview.....	33
Configuring self-registration options and form.....	34
Configuring password reset options.....	43
Configuring user name recovery options and form.....	44
Configuring the Self Service profile form.....	49
Changing security question options.....	54
Managing roles.....	56
Customizing the UI for Self Service applications.....	60
Self Service UI customization overview.....	60
Customizing branding.....	60
Customizing general Self Service UI text keys.....	64

Configuring email templates.....	64
Customizing the Self Service profile application.....	67
Customizing the UI for Self Service suite pages.....	71
Adding instances.....	81
Adding local language support.....	82
Adding languages.....	82
Providing translated text.....	82
Privacy Settings.....	83
Managing Notices.....	84
Modifying Notices.....	85
Viewing Notices.....	85
Chapter 7. Applications.....	87
Managing services.....	87
Services overview.....	87
Searching for services.....	88
Searching for service categories.....	88
Creating services.....	88
Creating service categories.....	96
Managing the membership of a service statically.....	96
Managing the membership of services dynamically.....	97
Managing web access.....	110
Web access overview.....	110
Searching for web application connections.....	111
Creating web connections.....	111
Adding a connection server.....	121
Creating Protected Object Policies.....	123
Creating Access Control Lists.....	126
Creating protected objects.....	128
Managing Launchpad services.....	130
Managing federated SSO web access.....	130
Federated SSO overview.....	130
Managing federated partner connections.....	131
Managing Launchpad services.....	147
Managing keys.....	147
Creating a client certificate.....	147
Searching for a client certificate.....	149
Creating a server certificate.....	150
Searching for a server certificate.....	151
Provisioning identities.....	151
Identity provisioning overview.....	151
Feed Management UI.....	152
Managing reverse proxy settings.....	154
Reverse proxy settings.....	155
Chapter 8. Mobile application.....	157
Overview.....	157
Getting started.....	158
Downloading the app.....	158
Logging in.....	158
Managing your devices.....	160
Deleting the app.....	161
Managing services and launching apps.....	161
Viewing services and launching applications.....	161
Requesting access to a service.....	162
Managing requests.....	164
Searching by employee.....	164

Searching by service.....	167
Chapter 9. Policies.....	171
Creating a global user policy.....	171
User policy settings.....	171
Chapter 10. Identity governance.....	175
Searching for a request.....	175
Approving, denying, and reassigning requests.....	176
Notices.....	179
Trademarks.....	180

Chapter 1. IBM Cloud Identity Portal

Welcome to the Cloud Identity Portal documentation, where you can find information about how to administer Cloud Identity Service.

Chapter 2. Service requirements



Service requirements include supported browsers for Cloud Identity Service.

Browsers

Supported browsers for Cloud Identity Portal administration and Self Service applications.

Table 1. Supported browsers

Browser	Version	Operating system
Microsoft Internet Explorer	Latest version, and version that precedes the latest version.	Windows.
Mozilla Firefox	Latest version.	Windows and Mac.
Google Chrome	Latest version.	Windows and Mac.
Safari	Latest version, and version that precedes the latest version.	Mac.

Note: Where the latest and preceding versions are supported, all modifications of those versions are supported. For example, if the latest version of a browser is 24.n, then 24.n and 23.n versions are supported.

Note: Microsoft Edge is the currently the latest Microsoft browser. Microsoft Internet Explorer 11 is currently the latest version of Internet Explorer.

Chapter 3. Cloud Identity Portal overview



Become familiar with Cloud Identity Portal key functions and concepts.

Features and functions

Cloud Identity Portal is a consolidated administration environment for you to manage all your Identity and Access Management processes.

Company Information

Company information provides company-level contact information, for those individuals in your organization that have responsibility for the management or maintenance of Cloud Identity Portal.

Directory Management

Directory management is the system and processes used to manage the identity of your users. Users can be organized into groups, and defined by roles, and can be associated with a number of services.

You can manage users, groups, roles, services, and user password policies. Additions and changes you make have an immediate effect on Cloud Identity Service authentication and authorization.

API Key Management

Use API Key Management to create, edit, and remove API credentials your organization can use to work with the public Cloud Identity Portal API.

Application Management

Application management is the configuration and customization of Self Service applications. Self Service applications include all the applications users need to apply for, and maintain their identity profiles.

Configuring Self Service applications, includes configuring self-registration options, and password reset options, and user name recovery options.

Customizing the UI for Self Service applications, includes customizing branding, email templates, labeling for table columns, and labeling for user profile sections.

Web Access Management

Web Access Management, is the management of network connections to protected web resources.

You manage web access by creating and managing network connections to protected web resources. You also control access to protected resources by creating authorization policies. Authorization policies include Access Control Lists (ACLs), Protected Object Policies (POPs), and a global user policy.

Federated Single Sign-on

Federated Single Sign-on (SSO) enables users that have a Cloud Identity Service account to access other third-party application services with their existing identity. A Cloud Identity Service environment can support multiple federation partners.

Pre-configured templates are provided for a number of the most popular partner application services that support a federated single sign-on using SAML 2.0. If no template exists for the partner you want to create a connection for, then a customized configuration can be used.

Identity Provisioning

Both users and groups can be synchronized or provisioned by or to external directories by using identity feeds.

Cloud Identity Service can interface with over 70 types of identity repositories, such as Active Directory, LDAP v3, relational databases, SOAP services, Message Queue, and SAP.

Request management

If the normal approver is not available and has no delegated approver, it can be necessary for a Cloud Identity Portal administrator to manage user requests for services.

Reporting

Cloud Identity Service provides ad hoc reporting capabilities on all audit event data within the audit repository. You can use a number of predefined reports, and you can define your own reports.

Chapter 4. Company profile



Company profile information provides company-level contact information. Account contacts have administrative responsibility for the maintenance of Cloud Identity Portal.

Overview

Company profile information provides company-level contact information. Account contacts have administrative responsibility for the maintenance of the Cloud Identity Portal. Generate API credentials your organization can use to work with the public Cloud Identity Portal API with API key management.

Adding account management users

You can add account management users. Account management users have administrative responsibility for the maintenance of Cloud Identity Portal.

Procedure

1. Click **Company Profile > Account Management** in the navigation menu, and click **Account Management** and **Add New Account**.
2. Enter a user name for the user in the **Username** field. Click **Check Availability** to check that the account user name is unique.
3. Enter the remaining contact details and credentials for the contact.

Note: The password might need a minimum number of characters, and minimum numbers of specified character types. Use the field help to discover the password requirements.

4. Click **Save**.

The contact is available in the **Account Management** page.

Managing API keys

Generate API credentials your organization can use to work with the public Cloud Identity Portal API.

About this task

Create, edit, and remove API keys.

Procedure

1. In the navigation pane, click **Company Profile > API Key Management**.
2. Manage your API keys.

Add a REST API key

- a. Click **+ Add New API Key**.
- b. Specify the following fields:

<i>Table 2. API key fields</i>	
Field	Description
Key Alias	Create an alternate name for the API key with fifty alphanumeric characters or less that is easy to identify.
Key Description	Describe what the key is used for and where it is.
Access Token Validity	<p>Specify for how many seconds this token is valid. The approximate number of hours or days for the value that you entered is shown next to this field. You obtain an access token after you send the <code>client ID</code>, <code>secret</code>, and <code>grant_type</code> to the URL <code>POST https://GmaApi/oauth/token</code>. Use this access token to make calls to the API.</p> <p>Note: The secret key will display once after you create your new API key. Once you save the changes for your new API key, the secret key will never display again.</p> <p>After the access token expires, obtain a new one with the <code>client ID</code>, <code>secret</code>, and <code>grant_type</code>. Alternatively, you can obtain a new access token by using the refresh token and the <code>client ID</code> and <code>secret</code>.</p>
Refresh Token Validity	Specify the number of seconds for the Refresh Token Validity time, which must be greater than the Access Token Validity value. The approximate number of hours or days for the value that you entered is shown next to this field.

Edit or delete a REST API key

- a. View the details of the API key that you want to edit or delete by searching in the **Narrow your search** bar or by clicking the arrow next to the key name.
- b. Select the API key name that you want to edit or delete.
- c. Take either of the following actions:
 - Edit and change the values for any of those described in Table 1.
 - Click **Remove Key** to permanently delete the key.

Chapter 5. People



People management is the system and processes used to manage the identity of your users. Users can be organized into groups, and defined by roles.

People management overview

People management tasks include managing users, groups, and services.

You can create, modify, delete, and search for users, groups, and services. Additions and changes you make have an immediate effect on Cloud Identity Service authentication and authorization. For example, if you create an account record for a user, that user can then access the Cloud Identity Service and Self Service applications. You might also add a user to a group to give them access to a specific web application. Service memberships might not take effect immediately if approval is required.

Users

You can add, modify, delete, and search for user records. A user record can be created as an identity or as an account. An account gives a user login access to Self Service applications, and potentially, other resources that are managed by Cloud Identity Service. An identity is only a record of information about a user.

A user record is composed of a number of user identity attributes. Many of these attributes are common to most Identity Management system, for example, given name, surname, and email address. Your organization also has a number of attributes that are unique to your own set of applications. Attributes are collected from sources of record or identity repositories already in your organization, during the initial configuration of Cloud Identity Service for your organization. Most of the existing user records are created from these existing identity repositories.

Groups

Various Identity and Access Management policy decisions are best enacted by treating users collectively. Users that share some common characteristics can be grouped. For example, a group of users that work in the same department of a company can be granted the same access to a specified web application. In this case, the group of users is defined and then that group is referenced by an access control list (ACL) policy. The policy grants (or denies) application access to all the users in that group.

The user membership of a group can be statically or dynamically defined. Static user membership requires you to manually add each user to the group, and to manually manage group membership. Dynamic user membership automatically selects users for membership. Membership is based on any matching combination of identity attribute values, other group or service memberships, or assignment of a manager role. For example, you might group users who are in a specific country or locality. You might group users who have an account within a specific account number range, and who are also members of another specified group.

Dynamic user membership is implemented by using a dynamic provisioning policy, in which you define the group membership selection criteria.

Schema management

You can manage your LDAP (Lightweight Directory Access Protocol) schema by adding custom identity attributes to extend the information help in user identity records.

Managing users

You can add, modify, delete, and search for user records.

Users overview

A user record can be created as an identity or as an account. An account gives a user login access to the Cloud Identity Service, Self Service applications, and other resources that are managed by Cloud Identity Service. An identity is only a record of information about a user.

A user record is composed of a number of user identity attributes. Many of these attributes are common to almost every Identity Management system, for example, first name, last name, and email address. Your organization also has a number of attributes that are unique to your own set of applications. Attributes are collected from sources of record or identity repositories already in your organization, during the initial configuration of Cloud Identity Service for your organization.

Group and service memberships can be assigned to users, and a custom user policy can be created for specific users. User policies define the maximum number of login failures, the maximum password age, and account expiration dates, and time-of-day constraints for users.

Searching for users

You can search for any user record in your organization to view details of the user or to modify details of the user.

About this task

You can search on the name, user name, or email address of the user if these values are entered for the user. You can use only the leading characters of the name, user name, or email address. You cannot use wildcards. You must enter at least the first 3 characters of the name, user name, or email address of the user. For example, to search for an account user record with the email address psmith@company.com, you might enter psm. The greater the number of leading characters that you enter, the greater the accuracy of the search.

If you want to search for a record by using the name of the user, you can use the first name or the last name of the user. For example, to search for a user who is called Paul Smith, you might enter pau or smi. You can also enter multiple strings that are separated by spaces in your search, for example, you might enter pau smi.

A maximum of 1000 user records can be returned by a search.

Procedure

1. In the navigation pane, click **People > Users**.
2. In the **Begin Search** field, enter at least the first 3 characters of the given name, surname, user name, or email address of the user.

You can enter multiple strings that are separated by spaces in your search.

The field label changes to **Filter Results**. Users matching your search criteria are listed. Select a user to modify or view.

Adding user records

You can add records for users. You can add a record as an account or as an identity. Only a user with an account is able to access Cloud Identity Service, protected resources, and Self Service applications.

Procedure

1. Click **People > Users** in the navigation pane, and click **Add User**.

Add a New User - Add information and settings for a user to be added to the system

User Information

Last Name (sn)

2. Enter the surname of the user in the **Last Name** field.
3. Select whether the user type is an account or identity.

An account is used to give a user login access to Cloud Identity Service. An identity is only a record of information about a user.

- To create the user record with an identity only, click **Identity**.
- To create the user record with an account, click **Account**, and complete the following steps:
 - a. Enter a user name for the user in the **User Name** field. Click **Check Availability** to check that the user name is unique.

User Information

Last Name (sn)

User Name (uid)

- b. Select the user status as **Active** or **Inactive**. An active status allows the user to log in to the Cloud Identity Portal.

User Settings

Profile Type Account Identity

User Status Active Inactive

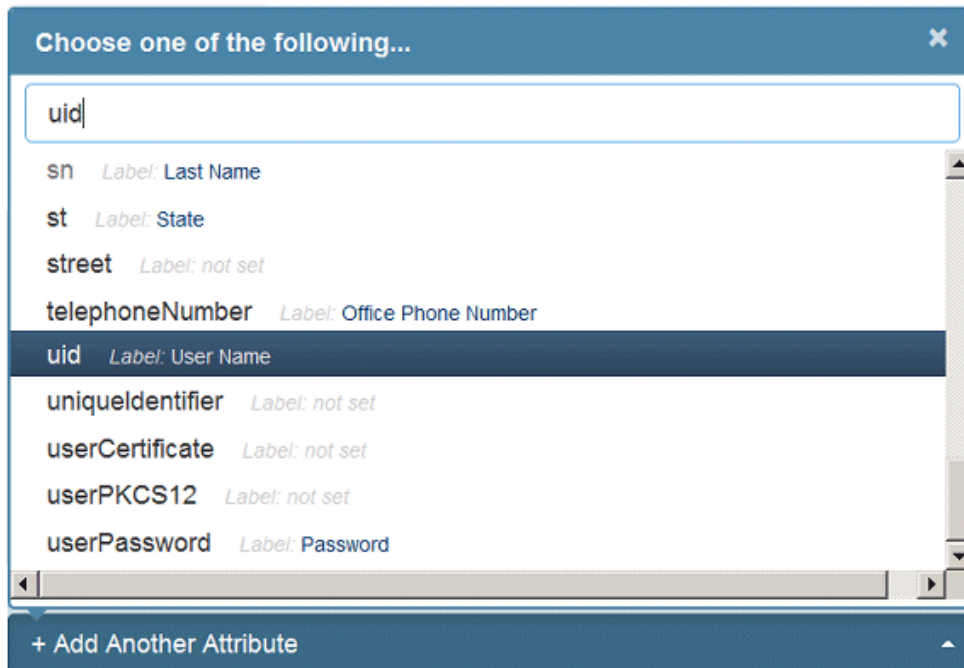
Password Status Valid Expired

Roles

- c. Select the password status as **Valid** or **Expired**. An expired status forces the user to change their password at their next successful login. If the status is valid, the user can log in without changing a password.
- d. Select the roles for the user. Click the **Roles** menu and check each role that applies to the user.

Note: If the profile type is an account, then the **gtwayPrincipalName** attribute is automatically assigned when the record is saved. An account record is automatically made a member of the **gatewaywamservice** when the record is saved.

4. Optional: Add more identity attributes for the user. Add as many attributes as you need. For example, you might add middle name and mobile number.
 - a) Click **Add Another Attribute**.



Search for the attribute you want to add by entering a string of characters in the search field. You can search on any string in the attribute. Attributes are listed by their registry name and by their Cloud Identity Service name (label) when available. Both names are included in the search. Labels are included only when they are available.

For example, to search for User Name, you might enter use or ser.

- b) Enter a value for the attribute.

Note: The **Password** attribute is used to reset the password. This field is normally populated during user self-registration. You cannot view a user password.

5. Click **Save Changes** to save the record.

Related tasks

Resetting user passwords

As an administrator of Cloud Identity Portal, you can reset a user password.

Adding membership of groups to a user

You can manually add membership of groups to a user. You can add membership to groups that are statically or dynamically managed.

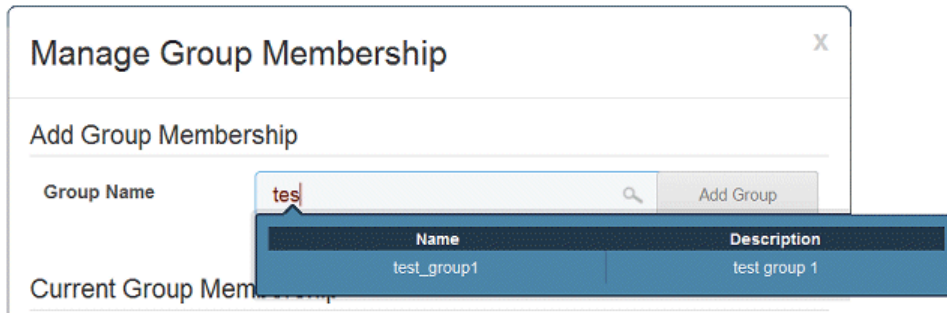
About this task

You can also add users to static groups when you [manage groups manually](#).

Note: If you manually add membership to a user for a group that is managed dynamically, the continued membership of the user is determined by the policy of the group at the next policy reconciliation.

Procedure

1. [Search for](#) and select the user.
2. In **User Settings**:
 - If the group is the first group you are adding the user to, click **Add New Group**.
 - If the user is already a member of one or more groups, click **Manage Group Membership**.



3. In the **Group Name** field, search for the group you want to add the user to. To search for a group, enter at least the first 3 characters of the name of the group.
4. Select the group and click **Add Group**.
5. Click **Done**.

Related tasks

Managing the membership of a group statically

A statically defined user membership requires you to manually add and remove each user member.

Managing the membership of groups dynamically

Dynamic provisioning policies allow the user membership of a group to be based on matching criteria. Users matching the criteria are automatically selected for membership of the group.

Adding membership of services to a user

You can manually add membership of services to a user. Adding membership of services to a user is subject to any service approvals that are in place.

About this task

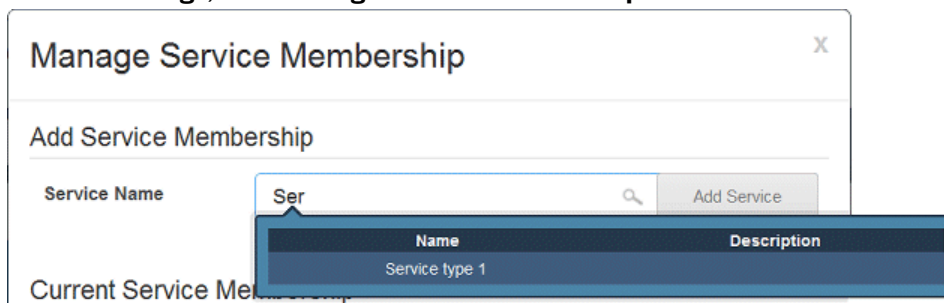
When you add membership of a service to a user and an approval policy is in place for that service, the user is not automatically added to the service. In this case, a request is generated for the user to become a member of the service and a pending service request email notification is sent to the approvers.

Note: If you manually add membership to a user for a service that is managed dynamically, the continued membership of the user is determined by the policy of the service at the next policy reconciliation.

You can also add users to the membership of services when you manage services.

Procedure

1. Search for and select the user.
2. In **User Settings**, click **Manage Service Membership**.



3. In the **Service Name** field, search for the service you want to add the user to. To search for a service, enter at least the first 3 characters of the name of the service.
4. Select the service and click **Add Service**.

Adding a user policy to a user

User policies define a number of password validation restrictions, account expiration dates, and time-of-day restrictions. Global user policies are applied to all users. A custom user policy is applied to a specific user.

About this task

Policy settings that are set at the user level, override corresponding settings in the global policy. By default, all of the user level policy values are unset. A policy setting that is unset at the user level inherits the setting, if any, from the global policy.

Procedure

1. Search for and select the user.
2. In **User Settings**, click **Manage User Policy**.
3. Set the user policy settings that you want.
4. Click **Save**.

You can apply the same user policy to other users.

5. Click **Done**.

User policy settings

Setting	Description
Maximum Login Failures	<p>The maximum number of failed logins a user can attempt before their account is locked. If this option is set to 0 or Unset, then the number of failed login attempts is limitless.</p> <ul style="list-style-type: none">• Set. The maximum number of failed login attempts. If this option is set to 0, then the number of failed login attempts is limitless.• Unset. No limit to the number of failed login attempts.
Disable Time Interval	<p>Specify whether user accounts are locked after the Max Login Failures count is exceeded.</p> <ul style="list-style-type: none">• Set. User accounts are locked after the Max Login Failures count is exceeded. Accounts are disabled permanently or temporarily.• Unset. User accounts never lock due to failed login attempts. Unset is equivalent to setting the Max Login Failures to 0 or Unset, users have an unlimited number of login attempts.• Disable Permanently. The user is locked out permanently until a Cloud Identity Portal administrator sets the User Status of the user to valid.• Disable Temporarily. The time, in seconds, that a user account will remain locked after the Max Login Failures count is exceeded. The account will be unlocked after the interval time is passed.
Minimum Length	<p>The minimum number of characters that are required for a valid account password.</p> <ul style="list-style-type: none">• Set. The minimum number of characters for a password.• Unset. No minimum password length.

Table 3. User policy settings (continued)

Setting	Description
Minimum Alphas	<p>The minimum number of alphabetic characters that are required for account passwords.</p> <ul style="list-style-type: none"> • Set. The minimum number of alphabetic characters that the password must contain. • Unset. No minimum is imposed.
Minimum Non-Alphas	<p>The minimum number of non-alphabetic characters (numbers or special characters) that are required for account passwords.</p> <ul style="list-style-type: none"> • Set. The minimum number of non-alphabetic characters that the password must contain. If set to 0, then no minimum is imposed. • Unset. No minimum is imposed.
Maximum Repeated Characters	<p>The maximum number of consecutive repeated characters that are allowed in an account password.</p> <ul style="list-style-type: none"> • Set. The maximum number of repeated characters that are allowed. • Unset. No limit to the number of repeated characters.
Spaces Allowed?	<p>Specifies whether account passwords can contain spaces.</p> <ul style="list-style-type: none"> • Set. Specify whether spaces are allowed. <ul style="list-style-type: none"> – Yes. Spaces are allowed. – No. Spaces are not allowed. • Unset. Spaces are allowed.
Password Expires?	<p>The maximum amount of time that passwords remain valid after creation, and then expire and must be changed.</p> <ul style="list-style-type: none"> • Yes. The number of days, hours, minutes, and seconds that a password is valid. If all values are set to 0, passwords never expire. • No. Passwords never expire.
Track Password Reuse?	<p>Specifies whether the same password can be used when a password is reset.</p> <ul style="list-style-type: none"> • Yes. Users cannot use the same password when they reset or change their password. Specify the number of new unique passwords that must be set before an old password can be reused. • No. Users can use the same password when they reset their password.
Account Expires?	<p>Specifies an expiration date after which all accounts are set to invalid. This setting is normally only used for individual user policy overrides. For example, if a contractor has a finite access period to a specific resource this option can be used to disable that access on a specific date.</p> <ul style="list-style-type: none"> • Set. The expiration date for accounts. Enter the date in MM/DD/YYYY format. • Unset. Unlimited period of validity, the validity of accounts never expires.

Table 3. User policy settings (continued)

Setting	Description
Limit Access?	<p>Specifies a time-of-day constraint for when users can access the system.</p> <ul style="list-style-type: none"> • Yes. The days and time of day that users can access the Cloud Identity Service. Time can be expressed as the local time for the service, or Coordinated Universal Time. • No. Users can access the Cloud Identity Service at any time.

Resetting user passwords

As an administrator of Cloud Identity Portal, you can reset a user password.

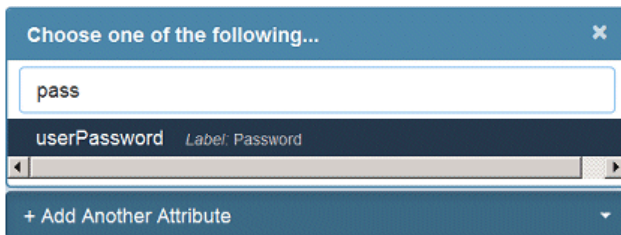
About this task

When you reset a user password as an administrator in the Cloud Identity Portal, you add the password attribute to the user account record. For security reasons, a user account record does not display the password attribute and the password value. When you add the password attribute and enter a value, you are resetting the password. After you reset the password, if you access the user account record again, the password attribute and value are not displayed.

If the user whose password is reset has an email address, they receive an email that notifies them that their password is reset.

Procedure

1. In the navigation pane, click **Directory Management > Users**.
2. Search for and select the user.
3. Click **Add Another Attribute**.



4. Search for the password attribute by entering a string of characters in the search field, and select the password attribute.
For example, enter pass.

Attributes are listed by their registry name and by their Cloud Identity Service name (label). Both names are included in the search.

5. Enter a password in the **Password** field.
The characters that you type are replaced by asterisk characters.
6. Click **Save Changes** to save the record.

Managing groups

A number of Identity and Access Management decisions are best implemented by treating groups of users in the same way. You can create groups by selecting users manually, or you can create dynamic policies that automate group membership.

Groups overview

Groups of users that share common characteristics can be grouped so that they can be treated collectively. For example, a group of users that work in the same department of a company can be granted the same access to a specified web application.

The user membership of a group can be statically or dynamically defined. Static user membership requires you to manually add each user to the group, and to manually manage group membership. Dynamic user membership automatically selects users for membership based on any matching combination of their identity attribute values, other group memberships, other service memberships, or whether they are assigned a role as a manager. For example, you might group users who are in a specific country or locality. You might group users who have an account within a specific account number range, and who are also members of another specified group.

Dynamic user membership is implemented by using a dynamic provisioning policy, in which you define the group membership selection criteria.

Any number of policies can be defined for a group. A policy can be applied on demand by reconciling the policy. A policy can also be applied according to a schedule. When a policy is applied, its selection criteria is evaluated and the user membership is updated so that non-matching users are removed and matching users are added.

Searching for groups

You can search for any group in your organization to view details of the group or to modify details of the group, and manage the membership of the group.

Procedure

1. In the navigation pane, click **People > Groups**.
2. In the **Filter Results** field, enter at least the first 3 characters of the group. The field label changes to **Searching For**.

Groups matching your search criteria are listed. Select a group to modify or view.

Creating groups

You can create new groups. After you create a group, you can select users to be members of the group by managing the group statically or dynamically.

Procedure

1. Click **People > Groups** in the navigation menu, and click **Add Group**.
2. Enter a name and description for the group.
Check whether the group name is in use by clicking **Check Availability**.
3. Click **Save Changes** to add the group.

What to do next

After the group is created, you can add members to the group manually or dynamically.

Managing the membership of a group statically

A statically defined user membership requires you to manually add and remove each user member.

Procedure

1. Search for and select the group that you want to add members to.
2. Click **Manage Group Membership**.

Manage Group Membership

Add Group Membership

User Name

First Name	Last Name	Email
Paul	Smith	psmith@company.com

Current Group Membership

3. In the **User Name** field, search for the user you want to add. To search for a user, enter the first 3 characters of the given name, surname, user name, or email address of the user.
4. Select the user and click **Add Membership**.
5. After you add all the users that you want, click **Done**.

Managing the membership of groups dynamically

Dynamic provisioning policies allow the user membership of a group to be based on matching criteria. Users matching the criteria are automatically selected for membership of the group.

Creating dynamic provisioning policies

Dynamic provisioning policies are used to determine the user membership of groups.

About this task

Membership is based on the selection criteria of the policy. For example, you might specify the membership of a group by an attribute that determines work location, or by an attribute that determines work location and membership of another group. A group can have one or more policies.

Procedure

1. Search for and select the group that you want to add a policy to.
2. For **Dynamic Provisioning Policy**, click **Manage Policy**.
3. Click **Add New Policy**.

Manage Policies

Delete	Variable	Operator	Value	Conjunction	Move
	Select Variable...				

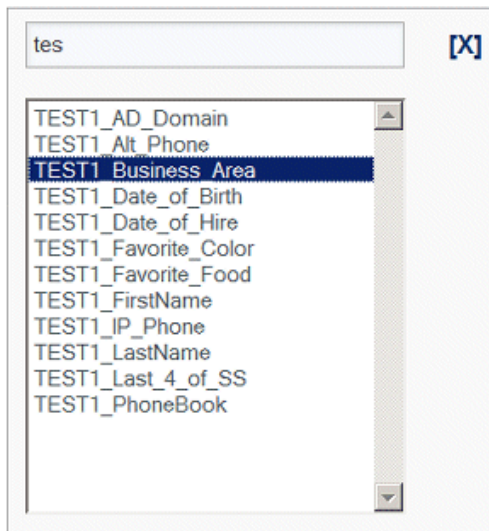
4. Enter a meaningful name for the policy in the **Policy Name** field.
5. Select the variables that you want to use, you can select one or more variables of any type to use in your policy.

You can select any combination of the following variable types:

- **Attribute.** Include users based on a user identity attribute.
- **Group.** Include or exclude users based on other group memberships.
- **Service.** Include or exclude users based on service memberships.
- **Manager.** Include users based on whether they are assigned the role of manager.

6. To use a user identity attribute as a variable:

- Click **Select Variable**, and click **Attribute**.
- Click in the **Filter Attributes** field, and enter the first few characters of the attribute. Double-click the attribute to select it.



c) Select an **Operator** and enter a **Value** for the attribute.

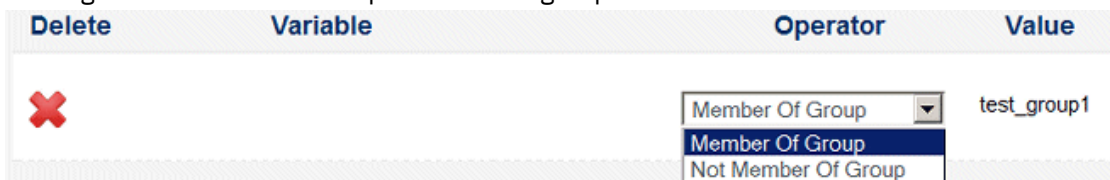


Note: You can use wildcards. For example, 11* can be entered to represent any number beginning with 11.

Tip: If your organization has user attributes that use date values, you can treat such an attribute as a time stamp. For more information about using time stamps, see [“Time stamp values”](#) on page 21. To search for and view the attributes in use for your organization, see [“Managing custom attributes”](#) on page 28.

7. To use membership or non-membership of another group as a variable:

- Click **Select Variable**, and click **Group**.
- Click in the **Filter Groups** field, and enter the first few characters of the group. Double-click the group to select it.
- Select whether membership is contingent on membership of this other group, or if membership is contingent on non-membership of this other group.




8. To use membership or non-membership of a service as a variable:


- a) Click **Select Variable**, and click **Service**.
 - b) Click in the **Filter Services** field, and enter the first few characters of the service. Double-click the service to select it.
 - c) Select whether membership is contingent on membership of this service, or if membership is contingent on non-membership of this service.
9. To use the manager role as a variable:
- a) Click **Select Variable**, and click **Manager**.

- b) Search for the user in the **Manager Search** window by entering search criteria in any of the fields. Click **Search**.
Only users that are assigned the role of manager and that match your search criteria are returned.
Note: You can use wildcards in your search. For example, you might enter Joh* to represent names that begin with Joh.
 - c) Select the user.
You can repeat the search to add more users.
10. Use the **Conjunction** field to combine one or more variables to determine the membership of the group. Use a conjunction value of And or Or to combine the result of one comparison criteria with the next row.

The grouping of variables (conditions) is from top to bottom so that the result of previous conditions is joined with the subsequent condition.

Use the arrow icons to move conditions up and down .

In the following example, only one variable is used to determine membership: the user identity attribute TEST1_Business_Area. To be a member, a user must have a value of London W4 for the attribute TEST1_Business_Area.

Delete	Variable	Operator	Value	Conjunction
	TEST1_Business_Area	=	London W4	-- Select

In the following example, two variables are used to determine membership. To be a member, a user must have a value of London W4 for the attribute TEST1_Business_Area, and must be a member of Group1.

Delete	Variable	Operator	Value	Conjunction
	TEST1_Business_Area	=	London W4	And
		Member Of Group	Group1	-- Select

In the following example, three variables are used to determine membership. To be a member, a user must have a value of London W4 for the attribute TEST1_Business_Area, and must be a member of Group1 or be a member of Group2.

Delete	Variable	Operator	Value	Conjunction
	TEST1_Business_Area	=	London W4	And
		Member Of Group	Group1	Or
		Member Of Group	Group2	-- Select

11. After all the conditions you want in the policy are defined, click **Save**.

What to do next

Simulate the policy to check that membership meets your expectations.

Time stamp values

If you want an attribute and attribute value to be treated as a time stamp, you can prefix the value with \$date\$.

The \$date\$ prefix assumes the default date format of yyyy-MM-dd HH:mm:ss. For example, you might enter \$date\$1970-01-01 00:00:00 to specify 1 January 1970 at midnight, or you can specify the current time by entering \$date\$now.

You can also specify a non-default format for the time stamp by including the format in the \$date\$ prefix by using SimpleDateFormat. For example, for a Z-timestamp you might enter \$date\${yyyy-MM-dd HH:mm:ssZ}\$1970-01-01 00:00:00-0400 to represent 1 Jan 1970 at midnight in the time zone 4 hours earlier than GMT/UTC. Changing the default format causes the same format to be applied to the attribute values that are retrieved. You must understand the format of the values that you want to retrieve. The format of retrieved date values must be consistent with the format you want to use. For more information about different date format patterns, see [SimpleDateFormat](#).

If either the value specified in the rule or the value it is compared with are not parsed without exception, then a warning or error is logged. For more information, contact your IBM support representative. Coordinated Universal Time (UTC) is the default time zone.

In the following example, two attribute variables are used to determine membership based on date of hire. To be a member, the date of hire for the user must be after the January 01, 2016 and before the current date and time.

Delete	Variable	Operator	Value	Conjunction	Move
	TEST1_Date_of_Hire	>	\$date\$2016-01-01 00:00:00	And	
	TEST1_Date_of_Hire	<	\$date\$now	-- Select	

Creating dynamic provisioning policies in expert mode

In some cases, the policy selection criteria for a group cannot be determined by using basic attribute comparison and other group or service membership. Membership might require the examination of attribute values (substrings) that vary based on the value of another attribute. In these cases, you must define the policy in expert mode.

Before you begin

To use expert mode, you must have good knowledge and fluency in coding in JavaScript.

About this task

You define policies in expert mode in JavaScript.

During policy evaluation, the JavaScript is run one time for each user in the registry. The JavaScript examines the registry attributes of the user and their memberships, and decides whether the user is to be included in the group. The JavaScript communicates this decision to Cloud Identity Service with a variable **inGroup**. If the result of the JavaScript is that **inGroup** equals TRUE, then the user is included in the group, otherwise the user is not included.

The JavaScript can use three methods to obtain Cloud Identity Service registry attributes, and group information about each user.

- String isMemberOfGroup(String groupName)
- String[] getAttributeValues(String attributeName)
- String evaluateAttribute(String attributeName, int operator, String constant)

Each of these methods can be invoked with another variable **ldap** that is available to the JavaScript. For example, to determine whether the current user is a member of a group that is named **accounting**, the following statement can be used:

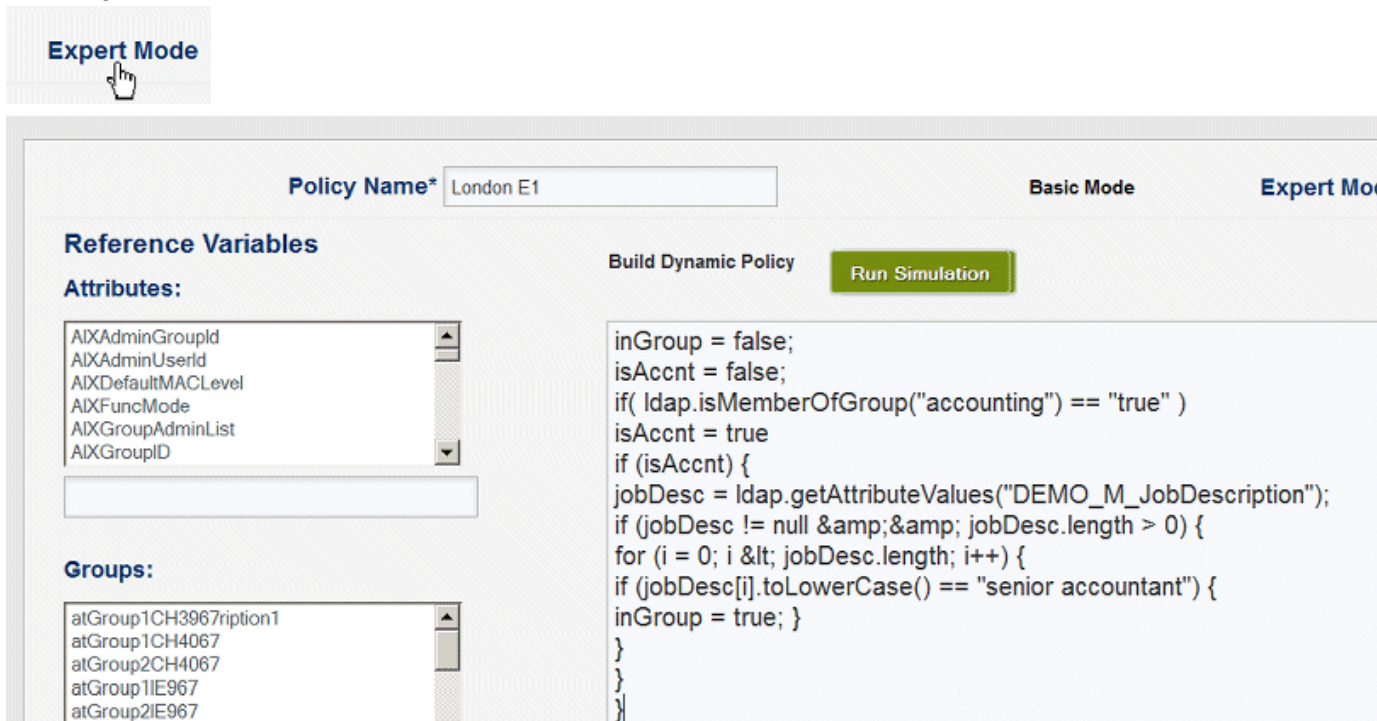
```
var isAccountant = ldap.isMemberOfGroup("accounting");
```

In the following JavaScript example the user is included in the policy group if the user is both a member of the **accounting** group, and has the value **senior accountant** in the attribute **DEMO_M_JobDescription**.

```
// assume user is not in group
inGroup = false;
isAccnt = false;
if( ldap.isMemberOfGroup("accounting") == "true" )
isAccnt = true
if (isAccnt) {
jobDesc = ldap.getAttributeValues("DEMO_M_JobDescription");
if (jobDesc != null && jobDesc.length > 0) {
for (i = 0; i < jobDesc.length; i++) {
if (jobDesc[i].toLowerCase() == "senior accountant") {
inGroup = true; }
}
}
}
```


Procedure

1. Search for and select the group that you want to add a policy to.
2. For **Dynamic Provisioning Policy**, click **Manage Policy**.
3. Click **Add New Policy**.
4. Click **Expert Mode**.



