Lifecycle Manager

Version: 8.3

Revised: April 2022

Contents

Lifecycle Manager Setup

> SailPoint IdentityIQ Lifecycle Manager is sold as a separate license and must be purchased and activated before it is available for use.

The Lifecycle Manager portion of IdentityIQ Setup includes of the following:

- Lifecycle Manager Configuration
- Configuring Full Text Searching
- Creating Direct Links to IdentityIQ

Lifecycle Manager Configuration

Use Lifecycle Configuration to customize the availability of tools and functionality based on end user needs. Lifecycle Manager configuration is divided into the following sections:

> IdentityIQ System Administrators can make any request regardless of the Lifecycle Manager Configuration settings.

- Configure Tab
- Business Processes Tab
- Identity Provisioning Policies Tab

Configure Tab

Use the Configure tab to customize your Lifecycle Manager configuration. The Configure tab includes the following.

General Options

Allow requesters to set request priorities

Use this option to enable requesters to set the priority level of their request. If this option is not selected, all requests have a default “Normal” priority level.

Enable Account Group Management

Use this option to enable provisioning of account groups through Lifecycle Manager requests.

Enable Full Text Search

Use this option to enable full text searching on the Lifecycle Manager request pages. Enabling full text searching might have some affect on the performance of those pages. For detailed information, see Configuring Full Text Searching.

You must run the Full Text Index Refresh task before full-text search is available. Refer to the system administration documentation for more information.

Base directory path used to store full text index files

The directory on the server in which full text index searches are stored.

Enable automatic index refresh

Enables the automatic refreshing of the full text index at the interval specified.

Allow Searching by Population when requesting access

Enable the use of populations as a search filter.

Allow Searching by Identity when requesting access

Enable the use of identities as a search filter.

Allow opt-in to viewing request access search result details

Use this option to limit the amount of information displayed for each item on the Access Request, Review and Submit panel and add a **View Details** button on each item to show the complete information. This feature enables more items to display on each table.

Show external service request details

Use this option to display the information such as request numbers and ID from external ticketing systems throughout IdentityIQ.

Maximum number of results returned in a Request Access search

Limit the number of items returned by an access request. Large lists are hard to scan and the search should be narrowed or refined.

Maximum number of selectable users in Request Access

Limit the number of selectable users returned by an access request. Large lists are hard to scan and the search should be narrowed or refined.

Applications that support additional account requests

Use the drop-down list to specify the applications on which multiple accounts can exist or be created.

Select **All Applications** to include all applications in your environment.

Request Role Options

Request Role Options

Select the role types that are available for role requests. Any options not selected are unavailable to any user attempting to make that type of request.

When searching for roles based on population, only return roles contained by at least the following percentage of the population

Specify the minimum percentage of a population whose roles must match any given search criteria.

Request Entitlement Options

When searching for entitlements based on population, only return entitlements contained by at least the following percentage of the population

Specify the minimum percentage of a population whose entitlements must match any given search criteria.

Entitlement Search Results must return less than this number of identities when searching by identity

Indicate the maximum amount of identities an entitlement search result can yield.

Create Identity Options

Require password on all identity creation requests.

Require a password on all identity creation requests.

Enable self-service registration

Enables new user self-registration and creates a link for registration on the IdentityIQ login page.

The `securityOfficerName` variable must be configured within the LCM Registration process variable before the self-service registration functionality is fully enabled. The default `securityOfficername` is the IdentityIQ system administrator. For more information, see the **System Configuration** documentation.

Follow these steps to setup self-service registration:

1. From the navigation menu bar, go to **Setup** > **Business Processes**.
2. In the Edit An Existing Process panel, select **LCM Registration**.
3. Click the **Process Variables** tab. You can use the **Advanced View** option to view or configure all available variables.
4. **Security Officer** is the default setting for the **Approvers** field.
5. To delete the **Security Officer** setting, click the **x** icon next to it.
6. To add another setting, click the down-arrow next to the **Approvers** field and select another entry.
7. The default entry for the **Fallback Approver** is the IdentityIQ system administrator. If desired, you can change the **Fallback Approver**.
8. When you are satisfied with all of the entries, click **Save** at the bottom of the screen.

URL of action button after successful registration

Enter a URL to redirect the browser to the specified page after successful user registration. If this field is blank, the user is redirected to the login page.

Prevent pruning of new identities for this many days

Select the number of days that must pass after the creation of an identity before it can be pruned. Default is 30 days.

Manage Account Options

Show Enable/Unlock decision buttons regardless of whether the account is disabled or unlocked.

Display the decision buttons on account management page for disabled or unlocked accounts.

Manage Account Actions

Choose which actions are enabled for Manage Accounts requests for yourself and subordinates. Options include the following:
Delete
Disable
Enable
Unlock
Deselected options are unavailable to a user attempting to make that type of request.
Select one or more applications from the Applications that support account only requests to specify which applications allow Account Only requests. Select All Applications to enable this feature for all applications.

Disable auto refresh account status

The status is automatically refreshed only for the accounts from applications that are not listed in the Disable auto refresh account status list AND accounts that support the Enable or Unlock feature AND accounts without the NO_RANDOM_ACESS feature.

Deactivate auto refresh for account status. By default, accounts from all applications support this feature.

Applications that do not support auto refresh account status

Select one or more applications to deactivate auto refresh.

Applications that support account only requests

Select applications from the drop-down list that support request for accounts that are not associated with a role or entitlement.

Select All Applications if un-associated accounts can be request for all applications.

Manage Password Options

Choose Enable password auto-generation when requesting for others to enable passwords to be auto-generated when requests are made on behalf of another user by an authorized user.

Password Validation Rule

Select a rule from the drop-down list to used when validating password creations.

AI Services

The AI Services section appears only if the AI Services feature has been integrated and configured in IdentityIQ.

See the **AI Services** documentation for more information.

Enable AI Services recommendations on approvals

Show AI Services recommendations for approval decisions in access reviews.

Enable AI Services recommendations on access requests

Show AI Services recommendations in access requests, to see access items that are recommended for you. This option is available only when the user is requesting access for themself, and does not appear when the user is requesting access for others.

Batch Request Approver

Require an approval before granting batch requests.

Manage Classifications Options

This option determines whether classification data is shown with access items, roles or entitlements, in access **requests**. This option is provided so that you can choose whether or not to alert requesters to the fact that certain roles or entitlements may allow access to sensitive or protected data. Classification data always appears in access **approvals**, regardless of this setting.

Manage Elevated Access Options

This option determines whether elevated access is shown on roles and entitlements in access requests.

Business Processes Tab

Use the Business Process tab on Lifecycle Manager Configuration to determine which business process is used when performing specified Lifecycle Manager actions.

Identity Provisioning Policies Tab

Identity Provisioning Policies are used to define identity attributes that must be set when creating an identity from a Lifecycle Manager request.

The following types of Identity Provisioning Policies are available:

- Create Identity
- Update identity
- Self-service Registration

> If an Update provisioning policy is defined, that policy overwrites the Create policy.

You must include the criteria required by the provisioning policy in the generated form before the request can be completed. Use the Provisioning Policy Editor to customize the look and function of the form fields generated from the provisioning policy.

Name

The name of your provisioning policy.

Description

A brief description of the provisioning policy.

Provisioning Policy Editor

Use the Edit Provisioning Policy Fields panel to customize the look and function of the form fields generated from the provisioning policy.

Attribute

Select the attribute field from the drop-down list to display on the form generated from the provisioning policy.

Display Name

The name displayed for the field in the form generated by the provisioning policy.

Help Text

The text you wish to appear when hovering the mouse over the help icon.

Type

Select the type of field from the drop-down list. Choose from the following:
Boolean — true or false values field
Date — calendar date field
Integer — only numerical values field
Long — similar to integer but is used for large numerical values
Identity — specific identity in IdentityIQ field
Secret — hidden text field
String — text field

Multi Valued

Choose this to have more than one selectable value in this field of the generated form. Click the plus sign to add another value.

Read Only

Determine how the read only value is derived:
Value — value based on the selection from the drop-down list
Rule — value is based on a specified rule
Script — value is determined by the execution of a script

Hidden

Determine how the hidden value is derived:
Value — value based on the selection from the drop-down list
Rule — value is based on a specified rule
Script — value is determined by the execution of a script

Owner

The owner of the provisioning policy. This is determined by selecting from the following:
None — no owner is assigned to this provisioning policy.
Application Owner — identity assigned as owner of the application in which the provisioning policy resides.
Role Owner — identity assigned as owner of the role in which the provisioning policy resides.
Rule — use a rule to determine the owner of this provisioning policy.
Script — use a script to determine the owner of this provisioning policy

Required

Choose whether or not to have the completion of this field a requirement for submitting the form.

Refresh Form on Change

Select this option to have the form associated with this policy refresh to reflex changes to this policy.

Display Only

Set this field as display only.

Authoritative

Boolean that specifies whether the field value should completely replace the current value rather than be merged with it; applicable only for multi-valued attributes

Value

Determine how the value is derived. Select from the following:
Literal — value is based on the information you provide
Rule — value is based on a specified rule
Script — value is determined by the execution of a script

Allowed Values

The value(s) which can be displayed in the field of the generated form. Choose from the following:
None — the field is blank
Literal — value is based on the information you provide
Rule — value is based on a specified rule
Script — value is determined by the execution of a script

Validation

Gives the ability to specify a script or rule for validating the user's value. For example, a script that validates that a password is 8 characters or longer.

Configuring Full Text Searching

When full text searching is enable, users can use the following types of searches to find the correct access to request:

- Keyword search — Users can search based on keywords that relate to role, entitlements and descriptions.
- Affinity search — Users can search for access based on what other users who are similar to them currently have.

Feature / Enhancement	Description	Benefit
Keyword search	Search that finds results based on role and entitlement names, descriptions and extended attributes using relevance-based search and predictive analytics.	Provides a familiar shopping experience for end users. The keyword search makes it possible for end users and managers to find the right access to request.
Affinity Search	Guides users to the right access to request by enabling them to find roles or entitlements assigned to specific users or a population of users.	Enables users to locate roles and entitlements by reviewing access that others in the organization have. The affinity search provides a controlled, governance-based approach that enables you to compare similar access and view any areas of risk, such as high identity risk scores or open policy violations.

Enabling Full Text Searching

To enable the most basic full text searching:

1. From the navigation menu bar, go to **gear icon->Lifecycle Manager Configuration** page. Select the **Enable Full Text Search** option on the **Addition Options** Tab.
2. Select the **Enable Full Text Search**.
3. Run the Full Text Index Refresh task. Refer to the system administration documentation for more information.

> The Full Text Index Refresh must run every time you make a change to roles, managed attributes, or the FullTextIndex objects in your enterprise. The index files are only updated when this task is run. If you do not select this option, you will have to schedule the Full Text Index Refresh to run periodically or you will have to remember to run it manually.

When you run the **Full Text Index Refresh** task the first time, files for each FullTextIndex object in your IdentityIQ configuration are created.

- Setting the Location of Index Files
- Adding Additional Fields

- Special Considerations

Setting the Location of Index Files

To set the location of the index files, edit the FullTextIndex objects and add an indexPath key.

For example, `<entry key="indexPath" value="`*indexFileLocation*`">` where **IndexFileLocation** is a fully qualified path name. By default the index files for roles, BundleIndex, managed attributes, ManagedAttributesIndex, and unstructured targets TargetAssociation are added to the `WEB-INF` folder of the directory where you installed IdentityIQ.

By default, after completing both steps above, you can do full text searches on the following fields:

- **Managed Attributes:** displayableName, description, and application.name
- **Roles:** name, displayableName, and description
- **Targets:** name and description

Adding Additional Fields

To add additional fields, edit the FullTextIndex objects and add a field with analyzed="true" set: <FullTextField analyzed="true" name="*myAttribute*"/>.

The following example illustrates how to add a new full text searchable field (division) and indicate a location for the index files (/tmp/indexlocation). This example is for the roles index file.

> Roles are also referred to as bundles in the product code.

Field options:

- **Analyzed** -– used to index the field and for full text searching. Add analyze fields to include custom attributes in full text search.
- **Indexed** – enables the field to be used in the advanced filters on the access request pages.
- **Stored** – enables the field to return in the search results and display on the access request pages, if the user interface is designed to support this use.
- **Ignored** – sets the field to not be used in full text searching nor filtering. This field does appear in the filter passed down from the user interface.

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE FullTextIndex PUBLIC "sailpoint.dtd" "sailpoint.dtd">
<FullTextIndex created="1346076712810" id="4028818239686c4f0139686c9f6900e7"
name="Bundle">
 <Attributes>
 <Map>
 <entry key="fields">
 <value>
 <List>
 <FullTextField analyzed="true" indexed="true" name="name"/>
 <FullTextField analyzed="true" indexed="true" name="displayableName"/>
 <FullTextField analyzed="true" name="description"/>
 <FullTextField indexed="true" name="assignedScope.path"/>
 <FullTextField indexed="true" name="type"/>
 <FullTextField name="defaultDescription" stored="true"/>
```

```
 <FullTextField ignored="true" name="disabled"/>
 <FullTextField name="riskScoreWeight" stored="true"/>
 <FullTextField name="owner.id"/>
 <FullTextField name="owner.name"/>
 <FullTextField name="owner.displayName" stored="true"/>
 <FullTextField name=“division” analyzed=“true” indexed=“true”>
 </List>
 </value>
 </entry>
 <entry key="indexPath" value="/tmp/indexlocation"/>
 </Map>
 </Attributes>
</FullTextIndex>
```

Special Considerations

When FullTextSearch is enabled, Bundle / Role references within filter objects in Request Object Authority rules should include only the following indexed attributes:

- name
- displayableName
- id
- description
- owner.name
- owner.id
- assignedScopePath (id of the associated scope).

> The only attributes that are indexed in the FullTextSearch index are listed above. If you use attributes that are not in this list, extra Bundles are returned during search, which can result in errors in the log.

Creating Direct Links to IdentityIQ

Lifecycle Manager enables you to create direct links into IdentityIQ pages from outside of the product from places such as emails, forms, or portal. These direct links can either use your single-sign on solution or require users to login to IdentityIQ as an intermediate step. Direct links can also use a number of filtering options enabling users to go directly to specific pages using specific filtering criteria.

IdentityIQ supports the following types of direct links:

- Desktop Direct Links
- Mobile Interface Direct Links

Desktop Direct Links

Direct links provide a method to link directly to IdentityIQ Desktop pages. For Example, use the following direct links to go to the Manage Accounts, or Manage Passwords, or Manage Identity pages for a user that is logged in to IdentityIQ, where *<hostName>* is the name of the host on which IdentityIQ is installed. The following direct links can be used:

Manage Accounts

```
https://<hostname>/identityiq/ui/rest/redirect?rp1=/identities/identities.jsf
&rp2=quickLinks/Manage+Account
```

Manage Specific Account

```
https://<hostname>/identityiq/ui/rest/redirect?rp1=/identities/identities.jsf
&rp2=identities/<identityId>/accounts
```

Manage Password

```
https://<hostname>/identityiq/ui/rest/redirect?rp1=/identities/identities.jsf
&rp2=quickLinks/Manage%20Passwords/identities
```

Manage Specific Password

```
https://<hostname>/identityiq/ui/rest/redirect?rp1=/identities/identities.jsf
&rp2=identities/<identityId>/password
```

Create Identity

```
https://<hostname>/identityiq/ui/rest/redirect?rp1=/identities/identities.jsf
&rp2=quickLinks/Create+Identity/createIdentity
```

Edit Identity

```
https://<hostname>/identityiq/ui/rest/redirect?rp1=/identities/identities.jsf
&rp2=quickLinks/Edit+Identity
```

Edit Specific Identity

```
https://<hostname>/identityiq/ui/rest/redirect?rp1=/identities/identities.jsf
&rp2=identities/<identityId>/edit
```

View Identity

```
https://<hostname>/identityiq/ui/rest/redirect?rp1=/identities/identities.jsf
&rp2=quickLinks/View%20Identity/identities
```

View Specific Identity

```
https://<hostname>/identityiq/ui/rest/redirect?rp1=/identities/identities.jsf
&rp2=identities/<identityId>/attributes
```

Access Request Details (previously named Track My Requests)

```
https://<host-
name>/iden-
tityiq/ui/rest/redirect?rp1=/identityRequest/identityRequest.jsf&rp2=requests
```

Track My Requests

```
https://<hostname>/identityiq/identityRequest/identityRequest.jsf
```

Manage Certifications

```
https://<hostname>/identityiq/certification/certifications.jsf#/
certifications
```

Policy Violation List Page

```
https://<hostname>/identityiq/policyViolation/policyViolation.jsf#/
policyViolations
```

Mobile Interface Direct Links

Use the following direct links to go directly to IdentityIQ Mobile pages:

Direct Link to Passwords (Mobile)

- Manage Password https://<hostname>/identityiq/ui/rest/redirect?rp1=/ui/index.jsf &rp2=quickLinks/Manage%20Passwords/identities
- Manage Specific Password https://<host-name>/identityiq/ui/rest/redirect?rp1=/ui/index.jsf &rp2=identities/<identityId>/passwords

Direct Link to Manage Accounts (Mobile)

- Manage Accounts https://<hostname>/identityiq/ui/rest/redirect?rp1=/ui/index.jsf &rp2=quickLinks/Manage%20Accounts/identities
- Manage Specific Account https://<host-name>/identityiq/ui/rest/redirect?rp1=/ui/index.jsf &rp2=identities/<identityId>/accounts

Direct Link to Manage Certifications (Mobile)

- Manage Certifications https://<hostname>/identityiq/ui/index.jsf#/certifications

Direct Link to Policy Violations (Mobile)

- Policy Violations List Page https://<hostname>/identityiq/ui/index.jsf#/listViolations

Direct Link to Access Management Page (Mobile)

Specific access request pages can be accessed through direct links using parameters. Query parameters can be appended to the Access Review Management tab URL:

> Your browser may require Special characters in the parameter values to be URL encoded. For example, spaces must be replaced with %20, & must be replaced with %26, and ? must be replaced with %3F.

```
https://<hostname>/identityiq/ui/rest/redirect?rp1=/accessRequest/accessRequest.jsf&rp2=
accessRequest/manageAccess/add?identityName=<identity1>&filterRoleType=<roleType1>&filte
rRoleStringAttr=<roleAttrib1>
```

The following parameters allow you to create direct links to the page with a variety of filters already selected:

Access Request Management Deep Link Parameters

Identity

identityName - name of identity the deep link is targeting.

Role Filters

filterRoleType
filterRole<attribute>

> Only role type and extended attributes are supported. Attributes from the bundle object are not supported.

Entitlement Filters

filterEntitlementApplication (multi)
filterEntitlementAttribute (multi)
filterEntitlementEntitlement (multi)
filterEntitlementOwner
filterEntitlement<attribute>

The (multi) params can be specified multiple times in a single URL. However, filterEntitlementOwner is NOT multi.

If an entitlement application has only one attribute defined, the direct link can omit the entitlement attribute on the URL and the defined attribute is used by default.

> With the exception of Application, Attribute, and Value, only extended attributes are supported.

Keyword Filters

filterKeyword

> If full text search indexing is enable, description is also searched for the keyword.

Access Request for Single User Pre-Selected

In the following example,

<hostName> is the name of the host on which IdentityIQ is installed
<identity1> is the name of the identity

```
https://<hostname>/identityiq/ui/rest/redirect?rp1=/accessRequest/accessRequest.jsf&rp2=
accessRequest/manageAccess/add?identityName=<identity1>
```

Access Request for Single User Pre-Selected — Filtering on Role Type

In the following example,

<hostName> is the name of the host on which IdentityIQ is installed

<identity1> is the name of the user <roleType1> is the requested role

```
https://<hostname>/identityiq/ui/rest/redirect?rp1=/accessRequest/accessRequest.jsf&rp2=
accessRequest/manageAccess/add?identityName=<identity1>&filterRoleType=<roleType1>
```

Access Request for Single User Pre-Selected — Filtering on Role Type and Role Extended Attribute

In the following example,

<hostName> is the name of the host on which IdentityIQ is installed

<identity1> is the name of the user

<roleType1> is the type of role

<roleAttrib1> is the role attribute

```
https://<hostname>/identityiq/ui/rest/redirect?rp1=/accessRequest/accessRequest.jsf&rp2=
accessRequest/manageAccess/add?identityName=<identity1>&filterRoleType=<roleType1>&filte
rRoleStringAttr=<roleAttrib1>
```

Access Request for Single User Pre-Selected — Filtering on a Single Entitlement Application/Attribute/Value

In the following example,

<hostName> is the name of the host on which IdentityIQ is installed

<identity1> is the name of the user

<entApp1> is the entitlement application

<entAttrib1> is the entitlement attribute (such as memberOf or groupmbr)

<entValue1> is the entitlement value

```
https://<hostname>/identityiq/ui/rest/redirect?rp1=/accessRequest/accessRequest.jsf&rp2=
accessRequest/manageAccess/add?identityName=<identity1>&filterEntitlementApplication=<en
tApp1>&filterEntitlementAttribute=<entAttrib1>&filterEntitlementEntitlement=<entValue1>
```

Access Request Logged In User Selected with Filtering on Multiple Applications

In the following example,

<hostName> is the name of the host on which IdentityIQ is installed

<identity1> is the name of the user

<entApp1> and <entApp2> are the entitlement applications

<entAttrib1> and <entAttrib2> are the entitlement attributes (such as memberOf or groupmbr)

<entValue1> and <entValue2> are the entitlement values

> In the following example, two entitlements are requested.