5. Enter the JavaScript you want to use to determine membership.

Attributes, **Groups**, and **Services** are listed in their respective boxes for your reference. You can search for an attribute, group, or service by entering the first few characters in the filter field below the appropriate box. You can copy and paste a selected attribute, group, or service.

6. After all the conditions to use in your policy are defined, click **Save** to save the policy.

What to do next

[Simulate the policy](#) to check membership meets your expectations.

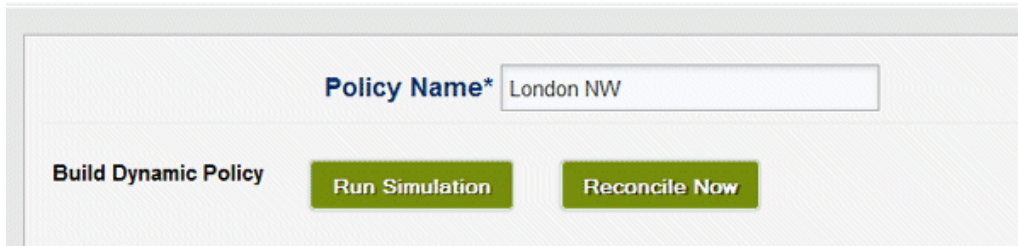
Simulating a policy

You simulate a policy to evaluate the user membership of a group to check whether the membership meets your expectations. The simulation does not change the membership of the group. It shows you which users comprise the proposed membership of the group. Results can be viewed and saved as a CSV file.

Procedure

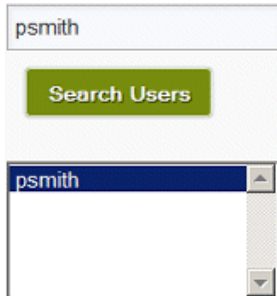
1. If you do not have the policy selected, [search for and select](#) the group. Open the **Manage Policies** window to edit the policy.
2. Click **Run Simulation**.

Manage Policies



3. Select a simulation type to run.

- **Simulate all users in the directory.** This option compares the policy selection to all users in Cloud Identity Service. Users that satisfy the policy are listed in the results as either being added or retained. Users that do not satisfy the policy are listed in the results as either removed from the group or not added.
- **Simulate all users currently in the group.** This option compares the policy selection criteria against the attributes of all users that are currently in the group. Each user in the group is listed in the results as either removed or retained. No new users are listed as added.
- **Simulate a single user.** This option compares the policy selection criteria against a selected user. That user is listed in the results as either retained, removed, added or not added. Search for the user by using their user name. Enter the first few characters of the user name in the **Filter Users** field, click **Search Users**, and select the user.

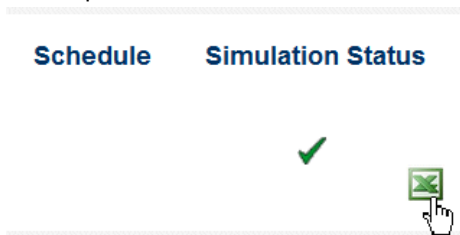


4. Click **Run Simulation**.


The results for a single user provisioning policy simulation are displayed in the **Simulate Provisioning Policy** window.

Close the **Simulate Policy** window to return to the **Manage Policies** window, and click **Cancel**.


5. Click **Refresh** in the **Manage Policies** window to view the results of simulations. When the simulation is complete, a check mark icon and a link to a CSV file are displayed.



6. View the results.

- Click the check mark icon  to open the **Simulation Results** window. You can select which results columns to view by clearing or checking the column header check boxes. Close the **Simulation Results** window to return to the **Manage Policies** window.

Note: Clicking **Clear Simulation Results** clears all the results from the **Simulation Results** window and the **Manage Policies** window.

- Click the CSV icon  to view the results in a CSV file. You can open the file or save the file.

What to do next

1. [Reconcile the policy.](#)
2. [Activate the policy.](#)

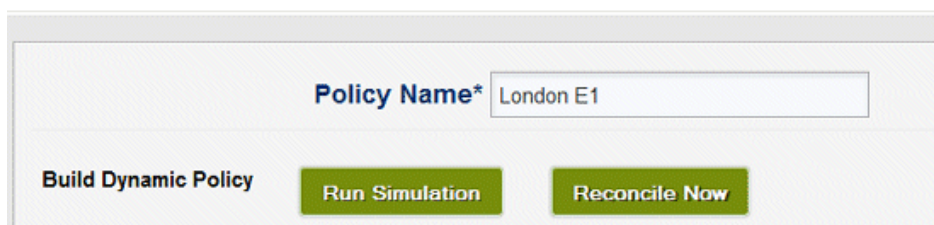
Reconciling a dynamic policy

After a policy is created, the policy can be reconciled. When a policy is reconciled, user membership for the group is implemented according to the policy selection criteria.

Procedure

1. [Search for and select the group.](#) Open the **Manage Policies** window to edit the policy.
2. Click **Reconcile Now**.

Manage Policies



A warning message is displayed. Click **OK** to reconcile the policy.

What to do next

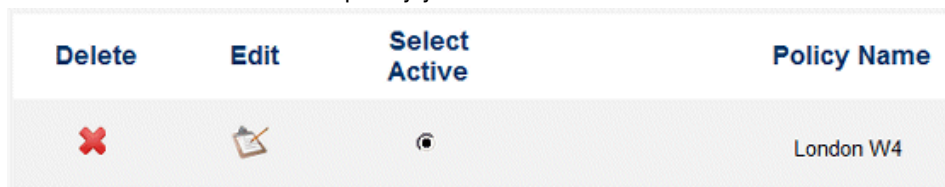
[Activate the policy.](#)



Activating and scheduling a dynamic policy

After a policy is created, simulated, and the simulation results validated, the policy is ready to be activated and scheduled. An activated policy runs on a schedule, so that the membership of a group is evaluated and updated every time that the schedule is run.

Procedure

1. If you do not have the policy selected, [search for and select](#) the group. Open the **Manage Policies** window to edit the policy.
2. Select **Select Active** for the policy you want to activate.



Delete	Edit	Select Active	Policy Name
		<input checked="" type="radio"/>	London W4

A warning message is displayed. Click **OK** to activate the policy.

3. Click the schedule icon  to open the **Dynamic Provisioning Policy Scheduler** window.

Dynamic Provisioning Policy Scheduler ✕

Enable Automatic Provisioning Schedule

Select one of the following scheduling frequencies:

Time of Day (applies to all selections): 12 : 00 AM

Once a day

Once a week Sunday

Once a month 1

Last day of the month

Select day(s)

Sunday
 Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Saturday

Save

4. Check the **Enable Automatic Provisioning Schedule** check box.
5. Choose the frequency with which to run the schedule:
 - **Once a day.** Select the **Time of Day**.
 - **Once a week.** Select the day from the drop-down list, and select the **Time of Day**.
 - **Once a month.** Select the day of the month from the drop-down list, and select the **Time of Day**.
 - **Last day of the month.** Select the **Time of Day**.
 - **Select days.** Check the check boxes for the days to run the schedule, and select the **Time of Day**.
6. Click **Save**.

Managing Classifiers

The user can create new classifiers and define which attributes need to be assigned to that.

About this task

The following table lists the classifiers which can be controlled by the user as per the GDPR requirements:

<i>Table 4. Classification Options</i>		
Name	Description	Enable/Disable
Allow Export	Allows the user to export data. The data is exported in JSON or SCIM format.	Disabled by default.

Table 4. Classification Options (continued)

Name	Description	Enable/Disable
Allow Alerts	Allows the user to notify/alert about the modifications in the attribute.	Disabled by default.
Allow Stop Usage	Allows the user to stop the automatic processing of the attribute.	Enabled by default.
Allow Delete	Allows the user to delete the attribute.	Disabled by default.
Allow Usage By	Allows the user to share his attributes with third party.	Enabled by default.

Adding classifiers

The user can add a new classifier.

About this task

You can create new classifiers and define which attributes need to be assigned to that. The following list specifies how the classifiers work:

1. Each classifier is configured to handle the attributes, allow the user to turn-off the attribute. For example, a user can turn-off the attribute of automated process.
2. Each attribute belongs to only one classifier.
3. One classifier can have many attributes.
4. A Default classifier is applied, with some restricted/default permissions in case the administrator has not assigned any classifier.
5. Each classifier name is unique to that client.

Procedure

1. Click **People > Schema Management** in the navigation menu.
2. Select **Attribute Classifiers**.
3. Click **Add New Classifier**.

4. Enter the Classifier name and **Check Availability** of the name. Each classifier must have unique name.

5. Toggle the switches as per the required restriction for GDPR compliance.
6. Click **Save Changes** to add this classifier.

Searching for classifiers

You can search for any classifier available for use.

Procedure

1. In the navigation pane, click **People > Schema Management**.
2. Select **Attribute Classifiers**.
3. In the **Narrow your Search** field, enter at least the first 3 characters of the classifier, the field label changes to **Searching For**.

Classifiers matching your search criteria are listed. Select an classifier to modify or view.

Managing custom attributes

A user record is composed of a number of user identity attributes. You can add custom attributes to the set of identity attributes used for your user records.

Attributes overview

User records are composed of a number of identity attributes. Most identity attributes are common to almost every Identity Management system, for example, given name, surname, and email address.

Common attributes are taken from a set of standard LDAP (Lightweight Directory Access Protocol) attributes. Your organization might also have a number of attributes that are unique to your own set of applications. These unique attributes are custom attributes. You can create more custom attributes.

Searching for attributes

You can search for any attribute available for use in your identity records.

Procedure

1. In the navigation pane, click **People > Schema Management**.
2. In the **Begin Search** field, enter at least the first 3 characters of the attribute, the field label changes to **Searching For**.

Attributes matching your search criteria are listed. Select an attribute to modify or view.

You can filter the list by using the **Show Default** and **Show User Added** check boxes. User added attributes are custom attributes. You can sort the list by clicking a column header to sort the list by that column.

Creating custom attributes

You can create new custom attributes to be used in identity records.

Before you begin

You must have a basic understanding of LDAP (Lightweight Directory Access Protocol), LDAP schemas, and the identity record requirements of your company.

Procedure

1. Click **People > Schema Management**, in the navigation pane.
2. Click **Add New Attribute**.

Add New Attribute
X

Attribute Name

 * ?

Description
 * ?

Type

String ▼

Multivalue

True

False

Classifier

J ▼

3. Enter a name and description for the attribute.

The name must be unique, you can check whether the name is unique by clicking **Check Availability**.

Note: For the name, you can use the alphanumeric characters a-z, A-Z, and 0-9. You can use the special characters hyphen (-), and underscore (_). You cannot use spaces.

For the description, you can use the alphanumeric characters a-z, A-Z, and 0-9. You can use the special characters hyphen (-), and underscore (_). You can also use spaces.

4. Enter attribute settings.

5. Select the classifier from the drop-down list. The Default classifier is assigned if the user does not select classifier here. The user needs to create and select a classifier for the GDPR compliance.

6. Click **Save Changes** to add the attribute.

Attribute settings

Attribute settings include type, and multiple value usage.

Table 5. Attribute settings	
Setting	Description
Type	Attribute type. <ul style="list-style-type: none"> • String. Unicode (UTF-8) string • Boolean. • Integer
Multivalue	Specifies whether the attribute can have many different values. <ul style="list-style-type: none"> • True. Multiple values are allowed. • False. Only a single value is allowed.

Managing the bulk import of users

You can bulk load user data to create user identity records in Cloud Identity Portal.

Before you begin

You need a working knowledge of JSON, System for Cross-domain Identity Management (SCIM) files, and a basic understanding of REST APIs.

SCIM files

You bulk load user data by uploading System for Cross-domain Identity Management (SCIM) files to Cloud Identity Portal.

SCIM files provide a platform-neutral schema for representing users in JSON format. For more information about SCIM, see [System for Cross-domain Identity Management](#). The SCIM file contains an array of operations, each of which represents the creation of a user record. Operations are processed through the Cloud Identity Portal administration REST API. Each successful operation creates a new user record in Cloud Identity Portal. You can create up to 5000 operations per SCIM file, and you can upload as many files as you need. The format and contents of an example SCIM file are shown here.

```
{
  "operations": [
    {
      "method": "POST",
      "path": "/Users",
      "bulkId": "importtest1",
      "data": {
        "userName": "userimporttest1",
        "active": true,
        "password": "core1234",
        "emails": [
          {
            "value": "nomail@gmail.com",
            "type": "",
            "primary": "true"
          }
        ],
        "name": {
          "familyName": "import",
          "middleName": "mid",
          "givenName": "ctest1"
        },
        "addresses": [
          {
            "streetAddress": "123 oak st",
            "locality": "fort worth",
            "region": "texas",
            "postalCode": "77077",
            "country": "USA",
            "type": "home",
            "primary": "true"
          }
        ],
        "title": "title",
        "preferredLanguage": "en-US",
        "userType": "Contractor"
      }
    },
    {
      "method": "POST",
      "path": "/Users",
      "bulkId": "importtest1",
      "data": {
        "userName": "userimporttest2",
        "active": true,
        "password": "core1234",
        "emails": [
          {
            "value": "nomail2@gmail.com",
            "type": "",
            "primary": "true"
          }
        ],
        "name": {
          "familyName": "import",
          "middleName": "mid",
          "givenName": "ctest2"
        },
        "addresses": [
          {
            "streetAddress": "123 oak st",
            "locality": "fort worth",
            "region": "texas",
            "postalCode": "77077",
            "country": "USA",
            "type": "home",
            "primary": "true"
          }
        ],
        "title": "title",
        "preferredLanguage": "en-US",
        "userType": "Contractor"
      }
    }
  ]
}
```

```

    }
  ]
}

```

Table 6. Operation parameters

Parameter	Type	Required	Description
method		Yes	The operation to be performed by the method. The operation is POST.
path	Path	Yes	Specifies the path to the object to update. The path is /Users.
bulkId	String	Yes	A transaction ID. A response status is associated with each transaction ID.
data	Object	Yes	Contains attributes for the user.
userName	String	Yes	Specifies the user name of the user. The user name must be unique.
active	Boolean	Yes	Specifies whether the user record is an identity or an account. Set to true if you want the user to have a Cloud Identity Service account. Users cannot authenticate to Cloud Identity Service or access Self Service applications without an account. If set to false, the user record is created as an identity and not an account.
password	String	Optional	A password to access Cloud Identity Service and Self Service applications.
emails	Object	Optional	Contains email addresses for the user.
value	String	Optional	A valid email address.
type	String	Optional	Email type, for example personal, office, or social.
primary	Boolean	Optional	Specifies whether the email is the primary email address for the user.
name	Object	Yes	Contains name attributes for the user.
familyName	String	Yes	The surname of the user.
middleName	String	Optional	The middle name of the user.
givenName	String	Optional	The given name of the user.
addresses	Object	Optional	Contains postal addresses for the user.
streetAddress	String	Optional	The site information for a postal address (the street, road, place, or avenue, and the number).
locality	String	Optional	The name of a locality, such as a city, or county.
region	String	Optional	The name of a geographic region, greater than the locality. For example, the full name of a state or province.
postalCode	String	Optional	The codes that are used by the postal service to identify postal service zones.
country	String	Optional	The name of a country.
type	String	Optional	The address type, for example home or office.

Table 6. Operation parameters (continued)

Parameter	Type	Required	Description
primary	String	Optional	Specifies whether the address is the primary address for the user.
title	String	Optional	A personal title for a person, for example Mr, Ms, Dr, Prof, and Rev.
preferredLanguage	String	Optional	The language code for the user. For example, en-us or fr-ca. If not specified, the preferred language set in LDAP is used. If no preferred language is set, then the default language of American English is used.
userType	String	Optional	The name of the type of user, for example Contractor.

Importing users

You import System for Cross-domain Identity Management (SCIM) files to create new users in Cloud Identity Portal.

Before you begin

You must create the SCIM files that you intend to upload.

Procedure

1. In the navigation pane, click **People > Import Users**.
2. Click **Upload SCIM** to browse to and select a file to upload.

Chapter 6. Self Service



Self Service application management is the configuration and customization of Self Service applications. Self Service applications include all the applications users need to apply for and maintain their identity profiles.

Configuring Self Service applications

Configuring Self Service applications, includes configuring self-registration options, password reset options, user name recovery options, and defining roles.

Configuration overview

Self Service applications are configured during the initial setup of Cloud Identity Service for your organization. You can change a number of settings and options to adapt to your changing needs.

Self Service applications allow users to control aspects of their account in Cloud Identity Service. For example, a user can self-register for an account to gain access to protected resources, they can reset their password, recover their user name, and manage their profile information. Access to Self Service application is determined by user role.

Self-registration

The self-registration application allows users to claim an account in Cloud Identity Service. Under most circumstances, every user is required to self-register before they can manage their profile and gain access to protected resources such as web applications and servers.

You can change self-registration options, including how accounts are provisioned and approved. You can add, remove, and rearrange sections and fields on the self-registration form.

Password reset

The password reset application is configurable to allow users to reset a forgotten password. You can change the password reset options, including the number of questions that must be answered and whether to use email verification.

The organization or tenant can use a one-time password instead of the security questions. Email, mobile or email and mobile can be used to validate one-time password.

User name recovery

When users are unable to remember their user name, they cannot log in or reset their password since they have no way of identifying their account. The user name recovery application allows users to recover their account user name if forgotten. You can change user name recovery options, including whether to display the user name on screen or to send the user name to the email address of the user.

Self Service profile

The Self Service profile application allows users to manage their own account profile information after they are registered and are able to authenticate to Cloud Identity Service. You can add, remove, and rearrange sections and fields on the profile setup form.

Security questions

Security questions are used to verify the identity of a user when they want to reset their password. Users must provide answers to security questions when they self-register. To verify the identity of a user during password reset, the answers that are provided during self-registration are matched against the answers that are provided during password reset.

During the initial configuration of Cloud Identity Service for your organization, a number of security questions are defined. You can add new questions to the questions that are already defined, and you can hide questions. You can set the minimum number of questions users must provide answers for when they self-register.

Roles

A role can be thought of as a functional title within your organization. For example, Manager, Administrator, or Help Desk contact. Roles define collections of users. Roles are used to control access to different Self Service applications and actions.

Related concepts

[Roles overview](#)

A role can be thought of as a functional title within your organization. For example, Manager, Administrator, or Help Desk contact. Roles are used to control access to different Self Service applications and actions, and to control access to different sections in the Self Service profile application.

Configuring self-registration options and form

You can modify self-registration provisioning and approval options, and the fields in the self-registration form.

Configuring self-registration options

Self-registration allows users to claim an account in Cloud Identity Service. Self-registration can be configured to work in different ways. You can change self-registration options, including how accounts are provisioned and approval options.

Procedure

1. In the navigation pane, click **Self Service > Self Registration**.
2. Select the [self-registration options](#) that you want.
3. Click **Save Changes**.

Self-registration options

Self-registration options include formatting, approval, and email options.

Option	Description
Enable Account Claiming	Enable users to claim accounts by using a link that is sent in an email. <ul style="list-style-type: none">• Yes. Users can claim an account by using a link in an email. The user receives a link in an email to claim an account. By clicking the link, the user can claim an account by self-registering successfully.• No. Users cannot claim an account by using an email link.

Table 7. Provisioning policies and formatting options (continued)

Option	Description
<p>Enable LDAP identity validation</p>	<p>User accounts can be provisioned based on validation of LDAP attributes. User identity records must exist before users can be provisioned by using LDAP identity validation. The values that are entered for attributes during self-registration by a user, are compared to values in their existing identity record. If the values match, the user can be provisioned. The LDAP attributes to use for validation must be selected and enabled for validation in the Form Setup.</p> <ul style="list-style-type: none"> • Yes. If the information is successfully validated, an account can be provisioned for the user. The LDAP attributes to use for validation must be selected and enabled for validation in the Form Setup. <p>When identity validation fails. When identity validation fails, one of the following options can be applied:</p> <ul style="list-style-type: none"> – Reject Registration. The user registration is rejected. An account is not created. – Manually Provision User. An account can be manually provisioned by a Cloud Identity Portal administrator. – Auto Provision User. Automatically create an account for the user. <p>If multiple identities are found. If more than one identity record is found that matches the registration information that is entered by a user, one of the following options can be applied:</p> <ul style="list-style-type: none"> – Reject Registration. The user registration is rejected. An account is not created. – Manually Provision User. An account for the user must be manually provisioned by a Cloud Identity Portal administrator. – Auto Provision User. Automatically create an account for the user. <ul style="list-style-type: none"> • No. Accounts cannot be provisioned based on validation of LDAP attributes.

Table 7. Provisioning policies and formatting options (continued)

Option	Description
<p>Preferred username format</p> <p>Alternate username format</p>	<p>The preferred and alternate user name formats. When a user self-registers, their user name can be generated in a number of ways. The alternate user name format is used when a user name exists for the preferred format. Both formats must be different.</p> <ul style="list-style-type: none"> • Allow the User to select their Username. The user provides a user name of their choosing. • User's email address. The user name is set to the email address entered by the user. • FirstName.LastName. The user name is composed of the first name and the last name of the user, separated by a period. For example, John.Smith. • FirstInitial.LastName. The user name is composed of the first initial of the first name and the last name of the user, separated by a period. For example, J.Smith. • LastName.FirstInitial. The user name is composed of the last name and the first initial of the first name of the user, separated by a period. For example, SmithJ. • FirstName.Middle.LastName. The user name is composed of the first name, middle initial, and the last name of the user, separated by periods. For example, JohnASmith. • Populate From. The user name is composed of the value that is entered by the user for a specified LDAP attribute. The attribute must be present in the Form Setup. • Invoke Custom Method. A user name can be using a custom format. • User UID.

Table 8. Approval and email options

Option	Description
<p>Require manual approval for registrations</p>	<p>A Cloud Identity Service user manually approves user registration. If a user has no existing identity record, manual approval can be used to provision an account. Manual approval can also be used for users with existing identity records.</p> <ul style="list-style-type: none"> • Yes. Manual approval for registrations is needed. You must select a default approver to approve registrations. If a user does not have an existing identity record, the manual approver is the default approver. If a user does have an existing identity record, a manager can approve the registration. <ul style="list-style-type: none"> – Require manager approval (when possible). A manager approves registrations. A manager can approve registrations only for users that have existing identity records. If no manager is applicable, the default approver approves the registration. <p>Search for the user in the Default approver field. Enter the first three characters of the first name, last name, or email address of the user to approve registrations. Select the user.</p> • No. Manual approval is not needed.

Table 8. Approval and email options (continued)

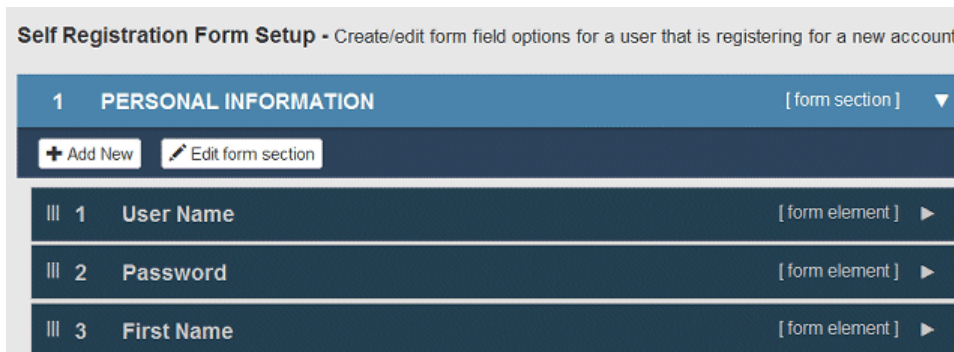
Option	Description
Require user to accept a policy agreement	A policy agreement must be accepted for registration. <ul style="list-style-type: none"> • Yes. The user must accept a policy agreement. • No. The user does not have to accept a policy agreement.
Require identity verification questions	Identity verification questions are used to validate a user when they reset a password. The answers for these questions are normally provided by users during registration. <ul style="list-style-type: none"> • Yes. The user must provide answers to identity verification questions. • No. The user does not provide answers to identity verification questions during registration.
Send email when registration is pending	Send an email to the user, Yes , or No .
Send email when a registration rejected	Send an email to the user, Yes , or No .
Send email when a registration succeeds	Send an email to the user, Yes , or No .

Configuring the self-registration form

The self-registration form is used to self-register. The form contains a number of fields that users complete during registration. You can reorder the fields and sections, add new sections, and add or remove fields.

Procedure

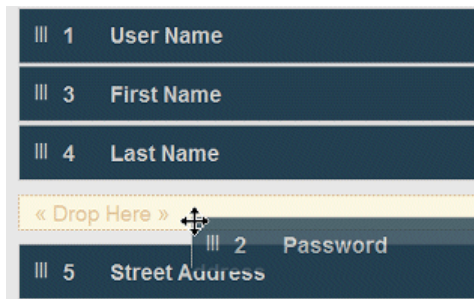
1. Click **Self Service > Self Registration** in the navigation menu, and click **Form Setup**.



2. Add a field:
 - a) Click **Add New > Add New Field**.
 - b) Select the attribute and field options to define the field.
 - c) Click **Save Changes** to add the field.
3. Optional: Add a section:
 - a) Click **Add New > Add New Section**.
 - b) Enter a **Label**, **Subheading**, and **Header** for the section.
The label, subheading, and header are used to identify the section on the form.
 - c) Click **Add New Field** to enter a new field in the section, select the attribute and field options to define the field.
 - d) Click **Save Changes** to save the new section.

You can add more fields to the section from the main **Self Registration Form Setup** window.

4. To change the order of a form and move a section or field to a new position, click and drag the field or section to the new position.



5. Click **Save Changes** to save the form.

Form options

Form options are used to set the properties of fields that are used in Self Service applications.

Depending on the form that is defined, some options might not be available.

Option	Description
LDAP attribute	LDAP attribute to be used as a field. If an attribute is selected that requires another user to be entered as a value, a search tool is added to the field. For example, a manager attribute might require another user to be entered. Depending on the field or form that is defined, some attributes cannot be selected.
Default Value	A default value for the field. If the field is editable, users can replace the default value.
Field Label	Label that is used to identity the field.

Table 9. Form field options (continued)

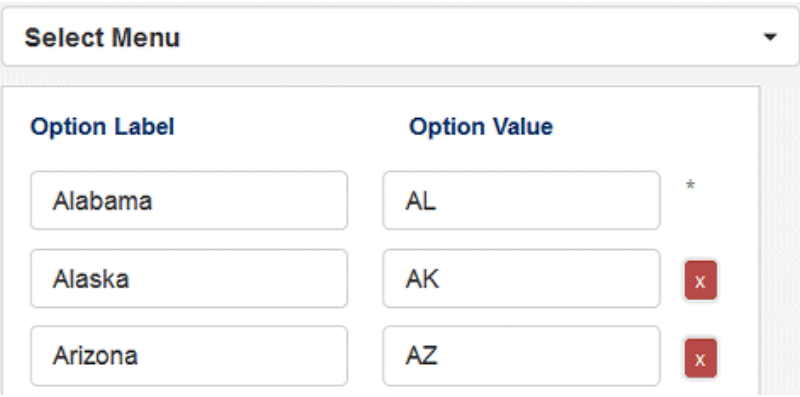
Option	Description
<p>Field Type</p>	<ul style="list-style-type: none"> • Checkboxes. Users can select one or more options as input for the field. • Password Field. Password fields are masked. • Radio Buttons. Users can select one option from a number of options as input for the field. • Select Menu. Users can select one option from a number of options as input for the field. • Text Field. Users input a value in to the field as entered text. • Text Area. Freeform text box. <p>For Checkboxes, Radio Buttons, and Select Menu, add the options for the field.</p> <ul style="list-style-type: none"> • Option Label. Label that is used to identify the option. • Option Value. Value of the option. <p>In this example, a select menu has a number of options for different states.</p> 
<p>Placeholder</p>	<p>Placeholder label.</p>
<p>Tool Tip</p>	<p>Field help text.</p>
<p>Editable</p>	<ul style="list-style-type: none"> • Yes. Users can enter a value in the field. • No. Users cannot enter a value in the field. Some fields are populated with existing data. For example, during self-registration a user might claim an account against an existing identity record in which case a field value can be used from the identity record.
<p>Required</p>	<ul style="list-style-type: none"> • Yes. The field is mandatory. <ul style="list-style-type: none"> – Self-registration form. Users cannot complete self-registration without providing a value for the field. – Self Service profile form. Users are prompted to enter values for any unpopulated mandatory fields. • No. The field is optional.

Table 9. Form field options (continued)

Option	Description
Require current password match	<p>Only for a password LDAP attribute.</p> <ul style="list-style-type: none"> • Yes. Users must enter the password twice, in separate fields. The value that they enter in each field must match to confirm that the password is correct. • No. The password is entered once, in one field only.
Masked	<p>Yes. The field is masked, and the value that is entered cannot be seen on the screen. Each character that is entered is replaced on-screen by an asterisk character.</p>
Require a matching field	<ul style="list-style-type: none"> • Yes. Users must enter the value twice, in separate fields. The value that they enter in each field must match to confirm that the value is correct. For example, when a user enters an email address, you can require them to enter the address twice. • No. The value is entered once, in one field only.
Validation	<p>Validation rules:</p> <ul style="list-style-type: none"> • Yes. The value that is entered must pass specified validation rules. For example, a date might have to pass a format validation rule such as mm/dd/yyyy. • No. Entered values are unvalidated. <p>Validation types:</p> <ul style="list-style-type: none"> • Date. Values must conform to a specified date format. For example, mm/dd/yyyy. • Email Address. Values must correspond to email address formats. For example, <i>text_string@text_string.com</i>. • Letters. Values must contain only alphabetic characters. • Maximum Character Length. Values cannot contain more than a specified number of characters. • Minimum Character Length. Values cannot contain less than a specified number of characters. • Number. Values must contain only numeric characters. • Password Strength. A password field must conform to basic, standard, or strong validation rules. Rules are based on the number and type of characters that must be entered. • US Phone Number. Values must conform to US phone number format. <p>Custom regular expressions. A regular expression that is evaluated against the value entered. If the expression evaluates to true, the value is valid.</p> <ul style="list-style-type: none"> • Pattern. A regular expression. For example, to restrict registrations to addresses in North Carolina use the regular expression <code>^NC\$</code> for the state attribute, where NC is defined as an optional value for the state attribute. • Error Message. Error message to display to users when an entered value is invalid.

Table 10. Form section options

Option	Description
Label	Section label.
Subheading	Subheading label.
Header	Header.

Self-registration form example

Widget Investment Corp

Employee Portal User Self Registration

Use the form below to register...

* indicates a required entry

1 PERSONAL INFORMATION
PERSONAL INFORMATION

User Name* ?

Password* ?

First Name* ?

Last Name* ?

Phone Number* ?

Street Address* ?

City* ?

State* ?

Country* ?

Account Number* ?

Email* ?

2 Department Information
Department Information

Date of hire ?
Enter the date in MM/DD/YYYY format.

Department number ?

3 SECURITY INFORMATION
SECURITY INFORMATION

Please select a question... ?

Please select a question... *

[+ Add more security questions](#)

Reset **Create Profile**

PERSONAL INFORMATION 1

DEPARTMENT INFORMATION 1

SECURITY INFORMATION 1

Number	Description
1	Section label.

Number	Description
2	Section header label.
3	Section subheading label.
4	Field label.
5	Mandatory field, indicated by asterisk.
6	Masked field. Password fields are always masked.
7	Select menu field.
8	Tooltip field help text.
9	Section number.
10	Text field.

Configuring password reset options

You can change the password reset options, including the number of security questions that must be answered and whether to use email verification.

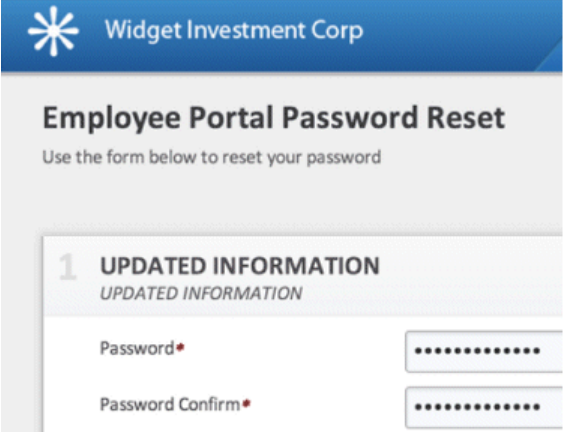
Procedure

1. In the navigation pane, click **Self Service > Password Reset**.
2. Select the [password reset options](#) you want.
3. Click **Save Changes**.

Password reset options

Option	Description
Required security questions	Applies only if Use multi-factor authentication is set to No . The minimum number of security questions that a user must answer to be able to reset their password.
Maximum failed attempts	Applies only if Use multi-factor authentication is set to No . The total number of incorrect answers that can be given to all questions. Users are locked out if the maximum number is exceeded.

Table 12. Password reset options (continued)

Option	Description
<p>Require email verification</p>	<p>Applies only if Use multi-factor authentication is set to No. Email verification requires the user to click a link sent to them by email after they requested a password reset.</p> <ul style="list-style-type: none"> • Yes. Email verification is needed, enter the time in minutes the link is valid for. They must use the link within a specified time limit. <p>The link takes the user to a password reset window.</p>  <ul style="list-style-type: none"> • No. No email is sent.
<p>Send email upon successful reset</p>	<ul style="list-style-type: none"> • Yes. An email is sent to the user that informs them that the password reset is successful. • No. No email is sent.

Configuring user name recovery options and form

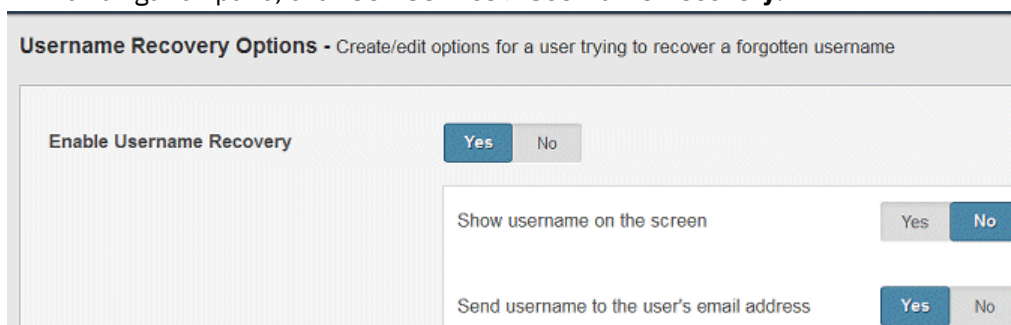
You can modify user name recovery options and fields.

Configuring user name recovery options

You can configure the user name recovery options, including whether to display the user name on screen or to send the user name to the email address of the user.

Procedure

1. In the navigation pane, click **Self Service > Username Recovery**.



2. Select the user name recovery options you want.
3. Click **Save Changes**.

User name recovery options

Table 13. User name recovery options	
Option	Description
Enable Username Recovery	<ul style="list-style-type: none">• Yes. User names can be recovered by using the user name recovery Self Service application.• No. No users are able to recover their user names by using the user name recovery Self Service application.
Show username on screen	<ul style="list-style-type: none">• Yes. The user name is displayed on-screen in the user name recovery Self Service application.• No. The user name is not displayed on-screen during user name recovery.
Send username to the user's email address	<ul style="list-style-type: none">• Yes. The user name is emailed to user.• No. No email is sent.

Configuring the user name recovery form

The username recovery form is used to recovery a username. The form contains a number of fields that users complete during username recovery. You can reorder the fields and sections, add new sections, and add or remove fields.

Procedure

1. Click **Self Service > Username Recovery** in the navigation menu, and click **Form Setup**.



2. Add a field:
 - a) Click **Add New > Add New Field**.
 - b) Select the attribute and field options to define the field.
 - c) Click **Save Changes** to add the field.
3. Optional: Add a section:
 - a) Click **Add New > Add New Section**.
 - b) Enter a **Label**, **Subheading**, and **Header** for the section.

The label, subheading, and header are used to identify the section on the form.
 - c) Click **Add New Field** to enter a new field in the section, select the attribute and field options to define the field.
 - d) Click **Save Changes** to save the new section.

You can add more fields to the section from the main **Username Recovery Form Setup** window.
4. To change the order of a form and move a section or field to a new position, click and drag the field or section to the new position.



5. Click **Save Changes** to save the form.

Form options

Form options are used to set the properties of fields that are used in Self Service applications.

Depending on the form that is defined, some options might not be available.

<i>Table 14. Form field options</i>	
Option	Description
LDAP attribute	LDAP attribute to be used as a field. If an attribute is selected that requires another user to be entered as a value, a search tool is added to the field. For example, a manager attribute might require another user to be entered. Depending on the field or form that is defined, some attributes cannot be selected.
Default Value	A default value for the field. If the field is editable, users can replace the default value.
Field Label	Label that is used to identity the field.

Table 14. Form field options (continued)

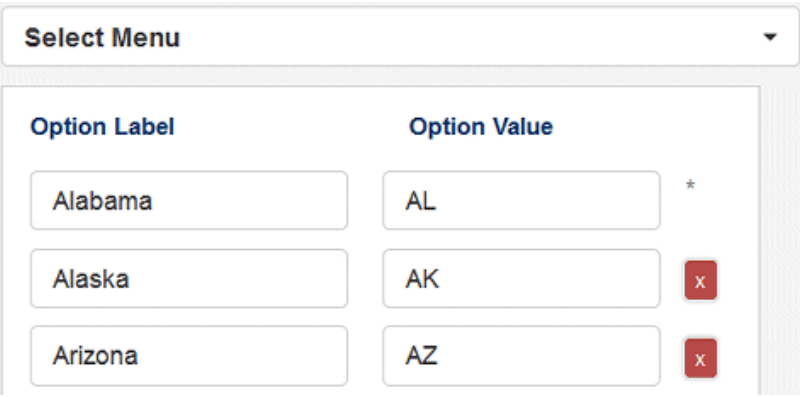
Option	Description
<p>Field Type</p>	<ul style="list-style-type: none"> • Checkboxes. Users can select one or more options as input for the field. • Password Field. Password fields are masked. • Radio Buttons. Users can select one option from a number of options as input for the field. • Select Menu. Users can select one option from a number of options as input for the field. • Text Field. Users input a value in to the field as entered text. • Text Area. Freeform text box. <p>For Checkboxes, Radio Buttons, and Select Menu, add the options for the field.</p> <ul style="list-style-type: none"> • Option Label. Label that is used to identify the option. • Option Value. Value of the option. <p>In this example, a select menu has a number of options for different states.</p> 
<p>Placeholder</p>	<p>Placeholder label.</p>
<p>Tool Tip</p>	<p>Field help text.</p>
<p>Editable</p>	<ul style="list-style-type: none"> • Yes. Users can enter a value in the field. • No. Users cannot enter a value in the field. Some fields are populated with existing data. For example, during self-registration a user might claim an account against an existing identity record in which case a field value can be used from the identity record.
<p>Required</p>	<ul style="list-style-type: none"> • Yes. The field is mandatory. <ul style="list-style-type: none"> – Self-registration form. Users cannot complete self-registration without providing a value for the field. – Self Service profile form. Users are prompted to enter values for any unpopulated mandatory fields. • No. The field is optional.

Table 14. Form field options (continued)

Option	Description
Require current password match	<p>Only for a password LDAP attribute.</p> <ul style="list-style-type: none"> • Yes. Users must enter the password twice, in separate fields. The value that they enter in each field must match to confirm that the password is correct. • No. The password is entered once, in one field only.
Masked	<p>Yes. The field is masked, and the value that is entered cannot be seen on the screen. Each character that is entered is replaced on-screen by an asterisk character.</p>
Require a matching field	<ul style="list-style-type: none"> • Yes. Users must enter the value twice, in separate fields. The value that they enter in each field must match to confirm that the value is correct. For example, when a user enters an email address, you can require them to enter the address twice. • No. The value is entered once, in one field only.
Validation	<p>Validation rules:</p> <ul style="list-style-type: none"> • Yes. The value that is entered must pass specified validation rules. For example, a date might have to pass a format validation rule such as mm/dd/yyyy. • No. Entered values are unvalidated. <p>Validation types:</p> <ul style="list-style-type: none"> • Date. Values must conform to a specified date format. For example, mm/dd/yyyy. • Email Address. Values must correspond to email address formats. For example, <i>text_string@text_string.com</i>. • Letters. Values must contain only alphabetic characters. • Maximum Character Length. Values cannot contain more than a specified number of characters. • Minimum Character Length. Values cannot contain less than a specified number of characters. • Number. Values must contain only numeric characters. • Password Strength. A password field must conform to basic, standard, or strong validation rules. Rules are based on the number and type of characters that must be entered. • US Phone Number. Values must conform to US phone number format. <p>Custom regular expressions. A regular expression that is evaluated against the value entered. If the expression evaluates to true, the value is valid.</p> <ul style="list-style-type: none"> • Pattern. A regular expression. For example, to restrict registrations to addresses in North Carolina use the regular expression <code>^NC\$</code> for the state attribute, where NC is defined as an optional value for the state attribute. • Error Message. Error message to display to users when an entered value is invalid.

Table 15. Form section options	
Option	Description
Label	Section label.
Subheading	Subheading label.
Header	Header.

User name recovery form example

The screenshot shows a form titled "Security Information" with a subheading "Security Information". The form contains four input fields, each with a callout number:

- 1**: The section number "1" next to the "Security Information" header.
- 2**: The section label "Security Information" below the header.
- 3**: The field label "LastName*" next to the text input field containing "turner".
- 4**: The masked field for "Social Security Number" containing ".....".
- 5**: The field label "Social Security Number" next to the masked input field.

Other fields include "Email*" with "turner@email.com" and "Account Number*" with "4488770924". Each input field has a green checkmark and a question mark icon to its right.

Table 16. User name form field and section elements	
Number	Description
1	Section number.
2	Section label.
3	Mandatory field, indicated by asterisk.
4	Masked field.
5	Field label.

Configuring the Self Service profile form

The Self Service profile form contains a number of fields that comprise the profile of a user in the Self Service profile application. You can reorder the fields and sections, add new sections, and add or remove fields.

Procedure

1. In the navigation pane, click **Self Service > Self Service Portal**.

Profile Form Setup - Create/edit form field options for a user that is editing their profile

1 Personal Data [form section] ▼	
+ Add New Edit form section	
1	User Name [form element] ▶
2	Password [form element] ▶
3	First Name [form element] ▶
4	Last Name [form element] ▶
5	Manager [form element] ▶

2. To add a field:
 - a) Click **Add New > Add New Field**.
 - b) Select the attribute and field options to define the field.
 - c) Click **Save Changes** to add the field.
3. To add a section:
 - a) Click **Add New > Add New Section**.
 - b) Enter a **Label**, **Subheading**, and **Header** for the section.
The label, subheading, and header are used to identify the section on the form.
 - c) Click **Add New Field** to enter a new field in the section, select the attribute and field options to define the field.
 - d) Click **Save Changes** to save the new section.
You can add more fields to the section from the main **Profile Form Setup** window.
4. To change the order of a form and move a section or field to a new position, click and drag the field or section to the new position.

1	User Name
3	First Name
4	Last Name
« Drop Here »	
2	Password
5	Street Address

5. Click **Save Changes** to save the form.

Form options

Form options are used to set the properties of fields that are used in Self Service applications.

Depending on the form that is defined, some options might not be available.

Table 17. Form field options

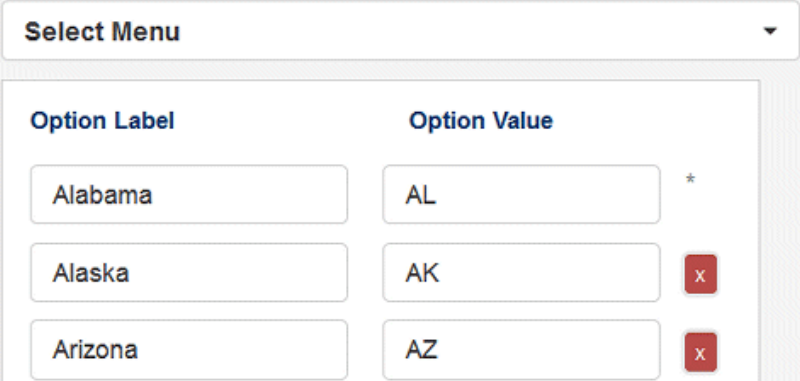
Option	Description
LDAP attribute	<p>LDAP attribute to be used as a field. If an attribute is selected that requires another user to be entered as a value, a search tool is added to the field. For example, a manager attribute might require another user to be entered.</p> <p>Depending on the field or form that is defined, some attributes cannot be selected.</p>
Default Value	<p>A default value for the field. If the field is editable, users can replace the default value.</p>
Field Label	<p>Label that is used to identify the field.</p>
Field Type	<ul style="list-style-type: none"> • Checkboxes. Users can select one or more options as input for the field. • Password Field. Password fields are masked. • Radio Buttons. Users can select one option from a number of options as input for the field. • Select Menu. Users can select one option from a number of options as input for the field. • Text Field. Users input a value in to the field as entered text. • Text Area. Freeform text box. <p>For Checkboxes, Radio Buttons, and Select Menu, add the options for the field.</p> <ul style="list-style-type: none"> • Option Label. Label that is used to identify the option. • Option Value. Value of the option. <p>In this example, a select menu has a number of options for different states.</p> 
Placeholder	<p>Placeholder label.</p>
Tool Tip	<p>Field help text.</p>
Editable	<ul style="list-style-type: none"> • Yes. Users can enter a value in the field. • No. Users cannot enter a value in the field. Some fields are populated with existing data. For example, during self-registration a user might claim an account against an existing identity record in which case a field value can be used from the identity record.

Table 17. Form field options (continued)

Option	Description
Required	<ul style="list-style-type: none"> • Yes. The field is mandatory. <ul style="list-style-type: none"> – Self-registration form. Users cannot complete self-registration without providing a value for the field. – Self Service profile form. Users are prompted to enter values for any unpopulated mandatory fields. • No. The field is optional.
Require current password match	<p>Only for a password LDAP attribute.</p> <ul style="list-style-type: none"> • Yes. Users must enter the password twice, in separate fields. The value that they enter in each field must match to confirm that the password is correct. • No. The password is entered once, in one field only.
Masked	<p>Yes. The field is masked, and the value that is entered cannot be seen on the screen. Each character that is entered is replaced on-screen by an asterisk character.</p>
Require a matching field	<ul style="list-style-type: none"> • Yes. Users must enter the value twice, in separate fields. The value that they enter in each field must match to confirm that the value is correct. For example, when a user enters an email address, you can require them to enter the address twice. • No. The value is entered once, in one field only.

Table 17. Form field options (continued)

Option	Description
Validation	<p>Validation rules:</p> <ul style="list-style-type: none"> • Yes. The value that is entered must pass specified validation rules. For example, a date might have to pass a format validation rule such as mm/dd/yyyy. • No. Entered values are unvalidated. <p>Validation types:</p> <ul style="list-style-type: none"> • Date. Values must conform to a specified date format. For example, mm/dd/yyyy. • Email Address. Values must correspond to email address formats. For example, <i>text_string@text_string.com</i>. • Letters. Values must contain only alphabetic characters. • Maximum Character Length. Values cannot contain more than a specified number of characters. • Minimum Character Length. Values cannot contain less than a specified number of characters. • Number. Values must contain only numeric characters. • Password Strength. A password field must conform to basic, standard, or strong validation rules. Rules are based on the number and type of characters that must be entered. • US Phone Number. Values must conform to US phone number format. <p>Custom regular expressions. A regular expression that is evaluated against the value entered. If the expression evaluates to true, the value is valid.</p> <ul style="list-style-type: none"> • Pattern. A regular expression. For example, to restrict registrations to addresses in North Carolina use the regular expression <code>^NC\$</code> for the state attribute, where NC is defined as an optional value for the state attribute. • Error Message. Error message to display to users when an entered value is invalid.

Table 18. Form section options

Option	Description
Label	Section label.
Subheading	Subheading label.
Header	Header.

Portal profile form example

Table 19. Self-registration form field and section elements

Number	Description
1	Section label.
2	Field label.
3	Mandatory field, indicated by asterisk.
4	Text field.
5	Text field, with user search tool.
6	Masked field. Password fields are always masked.

Changing security question options

During the initial configuration of Cloud Identity Service for your organization, a number of security questions are defined. The answers to security questions are used to verify users when they attempt to reset their password. You can add new security questions.

About this task

Users must provide answers to security questions when they self-register. Users can select the questions that they want to provide answers for from a pool of questions. You can add new questions, and you can set the minimum number of questions users must provide answers for when they self-register.

Procedure

1. In the navigation pane, click **Self Service > Security Questions**.

Create/edit security options for verifying a users' identity.

Security Questions Setup - NOTE: A hidden question will still be shown to users that have already answered the question.

Question Language English

* This setting is used for all languages

Minimum required questions* 1

Minimum answer characters* 1

Answers must be unique* Yes No

Security questions

In what year was your father born? Visible Hidden

In what year was your mother born? Visible Hidden

What is the name of your childhood best friend? Visible Hidden

Add a new question

Select from a predefined list of questions

Or you can add a custom question here

Add New Question

- Optional: Select a language that you want to provide user local language support for, from the **Question Language** drop-down list.

The languages that you can select are defined during the initial configuration of Cloud Identity Service for your organization. You add translations for questions that are already defined in the default language.

- Click **Choose a question to translate**, and select a question from the list.

The questions that are available are the questions that are already defined in the default language. The default language is English.

- Enter the translation in the text field, and click **Add Translation**.

Add Translation

What is your mothers maiden name?

Quel est votre premier nom de mères?

Add Translation

- Set the security questions setup options that you want.

- Click **Save Changes**.

Security questions options

Security questions options include the minimum number of security questions, uniqueness of questions, and minimum length of answers.

Table 20. Security questions options	
Option	Description
Enable salting and hashing of answers	Specifies whether to salt and hash answers to security questions. Hashing encodes an answer into a fixed-length string of characters, making the answer more secure from discovery. Salting randomizes hashes by adding a random string, making answers harder to decode. Important: If salting and hashing is enabled, it cannot be disabled.

Table 20. Security questions options (continued)

Option	Description
Minimum required questions	The minimum number of security questions that a user must provide answers for when they register. This option does not refer to the number of questions that must be answered during password reset. For example, a user might provide answers for 5 questions, but during password reset, only 3 answers are required. In this case, 3 questions are randomly chosen from the 5 originally answered during registration.
Minimum answer characters	The minimum number of characters that must be entered as an answer.
Answers must be unique	<ul style="list-style-type: none"> • Yes. Users cannot enter the same answer to different questions. • No. Answers to different questions can be the same.
Make default tab in profile on error	On login to Self Service portal, specifies whether the user is presented with the security questions tab first if security question errors are present.
Security questions	<p>Security questions can be hidden or visible.</p> <ul style="list-style-type: none"> • Visible. The question is available for the user to provide an answer to during registration. • Hidden. The question is not available to the user when they register, and they cannot provide an answer to the question.
Add a new question	<p>You can add a question by using two methods.</p> <ul style="list-style-type: none"> • Select from a predefined list of questions. Select from a list of questions. • Add a custom question. Enter the question in the text field, and click Add New Question. <p>Important: New security questions can be removed only before they are saved. After you add a question and save your changes, the question can be removed only by opening a support ticket.</p>

Managing roles

You can add and modify roles, but you cannot delete roles.

Roles overview

A role can be thought of as a functional title within your organization. For example, Manager, Administrator, or Help Desk contact. Roles are used to control access to different Self Service applications and actions, and to control access to different sections in the Self Service profile application.

Related concepts

[Configuration overview](#)

Self Service applications are configured during the initial setup of Cloud Identity Service for your organization. You can change a number of settings and options to adapt to your changing needs.

Related tasks

[Adding instances](#)

You can add a number of instances to be used by different roles in your organization.

Adding roles

A role can be thought of as a functional title within your organization. For example, Manager, Administrator, or Help Desk contact. Roles are assigned to users. Roles are used to control access to different Self Service applications and tasks.

About this task

Roles can be assigned to different instances. An instance is a grouping of configurations, options, and branding for Self Service applications. For example, an instance might define a set of color schemes, text translations, form layouts, and self-registration options. Then, for each role that is defined, an instance can be selected for that role. For example, a help desk role and a manager role might be assigned different instances. A role can be assigned only one instance, and a single instance can have many roles.

Procedure

1. In the navigation pane, click **Self Service > Self Service Roles**.
2. Click **Add a new Role**.
3. Enter a name for the role in the **Role Name** field.
4. Enter description for the role in the **Role Description** field. The maximum number of characters allowed is 100.
5. Optional: Select the instance of the Self Service applications from the **Instance** drop-down list.

Self Service applications can have different instances. An instance defines the windows, fields, labels, and other UI elements in Self Service applications. Different instances can be designed to meet the needs of different roles. The default Cloud Identity Service instance is selected. A role can be assigned only one instance.

6. Select the [role settings](#) that you want.
7. Click **Save Changes** to save the role.

Role settings



Role settings control access to different Self Service applications and actions for users who are assigned to the role. Role settings include profile management, password reset, user name lookup, self-registration options, search options, and profile view and edit permissions.

Setting	Description
Self Service Portal	Access for users to manage their own profiles of user information.

Table 21. Role settings (continued)

Setting	Description
Section Access	<p>Different sections in the Self Service portal and profile applications.</p> <ul style="list-style-type: none"> • Launchpad. Access to Launchpad. Launchpad provides a single location in Self Service portal from where users can access connected web applications and federated partner web applications. • Profile. Access for users to manage their own profile information. <ul style="list-style-type: none"> – Show profile as a page. Specifies whether to display profile information as a page or as a drop-down header. • Direct Reports. Access to manage the profiles of users that are direct reports. <ul style="list-style-type: none"> – Allow new user creation. Can create new users. – Can demote accounts. Can demote accounts to user identities. – Can toggle user status. Can activate or deactivate a user account. If an account is deactivated, a user cannot log in to Self Service. – Can expire password. Can expire user passwords. – Can modify user's role. Can modify user's role. • Requests. Access to manage pending approval and recertification requests. • Services. Access to view a list of services to which they belong, and the ability to request services. • User Control. Access to view profile information of other users in the User Control page. <ul style="list-style-type: none"> – Allow new user creation. Can create new users. – Can demote accounts. Can demote accounts to user identities. – Can toggle user status. Can activate or deactivate a user account. If an account is deactivated, a user cannot log in to Self Service. – Can expire password. Can expire user passwords. – Can modify user's role. Can modify user's role.
Section Settings	<ul style="list-style-type: none"> • Show Check Username button. Can check whether a user name exists when a new user is being created.
Password Reset	<p>Access for users to the password reset application to reset their own password. No authentication is needed for the application.</p>
Username Recovery	<p>Access for users to the user name recovery application to recover their own user name. No authentication is needed for the application.</p>
Self Registration	<p>Access to self-registration application to self-register. No authentication is needed for the application.</p>

Table 21. Role settings (continued)

Setting	Description
<p>User Search Settings</p> <p>Service Search Settings</p>	<p>The priority by which attributes are sorted and displayed when a search for a user or a service is made in Self Service applications.</p> <ul style="list-style-type: none"> • Search Results Priority. In search results, an attribute with a higher priority is displayed before an attribute with a lesser priority. To add an attribute to the search results, select an attribute from the Add New Attribute list and click . Click and drag an attribute to a new position to change its priority. • Search Results Filter. Attribute filtering rules can be applied to exclude users or services from a search. For example, you can exclude users that have a specific role. To add an exclusion filter, click Add Exclusion Filter. Select the attribute that you want to base the exclusion on from the When Attribute list. Enter the attribute value that you want to exclude in the Is Equal To field.
<p>View Permissions</p>	<p>View and edit permissions for user profiles. You can specify identity attributes to be viewable and editable for profiles in Self Service applications.</p> <ul style="list-style-type: none"> • Any Users Profile. Profiles of all users. • Users Own Profile. User's own profile. • Direct Reports Profile. Profiles of a user's direct reports. • Group Members Profile. Profiles of users with a specified group membership. • Service Members Profile. Profiles of users with a specified service membership. • Role Members Profile. Profiles of users with a specified role. <p>To add attribute view and edit permissions:</p> <ol style="list-style-type: none"> 1. Click Add View Permissions Filter. 2. Select the user profiles that you want to apply attribute view and edit permissions to, from the Applies when viewing list. <ul style="list-style-type: none"> For Role Members Profile, select the role from the who belongs to list. For Group Members Profile and Service Members Profile, search for and select the group or service from the who belongs to list. To search for the group or service, enter at least the first 3 characters of the group or service name. 3. Select the attribute that you want to apply permissions to from the Add Attribute menu, and click . You can add as many attributes as you need. <ul style="list-style-type: none"> Specify whether to make the attribute viewable and editable by clicking the appropriate Yes or No. 4. Click Save Changes.

Customizing the UI for Self Service applications

Customizing the UI for Self Service applications, includes customizing branding, labeling for text keys, email templates, labeling in the Self Service profile application, and labeling for Self Service application suite pages.

Self Service UI customization overview

Self Service applications are configured during the initial setup of Cloud Identity Service for your organization. You can customize the branding of Self Service applications. You can change the content of emails that are sent to users, and you can change UI column labels and other text keys.

Branding

You can control the branding of Self Service applications. Branding includes application color-scheme, logo, icons, and visual presentation of form elements.

Text keys

Text keys are used to provide default text for application headers and footers, error messages, button labels, attribute labels, and form section labels. You can change the text for text keys.

Email templates

Email templates are used to provide the content for email messages that are sent to users in response to some event. For example, the content of messages that are sent when a registration request is approved or when a password is reset. You can change the content of messages. You can change aspects of the font and paragraph styles that are used.

Portal

The Self Service profile portal or application allows users to manage their own account profile information after they are registered and able to authenticate to Cloud Identity Service. You can change the text that is used to label table column headers, and the text that is used for other UI elements.

Suite pages

Suite pages are the individual Self Service application pages that users access to manage aspects of their Cloud Identity Service identity or account. Suite pages include self-registration, password reset, user name recovery, and directory lookup. You can change the text that is used to label sections and headings in suite pages.

Customizing branding

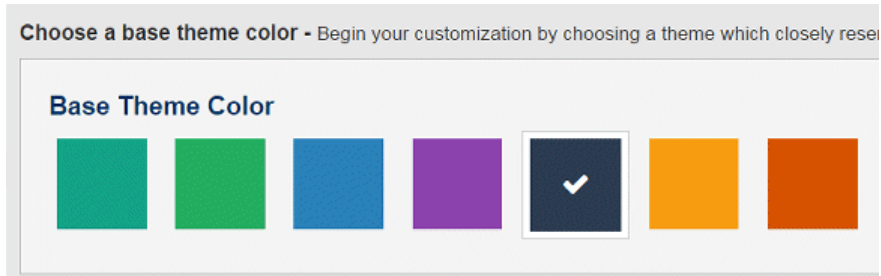
You can customize branding by changing the colors, logos, icons, and images that are used in Self Service applications.

Selecting a base theme color

You can select a color to be used as a base background color for all Self Service applications.

Procedure

1. Click **Self Service** > **Branding** in the navigation menu, and click **Themes**.



2. Select the base theme color.
A preview is displayed.
3. Click **Save**.

Selecting theme colors

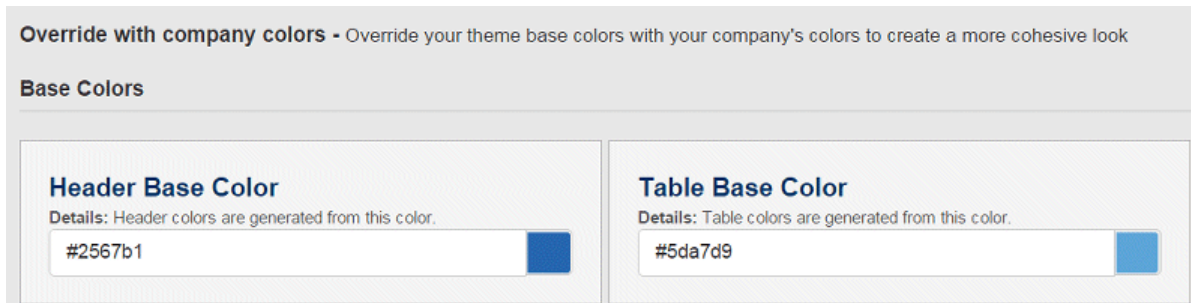
You can select individual base colors for a number of Self Service UI elements. You can also select colors to be used for messages and buttons.

About this task

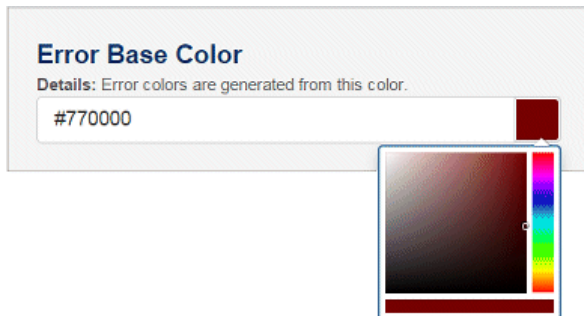
Selected colors override the base theme color.

Procedure

1. In the navigation pane, click **Self Service** > **Branding** in the navigation menu, and click **Colors**.



2. Change the color for an element by using one of the following methods.
 - Click in the color selection square.
 - Enter the HTML color code.



You can select colors for the following Self Service UI elements.

- Base
 - Header
 - Table
 - Profile
 - Link

- Error
- Button
 - Primary
 - Secondary
 - Alternate
- Message
 - Basic
 - Success
 - Loading
 - Feedback
 - Alert
 - Error

3. Click **Save**.

Selecting images

You can replace the images, logos, and icons, that are used in Self Service applications.

About this task

You change images by uploading files to replace currently used image files.

Note: A replacement file overwrites a current file. If a current file is not the original file, you can save the current version of a file before you replace it. Original files are always available to download and reuse. Image files have a maximum size of 50 KB.

Procedure

1. Click **Self Service > Branding** in the navigation menu, and click **Images**.
2. Optional: Download a currently used file, click **Download Current File**.
3. Upload a replacement file, click **Select New File**.

Image files

Image files are used for Self Service icons, images, and logos.

<i>Table 22. Image files</i>	
File	Description
Logo image	Header logo. This logo looks best when it has a transparent background. The size cannot be changed. Exceeding the current height or width can result in a distorted image.
Error icon	Failed operation or error image. This logo looks best when it has a transparent background. The size cannot be changed. Exceeding the current height or width can result in a distorted image.
Favorites icon	Favorites icon that is displayed in browser. The icon must be 16px by 16px so that it can display correctly as a bookmark icon in the browser.
Form elements	Check box and radio button images. This image sprite contains all of the images for each state of the form element in a single file. Each image must not exceed the height or width of the default image or it is trimmed (clipped) when it is loaded in the browser.
Page background	Tiled background image for profile management. This image tiles (repeats) vertically, and aligns to the left, when the page is loaded.

Table 22. Image files (continued)

File	Description
Data loading indicator	Data loading image. You can use a static or animated image. The sizes must not change.
Preloader image	Section is loading image. You can use a static or animated image. The sizes must not change.
Search field icon	Autocomplete or search enabled input field image. You must use a static image. The sizes must not change.
Searching icon	Search being performed image. You can use a static or animated image. The sizes must not change.
Success icon	Successful operation icon. This icon looks best when it has a transparent background. The size cannot be changed. Exceeding the current height or width can result in a distorted image.
Pages icon	Page icons on Self Service screens. This image sprite contains all of the images for each section of the user tools pages in a single file. Each image must not exceed the height or width of the default image or it is trimmed (clipped) when it is loaded in the browser.

Customizing login and error pages

You can replace the stylesheet, logo, and page title that are used for the Cloud Identity Service login page and error pages. You can also change and add text elements that appear at the foot of pages.

Before you begin

If you want to replace the stylesheet file, you must have a good understanding of CSS. The stylesheet is used to control the sizing, positioning, and styling of UI elements on the page.

About this task

You change the logo or stylesheet by uploading files to replace the currently used logo or stylesheet files. You enter text to change the page title and text elements. Text elements appear at the foot of the page. You can also provide local language support for text elements.

Note: The original files provide useful examples for customizing login and error pages.

Note: A replacement stylesheet or logo file overwrites a current file. If a current file is not the original file, you can download and save the current version of a file before you replace it. Original files are always available to download and reuse. Image files have a maximum size of 50 KB.

Procedure

1. Click **Self Service > Branding** in the navigation menu, and click **Global**.
2. Optional: Upload a new stylesheet file, click **Upload Stylesheet**.
3. Optional: Enter a new page title in the **Page Title** field.
4. Optional: Upload a new logo file, click **Upload Logo**.
5. Optional: Enter new text for a text element in the **Text Element** field.

Note: You can add translated versions of text elements to provide local language support in any of the languages available for your configuration of Cloud Identity Service.

6. Optional: Click **Add New Text Element** to enter a new text element.

Note: New text elements appear in order, below the previous element.

Note: You can preview the changes that you made by clicking **Preview Changes**.

7. Click **Save Changes**.

Related tasks

[Adding local language support](#)

You can add local language support so that text in Self Service applications, and messages, and emails are all in your chosen language.

Customizing general Self Service UI text keys

You can add text and change the text for general text keys that are used to label buttons, fields, columns, LDAP attributes, and other elements that are used throughout Self Service applications.

Procedure

1. Click **Self Service > Content Management** in the navigation menu, and click **General**.
2. Select the text keys that you want to customize from the **Text Keys** drop-down list.

You can add text and change the text keys for the following general text keys:

- **Autocomplete.** Autocomplete table text keys that are used in Service and User lookup tables.
 - **Button Labels.** Button labels that are used throughout Self Service applications.
 - **Error Messaging.** General error messaging, appearing at the top of the screen.
 - **Footer Text.** Footer text that appears at the bottom of Self Service applications.
 - **Form Labels.** Labels that are used in forms.
 - **Form Field Placeholder Text.** Placeholder text that is used in forms.
 - **Form Field Tooltip Text.** Form field tooltips.
 - **Header Text.** Text appearing at the top of Self Service applications.
 - **LDAP Attributes.** LDAP attribute names. LDAP attribute text keys can be used in searches for LDAP attributes.
 - **User Profile Layout.** Profile section layout headers.
 - **Validation Messaging (Custom).** Custom validation messaging. Used for customer supplied regular expression validations.
 - **Validation Messaging (Standard).** Standard validation messaging.
3. Change the text keys that you want, and click **Save Changes**.

Configuring email templates

Email templates are used to provide the content that is used for email messages that are sent to users. You can change the content and format of email templates.

Before you begin

A basic knowledge and fluency in HTML is required to edit the information in a template body.

Procedure

1. Click **Self Service > Content Management** in the navigation menu, and click **Email Templates**.

Email Template Employee Pending Approval Record **Template Language** English

Reply-To Address

Subject

Template Body

H1 H2 H3 H4 H5 H6 ¶ - B I S - ☰ ☷ - ☐ ☑ - ☒ ☓ - ☔ ☕ ☑

```
<html>
$firstName $lastName,<br/><br/>
Your employee $emplFirstName $emplLastName has pending approval records that
require attention.<br/><br/>
Please ensure that this employee logs in to the Gateway Self-Service system to
process their pending requests.<br/><br/>
</html>
```

2. From the **Email Template** menu, select the template that you want to configure.

3. You can change the following header details:

- **Reply-To Address.** The address of the sender.
- **Subject.** A description of the purpose of the email.

4. Enter or modify the message text in the template body.

Use the **Template Body** menu bar to format text, insert paragraphs, pictures, links, and attributes. Each icon inserts the appropriate HTML tags or attribute in the body of the template. Highlight text, or position the cursor at the point at which you want to apply formatting or insert an attribute, link, or picture.

5. Click **Save Changes**.

Email template formatting and content options

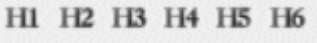






<i>Table 23. Email template body, format, and content options</i>	
Format and content options	Description
	Inserts headings 1 - 6. Font sizes from heading 1 - 6 are 36, 30, 24, 18, 14, and 12 pixels.
	Inserts a paragraph.
	Text formatting for Bold, Italic, and Strikethrough.
	List formatting for Bullet list, Numbered list, and List item.
	Inserts a picture. Specify a URL to link to a picture. You can specify alternative text for a picture. Alternative text is used to meet accessibility requirements. You can also specify whether to prevent the link from creating extra dialogs. Extra dialogs are pop-up windows.
	Insert a link to a web page. Specify a URL to link to the page. An area in the anchor tag is highlighted for you to enter link text, Your text to link . Enter text for the email recipient to click to access the linked page.
	Color of text.

Table 23. Email template body, format, and content options (continued)




Format and content options	Description
	<p>Enters an attribute. A number of attributes are available along with custom attributes.</p> <ul style="list-style-type: none"> • Approval Create Time. The date and time the service is requested. • Approval Grace Period. The length of time that is granted to approve the service request. • Approver First Name. The first name of the administrator responsible for approving or denying the request. • Approver Last Name. The last name of the administrator responsible for approving or denying the request. • Approver Reason. The approval or denial reason text provided by approver. • Client Name. The name of your organization. • Client Web Presence Name. The web presence name for your organization, which is defined during the initial setup process. • Connection Name. The name of the secure connection to Cloud Identity Service. • Deprovisioning Instructions. Instructions to delete an account. • Email Address. The email address of the user. • Email Minutes. The amount of time a password reset link is valid for. • Employee First Name. The first name of the employee with pending requests. • Employee Last Name. The last name of the employee with pending requests. • Title. The title of the user. • First Name. The first name of the user. • Last Name. The last name of the user. • Password Minutes. The amount of time available to change a password after a user clicks the reset link. • Password Reset URL. A link to reset a password. • Provisioning Instructions. Instructions to create an account. • Reason. The reason for action that is taken or the action that is requested. • Requester First Name. The first name of the user that submits the service request. • Requester Last Name. The last name of the user that submits the service request. • Service Description. A summary description of a service. • Service Name. The name of the service requested. • Username. The user name of the user. • gtwayManager. The first and last name of the manager of the user. • DepartmentNumber. The department number of the user.
	<p>Removes formatting from selected text.</p>

Table 23. Email template body, format, and content options (continued)

Format and content options	Description
	Previews the email.

Customizing the Self Service profile application

You can customize the Self Service portal profile application. You can change the text keys that are used to label columns and other elements of the portal.

About this task

The Self Service profile application allows users to manage their own account profile information, and to view and request services. It is also used to manage direct reports, service requests, and delegated users.

You can change the text that is used to label table column headers throughout the portal, and the text that is used for other UI elements.

Procedure

1. Click **Self Service > Content Management** in the navigation menu, and click **Portal**.

2. Select the UI section that you want to customize from the **Text Keys** menu.

You can change the text keys for the following UI regions:

- **Main Navigation.**
- **Service Table Columns.**
- **Direct Reports Table Columns.**
- **Requests Table Columns.**
- **User Control Table Columns.**
- **Table labels.**
- **Search Labels.**

3. Change the labels and text you want, and click **Save Changes**.

Main portal navigation key names and labels

Main portal navigation key names are used to label the main sections on the main Self Service portal page.

Key Name	Language	English
Main Navigation		
profileNavLabel		Profile
reportsNavLabel		Direct Reports 2
requestsNavLabel		Requests 3
servicesNavLabel		Services 4
usersNavLabel		User Control 5
		Save Changes

Widget Investment Corp Logo Welcome Back Paul | [Logout](#) English

Requests **3**
Direct Reports **2**
Services **4**
User Control **5**

Name	Description	Status
atService2CH406	atService2 description	
atService2IE967	atService2 description	
atService3CH386	atService3 description	
atService3CH386	atService3 description	

Services page key names and labels

Services page key names are used to label the **Services** page header and table columns.

Key Name Language English

Services Table Columns

col1Label **2**

col2Label **3**

col3Label **4**

col4Label

heading **1**

parentService

Services 1		
Name 2	Description 3	Status 4
Active Directory 1	All members with AD accounts	
AIX Server Farm	AIX unix server farm	
ApplicationX	Service to control provisioning to application X	

Direct Reports page key names and labels

Direct reports key names are used to label the **Direct Reports** page header and table columns.