```
https://<hostname>/identityiq/ui/rest/redirect?rp1=/accessRequest/accessRequest.jsf
&rp2=accessRequest/manageAccess/add?FidentityName=<identity1>
&filterEntitlementApplication=<entApp1>&filterEntitlementAttribute=<entAttrib1>
&filterEntitlementEntitlement=<entValue1>&filterEntitlementApplication=<entApp2>
&filterEntitlementAttribute=<entAttrib2>&filterEntitlementEntitlement=<entValue2>
```

Access Request Logged In User Selected with Filtering on a Keyword Search

In the following example,

<hostName> is the name of the host on which IdentityIQ is installed

<keyword1> is the specific keyword you want to find

```
https://<hostname>/identityiq/ui/rest/redirect?rp1=/accessRequest/accessRequest.jsf
&rp2=accessRequest/manageAccess/add?filterKeyword=<keyword1>
```

Direct Link to IdentityIQ Manage Access Review Page (Mobile)

Specific access request review pages can be accessed through direct links using parameters. Query parameters can be appended to the Access Request Review tab URL:

> Your browser may require Special characters in the parameter values to be URI encoded. For example, spaces must be replaced with %20, & must be replaced with %26, and ? must be replaced with %3F.

```
https://<hostname>:<port>/ui/rest/redirect?rp1=/ui/index.jsf&rp2=certification/<id>
```

The following parameters allow you to create direct links to the page with a variety of filters already selected:

Access Request Review Deep Link Parameters

Identity

filterKeyword — search term

If no identityName parameter is specified, the loggedInUser is used.

Role

To specify a role or entitlement using name or id:
role (multi) — name of id of role
entitlement (multi) — entitlement id

The (multi) params can be specified multiple times in a single URL.

Entitlements

To specify an entitlement without an id, use a combo:
entitlementApplication<X>
entitlementAttribute<X>
entitlementValue<X>

<X> corresponds to a matching integer, such as entitlementApplication1, entitilementAttribute1, entitlementValue1.

Access Request for Logged In User for a Single Role

In the following example,

<hostName> is the name of the host on which IdentityIQ is installed

<role1> is the name of the role

```
https://<hostName>/identityiq/ui/rest/redirect?rp1=/ui/index.jsf&rp2=accessRequest/revie
w?role=<role1>
```

Access Request for a Specified User for Multiple Roles

In the following example,

<hostName> is the name of the host on which IdentityIQ is installed

<identity1> is the name of the user

<role1> and <role2> are requested roles

```
https://<hostName>/identityiq/ui/rest/redirect?rp1=/ui/index.jsf&rp2=accessRequest/

review?identityName=<identity1>&role=<role1>&role=<role2>
```

Access Request for Logged In User for Single Entitlement Using Entitlement ID

In the following example,

<hostName> is the name of the host on which IdentityIQ is installed

<identity1> is the name of the user

<role1> and <role2> are requested roles

```
https://<hostName>/identityiq/ui/rest/redirect?rp1=/ui/index.jsf&rp2=accessRequest/

review?identityName=<identity1>&role=<role1>&role=<role2>
```

Multiple Entitlements for Specified User Using Entitlement Application/Attribute/Value

> If you define only one attribute defined for an application, the entitlementAttribute can be omitted and it will be filled in automatically. In all other cases, the attribute is required. In all cases, entitlementApplication and entitlementValue are required for each entitlement combination.

In the following example,

<hostName> is the name of the host on which IdentityIQ is installed

<identity1> is the name of the user

<entApp1> and <entApp2> are the entitlement applications

<entAttrib1> and <entAttrib2> are the entitlement attributes (such as memberOf or groupmbr)

<entValue1> and <entValue2> are the entitlement values

> In the following example, two entitlements are requested.

```
https://<hostname>/identityiq/ui/rest/redirect?rp1=/ui/index.jsf&rp2=accessRequest/manag
eAccess/add&identityName=<identity1>&filterEntitlementApplication=<entApp1>&filterEntitl
ementAttribute=<entAttrib1>&filterEntitlementEntitlement=<entValue1>&filterEntitlementAp
plication=<entApp2>&filterEntitlementAttribute=<entAttrib2>&filterEntitlementEntitlement
=<entValue2>
```

Direct Link to Pending Work Items (Mobile)

IdentityIQ supports the following mobile work items:

- Forms
- Approvals
- Request Violations

For all other types of work items, go to the desktop version of IdentityIQ and access the page associated with the work item.

You can link directly to any open work item such as a form or a violations. To access a direct link, a user must be logged in, have visibility to the work item and have authorization to access the item.

> Some work items, such as manager access reviews, are not supported as direct links. If a direct link contains a work item id that is not supported, a warning message displays that indicates the work item does not exist.

In the following example,

<hostname> is the name of the host on which IdentityIQ is installed
<workItemid> is the identifying number for the work item

```
https://<hostname>/SailPoint
IdentityIQ/ui/rest/redirect?rp1=/ui/index.jsf&rp2=commonWorkItem/<workItemid>
```

Using Direct Work Item Links in Email Templates

When you send an email with a direct link to a pending work item to a user, the email system variable must be configured to match server name and path of the currently deployed instance of IdentityIQ. Click the **Gear** icon in the navigation menu bar and go to **Global Settings -> Mail tab -> Email Templates -> Server Root Path**. For example, the default is set to `https://localhost:8080/IdentityIQ`. However, if you deploy from `/spt` on port 80, you should change the setting to `https://localhost/spt`.

> The $spTools.formatURL() is a velocity template function that formats the url correctly in the actual email sent to the user.