Key Name Language English

Direct Reports Table Columns

col1Label First Name **2**

col2Label Last Name **3**

col3Label Email Address **4**

col4Label Username **5**

col5Label Delegate **6**

col6Label

heading Direct Reports **1**

Save Changes

Direct Reports **1**

First Name 2	Last Name 3	Email Address 4	Username 5	Delegate 6
Adam	Jones		ajones	Adam Jones
Bertha	Jones		bjones	

Requests page key names and labels

Requests page key names are used to label the **Requests** page header and table columns.

Key Name Language English

Requests Table Columns

col1Label	Type 2
col2Label	Details 3
col3Label	Requestor 4
col4Label	Request Date 5
col5Label	Due Date 6
col6Label	Status 7
col7Label	
heading	Requests 1

Save Changes

Requests **1** Select All Deselect All Process Requests

Type 2	Details 3	Requestor 4	Request Date 5	Due Date 6	Status 7
<input type="checkbox"/> Service Group		Adam Jones	06/11/2015 09:48 AM	06/11/2015 09:48 AM	Access Pending

Showing 1 to 1 of 1 Requests Show 10 Requests First Previous **1** Next Last

User Control page key names and labels

User Control page key names are used to label the **User Control** page header and table columns.

Key Name	Language	English
User Control Table Columns		
col1Label	First Name	2
col2Label	Last Name	3
col3Label	Email Address	4
col4Label	Username	5
col5Label	Delegate	6
col6Label	Services	7
col7Label	Requests	8
col8Label	Direct Reports	9
col9Label		
heading	Users	1

Save Changes

Users	2	3	4	5	6	7	8	9
First Name	Last Name	Email Address	Username	Delegate	Services	Requests	Direct Reports	
Adam	Jones		ajones	Adam Jones	1	0	0	

The **col9Label** is an optional column. The admin user can add any label to **col9Label** field. If any label is added to this field, it has to be mapped correctly in database. User need to map the label with attribute. Label name could be anything but attribute name should be given in database. If mapping is not done in database user sees only column heading for this label but data in this column is blank on Self Service portal.

Customizing the UI for Self Service suite pages

You can customize the Self Service application suite pages. You can change the text keys that are used to label headers, fields, and other elements of the Self Service applications.

About this task

The Self Service applications allow users to manage a number of Self Service tasks, including self-registration, password reset, and user name recovery. You can change the text that is used to label fields and headers throughout the Self Service applications.

The text items that you can change depend on the options that are configured for your Self Service applications.

Procedure

1. Click **Self Service > Content Management** in the navigation menu, and click **Suite Pages**.
2. Select the Self Service application that you want to customize from the **Text Keys** menu.

You can change the text keys for the following Self Service applications:

- **New User Registration.**
- **Password Reset.**
- **Password Reset Verification.**
- **Username Recovery.**
- **Directory Lookup Text.**

3. Change the text keys that you want, and click **Save Changes**.

User registration key names

User registration key names are used to label headers and fields in the Self Service User Registration page.

Key Name	Language	English
New User Registration		
fieldgroup0headers		PERSONAL INFORMATION
fieldgroup0labels		PERSONAL INFORMATION
fieldgroup0sub-headers		PERSONAL INFORMATION
instructions		Use the form below to register... 2
pageHeading		Employee Portal User Self Registration 1
pageSubHeading		
personalInformationHeader		Enter your personal identity information
personalInformationLabel		PERSONAL INFORMATION
personalInformationSubHeader		
redirectText		<a >proceed="" a><="" href="../index.html" login<="" td="" to="">
securityInformationHeader		The following questions will be used to reset your password
securityInformationLabel		SECURITY INFORMATION
securityInformationSubHeader		A minimum of 3 security questions are required
successText	3	

Employee Portal User Self Registration 1

Use the form below to register...


2

* indicates a required entry

1 PERSONAL INFORMATION

PERSONAL INFORMATION

User Name*	<input type="text" value="test1_admin"/>	✓ ?
Password*	<input type="password" value="....."/>	✓ ?
First Name*	<input type="text" value="First Name"/>	?
Last Name*	<input type="text" value="Last Name"/>	?
Phone Number*	<input type="text"/>	?
Street Address*	<input type="text" value="Street Address"/>	?
City*	<input type="text" value="..."/>	▼
State*	<input type="text" value="..."/>	▼
Country*	<input type="text" value="..."/>	▼

PERSONAL INFORMATION 

Employee Portal User Self Registration

Use the form below to register...

* indicates a required entry

✓ [Congratulations you are now registered](#) 3

The user has been added!

Password reset key names

Password reset key names are used to label headers, sections, and fields in the Password Reset Self Service application.

Key Name	Language	English
Password Reset		
authText	An email will be sent to you allowing you to choo	7
checkEmail	Please check your email for password reset instr	9
forgotUsername	Did you forget your username?	6
instructions	Use the form below to reset your password	5
lockedHeader	ACCOUNT LOCKED	
lockedMsg	This account has been temporarily locked. You c	
pageHeading	Password Reset	4
pageSubHeading		
personalInformationHeader	Enter the username you use to log into your acco	
personalInformationLabel	PERSONAL INFORMATION	1
personalInformationSubHeader		
securityInformationHeader	Answer the following identity verification questio	
securityInformationLabel	SECURITY INFORMATION	2
securityInformationSubHeader		
updated	Your password has been successfully updated	8
updatedInformationHeader	Choose a new password	
updatedInformationLabel	UPDATED INFORMATION	3
updatedInformationSubHeader		
Save Changes		




Password Reset 4

The Password Reset Sub heading

Use the form below to reset your password

5

* indicates a required entry

1 PERSONAL INFORMATION <i>PERSONAL INFORMATION</i>	1
Username* <input type="text" value="jrtest6"/> ✓ ? <input type="button" value="Check Username"/> Did you forget your username?	PERSONAL INFORMATION 
2 SECURITY INFORMATION <i>SECURITY INFORMATION</i>	2
What is your employee number?* <input type="text" value="ibm"/> ✓	SECURITY INFORMATION 
3 UPDATED INFORMATION <i>UPDATED INFORMATION</i>	3
You will receive an email shortly with a link to reset your password 7	UPDATED INFORMATION 

Password Reset

Use the form below to reset your password

* indicates a required entry

✓ Security verification questions were successfully answered

Your password has been successfully updated 8

✓ Security verification questions were successfully answered

Please check your email for password reset instructions 9

Password reset verification key names

Password reset verification key names are used to label headers and fields in the Self Service Password Reset verification page.

Key Name	Language	English
Password Reset Verification		
instructions		Use the form below to reset your password 1
pageHeading		Employee Portal Password Reset 2
pageSubHeading		
updatedInformationHeader		Choose a new password
updatedInformationLabel		UPDATED INFORMATION
updatedInformationSubHeader		
Save Changes		

Employee Portal Password Reset **2**

Use the form below to reset your password **1**

* indicates a required entry

✓ **Security verification questions were successfully answered**

Your password has been successfully updated

Username recovery key names

Username recovery key names are used to label headers and fields in Self Service Username Recovery pages.

Key Name	Language	English
<h2>Username Recovery</h2>		
instructions		Use the form below to recover your username 1
notFound		That username was not found. Please try again
pageHeading		Employee Portal Username Recovery 2
pageSubHeading		
personalInformationHeader		Enter your personal identity information
personalInformationLabel		PERSONAL INFORMATION
personalInformationSubHeader		
usernameLabel		Username
usernameNotFound		Username not found. Please check that the information 3
usernameRecovered		Username Recovered 4
<p>Save Changes</p>		

Employee Portal Username Recovery **2**

Use the form below to recover your username **1**

* indicates a required entry

1 Security Information

Security Information

LastName*	<input type="text" value="turner"/>	✓	?
Email*	<input type="text" value="turner@email.com"/>	✓	?
Social Security Number	<input type="text" value="●●●●●●●●"/>	✓	?
Account Number*	<input type="text" value="4488770924"/>	✓	?

Reset

Recover Username

Employee Portal Username Recovery

Use the form below to recover your username

* indicates a required entry

✓ Username Recovered **4**

Your username has been sent to the email address you have set up in your profile. Occasionally it may take up to 20 minutes for the email to arrive. If you are unable to access that email address, or you do not receive the email, please contact the help desk.

Directory Lookup key names

Directory Look-up key names are used to label headers and fields in the Self Service Directory Look-up page.

Directory Lookup Text	
col10Label	Division 4
col1Label	First Name 3
col2Label	Last Name
col3Label	Title
col4Label	Work Phone
col5Label	7-Digit Phone
col6Label	Mobile Phone
col7Label	Alternate Phone
col8Label	Office
col9Label	Department
heading	Users
pageHeading	Directory Look-Up 1
pageSubHeading	Look-up a users information in the company 2
	<input type="button" value="Save Changes"/>

Directory Look-Up 1

Look-up a users information in the company directory using the search form below

First Name

Last Name

Title

Work Phone

7-Digit Phone

Mobile Phone

Alternate Phone

Office

Department

Division -- All -- 4 ▼

Adding instances

You can add a number of instances to be used by different roles in your organization.

About this task

An instance is a grouping of configurations and options for Self Service applications. For example, an instance might define text translations, form layouts, self-registration options, and other Self Service application options. For each role that is defined, an instance can be selected for that role. For example, a help desk role and a manager role might be assigned different instances to give them access to different Self Service application options. A role can be assigned only one instance, and a single instance can be used by many roles.

You can select an instance to use when you:

- [Configure Self Service applications](#)
- [Customize the UI for Self Service applications](#)

Instances can be created whenever you need them, from most of the Self Service configuration and customization tasks. In the following example, an instance is created from **Self Service > Content Management**.

Procedure

1. In the navigation pane, click **Content Management**.
2. Click **Add a new instance**.

3. Enter a name for the instance in the **Instance Name** field.
4. Select whether to base the instance on the default instance or another instance.
 - **New.** The instance is based on the configuration options that are created for the default instance.
 - **Copy from existing instance.** The instance is based on the configuration options that are created for the selected instance.
5. Click **Add New Instance**.

Related concepts

[Roles overview](#)

A role can be thought of as a functional title within your organization. For example, Manager, Administrator, or Help Desk contact. Roles are used to control access to different Self Service applications and actions, and to control access to different sections in the Self Service profile application.

Adding local language support

You can add local language support so that text in Self Service applications, and messages, and emails are all in your chosen language.

Adding languages

You can add supported languages to Cloud Identity Portal. Added languages can be used to provide the text in your chosen language in Self Service applications.

Procedure

1. In the navigation pane, click **Self Service > Available Languages**.
2. Select a language to add from the **Add a new language** menu.
The menu shows a list of all supported languages.
3. Click **Add New Language**.

One of the supported language can be set as default language.

Note: The language set as default language cannot be deleted.

Providing translated text

You can provide translated text to provide local language support for users of Self Service applications.

About this task

You can provide text for many aspects of Self Service applications, including email templates and security questions. You can select from a number of supported languages.

You can select a language to provide local language text for:

- [Security questions](#)
- [Self Service applications UI text](#)
- [Email templates](#)
- [Self Service profile portal](#)
- [Self Service application suite pages](#), including self-registration, password reset, username recovery, and directory lookup

In the following example, Autocomplete text keys are translated into French.

The screenshot shows a web interface for managing content. At the top, there are two tabs: 'Text Keys' and 'Instance'. Under 'Text Keys', a dropdown menu is set to 'Autocomplete'. Under 'Instance', it shows 'TEST1 Instance'. Below this is a header for 'Content Management' with a sub-header: 'Edit the keys below to use the terminology and language translations you prefer'. The main content area has a table with columns 'Key Name' and 'Language'. The 'Language' column has a dropdown menu set to 'Français'. Below the table, there is a section titled 'Autocomplete' with five rows of text keys and their corresponding values in French:

Key Name	Language
services-col1Label	nomer
services-col2Label	description
users-col1Label	prénom
users-col2Label	Nom De Famille
users-col3Label	Adresse e-mail

Privacy Settings

The user is allowed to self-delete his account.

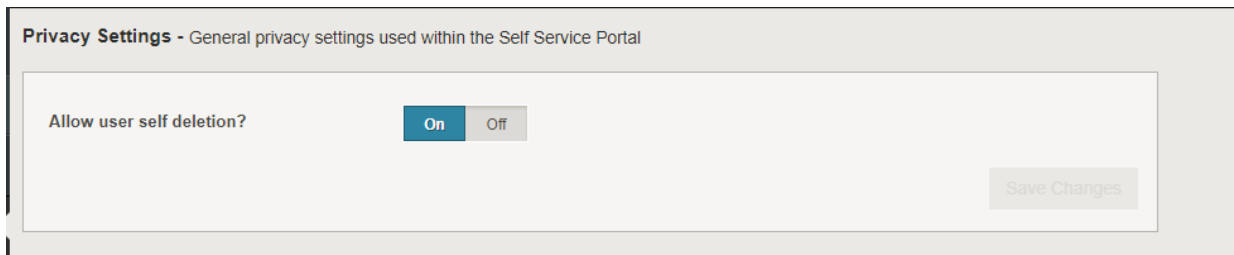
About this task

As per GDPR requirement, the user has right to self-delete his account. The user is displayed a 'Self Deletion Notice'. After the user agrees to the notice, the account is deleted.

It is mandatory to have at least one 'Self Deletion Notice' already setup in order to enable this Self Deletion flag. The enabling of this SelfDelete option is aborted if the user does not setup any 'Self Deletion Notice'. See [“Managing Notices” on page 84](#) for setting up notices.

Procedure

1. Click **Self Service > Privacy Settings** in the navigation menu.
2. Select **Allow user self deletion**.



3. Click **Save Changes** to save this selection option.

Managing Notices

The user can write or modify the notices.

About this task

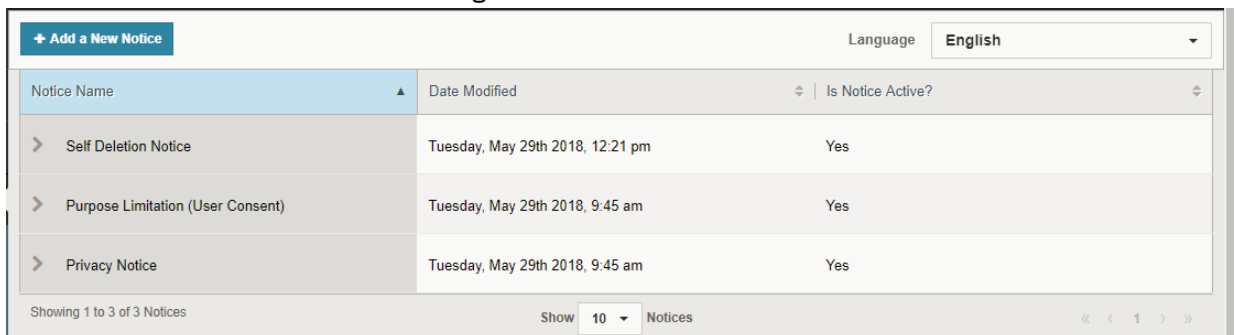
The user can create a new notice. The notice can be written in any of the listed languages. All notices are versioned so any update to the notice will generate a new version. All the previous versions are viewable to the user.

Three types of notices are provided:

1. Self deletion Notice
2. Purpose Limitation (User Consent)
3. Privacy Notice

Procedure

1. Click **Self Service > Notices** in the navigation menu.



2. Click **Add New Notice**.

Add A New Notice Language English X

Notification Type * Self Deletion Notice

Notification Verbiage *

Cancel Preview Notice

3. Select **Language** if other than English.
4. Select the **Notification Type**
5. Write the notice text in the **Notification Verbiage**.
6. Click **Preview Notice** to view the notice.
7. Click **Save Changes** to save this notice.

Modifying Notices

The user can modify the notice verbiage.

About this task

The user can modify the notice verbiage. For every modification, a new version is generated.

Procedure

1. Click **Self Service > Notices** in the navigation menu.
2. Select the notice to be modified.
3. Click **Modify Notice** and modify the notice text.
4. Click **Preview Notice** to view the notice.
5. Click **Add Notice**.

Viewing Notices

The user can view the previously created versioned notices.

About this task

The user can modify the notice verbiage. After modifying the notice, its is versioned and older one saves.

Procedure

1. Click **Self Service > Notices** in the navigation menu.
2. Click **View Previous Versions** to go through the older versioned notices.

Chapter 7. Applications



Applications management involves the management of network connections to company protected web resources, and to federated third-party web applications, and the management of user provisioning and services.

Managing services

A service provides extra features beyond features of a role or group. Generally, services are used to provide linkage between user identities and the systems external to Cloud Identity Service.

Services overview

Generally, services are used to provide linkage between user identities and the systems external to Cloud Identity Service to which users might need to be provisioned.

You can manage services, including service membership, by using Cloud Identity Service. Service membership can be managed manually or can be managed by using a dynamic provisioning policy. Each service must have a service owner. A service owner is a user who is typically defined as the owner or administrator of the external system to which the service is linked. Service categories can be used to group related services together to make it easier for Self Service users to manage their services.

The user membership of a service can be statically or dynamically defined. Static user membership requires you to manually add each user to the service, and to manually manage membership. Dynamic user membership automatically selects users for membership based on any matching combination of their identity attribute values, other group memberships, other service memberships, or whether they are assigned a role as a manager.

Dynamic user membership is implemented by using a dynamic provisioning policy, in which you define the membership selection criteria.

Any number of dynamic policies can be defined for a service. A policy can be applied on demand by reconciling the policy. A policy can also be applied according to a schedule. When a policy is applied, its selection criteria is evaluated, and the user membership is updated so that non-matching users are removed and matching users are added.

Services include options for creating dependencies between services, including parent and child relationships and container mappings. A parent and child relationship is used to enforce attaining membership in the parent service before attaining membership in any child services. Container mappings are used to define services that directly request a user's membership in each contained service when membership to the container is attained.

Notifications are used to send notification emails to various recipients. Notifications can include service-specific provisioning and deprovisioning information.

Recertification is used to provide control over who remains a member of a service over time. Recertification policies are defined in the same way as dynamic provisioning policies. Depending how the service is defined, any member that meets the criteria of a recertification policy has a recertification request sent to their manager, or the service owner, or both. The manager or service owner certifies whether the user still belongs to the service. Recertification can be required for policy-based service membership and manually controlled service membership. Recertification policies can be scheduled so that recertification occurs at a specified frequency.

Approvals are used to provide control over who can gain membership to a service. Approval can be required for dynamically controlled membership and manually controlled membership. Approval can

require action by a manager, a service owner, or both. Approvals can be applied to membership and recertification processes.

Searching for services

You can search for any service in your organization to view details of the service or to modify details of the service, and manage the membership of the service.

Procedure

1. Click **Applications** > **Services** in the navigation menu, and click **General**.
2. In the **Filter Results** field, enter at least the first 3 characters of the service. The field label changes to **Searching For**.

Services matching your search criteria are listed. Select a service to modify or view.

Searching for service categories

You can search for any service category to view or to modify details of the category, and to manage services that are grouped under the category.

Procedure

1. Click **Applications** > **Services** in the navigation menu, and click **Category Management**.
2. In the **Filter Results** field, enter at least the first 3 characters of the service category. The field label changes to **Searching For**.

Categories matching your search criteria are listed. Select a category to modify or view.

Creating services

You can add new services. After you add a service, you can select users to be members of the service by managing the service statically or dynamically.

Procedure

1. Click **Applications** > **Services** in the navigation menu, and click **Add Service**.
2. Enter a name, service owner, and description for the service.

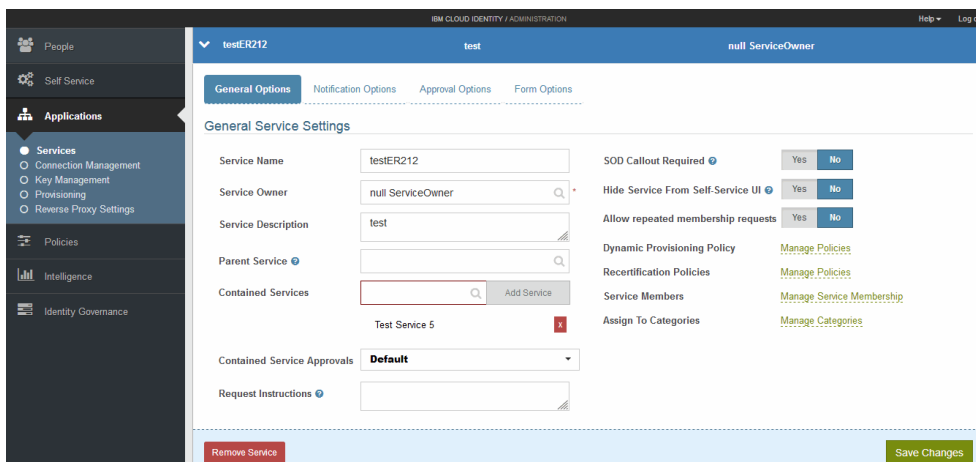
The service name must be unique. Check whether the service name is in use by clicking **Check Availability**.

To search for and select a user as the service owner, enter at least the first 3 digits of your search criteria in the **Service Owner** field. You can search for the first name, the last name, or the email address of the user. Select the user from the returned list.

3. Click **Save Changes** to add the service.

The service is saved. You are returned to the list of services.

4. Search for and select the service to enter **General Options**, **Notification Options**, **Approval Options**, and **Form Options**.



What to do next

After the service is created, you can add members to the service manually or dynamically, and you can create recertification policies.

Service settings

Service settings include general, notification, and approval options.

Setting	Description
Service Name	The service name.
Service Owner	The user name of the service owner.
Service Description	Description for the service.
Parent Service	Specifies whether membership of a parent service is required for membership of the service. Until membership of the parent service is acquired, users are ineligible for membership. To search for and select the parent service, enter at least the first 3 characters of the service name.
Contained Services	Specifies a contained service. Container mappings are used to define services that directly request a user's membership in each contained service when membership to the container is attained. To search for and select a contained service, enter at least the first 3 characters of the service name, select the service and click Add Service .
Request Instructions	Instructions to display to users when they request the service.
SOD Callout Required	Segregation/Separation of Duties. Specifies whether a workflow is required before the approval process is triggered to record service request approvals on an external system.
Hide Service From Self-Service UI	Specifies whether to show the service in the Self Service profile application.
Allow repeated membership requests	Specifies whether to allow repeated membership requests. <ul style="list-style-type: none"> • On. The service cannot contain permanent members. User membership automatically expires. Membership must be rerequested. • Off. User membership does not automatically expire.

Table 24. General options (continued)

Setting	Description
Dynamic Provisioning Policy	Manage policies. Manage the membership of the service by using dynamic provisioning policies.
Recertification Policies	Manage policies. Manage the recertification of the service by using recertification policies.
Service Members	Manage the membership of the service statically (manually).
Restrict requesting access	Specifies whether to restrict requesting access. <ul style="list-style-type: none"> • On. The service cannot be requested from self service. • Off. The service can be requested from self service.
Assign To Categories	<p>You can assign a service to one or more service categories. Service categories are used to group related services together, making it easier for users to manage their services in Self Service applications.</p> <p>Click Manage Categories to open the Assign Service to Categories window. To search for and select a category, enter at least the first 3 digits of the category name in the Category Name field. Select the category from the returned list, and click Add Category. Add the service to as many categories as you want, and click Done.</p>
Approval Process	<p>Specifies what should happen when the contained service gets processed.</p> <ul style="list-style-type: none"> • Default processing: All services should go through normal approval process. • Auto approve ALL services: All contained services should be considered approved. • Auto approve non-SOD enabled services only: All non-SOD enabled contained services should be considered approved. SOD enabled services should go through the normal SOD callout process. • Auto approve SOD enabled services only: All SOD enabled contained services should be considered approved. Non-SOD enabled services should go through the normal approval process.

Table 25. Notification options

Setting	Description
Recipient Type	Group, service, or user. Notification emails are sent to all the members of a group or service, or to a user. Notifications are sent on the occurrence of some event, for example, when a user is added to a service.
Recipient Name	The name of the group, service, or user to send the notifications to. To search for and select a group or service, enter at least the first 3 characters of the group or service name. Select the group or service from the returned list. To search for and select a user, enter at least the first 3 digits of your search criteria. You can search for the first name, the last name, or the email address of the user. Select the user from the returned list.
Provisioning Instructions	Instructions that must be followed by users when they are added into the service.

Table 25. Notification options (continued)

Setting	Description
Deprovisioning Instructions	Instructions that must be followed by users when they are removed from the service.
Notify members of assignment/revocation	Specifies whether a notification is sent to users when they are added to or removed from the service.
Notify managers of assignment/revocation	Specifies whether a notification is sent to the managers of users when users are added to or removed from the service.

Table 26. Approval and recertification options

Setting		Description
Approval Requirements	Delinquency Action	The action to take when a service approval request is not approved by the due date.
	Action Due Within	Number of days before the delinquency action is due.
	Manager Approval	<p>Specifies whether managers of users must grant approval before users can be given membership of the service.</p> <ul style="list-style-type: none"> • Dynamic <ul style="list-style-type: none"> – Checkbox is checked: When a dynamic policy is in operation, service request approval notification emails are automatically generated that notify the manager of pending service requests that they must manually approve. – Checkbox is cleared: Approvals are automatically made on behalf of the manager. • Request. Checkbox is checked: Requests are sent to the managers of users that request the service. Requests must be approved for users to be made members of the service.
	Service Owner	<p>Specifies whether service owners must grant approval before users can be given membership of the service.</p> <ul style="list-style-type: none"> • Dynamic <ul style="list-style-type: none"> – Checkbox is checked: When a dynamic policy is in operation, service request approval notification emails are automatically generated that notify the service owner of pending service requests that they must manually approve. – Checkbox is cleared: Approvals are automatically made on behalf of the service owner. • Request. Checkbox is checked: Requests are sent to the service owners of users that request the service. Requests must be approved for users to be made members of the service.

Table 26. Approval and recertification options (continued)

Setting		Description
Recertification Settings	Delinquency Action	The action to take when service membership is not recertified by the due date. The due date is the date set by the recertification schedule.
	Action Due Within	Number of days before the delinquency action is due.
	Manager Approval	Specifies whether managers of users must grant approval before users can be recertified. <ul style="list-style-type: none"> • Dynamic <ul style="list-style-type: none"> – Checkbox is checked: Recertification approval notification emails are automatically generated that notify the manager of pending recertification requests that they must manually approve. – Checkbox is cleared: Approvals are automatically made on behalf of the manager. • Request. Checkbox is checked: Requests are sent to the manager. Requests must be approved for users to be recertified.
	Service Owner	Specifies whether the service owner must grant approval before users can be recertified. <ul style="list-style-type: none"> • Dynamic <ul style="list-style-type: none"> – Checkbox is checked: Recertification approval notification emails are automatically generated that notify the service owner of pending recertification requests that they must manually approve. – Checkbox is cleared: Approvals are automatically made on behalf of the service owner. • Request. Checkbox is checked: Requests are sent to the service owner. Requests must be approved for users to be recertified.

Configuring service forms

Users or service owners must complete a form when they request or revoke service access. Each form contains a number of fields that users or service owners must complete when they request or revoke service access. You can reorder the fields and sections, add new sections, and add or remove fields.

Procedure

1. Click **Edit Form** for the form you want to edit, you can edit the following forms:
 - **Request Access Form.** Completed by a user when the user requests access to the service.
 - **Revoke Access Form.** Completed by a service owner when the service owner wants to remove a user's access to the service.



2. Add a field:

- a) Click **Add New > Add New Field**.
- b) Select the attribute and field options to define the field.
- c) Click **Save Changes** to add the field.

3. Add a section:

- a) Click **Add New > Add New Section**.
- b) Enter a **Label**, **Subheading**, and **Header** for the section.
The label, subheading, and header are used to identify the section on the form.
- c) Click **Add New Field** to enter a new field in the section, select the attribute and field options to define the field.
- d) Click **Save Changes** to save the new section.

You can add more fields to the section from the main **Form Setup** window.

4. To change the order of a form and move a section or field to a new position, click and drag the field or section to the new position.



5. Click **Save Changes** to save the form.

Form options

Form options are used to set the properties of fields that are used in Self Service applications.

Depending on the form that is defined, some options might not be available.

<i>Table 27. Form field options</i>	
Option	Description
LDAP attribute	LDAP attribute to be used as a field. If an attribute is selected that requires another user to be entered as a value, a search tool is added to the field. For example, a manager attribute might require another user to be entered. Depending on the field or form that is defined, some attributes cannot be selected.
Default Value	A default value for the field. If the field is editable, users can replace the default value.

Table 27. Form field options (continued)

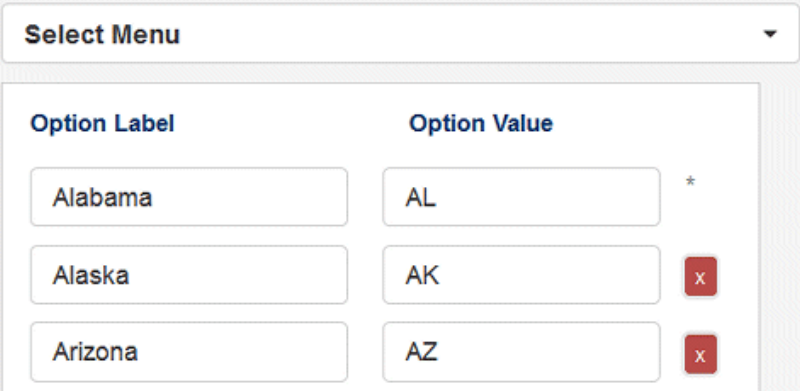
Option	Description
Field Label	Label that is used to identify the field.
Field Type	<ul style="list-style-type: none"> • Checkboxes. Users can select one or more options as input for the field. • Password Field. Password fields are masked. • Radio Buttons. Users can select one option from a number of options as input for the field. • Select Menu. Users can select one option from a number of options as input for the field. • Text Field. Users input a value in to the field as entered text. • Text Area. Freeform text box. <p>For Checkboxes, Radio Buttons, and Select Menu, add the options for the field.</p> <ul style="list-style-type: none"> • Option Label. Label that is used to identify the option. • Option Value. Value of the option. <p>In this example, a select menu has a number of options for different states.</p> 
Placeholder	Placeholder label.
Tool Tip	Field help text.
Editable	<ul style="list-style-type: none"> • Yes. Users can enter a value in the field. • No. Users cannot enter a value in the field. Some fields are populated with existing data. For example, during self-registration a user might claim an account against an existing identity record in which case a field value can be used from the identity record.
Required	<ul style="list-style-type: none"> • Yes. The field is mandatory. <ul style="list-style-type: none"> – Self-registration form. Users cannot complete self-registration without providing a value for the field. – Self Service profile form. Users are prompted to enter values for any unpopulated mandatory fields. • No. The field is optional.

Table 27. Form field options (continued)

Option	Description
Require current password match	<p>Only for a password LDAP attribute.</p> <ul style="list-style-type: none"> • Yes. Users must enter the password twice, in separate fields. The value that they enter in each field must match to confirm that the password is correct. • No. The password is entered once, in one field only.
Masked	<p>Yes. The field is masked, and the value that is entered cannot be seen on the screen. Each character that is entered is replaced on-screen by an asterisk character.</p>
Require a matching field	<ul style="list-style-type: none"> • Yes. Users must enter the value twice, in separate fields. The value that they enter in each field must match to confirm that the value is correct. For example, when a user enters an email address, you can require them to enter the address twice. • No. The value is entered once, in one field only.
Validation	<p>Validation rules:</p> <ul style="list-style-type: none"> • Yes. The value that is entered must pass specified validation rules. For example, a date might have to pass a format validation rule such as mm/dd/yyyy. • No. Entered values are unvalidated. <p>Validation types:</p> <ul style="list-style-type: none"> • Date. Values must conform to a specified date format. For example, mm/dd/yyyy. • Email Address. Values must correspond to email address formats. For example, <i>text_string@text_string.com</i>. • Letters. Values must contain only alphabetic characters. • Maximum Character Length. Values cannot contain more than a specified number of characters. • Minimum Character Length. Values cannot contain less than a specified number of characters. • Number. Values must contain only numeric characters. • Password Strength. A password field must conform to basic, standard, or strong validation rules. Rules are based on the number and type of characters that must be entered. • US Phone Number. Values must conform to US phone number format. <p>Custom regular expressions. A regular expression that is evaluated against the value entered. If the expression evaluates to true, the value is valid.</p> <ul style="list-style-type: none"> • Pattern. A regular expression. For example, to restrict registrations to addresses in North Carolina use the regular expression <code>^NC\$</code> for the state attribute, where NC is defined as an optional value for the state attribute. • Error Message. Error message to display to users when an entered value is invalid.

Option	Description
Label	Section label.
Subheading	Subheading label.
Header	Header.

Creating service categories

You can create service categories to group related services together. Service groups make it easier for users to manage their services in Self Service applications.

Procedure

1. Click **Applications** > **Services** in the navigation menu, and click **Category Management** and **Add a New Category**.
2. Enter a name and description for the category. The category name must be unique.
3. Click **Check Availability** to check whether the category name is available or not
4. Click **Add Category** to add the service category.
The category is saved. You are returned to the list of service categories.
5. Search for and select the category to add services to the category.
6. Click **Manage Services** to open the **Assign Services to Category** window.

To search for and select a service, enter at least the first 3 digits of the service name in the **Service Name** field. Select the service from the returned list, and click **Add Service**.

Add all the services that you want, and click **Done**.

Managing the membership of a service statically

A statically defined user membership requires you to manually add and remove each user member.

Procedure

1. Search for and select the service that you want to add members to.
2. Click **Manage Service Membership**.

Manage Service Membership

Add Service Membership

First Name	Last Name	Email
Paul	Smith	psmith@company.com

3. In the **User Name** field, search for the user you want to add. To search for a user, enter the first 3 characters of the given name, surname, user name, or email address of the user.
4. Select the user and click **Add Membership**.
5. After you add all the users that you want, click **Done**.

Managing the membership of services dynamically

Dynamic provisioning policies allow the user membership of a service to be based on matching criteria. Users matching the criteria are automatically selected for membership of the service.

Creating dynamic provisioning policies

Dynamic provisioning policies are used to determine the user membership of a service.

About this task

Membership is based on the selection criteria of the policy. For example, you might specify the membership of a service by an attribute that determines work location, or by an attribute that determines work location and membership of a group. A service can have one or more policies.

Procedure

1. Search for and select the service that you want to add the policy to.
2. For **Dynamic Provisioning Policy**, click **Manage Policy**.
3. Click **Add New Policy**.

Manage Policies

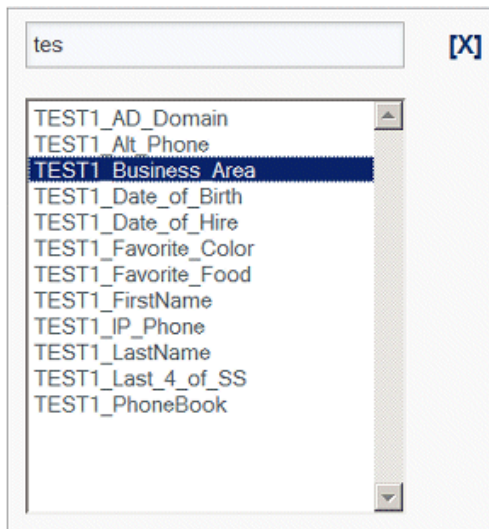
Delete	Variable	Operator	Value	Conjunction	Move
	Select Variable...				

4. Enter a meaningful name for the policy in the **Policy Name** field.
5. Select the variables that you want to use, you can select one or more variables of any type to use in your policy.

You can select any combination of the following variable types:

- **Attribute**. Include users based on a user identity attribute.
- **Group**. Include or exclude users based on group memberships.
- **Service**. Include or exclude users based on other service memberships.

- **Manager.** Include users based on whether they are assigned the role of manager.
- To use a user identity attribute as a variable:
 - Click **Select Variable**, and click **Attribute**.
 - Click in the **Filter Attributes** field, and enter the first few characters of the attribute. Double-click the attribute to select it.



- Select an **Operator** and enter a **Value** for the attribute.




Note: You can use wildcards. For example, 11* can be entered to represent any number beginning with 11.

Tip: If you want an attribute and attribute value to be treated as a time stamp, you can prefix the value with \$date\$. This prefix assumes the default date format of yyyy-MM-dd HH:mm:ss. For example, you might enter \$date\$1970-01-01 00:00:00 to represent 1 January 1970 at midnight.

You can also specify a non-default format for the time stamp by including the format in the \$date \$ prefix by using SimpleDateFormat. For example, for a Z-timestamp you might enter \$date{yyyy-MM-dd HH:mm:ssZ}\$1970-01-01 00:00:00-0400 to represent 1 Jan 1970 at midnight in the time zone 4 hours earlier than GMT/UTC. Changing the default format causes the same format to be applied to the attribute values that are retrieved. You must understand the format of the values that you want to retrieve and that they are consistent with the format you want to use. For more information on different format patterns, see [SimpleDateFormat](#).

If either the value specified in the rule or the value it is compared with are not parsed without exception, then a warning or error is logged. For more information, contact your IBM support representative. Coordinated Universal Time (UTC) is the default time zone.

- To use membership or non-membership of a group as a variable:
 - Click **Select Variable**, and click **Group**.
 - Click in the **Filter Groups** field, and enter the first few characters of the group. Double-click the group to select it.
 - Select if membership is contingent on membership of this group, or if membership is contingent on non-membership of this other group.

Delete	Variable	Operator	Value
		<input type="text" value="Member Of Group"/> <ul style="list-style-type: none"> Member Of Group Member Of Group Not Member Of Group 	test_group1


8. To use membership or non-membership of another service as a variable:
 - a) Click **Select Variable**, and click **Service**.
 - b) Click in the **Filter Services** field, and enter the first few characters of the service. Double-click the service to select it.
 - c) Select if membership is contingent on membership of this other service, or if membership is contingent on non-membership of this other service.
9. To use the manager role as a variable:
 - a) Click **Select Variable**, and click **Manager**.

Manager Search ✕

Login Name	<input type="text" value="joh*"/>
First Name	<input type="text"/>
Last Name	<input type="text"/>
Email	<input type="text"/>
TEST1_PhoneBook	<input type="text"/>

- b) Search for the user in the **Manager Search** window by entering search criteria in any of the fields. Click **Search**.
Only users that are assigned the role of manager and that match your search criteria are returned.
Note: You can use wildcards in your search. For example, you might enter Joh* to represent names that begin with Joh.
 - c) Select the user.
You can repeat the search to add more users.
10. Use the **Conjunction** field to combine one or more variables to determine the membership of the service. Use a conjunction value of And or Or to combine the result of one comparison criteria with the next row.

The grouping of variables (conditions) is from top to bottom, so that the result of previous conditions is joined with the subsequent condition.

Use the arrow icons to move conditions up and down .

In the following example, only one variable is used to determine membership: the user identity attribute TEST1_Business_Area. To be a member, a user must have a value of London W4 for the attribute TEST1_Business_Area.

Delete	Variable	Operator	Value	Conjunction
	TEST1_Business_Area	=	London W4	-- Select

In the following example, two variables are used to determine membership. To be a member, a user must have a value of London W4 for the attribute TEST1_Business_Area, and must be a member of Group1.

Delete	Variable	Operator	Value	Conjunction
	TEST1_Business_Area	=	London W4	And
		Member Of Group	Group1	-- Select

In the following example, three variables are used to determine membership. To be a member, a user must have a value of London W4 for the attribute TEST1_Business_Area, and must be a member of Group1 or be a member of Group2.

Delete	Variable	Operator	Value	Conjunction
	TEST1_Business_Area	=	London W4	And
		Member Of Group	Group1	Or
		Member Of Group	Group2	-- Select

11. After all the conditions you want in the policy are defined, click **Save**.

What to do next

[Simulate the policy](#) to check membership meets your expectations.

Creating dynamic provisioning policies in expert mode

In some cases, the policy selection criteria for a service cannot be determined by using basic attribute comparison and other service or group membership. Membership might require the examination of attribute values (substrings) that vary based on the value of another attribute. In these cases, you must define the policy in expert mode.

Before you begin

To use expert mode, you must have good knowledge and fluency in coding in JavaScript.

About this task

You define policies in expert mode in JavaScript.

During policy evaluation, the JavaScript is run one time for each user in the registry. The JavaScript examines the registry attributes of the user and their memberships, and decides whether the user is to be included in the service. The JavaScript communicates this decision to Cloud Identity Service with a variable **inGroup**. If the result of the JavaScript is that **inGroup** equals TRUE, then the user is included in the service, otherwise the user is not included.

The JavaScript can use three methods to obtain Cloud Identity Service registry attributes, and group information about each user.

- `String isMemberOfGroup(String groupName)`
- `String[] getAttributeValues(String attributeName)`
- `String evaluateAttribute(String attributeName, int operator, String constant)`

Each of these methods can be invoked with another variable **ldap** that is available to the JavaScript. For example, to determine whether the current user is a member of a group that is named **accounting**, the following statement can be used:

```
var isAccountant = ldap.isMemberOfGroup("accounting");
```

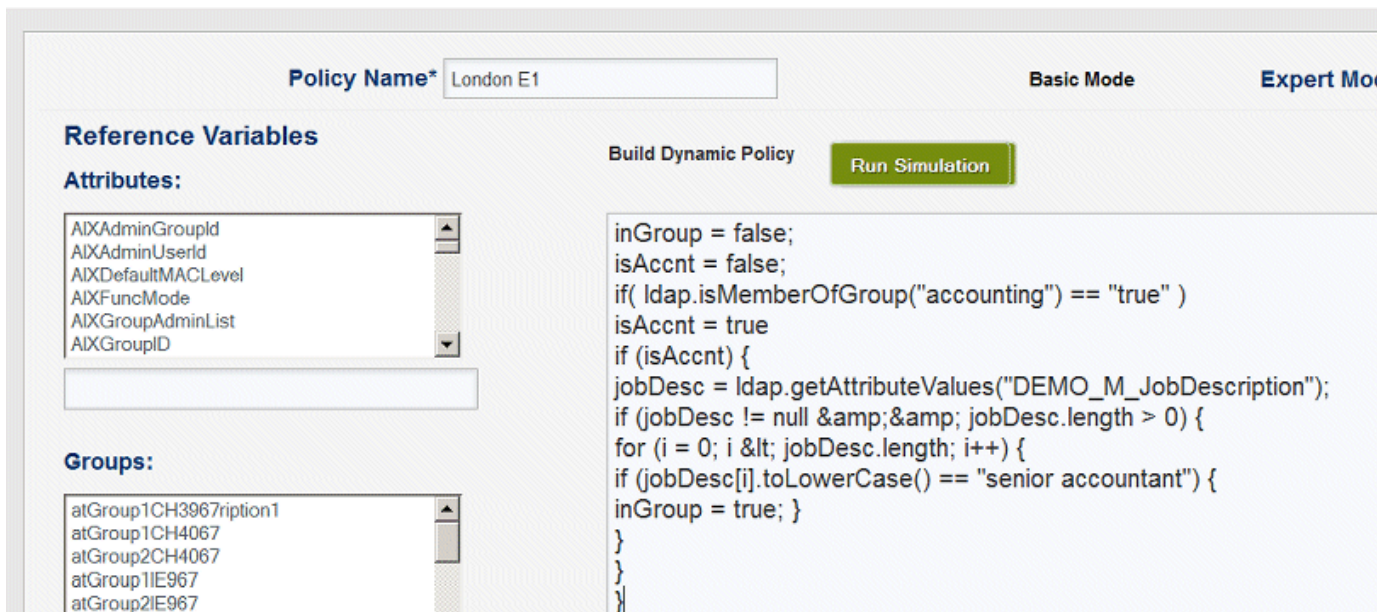
In the following JavaScript example the user is included in the policy if the user is both a member of the **accounting** group, and has the value **senior accountant** in the attribute **DEMO_M_JobDescription**.

```
// assume user is not in group
inGroup = false;
isAcct = false;
if( ldap.isMemberOfGroup("accounting") == "true" )
isAcct = true
if (isAcct) {
jobDesc = ldap.getAttributeValues("DEMO_M_JobDescription");
if (jobDesc != null && jobDesc.length > 0) {
for (i = 0; i < jobDesc.length; i++) {
if (jobDesc[i].toLowerCase() == "senior accountant") {
inGroup = true; }
}
}
}
```

Procedure

1. [Search for and select](#) the service that you want to add the policy to.
2. For **Dynamic Provisioning Policy**, click **Manage Policy**.
3. Click **Add New Policy**.
4. Click **Expert Mode**.





5. Enter the JavaScript you want to use to determine membership.

Attributes, **Groups**, and **Services** are listed in their respective boxes for your reference. You can search for an attribute, group, or service by entering the first few characters in the filter field below the appropriate box. You can copy and paste a selected attribute, group, or service.

6. After all the conditions to use in your policy are defined, click **Save** to save the policy.

What to do next

Simulate the policy to check membership meets your expectations.

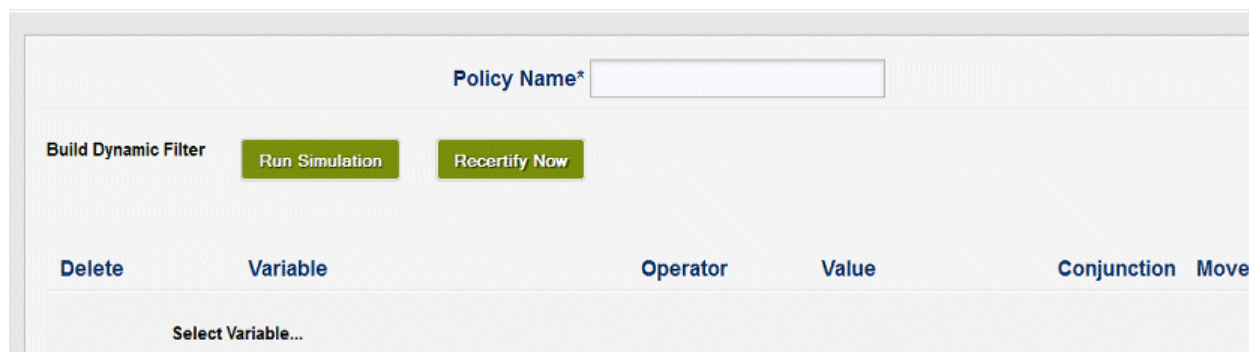
Creating recertification policies

Recertification policies are used to determine which users remain members of a service. Recertification policies are defined in the same way as dynamic provisioning policies. Continued membership is based on user identity attribute values, other group memberships, other service memberships, and the manager role. A service can have one or more recertification policies.

Procedure

1. Search for and select the service that you want to add the recertification policy to.
2. For **Recertification Policies**, click **Manage Policy**.
3. Click **Add New Policy**.

Manage Policies



4. Enter a meaningful name for the policy in the **Policy Name** field.

5. Select the variables that you want to use, you can select one or more variables of any type to use in your policy.

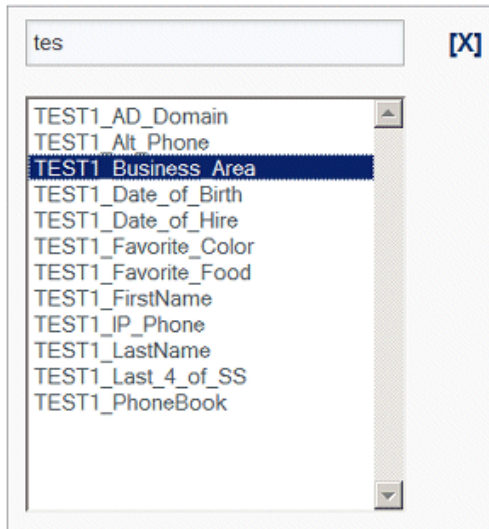
You can select any combination of the following variable types:

- **Attribute.** Include users based on a user identity attribute.
- **Group.** Include or exclude users based on other group memberships.
- **Service.** Include or exclude users based on other service memberships.
- **Manager.** Include users based on whether they are assigned the role of manager.

6. To use a user identity attribute as a variable:

a) Click **Select Variable**, and click **Attribute**.

b) Click in the **Filter Attributes** field, and enter the first few characters of the attribute. Double-click the attribute to select it.



c) Select an **Operator** and enter a **Value** for the attribute.



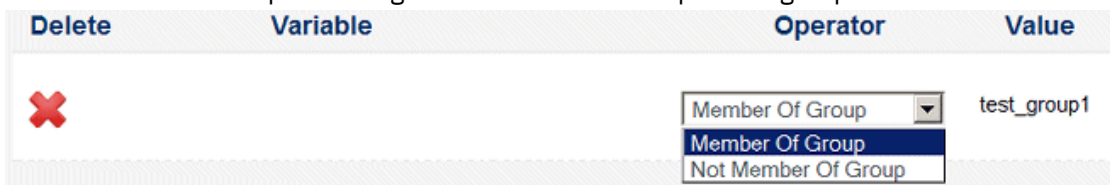
Note: You can use wildcards. For example, 11* can be entered to represent any number beginning with 11.

7. To use membership or non-membership of a group as a variable:

a) Click **Select Variable**, and click **Group**.

b) Click in the **Filter Groups** field, and enter the first few characters of the group. Double-click the group to select it.

c) Select whether continued membership is contingent on membership of this group, or whether continued membership is contingent on non-membership of this group.





8. To use membership or non-membership of another service as a variable:

a) Click **Select Variable**, and click **Service**.


- b) Click in the **Filter Services** field, and enter the first few characters of the service. Double-click the service to select it.
 - c) Select whether continued membership is contingent on membership of this other service, or whether continued membership is contingent on non-membership of this other service.
9. To use the manager role as a variable:
- a) Click **Select Variable**, and click **Manager**.

- b) Search for the user in the **Manager Search** window by entering search criteria in any of the fields. Click **Search**.
Only users that are assigned the role of manager and that match your search criteria are returned.
Note: You can use wildcards in your search. For example, you might enter Joh* to represent names that begin with Joh.
 - c) Select the user.
You can repeat the search to add more users.
10. Use the **Conjunction** field to combine one or more variables to determine the continued membership of the service. Use a conjunction value of And or Or to combine the result of one comparison criteria with the next row.

The grouping of variables (conditions) is from top to bottom, so that the result of previous conditions is joined with the subsequent condition.

Use the arrow icons to move conditions up and down  .

In the following example, only one variable is used to determine continued membership: the user identity attribute TEST1_Business_Area. To be a member, a user must have a value of London W4 for the attribute TEST1_Business_Area.

Delete	Variable	Operator	Value	Conjunction
	TEST1_Business_Area	=	London W4	-- Select

In the following example, two variables are used to determine continued membership. To be a member, a user must have a value of London W4 for the attribute TEST1_Business_Area, and must be a member of Group1.

Delete	Variable	Operator	Value	Conjunction
<input type="checkbox"/>	TEST1_Business_Area	=	London W4	And
<input type="checkbox"/>		Member Of Group	Group1	-- Select

In the following example, three variables are used to determine continued membership. To be a member, a user must have a value of London W4 for the attribute TEST1_Business_Area, and must be a member of Group1 or be a member of Group2.

Delete	Variable	Operator	Value	Conjunction
<input type="checkbox"/>	TEST1_Business_Area	=	London W4	And
<input type="checkbox"/>		Member Of Group	Group1	Or
<input type="checkbox"/>		Member Of Group	Group2	-- Select

11. After all the conditions you want in the policy are defined, click **Save**.

What to do next

Simulate the policy to check whether continued membership meets your expectations.

Simulating a policy

You simulate a policy to evaluate the user membership of a service to check whether the membership meets your expectations. You can simulate dynamic provisioning policies and recertification policies. The simulation does not change the membership of the service. It shows you which users comprise the proposed membership of the service. Results can be viewed and saved as a CSV file.

Procedure

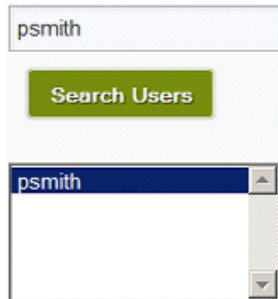
1. If you do not have the policy selected, [search for and select](#) the service. Open the **Manage Policies** window to edit the policy.
2. Click **Run Simulation**.

Manage Policies

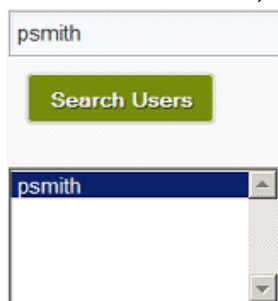
Policy Name*

3. Select a simulation type to run.

- Dynamic provisioning policies.
 - **Simulate all users in the directory.** This option compares the policy selection to all users in Cloud Identity Service. Users that satisfy the policy are listed in the results as either being added or retained. Users that do not satisfy the policy are listed in the results as either removed from the service or not added.
 - **Simulate all users currently in the group.** This option compares the policy selection criteria against the attributes of all users that are currently in the service. Each user in the service is listed in the results as either removed or retained. No new users are listed as added.
 - **Simulate a single user.** This option compares the policy selection criteria against a selected user. That user is listed in the results as either retained, removed, added or not added. Search for the user by using their user name. Enter the first few characters of the user name in the **Filter Users** field, click **Search Users**, and select the user.



- Recertification policies.
 - **Simulate all current service members.** This option compares the policy selection criteria against the attributes of all users that are currently in the service. Each user in the service is listed in the results as either included or excluded. No new users are listed as added.
 - **Simulate a single service member.** This option compares the policy selection criteria against a selected user. That user is listed in the results as either included, excluded, added or not added. Search for the user by using their user name. Enter the first few characters of the user name in the **Filter Users** field, click **Search Users**, and select the user.

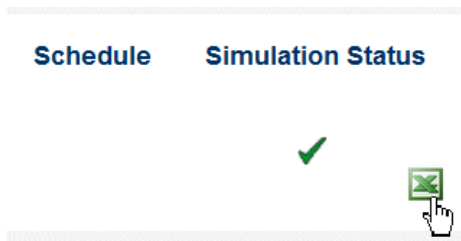


4. Click **Run Simulation**.


- The results for a single user provisioning policy simulation are displayed in the **Simulate Provisioning Policy** window.
- The results for a single user recertification policy simulation are displayed in the **Simulate Recertification Policy** window.

Close the **Simulate Policy** window to return to the **Manage Policies** window, and click **Cancel**.

5. Click **Refresh** in the **Manage Policies** window to view the results of simulations. When the simulation is complete, a check mark icon and a link to a CSV file are displayed.



6. View the results.

- Click the check mark icon  to open the **Simulation Results** window. You can select which results columns to view by clearing or checking the column header check boxes. Close the **Simulation Results** window to return to the **Manage Policies** window.

Note: Clicking **Clear Simulation Results** clears all the results from the **Simulation Results** window and the **Manage Policies** window.

- Click the CSV icon  to view the results in a CSV file. You can open the file or save the file.

What to do next

- For a dynamic provisioning policy, reconcile the policy and activate the policy.
- For a recertification policy, recertify the policy and activate the policy.

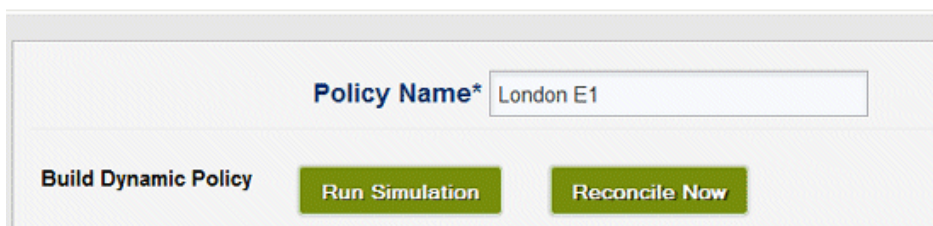
Reconciling a dynamic policy

After a policy is created, the policy can be reconciled. When a policy is reconciled, user membership for the service is implemented according to the policy selection criteria.

Procedure

1. Search for and select the service. Open the **Manage Policies** window to edit the policy.
2. Click **Reconcile Now**.

Manage Policies



A warning message is displayed. Click **OK** to reconcile the policy.

What to do next



Activate the policy.

Activating and scheduling a dynamic policy

After a policy is created, simulated, and the simulation results validated, the policy is ready to be activated and scheduled. An activated policy runs on a schedule, so that the membership of a service is evaluated and updated every time that the schedule is run.

Procedure

1. If you do not have the policy selected, search for and select the service. Open the **Manage Policies** window to edit the policy.
2. Select **Select Active** for the policy you want to activate.

Delete	Edit	Select Active	Policy Name
		<input checked="" type="radio"/>	London W4

A warning message is displayed. Click **OK** to activate the policy.

- Click the schedule icon  to open the **Dynamic Provisioning Policy Scheduler** window.

Dynamic Provisioning Policy Scheduler ✕

Enable Automatic Provisioning Schedule

Select one of the following scheduling frequencies:

Time of Day (applies to all selections): :

Once a day

Once a week

Once a month

Last day of the month

Select day(s)

- Sunday
- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday

Save

- Check the **Enable Automatic Provisioning Schedule** check box.
- Choose the frequency with which to run the schedule:
 - Once a day.** Select the **Time of Day**.
 - Once a week.** Select the day from the drop-down list, and select the **Time of Day**.
 - Once a month.** Select the day of the month from the drop-down list, and select the **Time of Day**.
 - Last day of the month.** Select the **Time of Day**.
 - Select days.** Check the check boxes for the days to run the schedule, and select the **Time of Day**.
- Click **Save**.

Recertifying a policy

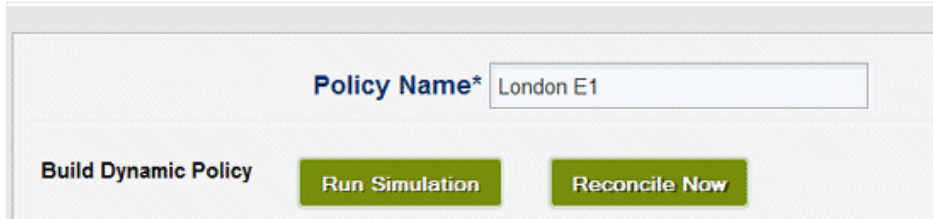
After a recertification policy is created, the policy can be recertified. When a policy is recertified, user membership for the service is implemented according to the recertification policy selection criteria.

Running a reconciliation immediately generates recertification approval requests that cannot be retracted.

Procedure

1. Search for and select the service. Open the **Manage Policies** window to edit the policy.
2. Click **Recertify Now**.

Manage Policies



The screenshot shows a window titled "Manage Policies". At the top, there is a label "Policy Name*" followed by a text input field containing "London E1". Below this, there are three buttons: "Build Dynamic Policy" (a text button), "Run Simulation" (a green button), and "Reconcile Now" (a green button).

A warning message is displayed.

3. Click **OK** to recertify the policy.

What to do next

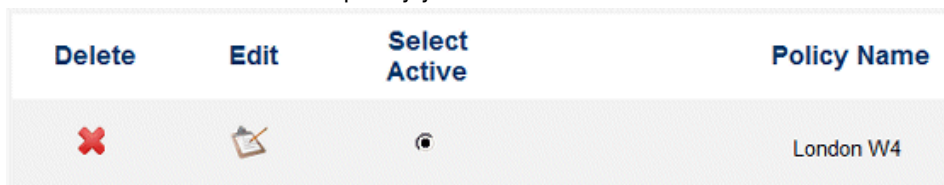
Activate the policy.

Activating and scheduling a recertification policy

After a policy is created, simulated, and the simulation results validated, the policy is ready to be activated and scheduled. An activated policy runs on a schedule, so that recertification of the service is requested for users every time that the schedule is run.


Procedure

1. If you do not have the policy selected, search for and select the service. Open the **Manage Policies** window to edit the policy.
2. Select **Select Active** for the policy you want to activate.



The screenshot shows a table with four columns: "Delete", "Edit", "Select Active", and "Policy Name". The "Delete" column contains a red 'X' icon. The "Edit" column contains a pencil icon. The "Select Active" column contains a radio button. The "Policy Name" column contains the text "London W4".

A warning message is displayed. Click **OK** to activate the policy.

3. Click the schedule icon  to open the **Recertification Schedule** window.

4. Check the **Enable Scheduled Execution** check box.
5. Select the time of day to run the policy in **Daily Start Time**.
6. Select the schedule type:
 - **Static Schedule.**
 - a. Select the date that the policy starts in **Start Date**. Dates are entered in MM/DD/YYYY format.
 - b. Select the frequency with which the policy is run from **Repetition Interval**.
 - **Rolling Schedule.**
 - a. Enter the interval frequency in days in **Repetition Interval**. The policy is run every number of days you enter, starting from the first interval. For example, if you enter 30, the policy is run in 30 days from today, and then 60 days, and then 90 days, and so on.
7. Click **Save Changes**.

Managing web access

Managing web access involves the management of network connections to protected web resources within your company.

Web access overview

You manage web access by creating and managing network connections to protected web resources. You also control access to protected resources by creating authorization policies. Authorization policies include Access Control Lists (ACLs), Protected Object Policies (POPs), and a global user policy.

Protected resources

Protected resources are web applications and servers that you want to secure behind Cloud Identity Service. Common examples of protected resources include web portals, Java™ Platform, Enterprise Edition application servers, Microsoft .NET web applications that run on IIS, and static HTML content servers.

After a user is authenticated, requests from that user will pass through the Cloud Identity Service to your protected resources. Each request is inspected by Cloud Identity Service and compared against your authorization policies. Factors such as role, group, and service membership, time of day, and network IP, can all play a part in whether a user is authorized to access a resource or perform a transaction.

You use the Web Applications interface to define and manage connections to client application servers. You also manage the policies that are attached to connections and path (protected) objects that make up the connection object space on each client application server.

Authorization policies

Access Control Lists (ACLs) define who can access which protected resources and what they can do with resources they have access to. Protected Object Policies (POPs) qualify access to resources by stipulating time-of-day constraints, and by stipulating constraints on ranges of IP addresses. A policy is enforced by attaching the policy to a junction or path object. When a policy is attached to a connection, the policy is applied to the connection and all child objects. An inherited policy is overridden if other policies are attached at a lower level.

Searching for web application connections

You can search for network connections to protected web applications to view, modify, or remove the connection.

Procedure

1. In the navigation pane, click **Applications > Connection Management**, and click **Web Applications**.
2. In the **Search** field, enter at least the first 3 characters of the connection.

The field label changes to **Searching For**.

Connections matching your search criteria are listed. Select a connection to modify or view.

Creating web connections

A connection represents the logical connection from a Cloud Identity Service web-proxy server to endpoints on a client application server or servers. Multiple server connections can be added to a connection.

Procedure

1. Click **Applications > Connection Management** in the navigation menu, and click **Web Applications**.

2. Enter the connection name and other [basic connection settings](#).
3. Enter settings for a [default connection server](#).
You can add [more server connections](#).
4. Click **Add Connection**.
5. Optional: Enter [optional settings](#).
6. Optional: Select or add an [ACL \(Access Control List\)](#).
7. Optional: Select or add a [POP \(Protected Object Policy\)](#).
8. Optional: Create [protected objects](#).
9. Click **Save**.

Connection settings

Connection settings include the connection type and name, server host information, and optional settings.

Basic settings

<i>Table 29. Basic connection settings</i>	
Setting	Description
Connection Name	The name of the connection. The name of the connection determines the URL path that is used to access the application server that is connected by the connection. For example, if the connection is called webapp_1 then the URL for the root of the application server is <code>https://client_Cloud_Identity_Service_address/webapp_1/</code> .
Description	Connection description.
Type	Connection protocol, TCP, or SSL.

Table 29. Basic connection settings (continued)

Setting	Description
Virtual Connection	<p>Virtual connections communicate with virtual hosts. HTTP Host headers are used in client requests to direct those requests to the appropriate location on connected servers.</p> <p>A user can access resources directly with the host name of the connected server (<code>http://protected-server/resource</code>), rather than indirectly with the host name of the WebSEAL server and a potentially modified resource path (<code>http://webseal/connection/resource</code>). Direct access to the resource by using the host name of the connected server does not require URL filtering.</p>
Connection Servers	<p>Not used when you create a new connection. The server addresses, paths, and ports to be set up for the connection. Click Add Server to add a server connection. For more information about adding a server, see “Adding a connection server” on page 121.</p>

Connection policies and rules

Table 30. Connection access policies and rules

Setting	Description
Access Control List (ACL)	<p>Restrict access to the resource by an ACL. Select Add a new list from the list to create an ACL, see “Creating Access Control Lists” on page 126.</p>
Protected Object Policy (POP)	<p>Restrict access to the resource by a POP. Select Add a new policy from the list to add a POP, see “Creating Protected Object Policies” on page 123.</p>

Connection object space

The connection object space represents the logical paths to protected objects below the connection. For example, paths to directories, files, programs, or locations. You can add as many protected objects to a connection as you need.

Table 31. Connection object space

Setting	Description
Object Name	<p>Object name. The protected object must be named after the object it represents. For example, if the object represents a page that is called <code>page1.jsp</code> that is at the root of the junction, then the path object must be created with the name <code>page1.jsp</code>.</p>
ACL	<p>The ACL applied to the object.</p>
POP	<p>The POP applied to the connection.</p>
Children	<p>Child objects.</p>

Optional settings

<i>Table 32. Optional settings</i>	
Setting	Description
Stateful Connection	Specifies that the connection supports stateful applications. By default, connections are not stateful.
Boolean Rule	Allows denied requests and failure reason information from authorization rules to be sent in the Boolean Rule header (AM_AZN_FAILURE) across the connection.
Thread Limit	Defines the soft and hard limits for consumption of worker threads.
HTTP Basic Authentication Header	<p>Defines how the WebSEAL reverse proxy server passes client identity information in HTTP basic authentication (BA) headers to the web application servers. Options for handling client identity information.</p> <ul style="list-style-type: none"> • Filter. Default option. This option is used when WebSEAL authentication is set to use BA header information. <ul style="list-style-type: none"> The WebSEAL BA header is used for all subsequent HTTP transactions. To the back-end server, WebSEAL appears logged on always. WebSEAL authentication that uses a client certificate is allowed with this option. If the back-end server requires actual client identity (from the browser), the CGI variables HTTP_IV_USER, HTTP_IV_GROUP, and HTTP_IV_CREDS can be used. For scripts and servlets, use the corresponding Cloud Identity Service specific HTTP headers. <ul style="list-style-type: none"> – iv-user – iv-groups – iv-creds • Ignore. WebSEAL authentication that uses a BA header is not allowed with this option. This option uses the BA header for the original client user name and password. <ul style="list-style-type: none"> WebSEAL authentication that uses a client certificate is allowed with this option. • Supply. WebSEAL authentication that uses a BA header is not allowed with this option. This option uses the BA header for the original client user name and a dummy password. <ul style="list-style-type: none"> WebSEAL authentication that uses a client certificate is allowed with this option.

Table 32. Optional settings (continued)

Setting	Description
<p>Client Headers</p>	<p>Client headers insert client user identity information specific to Cloud Identity Service in HTTP headers across the host connection. The header types can include any combination of the following HTTP header types.</p> <ul style="list-style-type: none"> • Default headers. <ul style="list-style-type: none"> – Short user names. Inserts the user login name into an HTTP header that is called iv-user and adds it to all back-end requests to the connection hosts. – Long user names. Inserts the Cloud Identity Service user Distinguished Name into an HTTP header that is called iv-user-l and adds it to all back-end requests to the connection hosts. – Group names. Inserts a comma-separated list of the groups the user belongs to in an HTTP header that is called iv-groups and adds it to all back-end requests to the connection hosts. – User credentials. Inserts the Cloud Identity Service user credential in a Base64 encoded string in an HTTP header that is called iv-creds. Adds it to all back-end requests to the connection hosts. – Insert client IP Address. Inserts the user IP address into an HTTP header that is called iv-remote-address and adds it to all back-end requests to the connection hosts. • Custom headers. <ul style="list-style-type: none"> – Custom attributes must be configured and enabled for your setup of Cloud Identity Service for custom headers to be available. Inserts the attribute that is selected into an HTTP header. A name for the header must be entered.
<p>HTTP Header Encoding</p>	<p>Specifies the encoding to use when HTTP headers are generated to send to connection hosts. This encoding prevents any potential data loss that might occur when converted to a non-UTF-8 code page. Possible values for encoding.</p> <ul style="list-style-type: none"> • UTF-8 Binary. Unencoded UTF-8 data. This setting allows data to be transmitted without data loss, and the customer does not need to URI-decode the data. This setting must be used with caution because it is not part of the HTTP specification. • UTF-8 URI Encoded. URI encoded UTF-8 data. All white space and non-ASCII bytes are encoded %XY, where X and Y are hex values (0-F). • Local Page Code Binary. Unencoded local code page data. This mode was used by versions of WebSEAL before Version 5.1. Use of this mode enables migration from previous versions, and is used in upgrade environments. Use with caution because data loss can potentially occur with this mode. • Local Code Page URI Encoded. URI encoded local code page data. Any UTF-8 characters that cannot be converted to a local code page are converted to question marks (?). Use this option with caution and only in environments where the local code page produces the wanted strings.

Table 32. Optional settings (continued)

Setting	Description
Basic Authentication	<p>Indicates that the connection host is also a WebSEAL server. If enabled, the connection between the servers is authenticated by using a proprietary authentication setup.</p> <ul style="list-style-type: none"> • WebSEAL username. The user ID that Cloud Identity Service WebSEAL servers use to authenticate to the connection hosts. • WebSEAL password. The password that Cloud Identity Service WebSEAL servers use to authenticate to the connection hosts.
Mutual Authentication	<p>Enables client authentication for the connection with a certificate.</p> <ul style="list-style-type: none"> • Certificate. The certificate to use.
Junction Cookie	<p>Insert ID via cookie script.</p>
Cookie Location	<p>Applicable only when Junction Cookie is enabled. Specifies the location in the pages that are served by connection hosts where the ID via cookie script is inserted.</p> <ul style="list-style-type: none"> • None. If None is specified, the script is written by default at the beginning of the response body. • Header. Inserts the script between the <head> </head> tags for HTML 4.01 compliance. • Trailer. Appends (instead of adding a prefix to) the script to the HTML page returned from the back-end server. • Trailer on Focus. Uses the onfocus event handler in the script to ensure that the correct connection cookie is used in a multiple-connection/multiple-browser-window scenario. • XHTML 1.0. Inserts an XHTML 1.0 (and HTML 4.01) compliant JavaScript block on the browser that interprets the document.
Cookie Handling	<ul style="list-style-type: none"> • Script Cookie . Supplies connection identification in a cookie to handle script-generated server relative URLs. • Preserve Cookie Path .Ensures unique Set-Cookie header name attributes for cookies set by connection hosts, by including each cookie path in the rewritten cookie name. • Preserve Cookie Name . Ensures that the Set-Cookie header set by a connection host is not rewritten by Cloud Identity Service to include the connection name in the cookie name.
Transparent Path Junction	<p>Non-virtual option. Specifies whether the connection uses a transparent path. Instead of adding a prefix to all filtered URLs with <i>/connection_name</i>, it is assumed that all content on the connection hosts is served from a context root that matches <i>/connection_name</i>. A transparent path avoids the need for Cloud Identity Service to filter server relative URLs.</p>

Basic connection settings

Table 33. Basic connection settings	
Setting	Description
Connection Name	The name of the connection. The name of the connection determines the URL path that is used to access the application server that is connected by the connection. For example, if the connection is called <code>webapp_1</code> then the URL for the root of the application server is <code>https://client_Cloud_Identity_Service_address/webapp_1/</code> .
Description	Connection description.
Type	Connection protocol, TCP, or SSL.
Virtual Connection	<p>Virtual connections communicate with virtual hosts. HTTP Host headers are used in client requests to direct those requests to the appropriate location on connected servers.</p> <p>A user can access resources directly with the host name of the connected server (<code>http://protected-server/resource</code>), rather than indirectly with the host name of the WebSEAL server and a potentially modified resource path (<code>http://webseal/connection/resource</code>). Direct access to the resource by using the host name of the connected server does not require URL filtering.</p>
Connection Servers	Not used when you create a new connection. The server addresses, paths, and ports to be set up for the connection. Click Add Server to add a server connection. For more information about adding a server, see “Adding a connection server” on page 121.

Default connection server settings

Table 34. Connection server settings	
Setting	Description
Location	The host name or IP address of the endpoint that forms the connection.
Port	The port on which to connect to the host system. Defaults to the default HTTPS port of 443. Needs to be specified only if the connection is to be made to a different port.
Distinguished Name	The certificate DN that is presented to Cloud Identity Service when connections to the application server are established. This field can be used to enhance security by allowing Cloud Identity Service to verify the certified identity of the server before a connection to it is established.
Virtual Host	<p>The HTTP Host header that is transmitted to the application server with the web requests. For HTTP version 1.1 compliant web servers, this header can be required to route the requests to the appropriate virtual host configuration.</p> <p>Note: Only required if the virtual host name differs from the value that is provided in the Location field.</p>

Table 34. Connection server settings (continued)

Setting	Description
Query Script Path	The location of the Query Contents tool that can optionally be installed on a client application server. The Query Contents tool allows Cloud Identity Service to inspect its web-space and represent it via the path object hierarchy that is displayed in the Connection Object Space panel. If not specified, this value defaults to <code>/cgi-bin/query_contents</code> .
Case sensitive URLs	Controls whether Cloud Identity Service treats URLs as case-insensitive when an authorization check is performed on a request to a connection host. After a successful ACL check, the original case of the URL is restored when the request is sent to the server.
Win32 support	<p>Controls whether Cloud Identity Service performs authorization checks against legacy Windows file paths. Cloud Identity Service performs security checks on client requests to connection hosts based on the file paths that are specified in the URL.</p> <p>A compromise in this security check can occur because Win32 file systems allow two different methods for accessing long file names. The first method acknowledges the entire file name, for example, <code>abcdefghijkl.txt</code>. The second method recognizes the old 8.3 file name format for compatibility with earlier versions, for example <code>abcdef~1.txt</code>.</p> <p>When you add a connection host in a Windows environment, it is important to restrict access control to one object representation only. This restriction is to prevent the possibility of back door access that bypasses the security mechanism. For this reason, the Win32 support option provides a number of measures of protection.</p> <ul style="list-style-type: none"> • Prevents the use of the 8.3 file name format. A user cannot avoid an explicit ACL on a long file name by using the short (8.3) form of the file name. Cloud Identity Service returns a 403 Forbidden error on any short form file name entered. • Disallows trailing dots in directory and file names. If a file or directory contains trailing dots, a 403 Forbidden error is returned. • Enforces case-insensitivity by setting the Case sensitive URLs option.