```
$spTools.formatURL('/ui/index.jsf#/commonWorkItem')/$item.id
```

Using Lifecycle Manager

> SailPoint IdentityIQ Lifecycle Manager is sold as a separate license and must be purchased and activated before it is available for use.

IdentityIQ Lifecycle Manager manages changes to user access and automates provisioning activities in your enterprise environment. The Lifecycle Manager maps directly to the lifecycle of a user in an organization and the core identity business processes associated with the user lifecycle activities.

- User Lifecycle Activities — joining, moving, leaving
- Core Identity Processes — provision, change, de-provision

The Lifecycle Manager can be configured to enable users to make requests through IdentityIQ and control which requests they can make.

Users

- Individual User — can make requests using the self-service feature
- Managers — can make requests for direct reports
- Help Desk Operators — can make requests for populations
- Other users — controls requests by all users not a part of the standard groups

User Requests

- New access — request entitlement and roles
- Account Management— create, manage, and delete accounts including enable, disable, and unlock, change and reset passwords, and track current requests
- Identity Management — create, edit, and view identities

Automated Change Management Using Configurable Event Triggers

Lifecycle Manager provides automated change management based on configurable identity lifecycle event triggers. These triggers are mapped to different identity-related events in an authoritative source, typically an human resources system. When a tracked event is detected, provisioning requests are generated. For example, when the status of an employee changes from active to terminated, this lifecycle event can be configured to trigger a de-provisioning request for all of the access associate with the employee. If an employee's job title changes, a trigger can launch the assignment of a new business role to replace the employee’s current business role.

IdentityIQ Governance Platform

Lifecycle Manager leverages the IdentityIQ Governance Platform to enhance compliance performance, improve security, and reduce risk.

SailPoint uses a combination of roles, policy, and risk to provide a framework for evaluating all requests for changes to access against predefined business policies.

- **IdentityIQ Role Model** — simplifies administration of user access by providing a predefined and planned structure for requesting and validating user access based on business or IT roles.
- **IdentityIQ Policy Model** — evaluates your corporate access policies during the access request and provisioning processes.
- **IdentityIQ Risk Model** — reduces operational risk by using a risk-based approach to identity governance and provisioning by enabling organizations to modify change management processes.

Identity Provisioning Broker

Lifecycle Manager uses the IdentityIQ Provisioning Broker to manage the final change manage activities that are the result of self-service access requests or automated lifecycle event triggers. The IdentityIQ Provisioning Broker is a key piece of the IdentityIQ architecture that enables organizations to coordinate changes to user access across different provisioning processes. When a provisioning change is triggered, the provisioning broker separates each request into its component parts and determines the appropriate provisioning implementation process. Provisioning options include:

- The SailPoint Automated Change Manager
- 3rd-party user provisioning solutions, such as Oracle IdM
- Service request systems, such as BMC Remedy
- Email generated to a system administrator

Lifecycle Manager Components

Lifecycle Manager is a part of your IdentityIQ solution that adds tools, work items and reports related to Lifecycle Manager core functionality.

New User Registration — a self-service feature that enables new users to request initial access to IdentityIQ. When access is granted, a new identity cube is created for the user.

Quicklink Cards — convenient links to request and track user access from your Home page.

- How to Manage Access
- How to Manage Identities

How to Manage Access

Lifecycle Manager adds Manage Access links to Home page. Use the links to perform the following functions:

> IdentityIQ System Administrators can make any request regardless of the Lifecycle Manager Configuration settings.

- Manage User Access
- Request Access Tasks
- Request Violations
- Manage Accounts
- Account Passwords
- Track My Requests

Requests are processed based on the business process defined when IdentityIQ is configured for your organization. If approval is not required, the roles are added or removed from the entitlements list and are available after the associated access is granted on the required applications. If approval is required, the request must first pass the approval process before being assigned.

Requests can be processed:

- Manually
- Through a work item
- By generating a help ticket, if your implementation is configured to work with a help desk solution
- Automatically through a provisioning provider

Manage Accounts

> The status for the accounts listed on the Manage Accounts page are refreshed automatically based on the conditions set during configuration.

You can use the **Manage Accounts** link to take action on any of the accounts assigned to a user. Based on how you system is configured, you can:

- View account information
- Delete and account
- Disable/Enable an account
- Refresh account status
- Request an account

Manage Accounts Page

The Manage Accounts page displays the user's cards that you can manage. From this page, you can:

- **Search** for a user — Enter a letter or combination of letters and click the **Search** icon.
- **Manage** a user's accounts — Select a user's card and click **Manage**.

The Accounts section lists information about accounts associated with the selected user. Information can include:

Account Selection Options:

Application

The application specific to the Account ID.

Account ID

Name of the account.

Status

The current status of the account.

Application

The application specific to the Account ID.

Last Refresh

The date the account information in IdentityIQ was last updated.

Last Action Status

The status of the last provisioning operation performed though IdentityIQ. This state is not updated by actions performed outside of IdentityIQ, so might not reflect the current state of the account.

The available actions are represented by icons defined in the legend on the page. Click an icon to perform the specified action.

> If the application does not support the action, the icon is not visible. These options are only available if configured by an administrator.

Click the **Refresh** icon to refresh the account status.

Click the **Information** icon to view information about the account.

Click the **Actions Menu** icon to perform available actions.

To request a new account for an application, click **Request Account** and select the application from the **Application** drop-down list.

Account Passwords

> If you click the Home button, exit the IdentityIQ application, or navigate away from the manage access pages before you complete all tasks, your entries are cleared and the access request is NOT submitted.

The Account Passwords link has the following options:

- Change — change a specific password or generate a new password for one or more accounts.
- Sync — synchronize a group of passwords.
- Generate — generate a single password for all selected accounts or generate a unique password for each selected account.
- Information icon — View details about the selected application.

Account Password Tasks

Based on how your system is configured, the following tasks can be available:

Change a Password for a Single Application

> If there are any errors associated with the manually submitted password the text fields are highlighted in red. Information is displayed below the text field that describes why the submitted password failed and the password policy.

To change an account password:

1. Navigate to the **Manage Passwords** page.
2. Select a user card and click **Manage.**
3. From the application list, navigate to the row for the application with the password you want to change and click **Change**.
4. In the row below the listing: you can:
   - Manually enter a new password, re-enter the password to confirm, and click **Submit**.
   - Or you can click **Generate** to generate a new password for the account.

Use Synchronize to Set up a Single Password for Multiple Applications

> You cannot synchronize passwords for accounts with incompatible password policies. The Synchronize Password option is not available for self service accounts. To set up a single password for a group of applications:

1. Navigate to the **Manage Passwords** page.
2. Select a user card and click **Manage.**
3. From the account list, select the accounts.

4. In the Synchronize Passwords dialog, enter the new password.
5. Re-enter the new password to confirm and click **Confirm**.

Use Generate to Manage a Group of Passwords

To generate passwords for a group of applications:

1. Navigate to the **Manage Passwords** page.
2. Select a user card and click **Manage.**
3. From the account list, select the accounts.
4. In the Generate Passwords dialog, select:
   - **Sync Password for All** to generate a new single password for all the selected accounts.
   - Or **Generate Password for All** to generate a new password for all the selected accounts.

Track My Requests

To track the progress of access requests you created, click **Manage Access -> Track My Access Requests**, use the **Track My Access Requests** link on your Home page, or **My Work -> Access Requests** to display the Access Request page.

Click on a item in the list to display detailed information about the requested items and any pending actions that still need to be taken on that request.

From the detailed history panel you can navigate further into the request to expand the details view, review the actual access request, and send messages to owners of the request reminding them that their action is required.

Click the **X** icon to cancel a request.

Access Request Options

Access Request ID

Identification number assigned to the access request.

Priority

Specifies the priority level to which the access request was designated.

Type

The type of access request.

Description

The a brief description of the access request.

Requester

The name of the user who assigned this work item to you.

Requestee

The name of the user to who was assigned this access request.

Request Date

The date the request was made.

Current Step

Status of the request. Status levels include:

Pending — Request was received but no action has taken place.
Approved — Request was approved. Additional action may be needed to complete the request.
Rejected — Request was denied.
Completed — All actions required for this access request have been fulfilled.
Cancelled — Request was cancelled.
Completed Pending Verification — The manual action for this request was completed, however the verification procedure has yet to have been run.

Completion Date

The date when the work item was completed.

Execution Status

Status of the request execution. Status levels include:

Executing — The request is going through the business process and has not completed.

Verifying — The request has finished the business process and is waiting for the Provisioning Scanner to verify it.

Terminated — The request was terminated before it was completed.

Completed — The request was completed and verified.

Track Request Details

To view detailed information about the requested items and any pending actions that still need to be taken on that request, click the Track Request Details option under the Actions (three-line) menu. This option is not available for some types of approvals, such as batch requests and native changes.

How to Manage Identities

Based on the IdentityIQ configuration, the following options can be available:

- Create Identity
- Edit Identity
- View Identity

Create Identity

To create new identity cubes in IdentityIQ, use the Create Identity page. The data fields are based on the fields defined as standard and/or searchable attributes in the IdentityIQ configuration.

Click Submit after all selections are completed.

Edit Identity

Use the Edit Identity page to edit identity attributes in IdentityIQ. The data fields are based on the fields defined as standard or searchable attributes in the IdentityIQ configuration.

Select an identity from the Available Identities list to display the Edit Identity Attributes page.

Use the search and filter features to limit the number of identities displayed.

Click **Submit** after all selections are completed to display the Review and Submit page.

View Identity

Use the **View Identity** option to view detailed information about an identity. This page can be accessed from the Quick-link menu, under the **Manage Identity** option.

The set of identities you can view will depend on your user rights in IdentityIQ. Some users can only see details about their own identity; other users may be able to see their own direct reports, or a wider set of identities. A **Search** option at the top of the page lets you search for specific identities,

If you have the ability to view multiple identities, click **Manage** on the identity you want to view, to open the Identity Details page.

Use the navigation bar on the left to view different elements of information about the identity.

Identity Details Menu

Based on the IdentityIQ configuration, the following options might be available:

- **Edit** — enablesyou to edit identity details.
- **Forward** — enables you to assign a user for forwarding.
- **Attributes** — lists the basic user identity information such as first name, last name, and email, as well as enabling you to update the user password and the forwarding user.
- **Access** — lists all of the user’s roles and entitlements.
- **Accounts** — lists account information for all of the applications to which the user has some level of access.
- **Account Passwords** — enables you to manage account passwords for one or more applications.
- **System Password** — enables you to manage IdentityIQ system passwords.

Lifecycle Manager Optional Links

The following items are optional Lifecycle Manager links that your administrator can configure:

- Manage Recycle Bin — provides support for deleted users, groups with all their attributes, and group memberships.
- Update My RSA Token PIN — provides support for updating you RSA Token PIN. See

How to Update My RSA Token PIN

> If you are logged in and have an RSA link associated with your identity, the Update My RSA Token PIN option is available.

To reset a PIN, click the **Update My RSA Token PIN** link on the Lifecycle Manager. The form displays the serial numbers of the tokens assigned to you. Select one of the multiple tokens (serial numbers) and type in a new PIN. The PIN is reset and changed in the target system. If you have multiple tokens and want to modify the PIN for all of the token, you must make a separate request for each token.

Manage User Access

IdentityIQ can be set up to request and manage access for yourself or for other identities. Based on how your system is configured, you can manage:

> If you click the Home button, exit the IdentityIQ application, or navigate away from the manage access pages before you complete all tasks, your entries are cleared and the access request is NOT submitted.

> When searching for a user to add or remove access, the elevated access icon will display on user that has elevated roles or entitlements.

- Access for Others — Users request and manage access for one or more identities. This option can also be set up to enable you to request access for yourself.
- Access for Yourself — Users request and manage access for themselves.

Access for Others

The following tabs are displayed for systems that are configured to request and manage access for one or more users:

> When removing access, only the roles and entitlements the user currently has assigned are available for removal.

- **Select Users** — Displays a list of available identities. You can choose one or more identities from the list.
- **Manage Access** — Use **Search** or **Filter** to find available roles and entitlements, or click **Browse all access** to display all available roles and entitlements. You can select **Add Access** to add new access. Select **Remove Access** to remove access for a single user.
- **Review and Submit** — Displays access request information. You can verify and submit your access requests.

Access for Yourself

The following tabs are displayed for systems that are configured to request and manage access for a single identity:

- **Manage My Access** — Use **Search** or **Filter** to find available roles and entitlements, or click **Browse all access** to display all available roles and entitlements. Click the check icon for each access item you want to add. You can also click **Remove Access** to see the access you currently have and select access you want to remove.
- **Recommended For You** — If AI Services has been configured for your organization, the **Search** field includes an option in the drop-down list to show access items that AI Services recommends for you, based on peer group analysis. You can also click the **Yes, show my recommendations** button to see recommended access. Recommendations are available only for your own access; if you are able to request access for other users (such as your direct reports), you will not be offered recommendations for those users. See the **AI Services** documentation for more information.
- **Review and Submit** — Displays your access request information. You can verify and submit your access requests.

Selecting and Deselecting Items

Click the check icon associated with the listing to select an item. Click **All** to select all displayed items. To deselect an item, click the highlighted check icon associated with the listing. If you do not want a selected user or an access item to be included in your access request, you must deselect it. Click **Home** to clear all items and cancel a request.

Request Access Tasks

Based on how your system is configured, you can perform the following tasks:

- Request Access
- Remove Access
- View Details
- View and Post Comments
- Edit an Access Request

Request Access

Based on how your system is configured, you can:

Request Access for Others

This option must be configured on the Lifecycle Manager configuration page.

1. On the **Select User** tab, click the check icon next on the card for one or more identities.

   To search for an identity, enter the name or first few letters of an identity in the search box and click the search icon. To limit the number of listings, click Filters, select specific filter criteria, and then click Apply

2. Navigate to the **Manage Access** tab and select the **Add Access** tab.

   To search, enter a term in the search box and click the search icon. Click the menu icon next to the search file to change between search types: Keyword, User Access, or Populations. To limit the number of listings, click Filters, select specific filter criteria, and than click Apply.

   Click **Browse all access items** to display the full list of access options available.

3. If a role or entitlement requires an account the identity does not have, the **Select Account** dialog displays. To create the new account, select the account and **click Apply**.
4. After IdentityIQ validates that the user does not currently have the requested access, the number of items you selected displays on the **Add Access** tab.
5. Navigate to the **Review and Submit** tab and review the access request information for each identity.
6. Before you complete the access request, you can:

- Remove an access request entry — Click the **X** icon next to the access item.
- Add an attachment (single user requests only) — See Add Attachments
- Add a comment — See View and Post Comments

- Change the priority — See Change Priority
- Change the sunrise/sunset dates — See Change Sunrise/Sunset Date

> After you click Submit, forms are issued if further information is needed before your request can be completed.
>
> If you are requesting access for a single identity, a popup is displayed enabling you to complete the form immediately or send it to your Home page.
>
> If you are requesting access for multiple identities, the forms are sent directly to your Home page and no popup is displayed.

7. When you have completed all your review tasks, click **Submit** to complete the access request.

Request Access for Yourself

If your system is set up to allow you to request access for yourself, a card with your identity details is the first card displayed on the Select User tab. This option must be configured in IdentityIQ.

1. On the **Manage My Access** tab, select the **Add Access** tab.

   To search, enter a term in the search box and click the search icon. To limit the number of listings, click **Filters,** select specific filter criteria, then click **Apply**.

   Click **Browse all access items** to display the full list of access options available.
2. Some roles allow related roles to be added. To add the additional roles, select the role or roles and click **Continue**.
3. Navigate to the **Review and Submit** tab and review the access request information.
4. Based on how your system is configured, you can:

- Remove an access request entry — Click the **X** icon next to the access item.
- Add an attachment (single user requests only) — See Add Attachments
- Add a comment — See View and Post Comments
- Change the priority — See Change Priority
- Change the sunrise/sunset dates — See Change Sunrise/Sunset Date

5. When you have completed all your review tasks, click **Submit** to complete the access request.

Request Access Containing a Permitted Role

A permitted role is generally a requested or assigned role and is not automatically granted to a user. Permitted roles are enabled by default. When permitted roles are available, they are displayed on the following tabs:

- **Add Access** — When you select a role that has permits, the associated permitted roles are displayed as cards after you complete the account selection setup.
- **Review** — Permitted roles are displayed below the associated assigned role.

> You can set Sunrise/Sunset dates and comments on permitted roles.

Remove Access

The remove access feature is only available for an individual user.

> If your system is set up to allow you to add or remove access for yourself, a card with your identity details is the first card displayed on the Select User tab.

1. On the **Select User** tab, click the arrow on the card for an identity.