Optional connection settings

Table 35. Optional settings

Setting	Description
Stateful Connection	Specifies that the connection supports stateful applications. By default, connections are not stateful.
Boolean Rule	Allows denied requests and failure reason information from authorization rules to be sent in the Boolean Rule header (AM_AZN_FAILURE) across the connection.
Thread Limit	Defines the soft and hard limits for consumption of worker threads.

Table 35. Optional settings (continued)

Setting	Description
<p>HTTP Basic Authentication Header</p>	<p>Defines how the WebSEAL reverse proxy server passes client identity information in HTTP basic authentication (BA) headers to the web application servers. Options for handling client identity information.</p> <ul style="list-style-type: none"> • Filter. Default option. This option is used when WebSEAL authentication is set to use BA header information. <p>The WebSEAL BA header is used for all subsequent HTTP transactions. To the back-end server, WebSEAL appears logged on always.</p> <p>WebSEAL authentication that uses a client certificate is allowed with this option.</p> <p>If the back-end server requires actual client identity (from the browser), the CGI variables HTTP_IV_USER, HTTP_IV_GROUP, and HTTP_IV_CREDS can be used. For scripts and servlets, use the corresponding Cloud Identity Service specific HTTP headers.</p> <ul style="list-style-type: none"> – iv-user – iv-groups – iv-creds • Ignore. WebSEAL authentication that uses a BA header is not allowed with this option. This option uses the BA header for the original client user name and password. <p>WebSEAL authentication that uses a client certificate is allowed with this option.</p> • Supply. WebSEAL authentication that uses a BA header is not allowed with this option. This option uses the BA header for the original client user name and a dummy password. <p>WebSEAL authentication that uses a client certificate is allowed with this option.</p>

Table 35. Optional settings (continued)

Setting	Description
<p>Client Headers</p>	<p>Client headers insert client user identity information specific to Cloud Identity Service in HTTP headers across the host connection. The header types can include any combination of the following HTTP header types.</p> <ul style="list-style-type: none"> • Default headers. <ul style="list-style-type: none"> – Short user names. Inserts the user login name into an HTTP header that is called iv-user and adds it to all back-end requests to the connection hosts. – Long user names. Inserts the Cloud Identity Service user Distinguished Name into an HTTP header that is called iv-user-l and adds it to all back-end requests to the connection hosts. – Group names. Inserts a comma-separated list of the groups the user belongs to in an HTTP header that is called iv-groups and adds it to all back-end requests to the connection hosts. – User credentials. Inserts the Cloud Identity Service user credential in a Base64 encoded string in an HTTP header that is called iv-creds. Adds it to all back-end requests to the connection hosts. – Insert client IP Address. Inserts the user IP address into an HTTP header that is called iv-remote-address and adds it to all back-end requests to the connection hosts. • Custom headers. <ul style="list-style-type: none"> – Custom attributes must be configured and enabled for your setup of Cloud Identity Service for custom headers to be available. Inserts the attribute that is selected into an HTTP header. A name for the header must be entered.
<p>HTTP Header Encoding</p>	<p>Specifies the encoding to use when HTTP headers are generated to send to connection hosts. This encoding prevents any potential data loss that might occur when converted to a non-UTF-8 code page. Possible values for encoding.</p> <ul style="list-style-type: none"> • UTF-8 Binary. Unencoded UTF-8 data. This setting allows data to be transmitted without data loss, and the customer does not need to URI-decode the data. This setting must be used with caution because it is not part of the HTTP specification. • UTF-8 URI Encoded. URI encoded UTF-8 data. All white space and non-ASCII bytes are encoded %XY, where X and Y are hex values (0-F). • Local Page Code Binary. Unencoded local code page data. This mode was used by versions of WebSEAL before Version 5.1. Use of this mode enables migration from previous versions, and is used in upgrade environments. Use with caution because data loss can potentially occur with this mode. • Local Code Page URI Encoded. URI encoded local code page data. Any UTF-8 characters that cannot be converted to a local code page are converted to question marks (?). Use this option with caution and only in environments where the local code page produces the wanted strings.

Table 35. Optional settings (continued)

Setting	Description
Basic Authentication	<p>Indicates that the connection host is also a WebSEAL server. If enabled, the connection between the servers is authenticated by using a proprietary authentication setup.</p> <ul style="list-style-type: none"> • WebSEAL username. The user ID that Cloud Identity Service WebSEAL servers use to authenticate to the connection hosts. • WebSEAL password. The password that Cloud Identity Service WebSEAL servers use to authenticate to the connection hosts.
Mutual Authentication	<p>Enables client authentication for the connection with a certificate.</p> <ul style="list-style-type: none"> • Certificate. The certificate to use.
Junction Cookie	<p>Insert ID via cookie script.</p>
Cookie Location	<p>Applicable only when Junction Cookie is enabled. Specifies the location in the pages that are served by connection hosts where the ID via cookie script is inserted.</p> <ul style="list-style-type: none"> • None. If None is specified, the script is written by default at the beginning of the response body. • Header. Inserts the script between the <head> </head> tags for HTML 4.01 compliance. • Trailer. Appends (instead of adding a prefix to) the script to the HTML page returned from the back-end server. • Trailer on Focus. Uses the onfocus event handler in the script to ensure that the correct connection cookie is used in a multiple-connection/multiple-browser-window scenario. • XHTML 1.0. Inserts an XHTML 1.0 (and HTML 4.01) compliant JavaScript block on the browser that interprets the document.
Cookie Handling	<ul style="list-style-type: none"> • Script Cookie . Supplies connection identification in a cookie to handle script-generated server relative URLs. • Preserve Cookie Path .Ensures unique Set-Cookie header name attributes for cookies set by connection hosts, by including each cookie path in the rewritten cookie name. • Preserve Cookie Name . Ensures that the Set-Cookie header set by a connection host is not rewritten by Cloud Identity Service to include the connection name in the cookie name.
Transparent Path Junction	<p>Non-virtual option. Specifies whether the connection uses a transparent path. Instead of adding a prefix to all filtered URLs with <i>/connection_name</i>, it is assumed that all content on the connection hosts is served from a context root that matches <i>/connection_name</i>. A transparent path avoids the need for Cloud Identity Service to filter server relative URLs.</p>

Adding a connection server

The connection server addresses, paths, and ports to be set up for the connection.

Procedure

1. If the connection you want to create the connection server for is not open, search for and select the connection.

2. From **Connection Servers**, click **Add new server**.

The screenshot shows a dialog box titled "Add a Connection Server" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Location:** A text input field with a red asterisk (*) to its right.
- Port:** A text input field with a red asterisk (*) to its right.
- Distinguished Name:** A text input field.
- Virtual Host:** A text input field.
- Query Script Path:** A text input field.
- Case Insensitive URL's:** A toggle control with "True" and "False" buttons. "False" is selected.
- Win32 Support:** A toggle control with "True" and "False" buttons. "False" is selected.

At the bottom right of the dialog, there are two buttons: a grey "Cancel" button and a green "Add Server" button.

3. Enter the connection server settings.

<i>Table 36. Connection server settings</i>	
Setting	Description
Location	The host name or IP address of the endpoint that forms the connection.
Port	The port on which to connect to the host system. Defaults to the default HTTPS port of 443. Needs to be specified only if the connection is to be made to a different port.
Distinguished Name	The certificate DN that is presented to Cloud Identity Service when connections to the application server are established. This field can be used to enhance security by allowing Cloud Identity Service to verify the certified identity of the server before a connection to it is established.
Virtual Host	The HTTP Host header that is transmitted to the application server with the web requests. For HTTP version 1.1 compliant web servers, this header can be required to route the requests to the appropriate virtual host configuration. Note: Only required if the virtual host name differs from the value that is provided in the Location field.
Query Script Path	The location of the Query Contents tool that can optionally be installed on a client application server. The Query Contents tool allows Cloud Identity Service to inspect its web-space and represent it via the path object hierarchy that is displayed in the Connection Object Space panel. If not specified, this value defaults to <code>/cgi-bin/query_contents</code> .

<i>Table 36. Connection server settings (continued)</i>	
Setting	Description
Case sensitive URLs	Controls whether Cloud Identity Service treats URLs as case-insensitive when an authorization check is performed on a request to a connection host. After a successful ACL check, the original case of the URL is restored when the request is sent to the server.
Win32 support	<p>Controls whether Cloud Identity Service performs authorization checks against legacy Windows file paths. Cloud Identity Service performs security checks on client requests to connection hosts based on the file paths that are specified in the URL.</p> <p>A compromise in this security check can occur because Win32 file systems allow two different methods for accessing long file names. The first method acknowledges the entire file name, for example, <code>abcdefghijkl.txt</code>. The second method recognizes the old 8.3 file name format for compatibility with earlier versions, for example <code>abcdef~1.txt</code>.</p> <p>When you add a connection host in a Windows environment, it is important to restrict access control to one object representation only. This restriction is to prevent the possibility of back door access that bypasses the security mechanism. For this reason, the Win32 support option provides a number of measures of protection.</p> <ul style="list-style-type: none"> • Prevents the use of the 8.3 file name format. A user cannot avoid an explicit ACL on a long file name by using the short (8.3) form of the file name. Cloud Identity Service returns a 403 Forbidden error on any short form file name entered. • Disallows trailing dots in directory and file names. If a file or directory contains trailing dots, a 403 Forbidden error is returned. • Enforces case-insensitivity by setting the Case sensitive URLs option.

4. Click **Add Server**.

Creating Protected Object Policies

You use Protected Object Policies (POPs) to qualify access requirements. You can use time of day and network location to qualify access requirements.

About this task

The policy comes in to force only when it is attached to a connection.

Procedure

1. If the connection you want to create the POP for is not open, search for and select the connection.
2. Select **Add a new policy** from the **Protected Object Policy (POP)** drop-down list.

Add a Protected Object Policy (POP) X

Name

Description

Access for Day / Time

MoTuWeThFrSaSu

LocalUTC

||

||

Duration: 00:00 - 24:00 [All Day]

Access by IP Address + Add IP Address

Cancel
Save New POP

3. Enter a name and description.
4. Enter the remaining POP settings.

Setting	Description
Access for Day/ Time	Specifies the days and time of day when access is permitted. Time can be expressed as the local time for the service host environment, or Coordinated Universal Time. Select days on which to permit access. Use the slider bar to restrict access to a selected time span.

Setting	Description										
Access by IP Address	IP authentication settings for Protected Object Policies (Pops). Access is qualified by IP address and authentication level. Users can be permitted or prevented from accessing the resource from the specified IP addresses. Click Add IP Address to add IP address constraints.										
	<table border="1"> <tr> <td>Any Other Network</td> <td>Used as a network range that matches any network that is not otherwise specified in the POP. Use this method to create a default entry that can either deny all unmatched IP addresses or allow anyone access who meets the authentication level requirement.</td> </tr> <tr> <td>IP Address</td> <td>The values for the network are TCP/IP addresses. Both the network and netmask options must be specified in the same IP version.</td> </tr> <tr> <td>Netmask</td> <td>The values for netmask are TCP/IP addresses. Both the network and netmask options must be specified in the same IP version. The number 0 in the netmask serves as a wildcard to mean all IP addresses for that subnet. For example, an IP address of 9.1.2.3 with a netmask of 255.255.255.0 applies to all IP addresses in the range of 9.1.2.[0-255].</td> </tr> <tr> <td>Forbidden</td> <td>Prohibits access.</td> </tr> <tr> <td>Authentication Level</td> <td>Application-specific integer values that define the step-up authentication levels. All integer values up to but not including 1000 are supported. 0 is the lowest level. Authentication levels are defined during the initial configuration of Cloud Identity Service for your organization.</td> </tr> </table>	Any Other Network	Used as a network range that matches any network that is not otherwise specified in the POP. Use this method to create a default entry that can either deny all unmatched IP addresses or allow anyone access who meets the authentication level requirement.	IP Address	The values for the network are TCP/IP addresses. Both the network and netmask options must be specified in the same IP version.	Netmask	The values for netmask are TCP/IP addresses. Both the network and netmask options must be specified in the same IP version. The number 0 in the netmask serves as a wildcard to mean all IP addresses for that subnet. For example, an IP address of 9.1.2.3 with a netmask of 255.255.255.0 applies to all IP addresses in the range of 9.1.2.[0-255].	Forbidden	Prohibits access.	Authentication Level	Application-specific integer values that define the step-up authentication levels. All integer values up to but not including 1000 are supported. 0 is the lowest level. Authentication levels are defined during the initial configuration of Cloud Identity Service for your organization.
	Any Other Network	Used as a network range that matches any network that is not otherwise specified in the POP. Use this method to create a default entry that can either deny all unmatched IP addresses or allow anyone access who meets the authentication level requirement.									
	IP Address	The values for the network are TCP/IP addresses. Both the network and netmask options must be specified in the same IP version.									
	Netmask	The values for netmask are TCP/IP addresses. Both the network and netmask options must be specified in the same IP version. The number 0 in the netmask serves as a wildcard to mean all IP addresses for that subnet. For example, an IP address of 9.1.2.3 with a netmask of 255.255.255.0 applies to all IP addresses in the range of 9.1.2.[0-255].									
	Forbidden	Prohibits access.									
Authentication Level	Application-specific integer values that define the step-up authentication levels. All integer values up to but not including 1000 are supported. 0 is the lowest level. Authentication levels are defined during the initial configuration of Cloud Identity Service for your organization.										
Multi-Factor Authentication	Specifies whether to enable multi-factor authentication.										

5. Click **Save New POP**.

Example

The default setting for a POP is where every network is allowed access at any authentication level:

- **Authentication Level** is 0

In the following example, client access that originates from one set of IP addresses is considered secure. Another network range is considered less secure and requires a higher authorization level. Access from any other network range must be rejected. Two IP authentication entries must be created for the POP, one for the range of secure IP addresses, and one for the insecure IP addresses.

The first range applies to any client that accesses the web resource with an IP address of 9.180.168.*.

- **IP Address** is 9.180.168.0
- **Netmask** is 255.255.255.0
- **Authentication Level** is 0

The second range uses the **Any Other Network** and **Forbidden** options to exclude IP addresses. Web clients whose origin IP address does not match the 9.180.168.* range, default to this range and are rejected. Only web clients with IP addresses in the range of 9.180.168.* can access a web resource that is protected by this POP. This example might apply to the Network Address Translation (NAT) range used by a corporate firewall.

- **Any Other Network** is enabled.

- **Forbidden** is true.

The **Protected Object Policy** page for the policy shows the two IP ranges.

Creating Access Control Lists

An Access Control List (ACL) provides a mapping between a user, groups, and services and a set of permissions. You can create new ACLs to grant users, group members, and service members access to a protected resource.

About this task

An ACL is composed of a set of ACL entries. Each ACL entry specifies users, groups, and services with a list of permissions that are granted to those users, groups, and services. An ACL comes in to force only when it is added to a connection.

Important: Default ACLs must not be modified or deleted.

Procedure

1. If the connection you want to create the ACL for is not open, search for and select the connection.
2. Select **Add a new list** from the **Access Control List (ACL)** drop-down list.

Add an Access Control List (ACL)

Name: SampleACL

Description: Allows DaR access

Access for Users:

- D Gill (TmdbvrxNA)
- D Gold (TdbvrA)

+ Add User

Access for Groups: + Add Group

Access for Services: + Add Service

Buttons: Cancel, Save ACL

3. Enter a name and description.
4. Enter the remaining ACL settings.

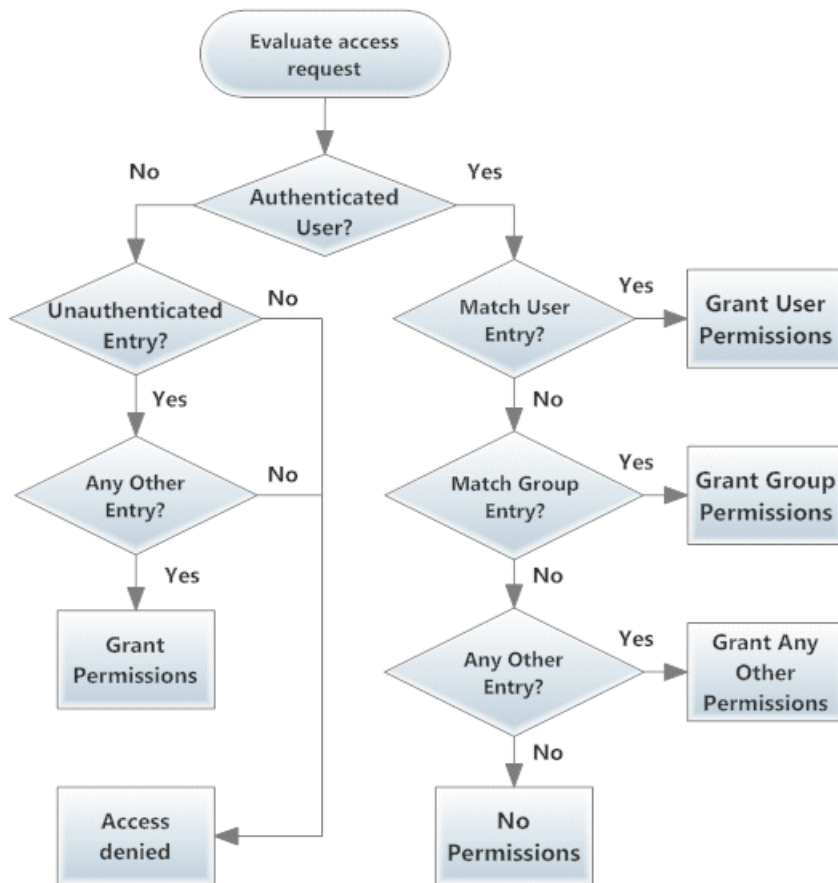
Setting	Description
Access for Users	<p>Access for individual users. Each added user is given access to the resource. Click Add User to add a user. To search for and select a user, enter the first 3 characters of the given name, surname, user name, or email address of the user. Select the permissions for each entry. You can use the following permissions for Cloud Identity Service users, groups, and services:</p> <ul style="list-style-type: none"> • r. Read. Allows users to view the object. • x. Execute. Allows users to run a file or script from the object. • T. Traverse. Allows users access to objects lower in the hierarchy. <p>Note: All other permissions apply to administrative functions and are not applicable to Cloud Identity Service users, groups, and services.</p>
Access for Groups	<p>Access for group members. Each member of an added group is given access to the resource. Click Add Group to add a group. To search for and select a group, enter at least the first 3 characters of the group name. Select the permissions for each entry.</p>
Access for Services	<p>Access for service members. Each member of an added service is given access to the resource. Click Add Service to add a service. To search for and select a service, enter at least the first 3 characters of the service name. Select the permissions for each entry.</p>
Unauthenticated Access	<p>Specifies access permissions for unauthenticated users. Permissions might be needed for unauthenticated users. For example, you might want to permit unauthenticated users access to resources lower in the hierarchy by setting the traverse permission. To set permissions, click Allow, and select permissions for unauthenticated users.</p>
Any Other Access	<p>Specifies access permissions for all other authenticated users who are not specified in access for users, groups, or services. Permissions might be needed for all authenticated users. For example, you might want to permit all authenticated users access to resources lower in the hierarchy by setting the traverse permission. To set permissions, click Allow, and select permissions for all other authenticated users.</p>

5. Click **Save New ACL**.

Access Control List evaluation

When users attempt to access a protected resource, the applicable Access Control List (ACL) for the protected resource is evaluated to determine whether access is granted.

The first stage in the evaluation is to determine whether the user that requests access has an active login session (authenticated) or does not have an active login session (unauthenticated).



When an authenticated user attempts to access a protected resource, the evaluation is done in the following order.

- Match the user ID with the User ACL entries. The evaluation stops on a User entry match. The permissions that are granted are the permissions in the matching User entry.
- If there is no matching User entry, then determine the groups to which the user belongs and match those groups to the Group entries in the ACL. The evaluation stops on any Group match. If more than one Group entry is matched, then the resulting permissions are the most permissive of the matching entries.
- If there is no matching User or Group entry, then grant the permissions of the Any-other entry, if it exists.
- If there is no matching User or Group entry, and no Any-other entry, then the user has no permissions.

When an unauthenticated user attempts to access a protected resource, the evaluation is done in the following way.

- If the ACL does not contain an entry for Unauthenticated, then access is denied.
- If the ACL does not contain an entry for Any-other, then access is denied.
- If the ACL contains an entry for Unauthenticated and an entry for Any-other, then grant the permissions that are given to both the Unauthenticated and Any-other entries. The permissions that are granted to unauthenticated users do not exceed the permissions that are given in the Any-other entry.

Creating protected objects

Protected objects represent the logical path elements that are made accessible via a connection.

About this task

The connection object space represents the logical paths to protected objects from the connection. For example, paths to directories, files, programs, or locations. You can add as many protected objects to a

connection as you need. You can select any existing object from the connection down to create as deep, and complex a hierarchy as you need.

You can attach Access Control Lists (ACLs) and Protected Object Policies (POPs) to protected object. When a policy is attached to an object, the policy is applied to the object and all child objects. An inherited policy is overridden if other policies are attached at a lower level.

Procedure

1. If the connection you want to add a protected object for is not open, search for and select the connection.
2. Click **Add a New Protected Object** from the **Connection Object Space**.

The screenshot shows a dialog box titled "Add New Protected Object" with a close button (X) in the top right corner. The dialog contains the following fields:

- Name:** A text input field with a red asterisk (*) indicating it is required.
- Description:** A text input field with a red asterisk (*) indicating it is required.
- Parent Object:** A dropdown menu with the selected value "/LukesUITestConnection" and a red asterisk (*) indicating it is required.
- Access Control List (ACL):** A dropdown menu with the selected value "Select an Access Control List".
- Protected Object Policy (POP):** A dropdown menu with the selected value "Select a Protected Object Policy".

At the bottom right of the dialog, there are two buttons: "Cancel" and "Add Protected Object".

3. Enter a name and description.

The protected object must be named after the object it represents. For example, if the object represents a page that is called `page1.jsp` that is at the root of the junction, then the path object must be created with the name `page1.jsp`.

4. Enter the remaining object settings.

Setting	Description
Parent object	The parent object of the protected object. The parent object can be the connection object, or any existing protected object below the connection.
Access Control List (ACL)	ACL to attach to the object.
Protected Object Policy (POP)	POP to attach to the object.

5. Click **Add Protected Object**.

Managing Launchpad services

Web connections and federated partner web connections can be made available from Launchpad in the Self Service portal for users. Users must be added to the appropriate services to access web connections through Launchpad.

Adding users to Launchpad services

Users can access web applications from Launchpad, a single location in their Self Service portal.

About this task

For each web connection and federated partner connection that is created, a corresponding service is created. The service is given the same name as the connection, or for federated web applications the same name as the connection alias. For the web application to be made available to a user from Launchpad, the user must be added to the appropriate service.

Note: Non-virtual connection names begin with a forward slash, for example `/my_connection_1`. The service names for non-virtual connections also begin with a forward slash.

Note: If a federated partner connection alias is changed, a new service with the new alias name is created. Members from the service that was previously used by the connection are migrated to the new service, and the old service is removed.

You can add users to a service by managing the service manually, or by managing the service dynamically by using a policy.

Procedure

Add users to a Launchpad service.

- [Add users by managing the service manually.](#)
- [Add users by managing the service dynamically.](#)

Managing federated SSO web access

Federated SSO (Single sign-on) web Access Management, involves the management of network connections to third-party applications. Federated Single sign-on (SSO) enables users that have a Cloud Identity Service account to access other third-party application services with their existing identity.

Federated SSO overview

Federated Single sign on (SSO) enables users that have a Cloud Identity Service account to seamlessly access services that are provided by one or more partner organizations, without a separate login at the partner site.

When a user clicks a federated sign-on URL, Cloud Identity Service constructs a digitally signed token that can be verified (and therefore trusted) by the partner organization. This token is submitted by the user's browser to the partner's Single Sign-on URL where a session is created.

A federated partner relationship involves two distinct roles for the two parties that are involved, the identity provider (IdP) and the service provider (SP). The identity provider supplies a trustworthy identity in the form of a digital token. The service provider validates the digital token, creates a session for the user, and allows the user to access their application environment. Cloud Identity Service is the identity provider and the partner is the service provider.

A single Cloud Identity Service environment can support multiple federation partners. For each federated sign-on URL, connection details that describe the partner federation properties must be defined. Each connection must have a public and private key pair that are provided by a personal certificate and a signer certificate.

Cloud Identity Portal provides pre-configured templates for a number of the most popular partner application services that support a federated single sign-on using SAML 2.0. If no template exists for the partner you want to create a connection for, then a customized configuration can be used.

Key management

Each connection must have a public and private key pair. These keys are provided by a personal certificate and a signer certificate.

A signer certificate represents a certificate and public key that is associated with some personal certificate. The purpose of the signer certificate is to verify personal certificates. The owner of the private key is able to establish connections with partner application services. The signer certificate explicitly trusts connections that are made to or by the owner of the associated personal certificate.

Only one personal certificate is enabled in Cloud Identity Portal. You do not have to explicitly select the personal certificate to use when you define a connection. By default, the enabled personal certificate is used for every connection you create. For every connection you create, you must select the appropriate signer certificate. Signer certificates are normally provided by service providers. You can import signer certificates. You can also create self-signed certificates and keys for low-sensitivity, non-production, or other rapid-use requirements.

Connection management

You can create any number of connections to support any number of federated partners. A number of pre-configured templates are provided for some of the most popular partner application services. You use these templates to create connections to your federated partners. Templates pre-configure as many of the partner connection details as possible. If no template exists for a partner, or you want to create a connection to an internal application or service, you can create a connection by using a generic template. Each connection that is successfully created generates a sign-on URL. This URL is used to initiate a Single Sign-on to your partner.

Some providers allow for the creation of user records on the service provider side at the first successful login attempt by a user. The creation of user records is called autoprovisioning.

Managing federated partner connections

Managing partner connections

Searching for federated web application connections

You can search for network connections to federated web applications to view, modify, or remove the connection.

Procedure

1. In the navigation pane, click **Applications > Connection Management**, and click **Federated Applications**.
2. In the **Search** field, enter at least the first 3 characters of the connection.
The field label changes to **Searching For**.
Connections matching your search criteria are listed. Select a connection to modify or view.

Adding a connection to a federated partner

You can create any number of connections to support any number of federated partners. A number of pre-configured templates are provided for some of the most popular partner application services.

About this task

Cloud Identity Portal provides a number of templates to add connections for federated partners. You can add a connection to other providers by using a generic template. The generic template can also be used to create connections for internal applications.

Some providers allow for the creation of user records on the service provider side at the first successful login attempt by a user. Autoprovisioning templates are available for partners that allow for the creation of user records. For the autoprovisioning of user records, service providers normally require additional information. This additional information is provided by mapping Cloud Identity Service LDAP attributes to corresponding partner attributes.

Procedure

1. Click **Applications > Connection Management** in the navigation menu, and click **Federated Applications > Add a New Connection**.

The screenshot shows a modal window titled "Add a New Connection" with a close button (X) in the top right corner. The window has a progress bar at the top with three steps: "1 Choose a Provider" (highlighted in blue), "2 Provider Details", and "3 Complete Setup". Below the progress bar, the text "Begin by choosing a provider to connect to" is displayed. The form contains three main sections: "Provider" with a dropdown menu showing "Choose one of the following Providers..." and a link "Add your own" below it; "Connection Alias" with a text input field; and "Status" with two buttons: "Enabled" and "Disabled". At the bottom of the form, there are three buttons: "Cancel", "Previous", and "Next".

2. Select the provider name from the **Provider** menu.
 - To create a connection based on a partner template, select the provider from the **Provider** menu. Where possible, providers are identified by an icon. If no provider icon is available, a generic icon is used.
 - To create a connection for a partner that has no template or for an internal application, click **Add your own** or select **Generic SAML2.0 Service Provider** from the **Provider** menu.
3. Enter the connection alias in the **Connection Alias** field.
4. Click **Next**.

5. Enter provider properties details.

Note: It is not possible to indicate all of the fields that are mandatory because validation of a connection is done on the server-side.

Note: For connections based on a template, a number of details are entered for you. Pre-entered default fields are hidden during connection setup. If you want to view or edit default fields, click **Show hidden items**. You can edit the values or settings for default fields. Changing the settings or values for default fields can cause the connection to be invalid.

To edit the default fields, click **Enable editing of default fields**. A warning is displayed. Click **Enable Fields** to edit default fields.

Important: For Clarizen connections, depending on the Clarizen environment you are using, the Assertion Consumer Service URL can have one of the following values:

- EU environment. <https://eu1.clarizen.com/Clarizen/Pages/Integrations/SAML/SamlResponse.aspx>
- SV environment. <https://app2.clarizen.com/Clarizen/Pages/Integrations/SAML/SamlResponse.aspx>
- TB environment. <https://app.clarizentb.com/Clarizen/Pages/Integrations/SAML/SamlResponse.aspx>

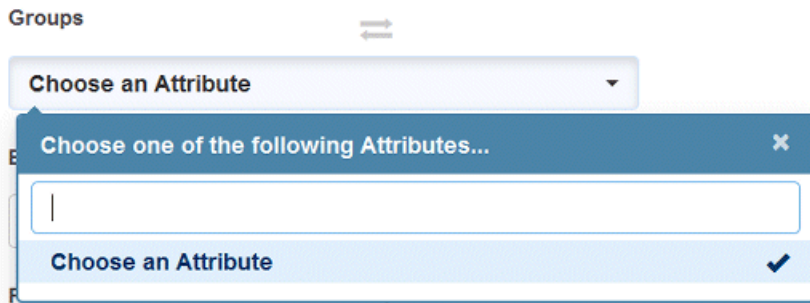
The template default value is <https://app2.clarizen.com/Clarizen/Pages/Integrations/SAML/SamlResponse.aspx>. If you need to change the value, use **Enable editing of default fields**.

6. For providers that require attribute mappings, enter the provider attribute mappings.

Some providers require a number of attributes to be mapped to Cloud Identity Service LDAP attributes. Attributes that are mapped are loaded into the SAML assertion and used by the service provider to identity the user. The value that is stored in the LDAP attribute is mapped to a variable for the provider.

Provider Attribute Mapping

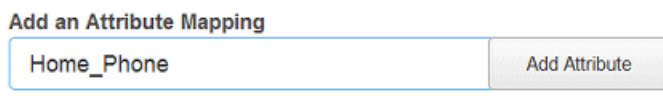
Connect the providers attribute with the value of an LDAP attribute



7. Optional: Enter and map to other attributes

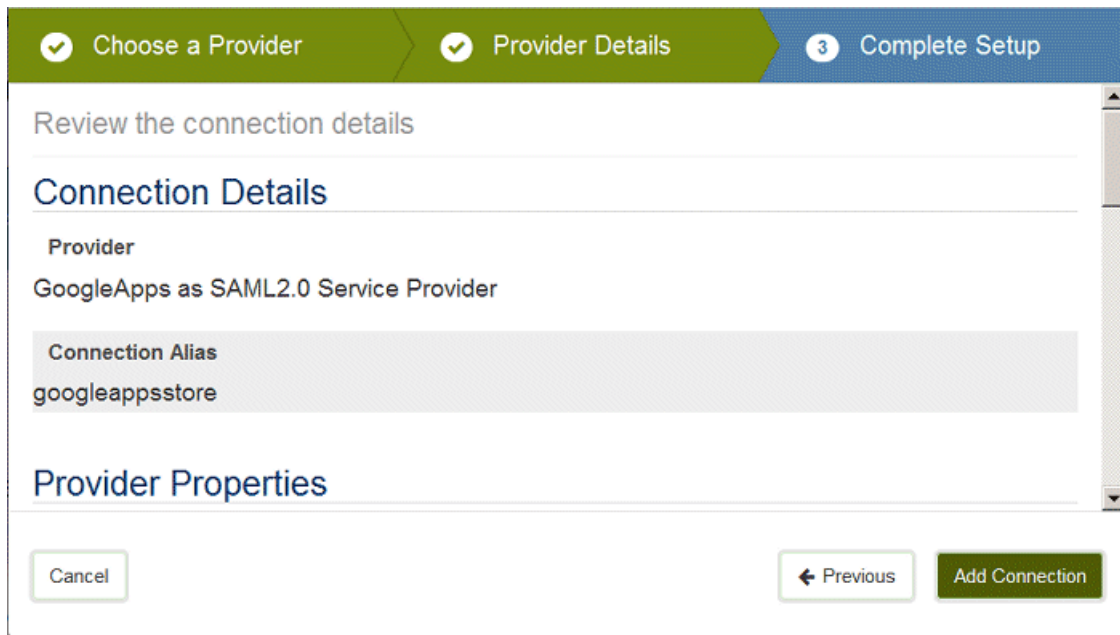
If the provider accepts other attribute mappings, you can add other attributes.

a) Enter the name of the partner attribute in the **Add an Attribute Mapping** field, and click **Add Attribute**.



b) Select the LDAP attribute to map to from the **Choose an Attribute** field.

8. Click **Next**.



9. Click **Add Connection**.

Federated partner connection settings

Connection settings for federated partners include connection alias, status, sign-on URL, attribute mapping properties, and service provider properties.

Setting	Description
Provider	The service provider.

Table 37. Provider information (continued)

Setting	Description
Connection Alias	The connection alias.
Status	The connection status. If the connection is disabled, the connection will fail.
Sign-On URL	The URL to initiate a Single Sign-on to your partner.

Table 38. Attribute mappings

Setting	Description
Provider Attribute Mapping	Required provider attribute mappings. Some providers require a number of attributes to be mapped to Cloud Identity Service LDAP attributes. Required attributes are loaded into the SAML assertion and used by the service provider to identify the user.
Add an Attribute Mapping	Optional attribute mappings.

Table 39. Provider properties

Setting	Description
Assertion Consumer Service URL	The endpoint of the service provider that receives assertions.
Company Name	The service provider company name.
Enabled	Specifies whether the partner is enabled. If the partner is not enabled, the connection will fail.
Encrypt Assertion	Specifies whether to encrypt assertions.
Encrypt Assertion Attributes	Specifies whether to encrypt assertion attributes.
Encryption Key Identifier	The name of the encryption key.
Encrypt Name Id	Specifies whether the name identifiers must be encrypted.
Identity Mapping Rule	An optional JavaScript internal mapping rule to modify the information that is required to build a SAML 2.0 token. The content of the JavaScript mapping rule must be provided.
Identity Mapping Rule Reference	An optional JavaScript internal mapping rule to modify the information that is required to build a SAML 2.0 token. A relative URI to a JavaScript mapping rule managed by the mapping rules REST API must be provided, for example, /iam/access/v8/mapping-rules/mapping_rule_id. When an identityMappingRuleReference is specified, it takes precedence over identityMappingRule .
Provider Id	A unique identifier that identifies the service provider.
Session Not On Or After	The number of seconds that the security context that is established for the principal must be discarded by the service provider.
Sign Assertion	Specifies whether to sign the assertions.
Signature Validation Key Identifier	The name of the signature validation key.
Sign Authn Response	Specifies whether to sign the authentication responses.

<i>Table 39. Provider properties (continued)</i>	
Setting	Description
Validate Authn Request	Specifies whether to validate the digital signature of an authentication request.

Quick Connect partner-side configuration

Single Sign-on (SSO) Quick Connect partner-side configuration.

For a partner configured in Cloud Identity Service, the Sign-On URL generated by the Quick Connect template needs to be provided to users. The Sign-On URL enables users to log in to a partner site through SAML SSO, by using a link normally made available to users from Cloud Identity Service. In partner-side configuration, an administrator must use the Cloud Identity Service Sign-On URL and a SAML assertion validation certificate to configure SAML 2.0 SSO settings for the Service Provider (SP) partner. In partner-side configuration, some process or method is used for creating users on the partner-side. Some partners support Just-in-time (JIT) provisioning. In JIT provisioning, if a Cloud Identity Service user does not exist on the partner-side, the user is automatically created by using attributes that are passed through the SAML assertion.

For SSO to work for all partners, normally the Cloud Identity Service user name must match the user name that is used by the SP. Exceptions to this requirement are partners where JIT provisioning is enabled, where the SAML subject is mapped to a federation ID on the SP side.

Quick Connect partner-side settings

For Single Sign-on to work with the pre-configured Quick Connect federation templates, some partner-side settings must use only certain values or settings. The following table does not list all of the partner-side SAML 2.0 settings. The table lists specific settings where only certain values or options are supported by the federation templates.

Administrators can override properties of the Quick Connect federation templates at connector level. Cloud Identity Service supports both Identity Provider (IdP) and SP initiated SSO.

Note: SAML assertions (replies) to all SPs are signed with the same key.

<i>Table 40. SAML 2.0 settings for Quick Connect federation templates</i>			
Partner	Applications and SAML 2.0 settings	Auto-provisioning support	IdP or SP initiated SSO
ADFS	<ol style="list-style-type: none"> In the Advanced tab of ADFS Claim Provider Trusts Properties, Secure Hash Algorithm must be set to RSA-SHA1. SAML2.0 Authentication Request must not be signed by ADFS. 	No	SP
Adobe Creative Cloud	N/A	No	SP
Adobe Echo Sign Provisioning	N/A	No	IdP and SP
Agiloft	N/A	Yes	SP
Aha	N/A	Yes	IdP and SP

Table 40. SAML 2.0 settings for Quick Connect federation templates (continued)

Partner	Applications and SAML 2.0 settings	Auto-provisioning support	IdP or SP initiated SSO
Amazon Web Services (AWS)	<ul style="list-style-type: none"> • Create an IAM role for SSO in AWS. The IAM role institutes trust with the identity provider and defines permissions for the federated user. • Select Role for Identity Access with the Grant Web SSO access to SAML providers option. • The Role and RoleSessionName fields are required in the SAML assertion. 	No	IdP
ANCILE uAlign			IdP and SP
AnswerHub			IdP and SP
ArcGIS		Yes	IdP and SP
Asana	N/A	No	IdP and SP
Assembla			IdP
BambooHR	N/A	No	IdP and SP
BIME	N/A	No	SP
Bitium	N/A	No	IdP and SP
BlueJeans	For IdP initiated SSO, the RelayState must be entered in the target ID.	Yes	IdP and SP
Bonusly	N/A	No	IdP and SP
Boomi Atmosphere®		No	IdP and SP
Box	<p>For both auto-provisioning enabled and disabled, the following settings are required.</p> <ol style="list-style-type: none"> 1. SAML Request must be signed for SP initiated SSO. 2. Signature Algorithm for signing SAML Request must be RSA-SHA1. 3. If BOX Groups and Email aliases are to be sent through SAML Assertion, the following attribute names must be used: <ul style="list-style-type: none"> • For BOX Groups, use <code>groups</code> as the attribute name. • For BOX Email Aliases, use <code>email_aliases</code> as the attribute name. <p>If BOX auto-provisioning is enabled, the following attribute names must be used.</p> <ol style="list-style-type: none"> 1. For First Name/GivenName, use <code>firstname</code> as the attribute name. 2. For Last Name/Surname, use <code>lastname</code> as the attribute name. 	Yes	IdP and SP
Brightcove	N/A	No	IdP and SP

Table 40. SAML 2.0 settings for Quick Connect federation templates (continued)

Partner	Applications and SAML 2.0 settings	Auto-provisioning support	IdP or SP initiated SSO
Chatter	Chatter is available in a Salesforce developer account. For information on SAML SSO configuration, see Salesforce SAML settings .	Yes	IdP and SP
Citrix applications	<p>A separate target ID for each application is needed for SP initiated SSO.</p> <p>Citrix applications.</p> <ul style="list-style-type: none"> • Citrix OpenVoice • Citrix Online • GoTo Assist • GoToAssist Concierge • GoToAssist Remote Support • GoToAssist Seeit • GoToAssist ServiceDesk • GoTo Webinar 		
Citrix Sharefile		No	IdP and SP
Clarizen	N/A	No	IdP and SP
ClearSlide	N/A	Yes	IdP and SP
Cloud Drop	<ul style="list-style-type: none"> • A Salesforce developer account must be available. For information on SAML SSO configuration, see Salesforce SAML settings. • From the Salesforce AppExchange, search for the Cloud Drop app and install on the Salesforce developer account 	Yes	IdP and SP

Table 40. SAML 2.0 settings for Quick Connect federation templates (continued)

Partner	Applications and SAML 2.0 settings	Auto-provisioning support	IdP or SP initiated SSO
Cloud Passage	<p>For auto-provisioning enabled, the following settings are required.</p> <ul style="list-style-type: none"> • admin. To specify whether the user is a Halo site administrator. • ghostport_access. To specify whether the user is a GhostPorts user. • portal_access. To specify whether the user has Portal access. • firstname. • lastname. • email. • sms. The mobile phone number of the user, for receiving SMS authentication codes. • Yubikey (optional). The YubiKey key value of the user. • Account ID. The ID that identifies your organization's Halo account to the identity provider. It is passed in the assertion as the consumer URL. 	Yes	IdP
Concur	N/A	No	IdP
CrashPlan	N/A	No	IdP
Data.com	Data.com is available in a Salesforce developer account. For information on SAML SSO configuration, see Salesforce SAML settings .	Yes	IdP and SP
Datadog	<p>A separate ACS URL is needed for both IdP and SP initiated SSO.</p> <ul style="list-style-type: none"> • IdP. https://app.datadoghq.com/account/saml/assertion/id/AccountID • SP. https://app.datadoghq.com/account/saml/assertion 	Yes	IdP and SP
Desk.com	N/A	Yes	IdP and SP
DeskPRO	N/A	Yes	IdP and SP
DocuSign	N/A	No	IdP and SP
Dropbox	N/A	No	IdP and SP
DupeBlocker	<ul style="list-style-type: none"> • A Salesforce developer account must be available. For information on SAML SSO configuration, see Salesforce SAML settings. • From the Salesforce AppExchange, search for the DupeBlocker app and install on the Salesforce developer account 	Yes	IdP and SP

Table 40. SAML 2.0 settings for Quick Connect federation templates (continued)

Partner	Applications and SAML 2.0 settings	Auto-provisioning support	IdP or SP initiated SSO
Egnyte	<ul style="list-style-type: none"> • Set Default user mapping to Email address. • Set Use Domain specific issuer value to Enabled. The URL is <code>https://egnyte.domain.egnyte.com</code>. 	No	IdP and SP
eSignLive		Yes	IdP and SP
Fairsail		Yes	IdP and SP
GitHub	N/A	Yes	IdP and SP
Google Analytics	Same as Google Apps SAML settings .	No	IdP and SP
Google Apps	<ul style="list-style-type: none"> • A domain-specific issuer is not supported by default by the Google Apps template. Only a static value of <code>google.com</code> is supported as the issuer/provider ID. • When SAML2.0 SSO is configured on Google Apps, the Use a Domain specific issuer option must not be selected. • The domain name must be verified. • For SP initiated SSO, the specific target ID must be provided in the URL for each application. <p>Google Apps applications.</p> <ul style="list-style-type: none"> • Google Admin • Google Books • Google Code • Google Drive • Google Forms • Google Groups • Google Hangouts • Google Keep • Google Maps • Google Photos • Google Play • Google Sheets • Google Slides • Google Translate • Google Trends • Google Videos • Google + • Blogger • Gmail 	No	IdP and SP
Google Calendar	Same as Google Apps SAML settings .	No	IdP and SP

Table 40. SAML 2.0 settings for Quick Connect federation templates (continued)

Partner	Applications and SAML 2.0 settings	Auto-provisioning support	IdP or SP initiated SSO
Google Docs	Same as Google Apps SAML settings .	No	IdP and SP
Google Finance	Same as Google Apps SAML settings .	No	IdP and SP
Google Site	Same as Google Apps SAML settings .	No	IdP and SP
GoToMeeting	A valid domain for your organization must be registered and verified for SAML2.0 SSO.	No	IdP and SP
Greenhouse	N/A	Yes	IdP and SP
HappyFox	N/A	Yes	IdP and SP
Huddle	N/A	Yes	IdP and SP
IBM® Bluemix®	N/A	Yes	IdP and SP
IBM Blueworks Live	N/A	Yes	IdP and SP
IBM Cloud Security Enforcer	<ul style="list-style-type: none"> • Provide an authentication URL and a target URL for both dashboard and launchpad access, for example: <ul style="list-style-type: none"> – <code>https://my_domainName/isam/mtfim/sps/saml20ip/saml20/logininitial?PartnerId=https://partner_provider_domain_name/idaas/mtfim/sps/idaas/saml20&NameIdFormat=Email&Target=https://partnerProvider_Domainname/ui/launchpad</code> – <code>https://my_domainName/isam/mtfim/sps/saml20ip/saml20/logininitial?PartnerId=https://partner_provider_domain_name/idaas/mtfim/sps/idaas/saml20&NameIdFormat=Email&Target=https://partnerProvider_Domainname/ui/dashboard</code> • To ensure access to the dashboard, the SAML assertion must contain the attribute groups with value admin. 	No	IdP and SP

Table 40. SAML 2.0 settings for Quick Connect federation templates (continued)

Partner	Applications and SAML 2.0 settings	Auto-provisioning support	IdP or SP initiated SSO
IBM Connections Cloud	For IdP initiated SSO, the target ID must be provided for each application. IBM Connections Cloud applications. <ul style="list-style-type: none"> • IBM Connections Activities • IBM Connections Chat • IBM Connections Files • IBM Connections Meetings • IBM Connections Notebook • IBM Connections ToDo • IBM SmartCloud® Notes® Web • IBM Verse® 	No	IdP and SP
IBM Kenexa® Talent Suite		No	IdP and SP
IBM MaaS360®		No	SP
IBM Softlayer	N/A	No	IdP
Igloo Software	The provider ID and target ID must be provided in the ACS (Assertion Consumer Service) URL.	Yes	IdP and SP
Informatica Cloud		Yes	IdP and SP
Intacct	The SSO Issuer URL at Intacct must be https://saml.intacct.com .	No	IdP and SP
Invision	N/A	No	IdP
JIRA (Atlassian)	N/A	No	IdP and SP
Kanban Tool			IdP and SP
kiteworks	N/A	Yes	IdP and SP
Knowledge	A Salesforce developer account must be available. For information on SAML SSO configuration, see Salesforce SAML settings .	Yes	IdP and SP
Lesson.ly		No	IdP and SP
LiquidPlanner	N/A	No	IdP and SP
Litmos			IdP
LivePerson	N/A	No	IdP

Table 40. SAML 2.0 settings for Quick Connect federation templates (continued)

Partner	Applications and SAML 2.0 settings	Auto-provisioning support	IdP or SP initiated SSO
LogMeIn	Provide an authentication URL and a target URL, for example: <ul style="list-style-type: none"> • https://my_DomainName/isam/mtfim/sps/saml20ip/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https://accounts.logme.in&NameIdFormat=Email&Target=https://secure.logmein.com/central/Central.aspx 	Yes	IdP and SP
Lucidchart	In SAML, select Send Nameid format in SAML Request .	Yes	IdP and SP
Mozy	Provide an authentication URL that has a RequestBinding, PartnerID, and NameIDFormat , for example: <ul style="list-style-type: none"> • https://my_domain/isam/mtfim/sps/saml20ip/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https://auth2.mozy.com/mozy_domain/saml&NameIdFormat=Email 	No	IdP and SP
Namely	N/A	No	IdP and SP
NetSuite	N/A	No	IdP
New Relic	N/A	No	IdP and SP
Office 365	<ul style="list-style-type: none"> • Log in to Microsoft Office 365 and add a domain. • Verify the domain. • Federate the domain by using power shell commands. Use the Azure Active Directory Module for Windows PowerShell tool. 	No	SP
Okta	N/A	Yes	IdP and SP
OneDrive/SkyDrive	OneDrive is available in an Office 365 account. For more information, see Office 365 SAML settings .	No	SP
OpenDataSoft	The target ID must be provided in the SSO URL.	No	IdP and SP
OpenDNS		No	IdP and SP
PagerDuty	N/A	Yes	IdP and SP
ProofHQ	N/A	Yes	IdP and SP
Redbooth	N/A	No	IdP and SP
Remedyforce	Get a Remedyforce account. For information on SAML SSO configuration, see Salesforce SAML settings .	Yes	IdP and SP
Roambi Business	The target ID must be provided in the SSO URL.	No	IdP and SP

Table 40. SAML 2.0 settings for Quick Connect federation templates (continued)

Partner	Applications and SAML 2.0 settings	Auto-provisioning support	IdP or SP initiated SSO
Sales Cloud	Register for a Salesforce service cloud account. For information on SAML SSO configuration, see Salesforce SAML settings .	Yes	IdP and SP
Salesforce	For JIT provisioning enabled, the following settings are required: <ul style="list-style-type: none"> • Request Signature Method must be set to RSA-SHA1. • Assertion Decryption Certificate must be set to Assertion not encrypted. • SAML Identity Location must be set to Identity is in the NameIdentifier element of the Subject statement. • Service Provider Initiated Request Binding must be set to HTTP Redirect. • SAML Identity Type must be set to Federation ID from the User object. • User Provisioning Type must be set to Standard. 	Yes	IdP and SP
Samanage	N/A	Yes	IdP and SP
SAP Netweaver		No	IdP and SP
Service Cloud	Register for a Salesforce service cloud account. For information on SAML SSO configuration, see Salesforce SAML settings .	Yes	IdP and SP
ServiceNow	N/A	No	IdP and SP
SharePoint Online	SharePoint Online is available in an Office 365 account. For more information, see Office 365 SAML settings .	No	SP
Skilljar		Yes	IdP and SP
Slack	The Service Provider ID must be set to <code>https://DomainName.slack.com/</code> .	Yes	IdP and SP
Small Improvements		No	IdP and SP
Soonr Workplace	N/A	No	IdP and SP
SpringCM	Provide an authentication URL and a target URL, for example: <ul style="list-style-type: none"> • <code>https://ISAM_DomainName/isam/mtfim/sps/saml20ip/saml20/logininitial?PartnerId=https://Partner_DomainName/atlas/sso&NameIdFormat=Email&Target=https://Partner_Provider_DomainName/atlas/Documents/BrowseDocuments.aspx?aid=ID</code> 	No	IdP and SP
StatusPage	N/A	No	IdP and SP

Table 40. SAML 2.0 settings for Quick Connect federation templates (continued)

Partner	Applications and SAML 2.0 settings	Auto-provisioning support	IdP or SP initiated SSO
SuccessFactors	The following settings are required. <ul style="list-style-type: none"> • Require Mandatory Signature must be set to Assertion. • Enable SAML Flag must be set to Enabled. • SAML Profile must be set to Browser/Post Profile. • NameID Format must be set to unspecified. • Enable sp initiated login (AuthnRequest) must be set to Yes. • Default issuer must be selected. 	No	IdP and SP
SugarCRM	N/A	No	IdP and SP
Symantec Endpoint Manager			IdP and SP
Syncplicity	N/A	No	SP
Tableau			IdP and SP
TOPdesk		No	IdP and SP
Unifyle	N/A	Yes	IdP and SP
UserVoice			IdP and SP
Ustream®		No	IdP and SP
VersionOne	The target ID must be provided in the SSO URL.	No	IdP and SP
WalkMe	<ul style="list-style-type: none"> • A Salesforce developer account must be available. For information on SAML SSO configuration, see Salesforce SAML settings. • Install The WalkMe app on the Salesforce developer account. 	Yes	IdP and SP
WebEx	<ul style="list-style-type: none"> • In the SAML assertion, the NameID Format must be email. • When a user is created in Cloud Identity Portal, the UID and gtwayPrincipalName must be different. The gtwayPrincipalName must be in email format and UID must be same as the user name of the Provider. 	Yes	IdP and SP
WordPress	N/A	Yes	IdP and SP
Workday	<ul style="list-style-type: none"> • For IdP and SP initiated SSO, the Service Provider ID option must be set to <code>http://www.workday.com/</code>. • For SP initiated SSO, the Do Not Deflate SP-initiated Authentication Request option must be selected. • The Sign SP-Initiated Authentication Request option must be cleared. 	No	IdP and SP

Table 40. SAML 2.0 settings for Quick Connect federation templates (continued)

Partner	Applications and SAML 2.0 settings	Auto-provisioning support	IdP or SP initiated SSO
Yammer	Yammer is available in an Office 365 account. For more information, see Office 365 SAML settings .	No	SP
Zendesk	N/A	No	IdP and SP
Zoho applications	<p>N/A</p> <p>Zoho applications.</p> <ul style="list-style-type: none"> • Site 24x7 (Service Desk Plus) • ZoHo Books • Zoho Bugtracker • Zoho Campaigns • Zoho Chat • Zoho Connect • Zoho CRM • Zoho Docs • Zoho Forms • Zoho Invoice • Zoho Mail • Zoho Meeting • Zoho Projects • Zoho Reports • Zoho SalesIQ • Zoho Sites • Zoho Social • Zoho Support • Zoho Survey • Zoho Vault 	No	IdP and SP
Zscaler	<p>For both auto-provisioning enabled and disabled, for IdP initiated SSO the Target ID must be appended to the login URL, for example:</p> <ul style="list-style-type: none"> • <code>https://my_domain/isam/mtfim/sps/saml20ip/saml20/logininitial?PartnerId=zscalerbeta.net&Target=http://gateway.zscalerbeta.net/test</code> 	Yes	IdP and SP
Zuora	For IdP SSO login, the federated ID must be provided.	No	IdP

Managing Launchpad services

Web connections and federated partner web connections can be made available from Launchpad in the Self Service portal for users. Users must be added to the appropriate services to access web connections through Launchpad.

Adding users to Launchpad services

Users can access web applications from Launchpad, a single location in their Self Service portal.

About this task

For each web connection and federated partner connection that is created, a corresponding service is created. The service is given the same name as the connection, or for federated web applications the same name as the connection alias. For the web application to be made available to a user from Launchpad, the user must be added to the appropriate service.

Note: Non-virtual connection names begin with a forward slash, for example `/my_connection_1`. The service names for non-virtual connections also begin with a forward slash.

Note: If a federated partner connection alias is changed, a new service with the new alias name is created. Members from the service that was previously used by the connection are migrated to the new service, and the old service is removed.

You can add users to a service by managing the service manually, or by managing the service dynamically by using a policy.

Procedure

Add users to a Launchpad service.

- [Add users by managing the service manually.](#)
- [Add users by managing the service dynamically.](#)

Managing keys

You can manage the client and server certificates that you use to secure your connections.

Creating a client certificate

Client certificates contain a private key and a public key. A client certificate is used by a client system to make authenticated requests to a remote server. You can create client certificates or if you have a certificate file that you want to use, you can upload the file to Cloud Identity Portal.

About this task

By default, the enabled certificate is used for every connection you create. Only one key can be enabled at any one time.

Procedure

1. Click **Applications** > **Key Management** in the navigation menu, and click **Client Certificates** and **Add a New Key**.

Add a New Key X

Key Creation Action Upload Key Generate Key *

Status Enabled Disabled * *Enabling this key will disable all other keys*

Key Label

Expires in days

Key Size

Cancel Add a New Key

2. Enter the client certificate key settings.
3. Click **Add a New Key**.

Client certificate key settings

Client certificate key settings include the key label, time to expire, and key size.

<i>Table 41. Client certificate key settings</i>	
Setting	Description
Key Creation Action	<ul style="list-style-type: none"> Upload Key. If you have a certificate file that you want to use, you can upload the file. Generate Key. If you do not have a certificate file, Cloud Identity Portal can generate a key.
Status	<ul style="list-style-type: none"> Enabled. If you enable the key, the previously enabled key and all other certificates keys are disabled. Only one key can be enabled at any one time. Important: If you enable the key, the previously enabled key is disabled. All connections that use the previously enabled key are invalid. Disabled. The key is disabled.
Key Label	<ul style="list-style-type: none"> For an uploaded key, a label must be entered when the status is set to Enabled. The key label is the name of the certificate file that you are uploading. For a generated key, a unique identifier that represents a certificate. The label provides a name with which to refer to a certificate when key management functions are performed.
Key File	For an uploaded key only, click Browse to browse to and select the file to upload. JKS, PEM, and P12 formats are supported.
Key Password	For an uploaded key only, the key password. The password must match the password in the certificate file you are uploading.

Table 41. Client certificate key settings (continued)

Setting	Description
Expires in	The number of days the key is valid for.
Key Size	The key size.

Searching for a client certificate

You search for a certificate when you want to enable, disable, or remove the certificate.

Procedure

1. Click **Applications > Key Management** in the navigation menu, and click **Client Certificates**.
2. In the **Narrow Your Search** field, enter your search criteria.

You can search on any 3 character string that is contained in the certificate key label. For example, to search for a certificate with the key label certificate1, you might enter cer or te1.

Certificates that match your search criteria are listed. You can select a certificate to enable, disable, remove, or replace.

Enabling and disabling keys

Only one key can be enabled at any one time.

About this task

When you enable a certificate key, it automatically disables the previously enabled key. You can disable the currently enabled key only by enabling a different key.

Important: If you enable a key, the previously enabled key is disabled. All connections that use the previously enabled key are invalid.

Procedure

1. Search for and select the key that you want to enable.

The screenshot shows a key management interface for a key named 'testserver_key2'. The key is currently 'Disabled'. The interface includes a 'Key Label' field containing 'testserver_key2', a 'Key File' field indicating it is in '.p12 format', and a 'Replace Key' button. The 'Status' section shows two buttons: 'Enabled' and 'Disabled', with 'Disabled' selected. A 'Remove Key' button is located at the bottom of the key's details.

2. Click **Enabled**.

The key is enabled. All new connections now use the newly enabled certificate key.

Downloading a certificate

You can download a certificate.

About this task

For a partner connection where the partner encrypts authentication requests and validates authentication signatures, you can download the public certificate for the private certificate key that is used in the connection.

The public certificate is used in partner-side connector configuration.

Procedure

1. Search for and select the key that you want to download a public certificate for.
2. Click **Download Public Certificate**.
3. Save the file.

Removing a key

You can remove a certificate when it is no longer needed. A key must be disabled to be removed.

Procedure

1. Search for and select the key that you want to remove.
2. Click **Remove Key**.
You are asked to confirm the removal. Click **Remove Key**.

The key is removed.

Replacing a key

In any environment that uses certificates, it is necessary to update certificates and their keys. You might also need to replace a certificate when it is expired.

Procedure

1. Search for and select the key that you want to replace.
2. Click **Replace Key**.

Creating a server certificate

Server certificates are used to identify a server. If you have a server certificate file you want to add, you can upload the file to Cloud Identity Portal.

Procedure

1. Click **Applications > Key Management** in the navigation menu, and click **Server Certificates** and **Add a New Key**.

The screenshot shows a modal dialog titled "Add a New Key" with a close button (X) in the top right corner. The dialog contains two input fields. The first is labeled "Key Label" and has a red asterisk to its right. Below it is a note: "* Label must match label in uploaded Key File". The second field is labeled "Key File" and has a blue "Browse..." button and a red asterisk to its right. At the bottom right of the dialog are two buttons: "Cancel" and "Add a New Key".

2. Enter the key label in the **Key Label** field.
The key label must match the name of the certificate file that you are uploading.
3. Click **Browse** to browse to and select the certificate file to upload.
4. Click **Add a New Key**.

Searching for a server certificate

You search for certificate when you want to remove or replace the certificate.

Procedure

1. Click **Applications > Key Management** in the navigation menu, and click **Server Certificates**.
2. In the **Narrow Your Search** field, enter your search criteria.

You can search on any 3 character string that is contained in the personal certificate key label. For example, to search for a certificate with the key label certificate1, you might enter cer or te1.

Certificates that match your search criteria are listed. You can select a certificate to remove or replace.

Removing a key

You can remove a certificate when it is no longer needed.

About this task

Important: When you remove a certificate, any connections that use the certificate fail. To keep connections valid, you must select a valid certificate for the connection.

Procedure

1. Search for and select the key that you want to remove.
2. Click **Remove Key**.

You are asked to confirm the removal. Click **Remove Key**.

The certificate is removed.

Replacing a key

In any environment that uses certificates, it is necessary to update certificates and their keys. You might need to replace a certificate when it expires.

Procedure

1. Search for and select the key that you want to replace.
2. Click **Replace Key**.

Provisioning identities

Identity Management feeds allow identity data to flow between external identity repositories and the Cloud Identity Service Identity Management environment. Identity provisioning can be inbound and outbound.

Identity provisioning overview

User records can be provisioned by or to external identity repositories by using Identity Management feeds.

Cloud Identity Service can interface with many types of identity repositories, such as Active Directory, LDAP v3, relational databases, SOAP services, Message Queue, and SAP. Users can be automatically added to, modified in, and deleted from Cloud Identity Service through integration with these other identity repositories by defining an inbound connection. Users can be added to, modified in, and deleted from external repositories by using an outbound connection.

Identity repositories

Identity data might be kept in many different systems throughout your organization. These systems are referred to as identity repositories. Each repository might contain different types of identity data. For

example, some might contain simple account-related data to be used by a specific application, such as an SQL database. Other identity repositories might contain more comprehensive identity data that is meaningful to various systems, like Oracle PeopleSoft. The data in these repositories is composed of identity attributes. Identity attributes identify users and comprise user records. For example, a user record might be composed of a user name, given name, surname, email address, and job role. Cloud Identity Service acts as an Identity Management (IDM) system by using its identity provisioning capabilities to keep identity data accurate, consistent, and current, between the different repositories in your organization.

Feed management

As repositories are integrated with Cloud Identity Service, defining how to connect to, and provision identity data between these systems is key to synchronizing data between repositories. Feed management enables identity data, such as attributes, groups, roles, and account information, to flow between your other identity repositories and Cloud Identity Service.

An IDM system can be thought of as a hub-and-spoke model. Cloud Identity Service sits in the middle of all your identity repositories as the hub. Identity data flows into and out of Cloud Identity Service, from and to your other identity repositories. Data that flows from an identity repository to Cloud Identity Service is inbound, while data that flows from Cloud Identity Service is outbound.

An Identity Management feed contains many types of business rules that define how Cloud Identity Service interacts with other identity repositories:

- Connection information. Connection information determines how and when Cloud Identity Service connects to a repository, and how to parse and interpret information from that repository.
- Provisioning policy. A master provisioning policy determines under what circumstances Cloud Identity Service transmits or receives identity data to or from a repository. Provisioning policies also determine what data to ignore.
- Attribute and group mapping information. Attributes and groups in different identity repositories do not use the same naming conventions. Identity attributes can be mapped between the different repositories to the information contained in Cloud Identity Service. The mapping functions of Cloud Identity Service Identity Management feeds allow simple and complex mapping logic, including mapping between groups.

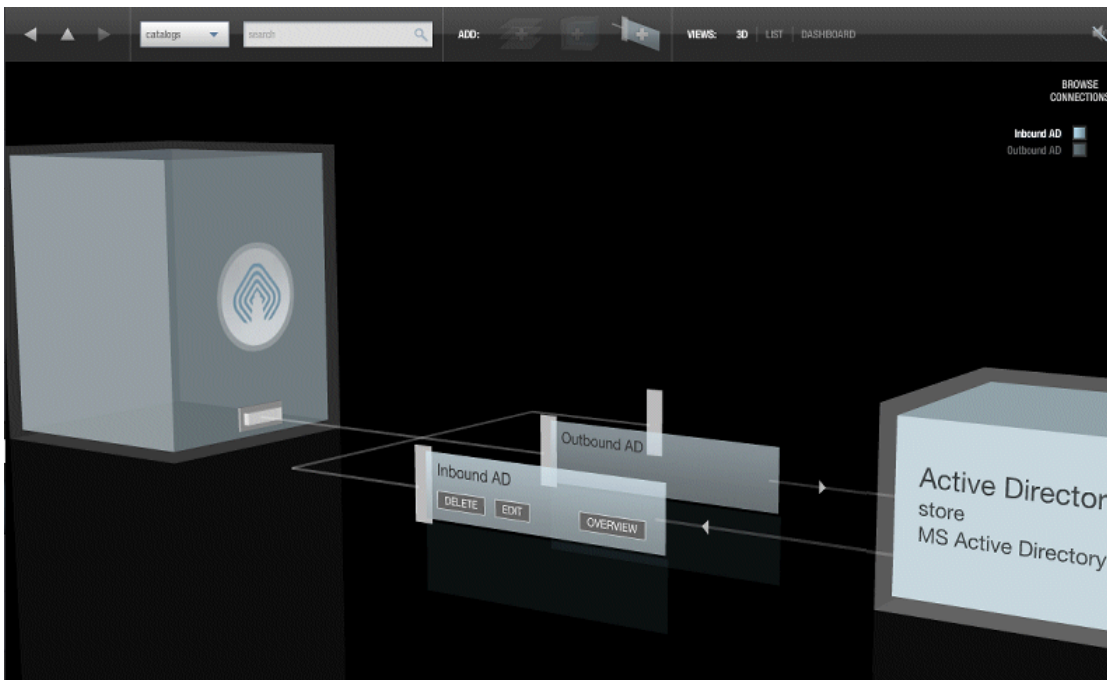
Assembly Lines

In Cloud Identity Service, Identity Management feeds are called Assembly Lines. Assembly Lines are configured during the initial setup of Cloud Identity Service for your organization. Assembly Lines are defined by using Template Assembly Lines (TALs). Each TAL contains a number of configurable options for connections.

Feed Management UI

The Feed Management UI provides a graphical representation of configured management feeds.

Cloud Identity Service can interface with many types of identity repositories, such as Active Directory, LDAP v3, relational databases, SOAP services, Message Queue, SAP, and PeopleSoft. Users can be automatically added to Cloud Identity Service through integration with these other identity repositories, and users can be added from Cloud Identity Service to external repositories.



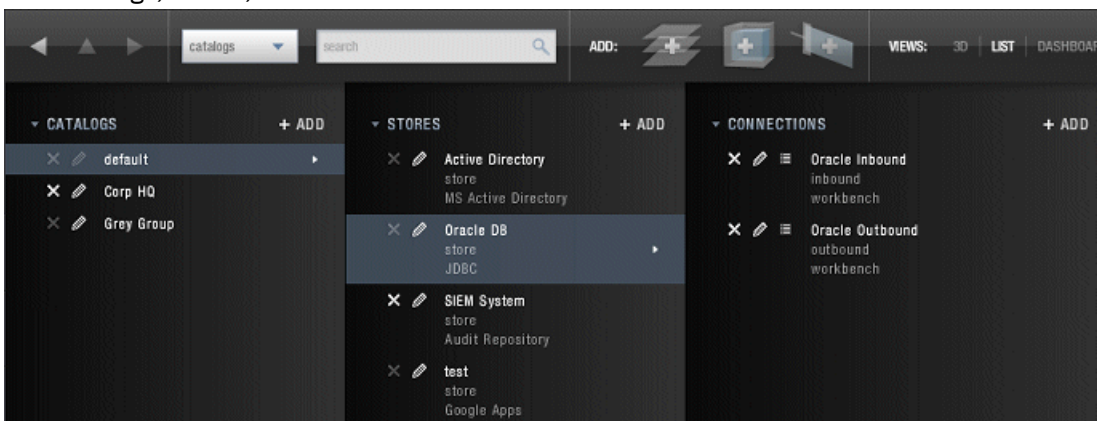
Catalogs, stores, and connections

Catalogs provide a way to group external identity repositories that are connected to Cloud Identity Service services. For example, a catalog might be defined for corporate a department such as Finance or IT. Stores are external identity repositories that are grouped under catalogs. Cloud Identity Service can support the most common identity repositories, such as Active Directory, LDAP v3, relational databases, SOAP services, Message Queue, and SAP.

Connections define how Cloud Identity Service connects to and interacts with external identity repositories. Connections can be inbound and outbound.

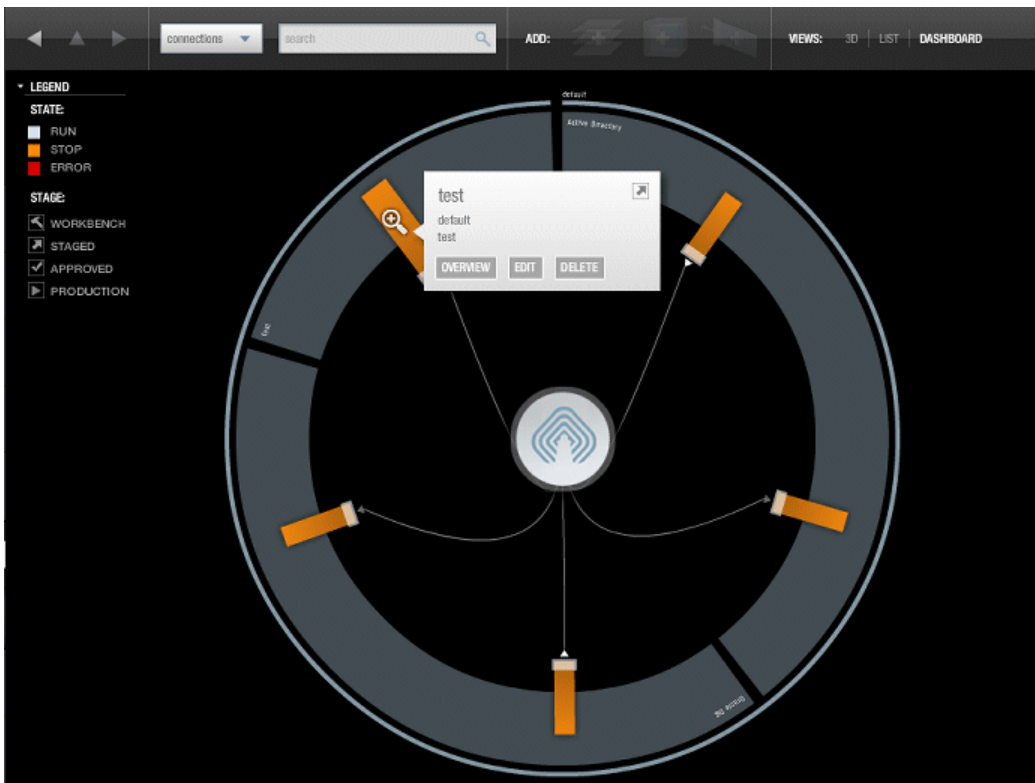
List view

You can view your feed management system in the List view, making it easier to browse, view, add, and edit catalogs, stores, and connections.

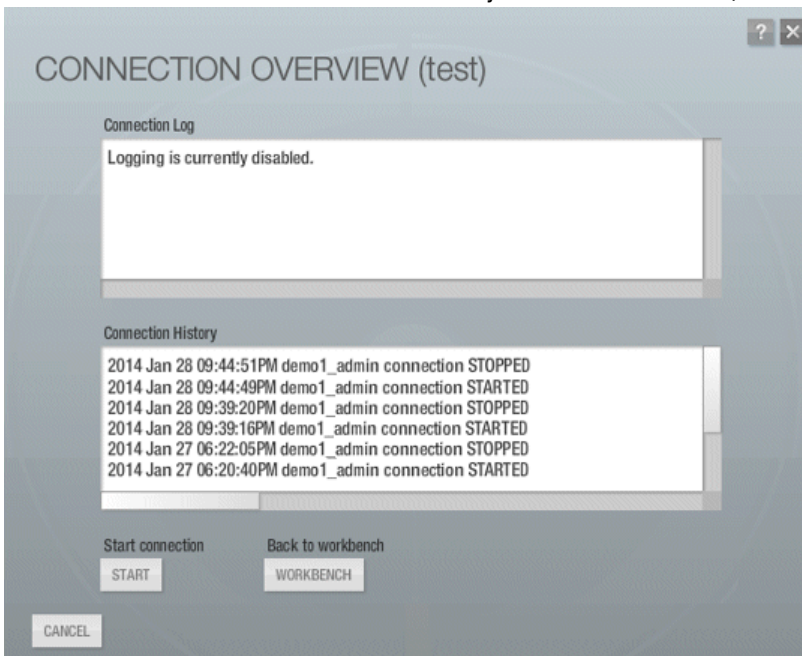


Dashboard view

After connections to stores are established, administrators can view the entire feed management system from the Dashboard. Color coding indicates the state of connections.



Administrators can view the event history of each connection, and can start and stop a connection.



Managing reverse proxy settings

You can manage reverse proxy settings to change the timeout values for user sessions for protected resources.

Procedure

Click **Applications > Reverse Proxy Settings**.

Reverse proxy settings

The timeout values for user sessions apply to all sessions for all web resources that are secured behind Cloud Identity Service.

Timeout value

The timeout value sets the maximum lifetime timeout value for all authenticated or unauthenticated user sessions. The timeout value determines the length of time authorization credential information remains valid for. Users must reauthenticate when the specified timeout limit is reached. The default session entry lifetime timeout 3600 seconds. A value of 0 disables the timeout feature (timeout value is unlimited).

Inactive timeout value

The inactive timeout value sets the timeout value for user session inactivity. For example, if a user is inactive for a period longer than the inactive timeout value, the session is ended or the session is flagged as requiring reauthentication. The default login session inactive timeout is 600 seconds. A value of 0 disables this inactivity timeout feature (inactive timeout value is unlimited).

Chapter 8. Mobile application



Users can use the IBM mobile app to access Self Service applications by using their mobile devices.

The IBM mobile app is also a prerequisite to receive one-time passwords (OTP) and push notifications to authenticate to Self Service applications.

Overview

The IBM mobile app provides users with access to Self Service applications from their mobile devices.

What does IBM mobile do?

Users can make service requests from their mobile devices with the IBM mobile app, and managers can approve and decline service requests. You can access applications that are linked to your services. The IBM mobile app also has a one-time password generator for two-step authentication to Self Service applications.

Why do you need IBM mobile?

You need the app to access Self Service applications from your mobile devices, and to launch service applications from your mobile devices.

You also need the app if your company uses multi-factor authentication to access Self Service applications with push notification or one-time password (OTP).

Which mobile devices are supported by IBM mobile?

IBM mobile supports Apple devices that run iOS Version 10.0.0 or later and Android devices that run Lollipop or later.

What is multi-factor authentication (MFA)?

MFA requires more than one method of authentication from separate sources to verify a user's identity. Cloud Identity Service uses a two-step MFA. Your identity is verified by entering a user name and password, and by entering a code or accepting a notification sent to your mobile device.

Two-step verification works in the following way.

1. Sign in to your Self Service application as you normally do, with your user name and password.
2. A verification notification is sent to your mobile device, by using an SMS message, or a generated OTP, or as a push notification.
3. Verify your identity on your mobile device by entering the code or accepting the notification.

Getting started

Get started with the IBM mobile app by downloading and installing the app, and connecting your device to your Cloud Identity Service account.

Downloading the app

Install the app on your device.

Procedure

1. Start the App Store (iOS) or Google Play Store (Android) app.
2. Search for IBM mobile app.
3. Tap **Get** and **Install** to download the app.
4. Tap the app icon to open the app.

Logging in

Log in to your Cloud Identity Service account on your mobile device.

About this task

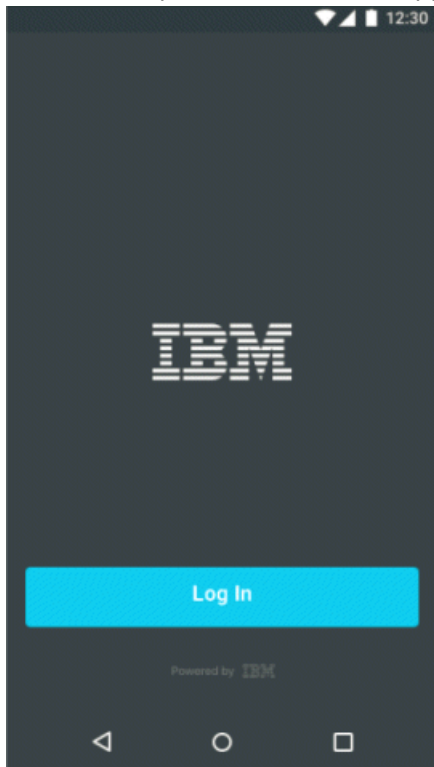
You can scan a QR code to log in to your account or you can use a one-time password (OTP) code. When your session expires, you can log in again by entering your user name and password.

Logging in with a QR code

Scan a QR code to log in to your account. If you cannot scan the QR code, you can enter a code manually.

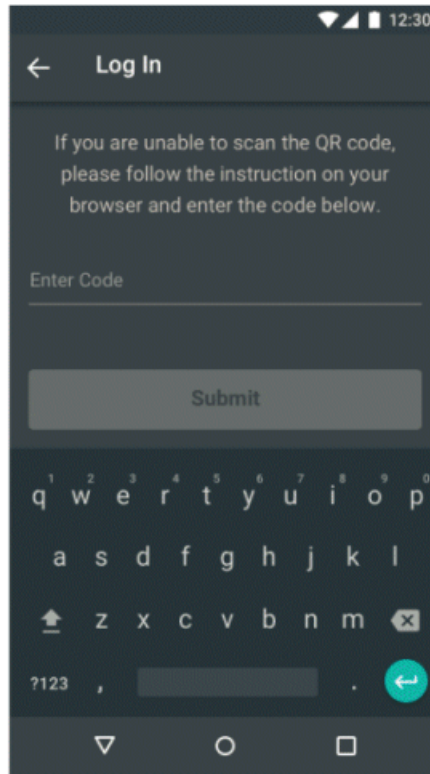
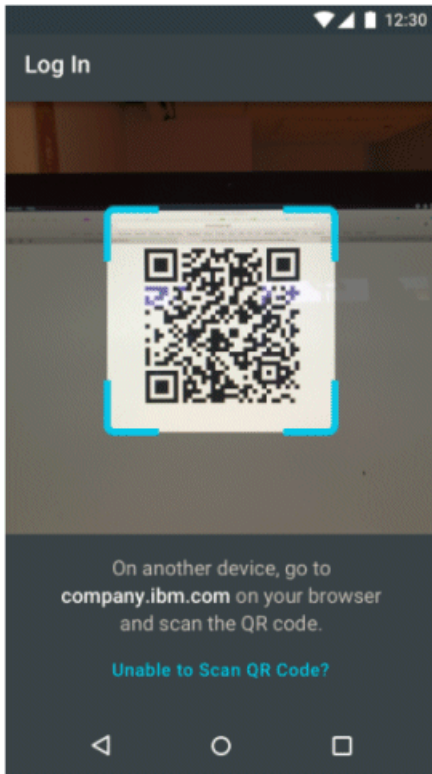
Procedure

1. Locate and open the IBM mobile app on your device, and tap **Log In**.

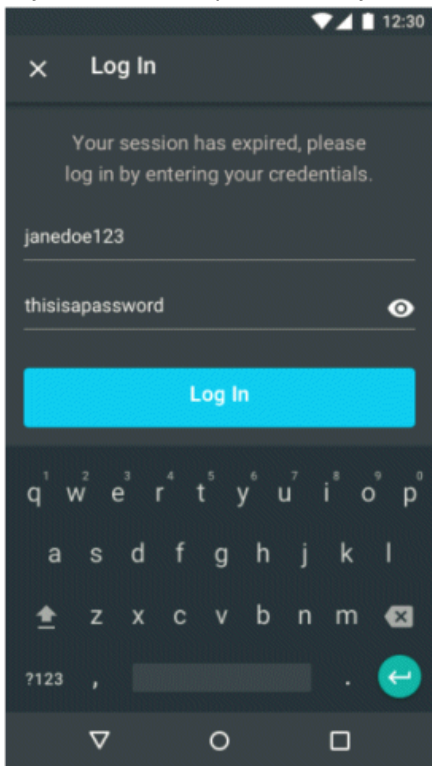


A QR code is sent to your account.

2. On another device, go to **company.ibm.com** and scan the QR code. If you are unable to scan the QR code, tap **Unable to scan QR code** and follow the instructions to enter a code manually.



3. If your session expires, enter your user name and password and tap **Log In**.

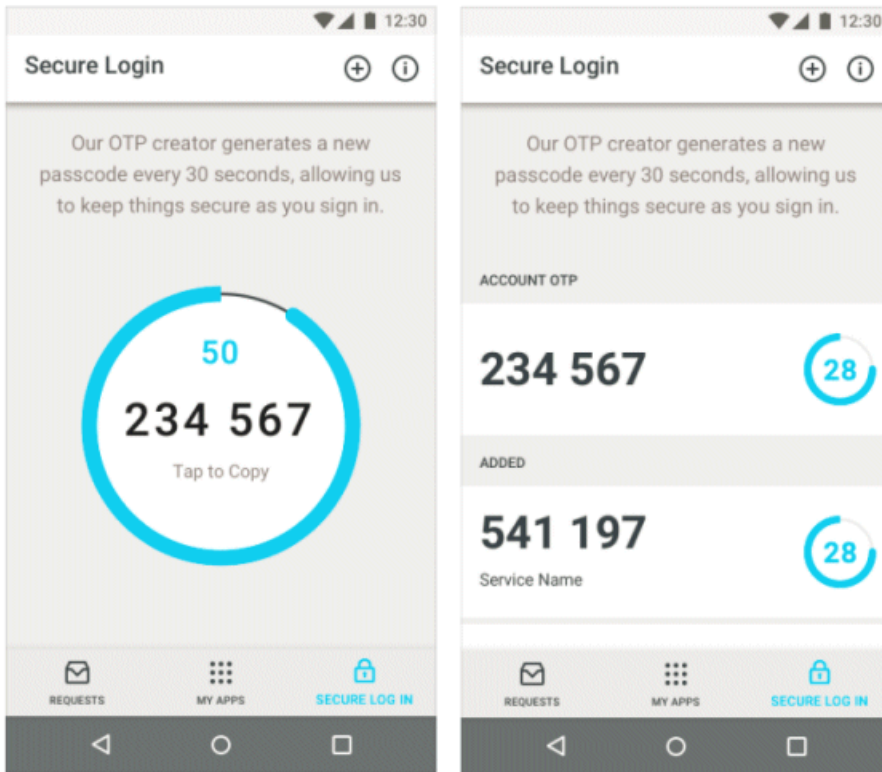


Logging in with a one-time password

Log in using an OTP code.

Procedure

Locate and open the IBM mobile app on your device and tap **Secure Log In**, select the OTP generating service that you want to use.



You can add an OTP generating service by scanning a QR code or manually entering a code.

Managing your devices

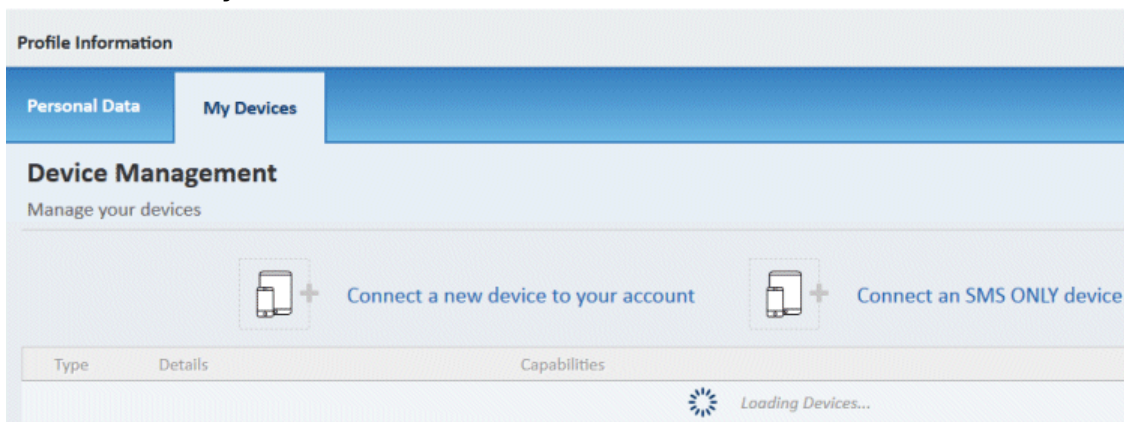
Register and manage your devices from the Cloud Identity Service Self Service portal.

About this task

Add new devices and remove devices you no longer use. You can add SMS only devices and fully enabled devices by scanning a QR code or entering a code manually. You register a device when on your first log in the Self Service portal.

Procedure

1. Log in to the Self Service portal from your computer.
2. Select **Profile > My Devices**.



3. Add or remove devices.

Deleting the app

Delete the app if you no longer use the device, or no longer need access to Cloud Identity Service.

About this task

Note: Deleting the IBM mobile app does not remove any two-step verification that is in force for your Cloud Identity Service account.

Procedure

1. Locate and select the IBM mobile app on your device.
2. Tap **Delete**.

Managing services and launching apps

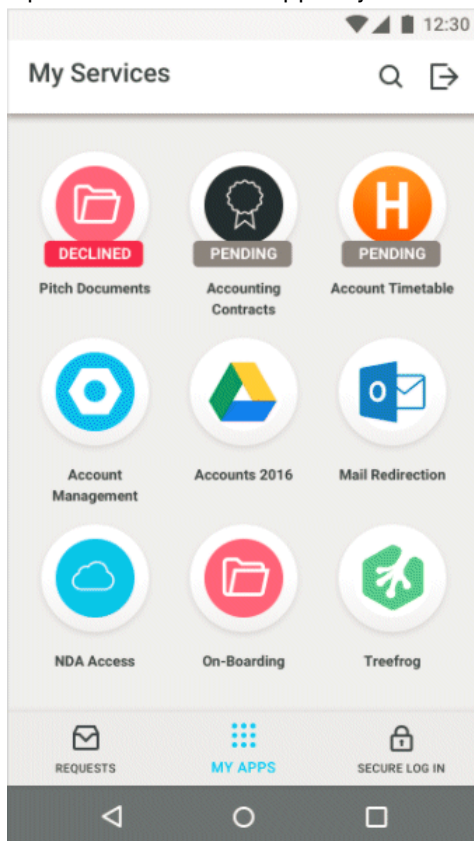
Use the IBM mobile app to view your services and to request access to services.

Viewing services and launching applications

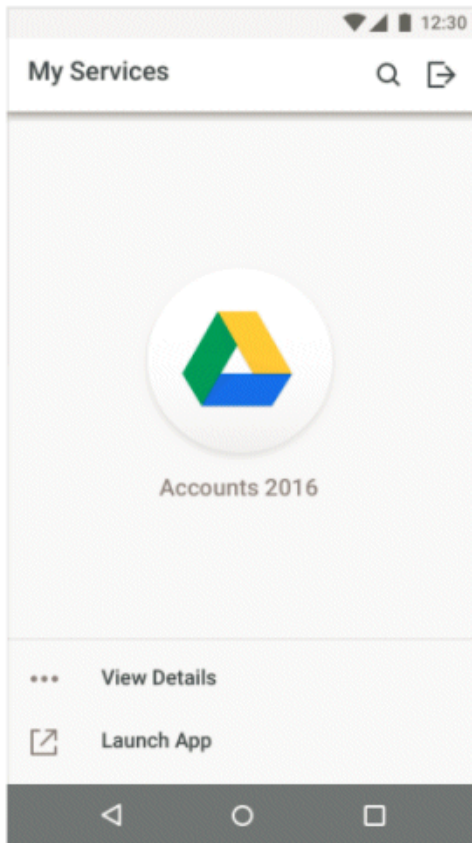
You can view services that you have access to, and you can launch linked applications.

Procedure

1. Open the IBM mobile app on your device, and tap **My Apps**.



2. Tap the icon to open the service.



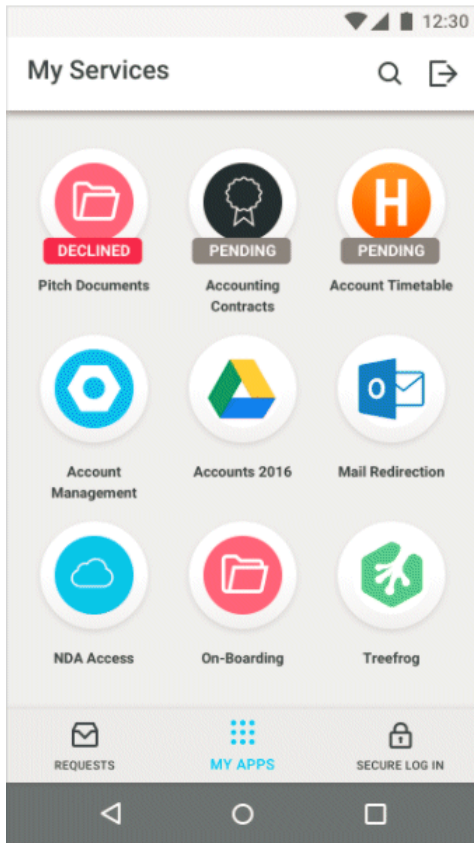
3. Tap **View Details** to view details of the service, or tap **Launch App** to launch the application that is linked to the service.

Requesting access to a service

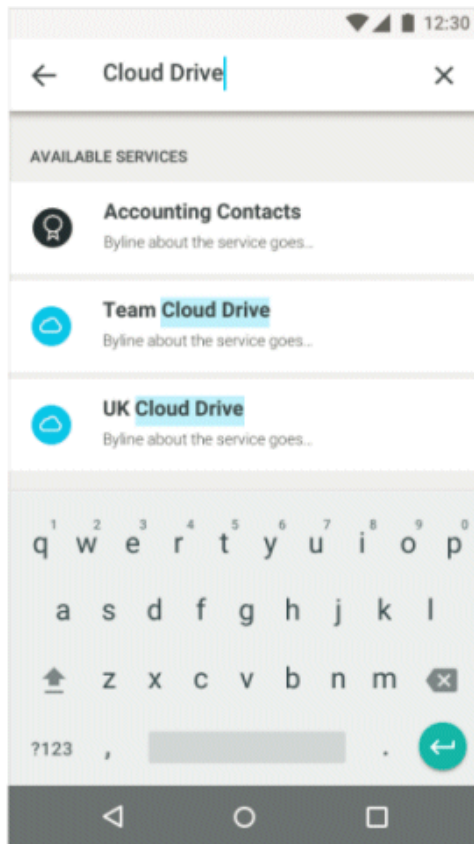
To gain access to services and linked applications, search for the service and submit a request.

Procedure

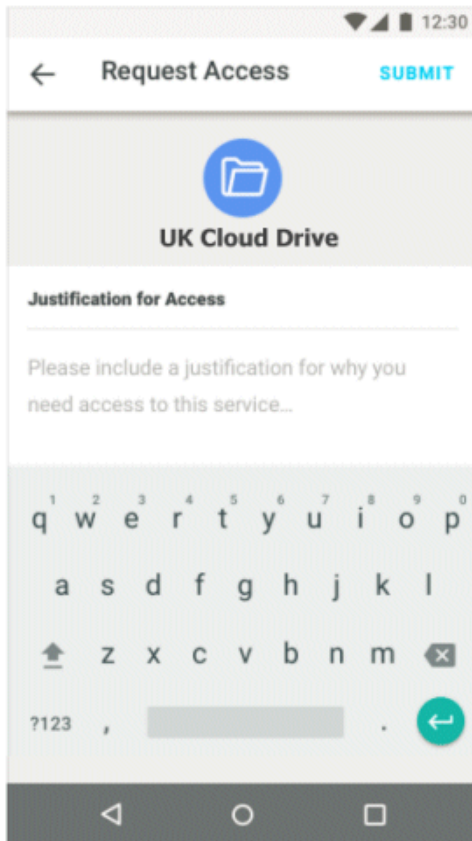
1. Open the IBM mobile app on your device, and tap **My Apps**.



2. Search for the service from the available services.



3. Tap the service to select it, enter a justification for requesting the service and tap **Submit**.



The status of the service changes to pending. Your manager can accept or decline your request.

Managing requests

Use the IBM mobile app to approve and deny requests for services.

About this task

This task is for user managers to approve or deny an employee requests to access services. You can select requests by searching by employee or by searching by service.

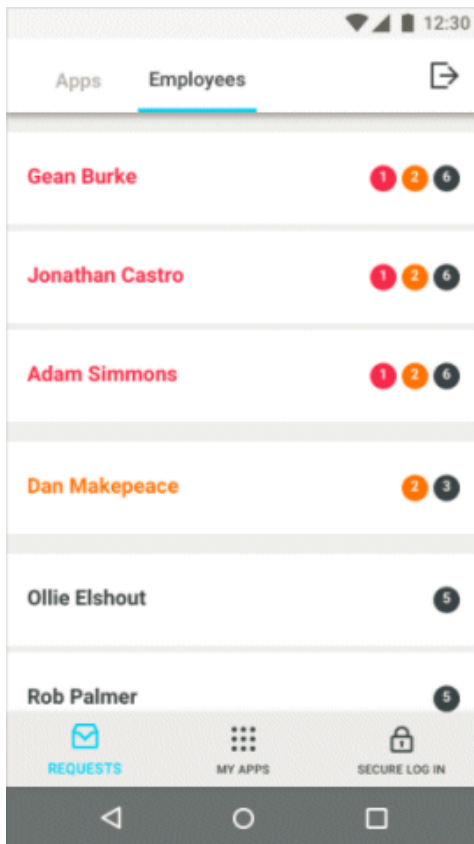
The number of outstanding approvals and their status is shown for each of your managed users. Overdue approvals are colored red. Nearly due approvals are colored yellow. Approvals that are not overdue or nearly overdue are colored dark gray.

Searching by employee

Search for approvals by employee.

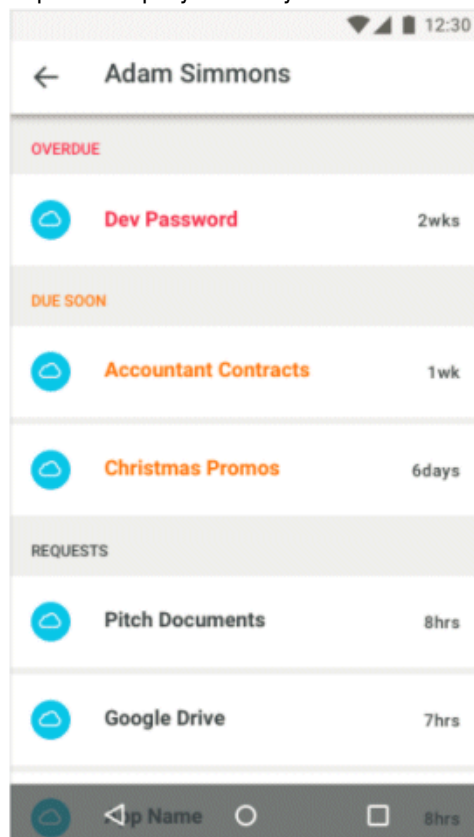
Procedure

1. Open the IBM mobile app on your device, tap **Requests** and tap **Employees**.



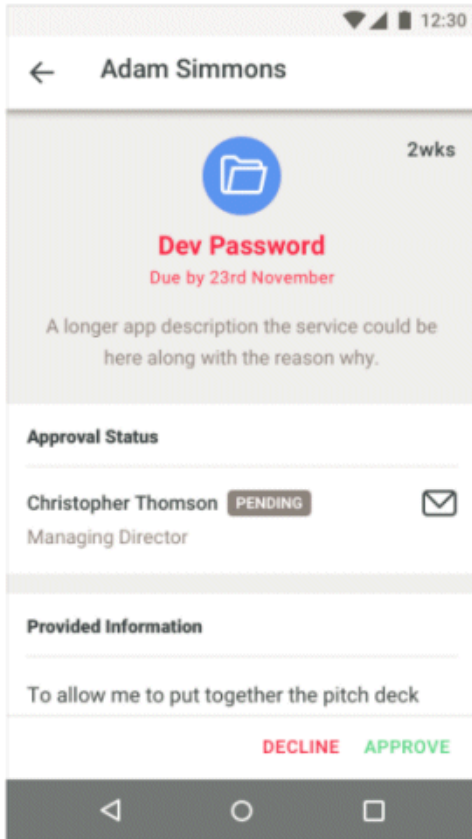
Employee requests are ordered by approval due date and time. Employees with the most overdue requests are shown first. The number of requests and the status of the requests is also displayed.

2. Tap the employee that you want to manage requests for.



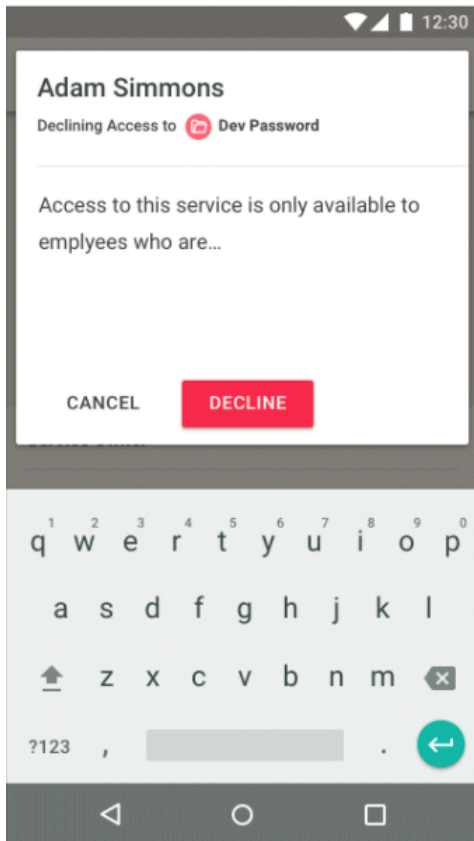
Requests are now ordered by service and by the due date and time.

3. Tap a service to view the request for that service.



4. Approve or decline the request:

- Tap **Approve** to approve the request.
- Tap **Decline** to decline the request, enter a justification if needed.

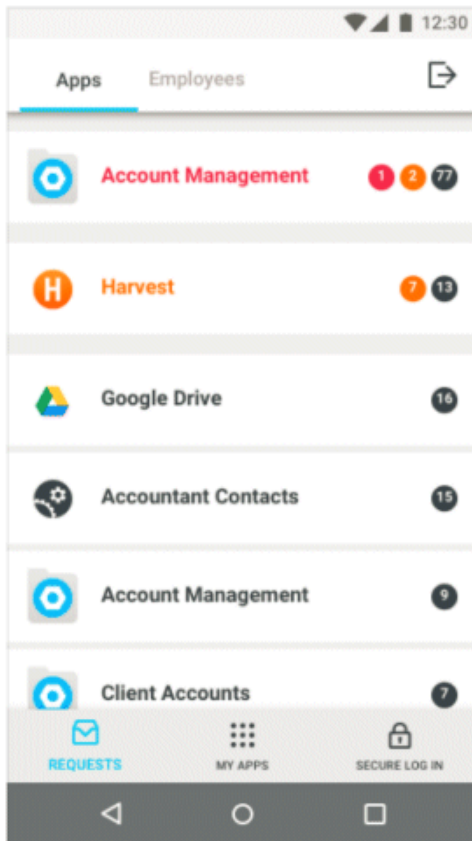


Searching by service

Search for approvals by service.

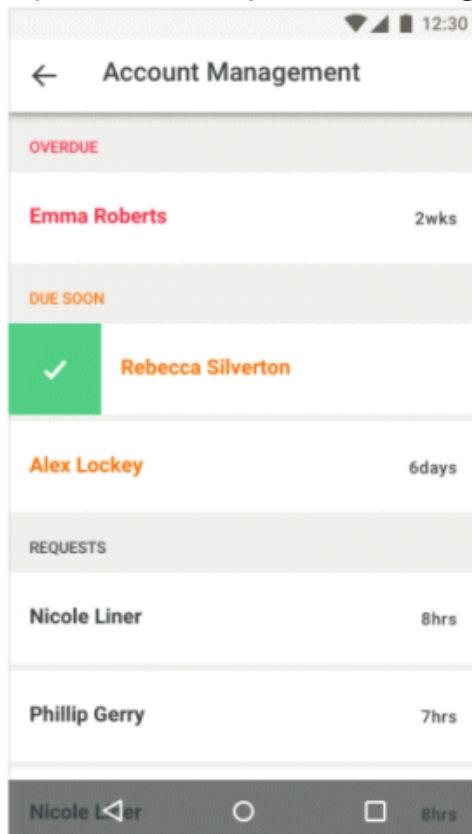
Procedure

1. Open the IBM mobile app on your device, tap **Requests** and tap **Apps**.





Requests are ordered by approval due date and time. Services with the most overdue requests are shown first. The number of requests and the status of the requests is also displayed.

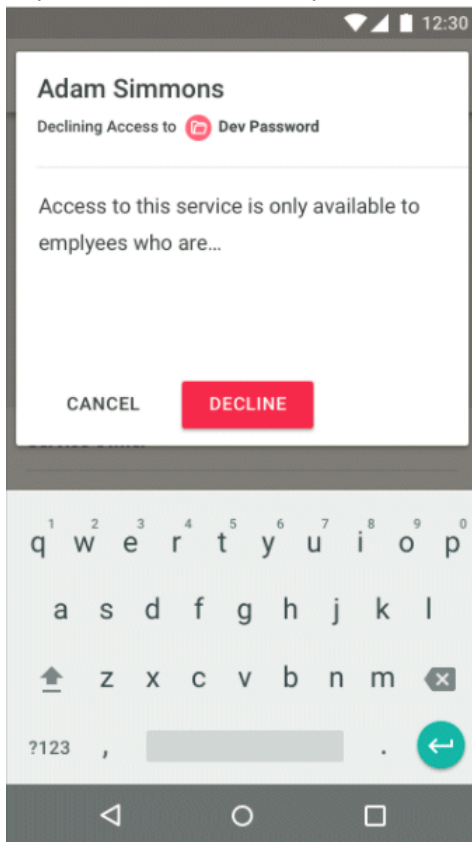
2. Tap the service that you want to manage requests for.



Requests are now ordered by employee and by the due date and time.

3. Select the employee that you want to manage the request for, and approve or decline the request:

- Tap  to approve the request.
- Tap  to decline the request, enter a justification if needed.



Chapter 9. Policies



Policies are used to determine or refine user access to different resources.

Creating a global user policy

User policies define the maximum number of login failures, the maximum password age, and account expiration dates for users. Global user policies are applied to all users.

Procedure

1. In the navigation pane, click **Policies > Global User Policies**.
2. Set the user policy settings that you want.
3. Click **Save**.

User policy settings

Setting	Description
Maximum Login Failures	<p>The maximum number of failed logins a user can attempt before their account is locked. If this option is set to 0 or Unset, then the number of failed login attempts is limitless.</p> <ul style="list-style-type: none">• Set. The maximum number of failed login attempts. If this option is set to 0, then the number of failed login attempts is limitless.• Unset. No limit to the number of failed login attempts.
Disable Time Interval	<p>Specify whether user accounts are locked after the Max Login Failures count is exceeded.</p> <ul style="list-style-type: none">• Set. User accounts are locked after the Max Login Failures count is exceeded. Accounts are disabled permanently or temporarily.• Unset. User accounts never lock due to failed login attempts. Unset is equivalent to setting the Max Login Failures to 0 or Unset, users have an unlimited number of login attempts.• Disable Permanently. The user is locked out permanently until a Cloud Identity Portal administrator sets the User Status of the user to valid.• Disable Temporarily. The time, in seconds, that a user account will remain locked after the Max Login Failures count is exceeded. The account will be unlocked after the interval time is passed.

Table 42. User policy settings (continued)

Setting	Description
Minimum Length	<p>The minimum number of characters that are required for a valid account password.</p> <ul style="list-style-type: none"> • Set. The minimum number of characters for a password. • Unset. No minimum password length.
Minimum Alphas	<p>The minimum number of alphabetic characters that are required for account passwords.</p> <ul style="list-style-type: none"> • Set. The minimum number of alphabetic characters that the password must contain. • Unset. No minimum is imposed.
Minimum Non-Alphas	<p>The minimum number of non-alphabetic characters (numbers or special characters) that are required for account passwords.</p> <ul style="list-style-type: none"> • Set. The minimum number of non-alphabetic characters that the password must contain. If set to 0, then no minimum is imposed. • Unset. No minimum is imposed.
Maximum Repeated Characters	<p>The maximum number of consecutive repeated characters that are allowed in an account password.</p> <ul style="list-style-type: none"> • Set. The maximum number of repeated characters that are allowed. • Unset. No limit to the number of repeated characters.
Spaces Allowed?	<p>Specifies whether account passwords can contain spaces.</p> <ul style="list-style-type: none"> • Set. Specify whether spaces are allowed. <ul style="list-style-type: none"> – Yes. Spaces are allowed. – No. Spaces are not allowed. • Unset. Spaces are allowed.
Password Expires?	<p>The maximum amount of time that passwords remain valid after creation, and then expire and must be changed.</p> <ul style="list-style-type: none"> • Yes. The number of days, hours, minutes, and seconds that a password is valid. If all values are set to 0, passwords never expire. • No. Passwords never expire.
Track Password Reuse?	<p>Specifies whether the same password can be used when a password is reset.</p> <ul style="list-style-type: none"> • Yes. Users cannot use the same password when they reset or change their password. Specify the number of new unique passwords that must be set before an old password can be reused. • No. Users can use the same password when they reset their password.

Table 42. User policy settings (continued)

Setting	Description
Account Expires?	<p>Specifies an expiration date after which all accounts are set to invalid. This setting is normally only used for individual user policy overrides. For example, if a contractor has a finite access period to a specific resource this option can be used to disable that access on a specific date.</p> <ul style="list-style-type: none">• Set. The expiration date for accounts. Enter the date in MM/DD/YYYY format.• Unset. Unlimited period of validity, the validity of accounts never expires.
Limit Access?	<p>Specifies a time-of-day constraint for when users can access the system.</p> <ul style="list-style-type: none">• Yes. The days and time of day that users can access the Cloud Identity Service. Time can be expressed as the local time for the service, or Coordinated Universal Time.• No. Users can access the Cloud Identity Service at any time.

Chapter 10. Identity governance



Normally, requests are managed in Self Service applications by specified managers. Administrators can manage user requests when needed, in Cloud Identity Portal.

If the normal approver is not available and has no delegated approver, it can be necessary for a Cloud Identity Portal administrator to manage user requests for services.

Searching for a request

You search for a request when you want to approve, reassign, or deny a request. You can also send a reminder to the request approver.

Procedure

1. In the navigation pane, click **Identity Governance > Request Management**.
2. In the **Refine your results** field, enter your search criteria.

You can search on the first 3 or more characters of the first or last name or username of the person the request is made for. You can also search on the first 3 or more characters of the first or last name or username of the approver. You can also search on the first 3 or more characters of the first or last name or username of the person the request is made by or service name or record type of request. For example, to search for requests for an approver that is called John Smith, you might enter `smi` or `joh` or `John Smith`.

<input type="checkbox"/>	Requested For	Details	Type
<input type="checkbox"/>	Monica PorterPortland	CMB Test 01	Service Group
<input type="checkbox"/>	Monica PorterPortland	Interesting Application	Service Group
<input type="checkbox"/>	Monica PorterPortland <i>Requested by: Sue Crawford</i>	Demo Exchange	Service Group

Requests that match your search criteria are listed.

You can filter the list by using the **All**, **Past Due**, and **Due Soon** check boxes. You can sort the list by clicking a column header to sort the list by that column.

Approving, denying, and reassigning requests

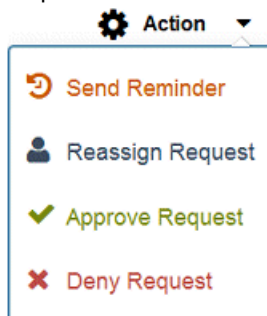
If no action is taken for a request by an approver, you can approve, reassign, or deny a request. You can also send a reminder to the request approver.

About this task

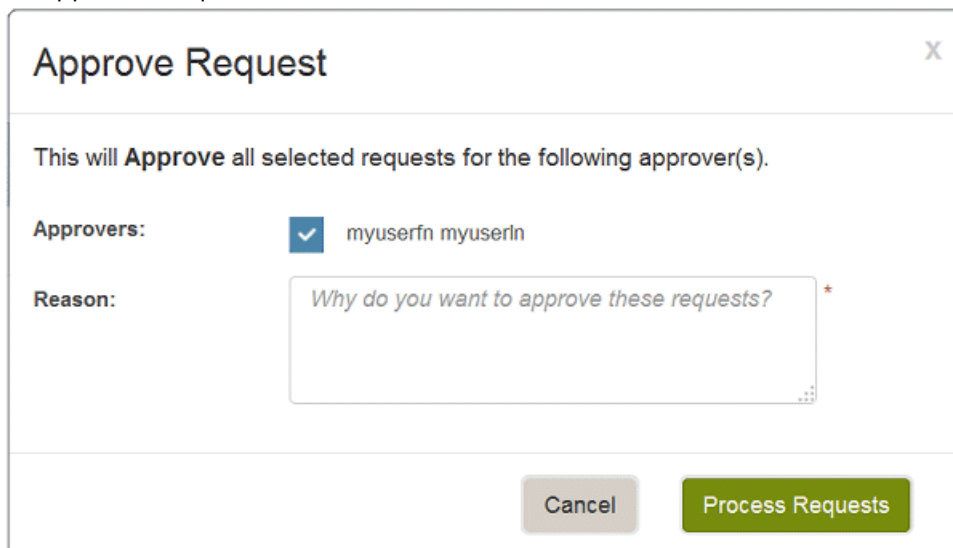
Expired approvals are shown in rows that are colored red. Nearly expired approvals are shown in rows that are colored yellow.

Procedure

1. Search for the request.
2. Select the request, click the **Action** menu, and select the action that you want to perform for the request.



- To approve a request:

A screenshot of a dialog box titled 'Approve Request'. The dialog has a close button (X) in the top right corner. Below the title, it says 'This will Approve all selected requests for the following approver(s)'. Under 'Approvers:', there is a checked checkbox next to the text 'myuserfn myuserfn'. Below that, there is a 'Reason:' label followed by a text input field containing the placeholder text 'Why do you want to approve these requests?'. At the bottom of the dialog, there are two buttons: 'Cancel' and 'Process Requests'.

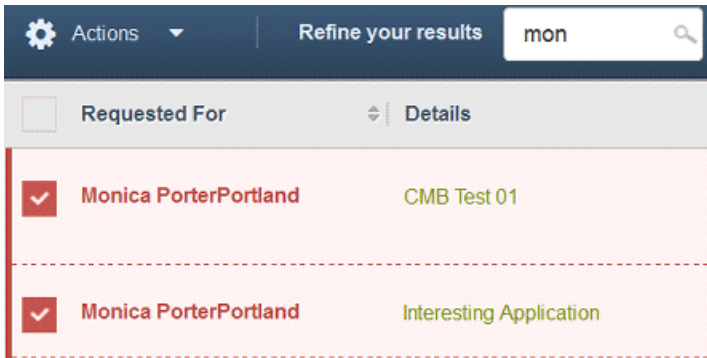
- a. Select the approvers on whose behalf the request is being approved.
 - b. Enter a reason for approving the request.
 - c. Click **Process Requests**.
- To reassign a request:
 - a. Select the approvers on whose behalf the request is being reassigned.
 - b. Search for and select the user who the request is being reassigned to.

New Approver:

You can search on the first three or more characters of the first name or last name of the manager.

- c. Enter a reason for reassigning the request.
- d. Click **Process Requests**.
- To send a reminder to the approver:
 - a. Select the approvers to send the reminder to.
 - b. Enter a reason for sending the reminder.
 - c. Click **Process Requests**.

You can also perform an action for multiple requests by selecting the required request check boxes.



You can select all requests by using the check box in the column header. Use the **Action** menu in the column header to perform an action for multiple requests.

Notices

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

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

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

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

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

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

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

IBM Corporation
224A/101
11400 Burnet Road
Austin, TX 79758 U.S.A

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

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

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

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

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

Trademarks

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

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

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

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