2. Navigate to the **Manage Access** tab and select the **Remove Access** tab. The current access for the selected user is displayed.

   To search, enter a term in the search box and click the search icon. To limit the number of listings, click **Filters,** select specific filter criteria, then click **Apply**. Search in the Remove Access area includes a **Status** filter that allows you to filter results for **Active** or **Requested** access.
3. Full Text search is not available for Remove Access.
4. Click the check icon next to the access items you want to remove. The number of items you selected to be deleted is displayed in a circle on the **Remove Access** tab.
5. Navigate to the **Review and Submit** tab and review the information about the access you want to remove for the individual user.
6. Before you complete the access actions, you can:
   - Remove an access request entry — Click the **X** icon next to the access item.
   - Add an attachment — See Add Attachments
   - Add a comment — See View and Post Comments
   - View Details — See View Details
7. When you have completed all your review tasks, click **Submit**.

View Details

You can view the following information about a user:

View User Details

Based on how your system is configured, you can view items such as User Name, Last Name, First, email, Location Owner, Region, and more.

1. Navigate to the **Manage User Access** page.
2. On the **Select User** tab, click the user icon on any user card.

To view user details from the Review tab, click the user name next to the user icon to return to the Select User tab and than click the user icon on the user card.

View Role Details

For any role, you can view information such as the application associated with the role, the Attribute, the Name of the role and how the role was assigned.

1. Navigate to the **Manage User Access** page.
2. On the **Manage Access** tab, click **Details** for any role listing.

Add Attachments

> IdentityIQ does not perform file content validation or verification on attachments. It is your responsibility to ensure that only files that do not violate security policies within your environment are included as attachments.

> Attachments are only available for single user access requests. If attachments are enabled, you will see the attachment icon on all request items, but it will only be active on requests that support attachments.

You can add attachments to access request items using the attachments button, paper clip icon. The number next to the icon indicates the number of files attached to that access request item. Based on how your system is configured, you can have the ability to add attachments, for example a training certificate or notarized document of authorization, or you might be required to add an attachment for specific items.

There might be an attachment size limit set during the configuration of IdentityIQ. If you run into issues, contact your administrator. For information how how file attachment options are configured, see the **System Configuration** documentation.

> If attachments are required, it will be indicated in the icon and you will receive a warning if you try to submit the request with out an attachment.

> If attachments are required for an item and you include that item in a request for multiple users, a message is displayed instructing you to amend the request as required.

> Adding any attachment will fulfill the required attachment rules. IdentityIQ does not validate to ensure the correct item was attached.

1. On the **Review and Submit** tab, select the attachments icon for the request item.
2. In the attachments overlay, add attachments by dragging and dropping or uploading files.
3. Click **OK** after all files are loaded.

Attachment Overlay

The information displayed on the attachment overlay is controlled using AttachmentConfig rules. Every time a user accesses the **Review and Submit** tab of an access request, every AttachmentConfig rule is reviewed and the attachment overlay is constructed based on that input, possibly with the names of required or suggested attachments displayed in a list.

Required attachment names are display with a red asterisk. All required attachments should be included in the access request, but any attachment will satisfy the requirement rules. IdentityIQ does not validate the attached files.

Drag and drop or upload the attachments to add them to the **Attached to This Item** list.

The **Attached to This Item** list contains any files already attached to this request item. From this list you can:

- Add or edit comments — click the pencil icon to add or edit comments
- Download and view — download and view the attachment
- Remove — remove the attachment from the request and delete it from the database

View and Post Comments

> Assignment notes can only be added to assigned roles. You cannot add assignment notes to permitted roles.

You can view or post comments and assignment notes to an access request using the comments button, talk bubble icon. The number next to the icon indicates the number of comments and notes for the access request. If comments are **required** for this item, the comment icon is flagged with a red asterisk. Comments can be made at the overall request level and at the individual request item level; when comments are required, a comment at the request satisfies the requirement for comments at the individual request item level.

When you add a comment or assignment note to an access request line item, the note icon turns green.

Based on how your system is configured, you can:

View or Post Access Request Line Item Comments

Before you complete and access request, you can view or post a comment to line items for entitlements and roles.

> If an Assignment note is not permitted for the item, the title of the dialog is Comment.

1. On the **Review and Submit** tab, select the comments icon for the request item.
2. In the **Comments and Notes** dialog, select the **Comments** tab.
3. To post a new comment, type your comments in the text box and click **Save**.

Post an Assignment Note to Access Request Line Items

Before you complete an access request, you can post an assignment note to line items for roles.

> If an assignment note is not permitted for the item, the Assignment Notes tab is not displayed.

1. On the **Review and Submit** tab, select the comments icon for the request item.
2. In the **Comments and Notes** dialog, select the **Assignment Notes** tab.
3. Type your note in the text box and click **Save**.

Edit an Access Request

Before you submit an Access Request, you make the following edits from the **Review and Submit** tab:

Change Priority

> For this feature to be available to users, the Administrator must enable the option to Allow requesters to set request priorities.

If your system is set up to allow priorities for access requests, you can change the priority for an access request. The default setting is **NormalPriority**. When you create an access request, you can change the priority to **High Priority** or **Low Priority.**

Before you complete an access request, you can change the priority for an access request:

1. On the **Review** tab, click the button with the flag icon.
2. Select **High Priority**, **Normal Priority**, or **Low Priority**.

Change Sunrise/Sunset Date

Sunrise and sunset dates support the temporary assignment of roles and entitlements by letting you set a beginning (sunrise) and an end (sunset) date for access. Access is deprovisioned when the sunset date arrives.

> For this feature to be available to users, the administrator must enable the option to allow Sunrise/Sunset dates on role assignment.

> If you specify a global Sunrise/Sunset date on an entire access request, and than change the global setting, the new global setting overrides any individual line item date settings you made.

Before you complete an access request, you can set a beginning and ending date for an:

> If all the dates in access request are the same, the global date icon is green. If the dates for one or more line items in the access request are difference, the date icon is gray.

To set the global sunrise/sunset dates for a line items in an access request:

1. On the **Review** tab, click the date icon for the line item in the access request.
2. In the Set Sunrise/Sunset dates dialog, type a new date in the field in the mm/dd/yyyy format or click the calendar to select a date.
3. Click **Save** to save the new dates.

To set the global sunrise/sunset dates for an access request:

1. On the **Review** tab, click the date icon for the access request.
2. In the Set Sunrise/Sunset dates dialog, type a new date in the field in the mm/dd/yyyy format or click the calendar to select a date.
3. Click **Save** to save the new dates.

Request Violations

> The section only applies for single identity access requests. If a request for multiple users contains violations, the request goes through and notifications are sent.

When you submit an access request that results in a policy violation and IdentityIQ is configured to have interactive violation handling, a warning message appears at the top of the page with a list of the violations. Click a violation to view details about the violation possibly including compensating controls and correction advice if they were included.

Access Request Violations Options

For access requests that generate policy violations, IdentityIQ can be configured to:

Reject and Cancel Requests with Policy Violations

If you submit an access request that results in a policy violation and IdentityIQ is configured to reject any requests with policy violations, the request fails and is canceled. You can navigate to the Manage Use Access page and create a new request.

Reject Requests with Policy Violations - Interactive

If you submit an access request that results in a policy violation and IdentityIQ is configured to reject any requests with policy violations, the request fails. If you are notified that the request failed because of a policy violation, and you are still on the Manage User Access page, you can:

- Change the access request
- Cancel the access request

Allow Requests with Policy Violations - Non-Interactive

If you submit an access request that results in a policy violation and IdentityIQ is configured to allow any requests with policy violations, the request goes through and you are not notified.

Allow Requests with Policy Violations - Interactive

> When you continue with an access request with a violation, IdentityIQ can be configured to allow the violation with no user interaction or require users to add a comment or sunset date.

If you submit an access request that results in a policy violation and IdentityIQ is configured to allow requests with policy violations, and notify the requester, the request continues. When you are notified of the violation, you can:

- Change the access request
- Cancel the access request
- Continue with the access request

Approve Access Requests

Use the Approve Access Requests interface to make decisions on access request approvals that are assigned to you. If you are a member of any workgroups, the listings include approvals for those workgroups.

Click the **Approve Access Requests** Quicklink card or select **Approve Access Requests** in the Quicklink menu to access the Approvals page, which shows the access request approvals that are assigned to you. Use this page to view and manage your approval requests. Approval items include the following types of Lifecycle Manager access requests:

- Role Requests
- Entitlement Requests
- Account Requests

Approval items are shown in an expanded view by default, showing full details for all items in the request. Click **Collapse All** to switch to a more compact display showing only the approval-level details, without item details. Click **Expand All** to expand the listing to the detailed view.

To sort the list, click the arrow next to **Sort By** and select a sort type, **Newest**, **Oldest**, or **Priority**.

Use the **Filter** icon to filter the items that are displayed on the page. You can filter by **Owner**, **Requester**, or **Assignee**. When you have selected your filtering criteria, click **Apply**. When filtering is applied, the **Filter** icon turns green to alert you that you are seeing a filtered subset of your items. To clear filtering criteria and return to viewing all items, click **Filter** again, and click **Clear** to remove your filter criteria.

Use **Collapse All** or **Expand All** to control how the items are displayed.

Use the **Search** field to search for approval items by **Work Item ID** or **Requestee Name**.

Click **Recommendations** to display the Decision Recommendation popup. The recommendations icon is only displayed If SailPoint AI Services was purchased and activated for your installation of IdentityIQ. See the **AI Services documentation** for more information.

Approval Tasks

You can perform the following tasks:

- Complete an Approval
- Forward an Approval
- View Details
- View Attachments
- View and Post Comments

Complete an Approval

> A Policy Violation alert is displayed at the top of any approval that causes a violation if the request is approved.

You can take approval actions both at the overall approval request level, or at the individual request item level.

If SailPoint AI Services was purchased and activated for your installation of IdentityIQ, recommendation icons are displayed with each item for which a recommendation is available. Click the icon to see the recommendation details. See the *SailPoint AI Services* documentation for more information.

For each approval request you can:

- **Approve All** items, **Deny All** items, or **Forward** the approval.
- Make a decision on each individual approval item to **Approve** or **Deny** the request.
- Use an electronic signature to sign an approval if your installation is configured to use this feature.

> If the approval request was set up to use electronic signature, the Electronic Signature dialog displays automatically. Use the same credentials you use to sign in to the product.

The Complete Approval dialog displays when you click **Approve All** or **Deny All** for an approval, or after you click the **Approve** or **Deny** button for the last individual item in an approval. To complete the approval, click **Complete**. To change your approval decisions, click **Cancel**.

Forward an Approval

You can forward an approval to another identity or workgroup, to pass the responsibility for approval decisions to them. Forwarded approvals can not be recalled, and once you forward an approval, you can no longer view informatoin about it. To forward an approval:

1. Click the **Forward** icon in the Actions (three-line) menu for an approval.
2. Enter the name or a few letters of the name of the new owner of the approval. Alternatively, you can click the down icon and select a name from the list.
3. Add any forwarding comments and click **Forward**.

View Details

You can view detailed information about an approval, its forwarding history, and information about any approval line item.

> For small form factors such a mobile phones, the Details button is displayed in the Actions menu.

You can view the following types of details:

View Approval Details

Click the **Info** button for the overall approval to open the Details dialog. It shows the following items.

- **Work Item Details** tab— displays the work item and Access Request ID number, who made the request, who owns the approval, when the approval was created and the priority.
- **Identity Details** tab — displays the attributes that the Administrator configures for the Identity Mappings and can include attributes such as user name, first and last name for the identity, the email for the identity and the owner of the location and region for the identity.
- **Forwarding History** tab — displays the name of the person who forwarded the approval, the date the approval

was forwarded and any comments. Approvals that are forwarded to or from a workgroup display the name of the workgroup. If there are multiple forwards, all ownership changes are displayed.

View Approval Line Item Details

Click the **Info** button for an individual approval item to see these Details.

For **Roles**:

> If the requestor includes an Assignment Note when an approval request for a role and an account selection is required, the Assignment Note is displayed at the bottom of the Details tab.

- **Details** — displays the requested action and the name of the role. For Entitlement and account requests, information about the account and application is displayed.
- **Account Details** — displays the specific role name, the account name and the application for roles requests.
- **Entitlements** — displays the associated applications, attributes, entitlement name, and how it was assigned.

For **Entitlements**:

- A single panel listing the **Action**, **Attribute**, **Value**, **Account Name**, **Application**, and **Entitlement Owner**.

View Attachments

The attachments icon, paper clip, indicates if there are attachments included with this requested item and their number. Click the icon to display the attachment overlay containing the attachment list. Download to view the attachments from the list.

View and Post Comments

You can view or post comments for an approval or for an individual approval item, using the **Comments** button. The number next to **Comments** indicates the number of comments that exist for the approval or approval item. If no number is displayed, there are no current comments.

> For small form factors such as mobile phones, the Comments button is displayed in the Actions menu.

You can perform the following tasks:

View Approval or Approval Line Item Comments

Click **Comments** for the overall approval or an approval item to view the comments. The Comments dialog lists the comments from the oldest to the newest with the oldest comments at the top. For each comment, the following information is displayed:

> All approvers can view all comments made by other users.

- Posted comment
- Name of the user who posted the comment
- Date and time the comment was posted

Post Approval or Approval Line Item Comments

To post a new comment:

- Click **Comments** for the approval or approval item
- Type your comment in the text box at the bottom on the Comments dialog.
- Click **Post**.

Required Comments for Approvals and Denials

IdentityIQ can be configured to require comments for any approval and, separately, for any denial of access. This setting is defined in the provisioning business process that manages approvals. The default business process for this is the **LCM Provisioning** business process.

To require comments on approvals and denials, click **Setup > Business Processes**, and choose the **LCM Provisioning** business process (or your custom provisioning business process if you have implemented one). On the **Process Variables** tab, use the checkboxes to determine when comments are required: **Require comments for approval** and **Require comments for denial**.

In the approvals UI, if comments are **required** for the item, the comment icon is flagged with a red asterisk. Comments can be made at the overall approval level and at the individual approval item level; when comments are required, a comment at the overall request level satisfies the requirement for comments at the individual approval item level. If bulk decisions are enabled in your system, a pop-up dialog will open for the required comments when approvals or denials are made in bulk.

Lifecycle Events

> You must have IdentityIQ administrative capabilities to setup this function. For information about setting up administrative capabilities, contact your IdentityIQ administrator.

Use the Lifecycle Events page to create new events or to configure existing events in your enterprise to trigger business process. When changes are detected during an identity refresh, IdentityIQ can be set up to launch event-based business processes.

To access the Lifecycle Events page, navigate to **Setup -> Lifecycle Events**.

- Lifecycle Events Page
- How To Create Lifecycle Events

Lifecycle Events Page

The Lifecycle Events page displays the following information about existing lifecycle events:

Name

The name assigned when the certification event was created.

This name is used to identify the certification event. This name is not displayed in the certifications that are created when this event is triggered.

Type

The event type associated with this certification event.

Attribute Name

The specified attribute when the **Event type** is set as **Attribute Change**.

Owner

The user who created the event certification.

Disabled

The Enabled/Disabled status of the event.

Use the Lifecycle Events page to edit or create a lifecycle event and the associated event behavior.

How To Create Lifecycle Events

Lifecycle events can be configured to run based on events that occur in IdentityIQ. For example, when a manager change is detected for an identity, an event-based business process can be configured to run and to send any requests to the newly-assigned manager.

- Lifecycle Events
- Lifecycle Events Page

Lifecycle Event Parameters:

> The options displayed are dependent on the event type selected.

Name

Assign an intuitive name for the event. This name is used to identify the event. This name is not displayed in the requests that are created when an event is triggered.

Description

Assign a brief description of the event.

Event Type

The fields displayed above Disabled are dependent on the Event Type specified here.

Specify an event-type:

- **Create** - launch a certification when a new identity is discovered.
- **Manager Transfer** - launch a business process when the manager changes for an identity.
- **Attribute Change** - launch a business process when a change is detected for the specified attribute.
- **Rule** - use a rule to determine when to launch a business process. To make changes to your rules, click the "..." icon to launch the Rule Editor.
- **Native Change** - launch a business process when a change is detected on a native application that was configured to pass this information to IdentityIQ.
- **Alert -** launch a business process when an alert is triggered.
- **Rapid Setup -** launch a rapid setup business process when the selected RapidSetup Process is detected.

Attribute

Select the identity attribute from the list to associate with this event. The attribute drop-down list contains all of the standard and extended identity attributes configured in your deployment of IdentityIQ.

Previous Manager Filter

For Manager Transfer event types only:

IdentityIQ launches business processes only when identities are transferred from the specified manager.

If no manager is specified, all managers are included.

New Manager Filter

For Manager Transfer event types only:

IdentityIQ launches business processes only when identities are transferred from the specified manager.

If no manager is specified, all managers are included.

Previous Value Filter

For Attribute Change event types only:

IdentityIQ launches business processes only when the attribute value specified has changed.

If no value is specified, all values are included.

New Value Filter

For Attribute Change event types only:
IdentityIQ launches business processes only when the attribute value specified is newly assigned.
If no value is specified, all values are included.

RapidSetup Process

The RapidSetup business process context in which this lifecycle event should be evaluated.

Disabled

Enabled / Disables status of the event.

Rule

For Rule event types only:

Select the event rule used to launch business processes.
Rules are created as part of the configuration process of IdentityIQ.

Include Identities

Select a rule to define the population.

None — only the identities specified in the **Included Identities** list are in the population.

All — include all identities in the population.

Match List — only identities whose criteria match that specified in the list. Add identity attributes, application attributes and application permissions. Customize further by creating attribute groups to which this assignment rule applies.
If the "Is Null" check box is selected, the associated value text box is disabled. When the "is null" match is processed, the term matches users on the chosen application who have a null value for that attribute/permission.

Filter — a custom database query.

Script — a custom script.

Rule — select an existing rule from the drop-down list.
Click **Edit Rule** to launch the Rule Editor.

Population — select an existing population.

Threshold Type and Threshold Value

To use an Identity Processing Threshold to stop lifecycle events before they are fully processed, in case of accidentally-triggered business process, set a type and **value** for the threshold.

For more information, see **Identity Processing Thresholds** in the **Rapid Setup** documentation.

Fixed — must be a positive whole number greater than 1.

Decimals are not allowed when using a Fixed Threshold.

Percentage — must be a positive whole number between 1 and 100.

Business Process

Select the business process triggered by this event.

The business process drop-down list contains all of the standard and extended business processes configured in your IdentityIQ deployment.

Lifecycle Manager Reports

Lifecyle Manager Reports enable you to monitor and analyze information about Lifecycle Manager requests.

The following reports provide information that is specific to the functions of Lifecycle Manager:

- Access Request Status Report
- Account Requests Status Report
- Identity Requests Status Report
- Password Management Requests Report
- Registration Requests Status Report

> An identity must have IdentityIQ administrative capabilities to use this option. For information about setting up administrative capabilities, contact your IdentityIQ administrator.

To access these report templates, navigate to **Intelligence -> Reports** and select a report from the list.

Lifecycle Manager Reports have the following sections:

> All reports use a set of standard properties to handle basic information, such as naming and descriptions, and controls settings. Controls include items such as scope and required sign off. You must enter the name before you run a report.

- Standard Properties — see Standard Properties
- Parameters — see the individual report descriptions for their unique parameters.
- Report Layout — see Report Layout

The report information in the detailed results format can be exported to a .csv file and used in spreadsheets.

Access Request Status Report

The Access Request Status report shows details about access requests (role and entitlement requests) submitted through Lifecycle Manager. The summary section displays a graph to illustrate the ratio of pending to completed requests included in the report. The detail section shows the access request ID, the requester, the target identity, the entitlement owner, and the date and type of request made, along with various details about the request including its current status.

> To report on access requests that were triggered by lifecycle events, such as Rapid Setup joiner, mover, or leaver events, or standard Lifecycle Events, use the Lifecycle Events Status Report.

Use the following criteria to determine the information to use in this report. You can use any combination of options to build a report. You can use the Shift and Crtl keys to select multiple items from lists.

> If you select no options from a list, all options in the list are included in the report.

Applications

Show only access requests pertaining to one of the selected applications.

Approvers

Include only access requests approved by, or submitted for approval to, the selected identity or identities.

Requesters

Include only access requests originally created by one of the selected identities.

Entitlements

Show only access requests that included a request for access to the selected application-attribute-entitlement combination(s).

Roles

Show only access requests that included a request for one or more of the selected roles.

Target Identities

Include only access requests made for one or more of the selected identities.

Status

Show only access requests currently in the specified state: **Completed**, **Approved**, **Rejected**, **Pending**, **Cancelled**.

Requested Date Range

Show only access requests made during the specified date range; date ranges can be open-ended in either direction (no start or no end date), as needed.

Finished Date Range

Show only access requests whose end date is during the specified date range; date ranges can be open-ended in either direction (no start or no end date), as needed.

Account Requests Status Report

The Account Requests Status report shows information about account requests submitted through Lifecycle Manager; this can include requests for new accounts or management of existing accounts (account deletion, disable/enable account, etc.). It shows the access request ID associated with each request, the requester, the target identity, the application name and owner, the account native identity (if the request is for an existing account), and the date and type of request made, along with various details about the request including its current status.

Use the following criteria to determine the information to use in this report. You can use any combination of options to build a report. If you do not select options from a list, all options in the list are included in the report. You can use the Shift and Crtl keys to select multiple items from lists.

Approvers

Include only account requests approved by, or submitted for approval to, the selected identity or identities. If no approvers are selected, all approvers are included.
Click the arrow to the right of the suggestion field to display a list of all approvers, or enter a few letters in the field to display a list of approvers that start with those letters.

Requestors

Include only account requests originally created by one of the selected identities. If no requestors are specified, all requestors are included.
Click the arrow to the right of the suggestion field to display a list of all requestors, or enter a few letters in the field to display a list of requestors that start with those letters.

Applications

Show only account requests pertaining to accounts on one of the selected applications. If no applications are specified, all applications are included.
Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with those letters.

Target Identities

Include only account requests made for one or more of the selected identities. If no target identity are specified, all target identities are included.
Click the arrow to the right of the suggestion field to display a list of all target identities, or enter a few letters in the field to display a list of target identities that start with those letters.

Request Start and End Date(s)

The account request date range. The report provides all requests created on or after the start date and on or before the end date.
You can enter the date manually, or click the **...** icon to select a date from the calendar. Date ranges can be open-ended in either direction (no start or no end date), as needed.

Approval Start and End Date(s)

The account approval date range. The report provides all approvals created on or after the start date and on or before the end date.
You can enter the date manually, or click the **...** icon to select a date from the calendar. Date ranges can be open-ended in either direction (no start or no end date), as needed.

Status

Show only account requests currently in the specified state (completed, approved, rejected, pending, canceled). If none are specified, all status levels are included.

Identity Requests Status Report

The Identity Requests Status report shows details about identity requests submitted through Lifecycle Manager; this includes both Create Identity and Edit Identity actions. Requests to create a new identity are expanded into separate requests for each attribute value, so the report displays those each on separate lines. The identity creation action is also represented as its own record in the report. The same is true for edit requests which change more than one attribute: a separate request line item is generated for each attribute. Each line on the report shows the access request ID associated with the request, the requester, the target identity name, the approval owner (commonly the identity's manager), the date of the request, and the operation to be performed, along with various other details about the request including its current status.

Use the following criteria to determine what information to use in this report. You can use any combination of options to build a report. If you do not select any options from a list, all options in the list are included in the report. You can use the Shift and Crtl keys to select multiple items from lists.

Approvers

Select the approvers to include in the report. If no approvers are specified, all approvers are included.
Click the arrow to the right of the suggestion field to display a list of all approvers, or enter a few letters in the field to display a list of approvers that start with those letters.

Requestors

Select the requestors to include in the report. If no requestors are specified, all requestors are included.
Click the arrow to the right of the suggestion field to display a list of all requestors, or enter a few letters in the field to display a list of requestors that start with those letters.

Target Identity

Select the target identity to include in the report. If no target identity are specified, all target identities are included.
Click the arrow to the right of the suggestion field to display a list of all target identities, or enter a few letters in the field to display a list of target identities that start with those letters.

Status

Select the status to include in the report. If none are specified, all status levels are included.

Request Date Range

The identity creation request date range. The report provides all requests created on or after the start date and on or before the end date.
You can enter the date manually, or click the calendar icon to select a date from the calendar. Date ranges can be open-ended in either direction (no start or no end date), as needed.

Finished Date Range

The identity creation finished date range. The report provides all requests the finished on or after the start date and on or before the end date.
You can enter the date manually, or click the calendar icon to select a date from the calendar. Date ranges can be open-ended in either direction (no start or no end date), as needed.

Lifecycle Events Status Report

The Lifecycle Events Status Report report shows details about access requests that were triggered by lifecycle events, such as Rapid Setup joiner, mover, or leaver events, or standard Lifecycle events.

Report details can include the access request ID, the requester, the target identity, the entitlement owner, and the date and type of request made, along with various details about the request including its current status. What appears in the report details will depend on the columns you selected for inclusion in the Report Layout tab.

Use the following criteria to determine the information to use in this report. You can use any combination of options to build a report. You can use the Shift and Crtl keys to select multiple items from lists.

> If you select no options from a list, all options in the list are included in the report.

Applications

Show only access requests pertaining to one of the selected applications.

Approvers

Include only access requests approved by, or submitted for approval to, the selected identity or identities.

Requesters

Include only access requests originally created by one of the selected identities.

Entitlements

Show only access requests that included a request for access to the selected application-attribute-entitlement combination(s).

Roles

Show only access requests that included a request for one or more of the selected roles.

Target Identities

Include only access requests made for one or more of the selected identities.

Status

Show only access requests currently in the specified state: **Completed**, **Approved**, **Rejected**, **Pending**, **Cancelled**.

Requested Date Range

Show only access requests made during the specified date range; date ranges can be open-ended in either direction (no start or no end date), as needed.

Finished Date Range

Show only access requests whose end date is during the specified date range; date ranges can be open-ended in either direction (no start or no end date), as needed.

Password Management Requests Report

This report shows password change requests that meet the filter criteria selected. Passwords can be changed through the Change Password option in Lifecycle Manager, through the Forgot Password option (secondary authentication through security questions), and as a result of an expired password where the system forces the user to change their password. The reason for the change is included in the report, along with the requester, the target identity, the date of the request, the application and account native identity for which the password is being changed, and the completion date (along with any comments) for the request.

Use the following criteria to determine what information is used in this report. You can use any combination of options to build a report.

> If you do not select any options from a list, all options in the list are included in the report.

Applications

Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with those letters.

Requestors

Select the requestors to include in the report. If no requestors are specified, all requestors are included.
Click the arrow to the right of the suggestion field to display a list of all requestors, or enter a few letters in the field to display a list of requestors that start with those letters.

Roles

Type or use the drop-down list to select the roles to include in the report. If no roles are specified, all roles are included.

Target Identity

Select the target identity to include in the report. If no target identity are specified, all target identities are included.
Click the arrow to the right of the suggestion field to display a list of all target identities, or enter a few letters in the field to display a list of target identities that start with those letters.

Cause

Select the cause type to include in the report. If no cause types are specified, all types are included.
Choose from the following types:

- **Expired Password**
- **Forgotten Password**
- **Change Request**

Status

Select the status to include in the report. If none are specified, all status levels are included.

Request Date Range

The edit identity request date range. The report provides all requests created on or after the start date and on or before the end date.
You can enter the date manually, or click the **...** icon to select a date from the calendar. Date ranges can be open-ended in either direction (no start or no end date), as needed.

Finished Date Range

The edit identity request completion date range. The report provides all requests that were completed on or after the start date and on or before the end date.
You can enter the date manually, or click the **...** icon to select a date from the calendar. Date ranges can be open-ended in either direction (no start or no end date), as needed.

Registration Requests Status Report

This report shows the status of self-service registration requests submitted to IdentityIQ, when that feature is enabled for the installation. It shows the username for the self-registering user along with the current status, the approving or rejecting identity, and any available comments.

The following criteria is used to determine what information is used in this report. You can use any combination of options to build a report. If you do not select any options from a list, all options in the list are included in the report.

Approvers

Select the approvers to include in the report. If no approvers are specified, all approvers are included.
Click the arrow to the right of the suggestion field to display a list of all approvers, or enter a few letters in the field to display a list of approvers that start with those letters.

Target Identities

Select the target identity to include in the report. If no target identity are specified, all target identities are included.
Click the arrow to the right of the suggestion field to display a list of all target identities, or enter a few letters in the field to display a list of target identities that start with those letters.

Request Date Range

The edit identity request date range. The report provides all requests created on or after the start date and on or before the end date.
You can enter the date manually, or click the **...** icon to select a date from the calendar. Date ranges can be open-ended in either direction (no start or no end date), as needed.

Finished Date Range

The edit identity request completion date range. The report provides all requests that were completed on or after the start date and on or before the end date.
You can enter the date manually, or click the **...** icon to select a date from the calendar. Date ranges can be open-ended in either direction (no start or no end date), as needed.

Status

Select the status to include in the report. If none are specified, all status levels are included.

Batch Requests

Batch Requests

> If the order of operations is important, create a separate file for each request type and run them sequentially.

Batch Requests enable you to generate specific types of access requests for more than one user at a time. The required data is gathered from a prepared comma-delimited file for each request type. The batch files require comma-delimited data that represents the individual requests. In most cases the native identity or identity name can be used to specify the request target.

There might be an batch size limit set during the configuration of IdentityIQ. If you run into issues, contact your administrator.

To access the Batch Request option, navigate to **Setup -> Batch Requests**.

> An identity must have **IdentityIQ** administrative capabilities to use this option. For information about setting up administrative capabilities, contact your IdentityIQ administrator.

For more information, see:

- Batch Requests Page — provides information on how to view, create, stop, or delete batch requests
- Batch Request Types and Examples — provides descriptions and examples of the types of batch requests
- Batch Request Details Page — provides information on how to view specific information about a batch request
- Create Batch Request Page — provides information on how to import prepared comma-delimited files and set the parameters of the batch request.

Batch Requests Page

Use the Batch Requests page to:

- View all batch requests that are assigned to you or to one of your workgroups
- View all batch requests that you requested
- Create a new batch request
- Stop or delete an existing batch request

You can perform the following tasks:

- View details about a batch request — Double-click on a batch request entry in the table. See Batch Request Details Page.
- Create a new batch request — Click New Batch Request at the top of the table. See Create Batch Request Page.
- Stop or delete a batch request — Right-click the batch request entry in the table.

View Batch Requests

To sort the information in the table by ascending or descending order, click the table header. Alternatively, mouse over the header row and use the drop-down arrow to select ascending or descending order. To select which rows are displayed:

1. Mouse over a header row.
2. Click the drop-down arrow.
3. Mouse over Columns to display the column options.
4. Use the check boxes to select which columns appear in the table.

Use the search field at the top of the table to filter the results of the Batch File Name column. Double-click a batch request line item to view the Batch Request Details page. Right-click a line item to Terminate or Delete the batch request.

Column Name	Description
Batch File Name	The file location where the batch file is originated.
Request Date	The date the batch request was generated.
Run Date	The date the batch request was executed.
Completed Date	The date the batch request was completed.
Record Count	The number of items within the batch request.
Status	The current status of the batch request. Scheduled — Batch request is scheduled to run at a later date. Running — Batch request is currently running. Executed — Batch request was run successfully. Terminated — Batch request process was cancelled.

Batch Request Types and Examples

This section describes the batch request types and criteria required in the comma-delimited file with examples. IdentityIQ supports the following types of batch requests:

- Create Identity
- Modify Identity
- Create Account
- Delete Account
- Enable/Disable Account
- Unlock Account
- Add Role
- Remove Role
- Add Entitlement

- Remove Entitlement
- Change Password

Batch request types with similar data and columns can be mixed in the same file. The following batch request types must be in a separate file:

> To specify multiple entitlements or roles in the same request, use the pipe (|) delimiter to separate each role or entitlement.

- Create Identity
- Modify Identity
- Change Password

Create Identity

Use a Create Identity batch request to create a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for a Create Identity batch request is **CreateIdentity**.

Example:

```
operation, name, location, email, department
 CreateIdentity, Alex Smith, Austin, asmith@adept.com, Accounting
 CreateIdentity, Bob Smith, Austin, asmith@adept.com, Engineering
 CreateIdentity, Mark Smith, Austin, asmith@adept.com, Accounting
 CreateIdentity, John Smith, Austin, johnsmith@adept.com, Finance
```

Modify Identity

Use a Modify Identity batch request to modify or change the data of a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for a Modify Identity batch request is **ModifyIdentity**.

Example:

```
operation, identityName, location, email, department
 ModifyIdentity, Alex Smith, Austin, asmith@adept.com, Accounting
 ModifyIdentity, Bob Smith, Austin, asmith@adept.com, Engineering
 ModifyIdentity, Mark Smith, Austin, asmith@adept.com, Accounting
 ModifyIdentity, John Smith, Austin, johnsmith@adept.com, Finance
```

Create Account

Use a Create Account batch request to create accounts for a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for a Create Account batch request is **CreateAccount**.

Example:

```
operation, application, nativeIdentity | identityName, email
 CreateAccount, AdminsApp, atoby, atoby@example.com
 CreateAccount, AdminsApp, jsmith, jsmith@example.com
```

Delete Account

Use a Delete Account batch request to delete accounts for a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for a Delete Account batch request is **DeleteAccount**.

Example:

```
operation, application, nativeIdentity | identityName, email
 DeleteAccount, AdminsApp, atoby, atoby@example.com
 DeleteAccount, AdminsApp, jsmith, jsmith@example.com
```

Enable/Disable Account

Use an Enable/Disable Account batch request to enable or disable accounts on a specific application for a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for an Enable Account batch request is **EnableAccount.** The operation in the spreadsheet for an Disable Account batch request is **DisableAccount**.

Example:

```
operation, application, nativeIdentity | identityName
 EnableAccount, AdminsApp, abell
 EnableAccount, AdminsApp, jsmith
 EnableAccount, AdminsApp, mjohnson
```

Unlock Account

Use an Unlock Account batch request to unlock application accounts for a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for an Unlock Account batch request is **UnlockAccount**.

Example:

```
operation, application, nativeIdentity | identityName
 UnlockAccount, AdminsApp, abell
 UnlockAccount, AdminsApp, jsmith
 UnlockAccount, AdminsApp, mjohnson
```

Add Role

Use an Add Role batch request to add one or more roles to a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for an Add Role batch request is **AddRole**.

Example:

```
operation, roles, identityName
 AddRole, Helpdesk Associate
 AddRole, Benefits Manager, 222
 AddRole, Accounting, 222
 AddRole, Helpdesk Associate, 222
```

Remove Role

Use a Remove Role batch request to remove one or more roles from a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for a Remove Role batch request is **RemoveRole**.

Example:

```
operation, roles, identityName
 RemoveRole, Helpdesk Associate, 122
```

```
RemoveRole, Helpdesk Associate, 132
RemoveRole, Helpdesk Associate, 143
RemoveRole, Helpdesk Associate, 156
```

Add Entitlement

Use an Add Entitlement batch request to add one or more entitlements to a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for an Add Entitlement batch request is **AddEntitlement**.

Example:

```
operation, application, attributeName, attributeValue, nativeIdentity | identityName
 AddEntitlement, Procurement_System, group, @Audit, id1
 AddEntitlement, Procurement_System, group, @Audit, id2
 AddEntitlement, Procurement_System, group, @Audit, id3
 AddEntitlement, Procurement_System, group, @Audit, id4
 AddEntitlement, Procurement_System, group, @Audit, id5
```

Remove Entitlement

Use a Remove Entitlement batch request to remove one or more entitlements from a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for a Remove Entitlement batch request is **RemoveEntitlement**.

Example:

```
operation, application, attributeName, attributeValue, nativeIdentity | identityName
 RemoveEntitlement, Procurement_System, group, @Audit, id1
 RemoveEntitlement, Procurement_System, group, @Audit, id2
 RemoveEntitlement, Procurement_System, group, @Audit, id3
 RemoveEntitlement, Procurement_System, group, @Audit, id4
 RemoveEntitlement, Procurement_System, @Audit, id5
```

Change Password

Use a Change Password batch request to change or reset passwords for a list of identities from a prepared comma-delimited spreadsheet. The operation in the spreadsheet for a Change Password batch request is **ChangePassword**.

Example:

```
operation, application, password, nativeIdentity | identityName
 ChangePassword, Active_Directory, 1111, jsmith
 ChangePassword, Active_Directory, 1111, mjohson
 ChangePassword, Active_Directory, 1111, ajones
```

Batch Request Details Page

Use the Batch Request Details page to view specific information about a batch request. The page is divided into two sections. The upper section provides information about the batch request as a whole including:

- File Name
- Date Requested
- Date Launched
- Date Completed

- Status
- Total Records
- Total Completed
- Total Errors
- Total Invalid

The lower section includes the Batch Request Items table which displays information for each record in the batch request.

Request Data

Displays the comma-delimited data of the requested operation.

Status

Displays the current status of the record's request.

Running —Requested item is still processing. This could indicate an approval or manual work item completion is needed.
Finished —The request process completed.
Terminated — The request was manually cancelled.
Invalid — Something was wrong with the request. Click the cell to show further details.

Result

Displays the result of the record's request.

Success — The request completed.
Failed — The request failed due to a general validation error.
Approval —The request is waiting on an approval.
ManualWorkItem — Indicates the request failed because the request type requires the generation of a manual work item and this was not a configured option in the batch request.
PolicyViolation — The request failed because of a policy violation.
ProvisioningForm —Indicates the request failed because the request type requires the generation of a provisioning form and this was not a configured option in the batch request.
Skipped — Something was wrong with the request and it was skipped. Click the cell to show further details.

Identity Request ID*

> You must select **Identity Request ID** when you create the batch request.

The request ID generated by the batch request.

Create Batch Request Page

Use the Create Batch Request page to import prepared comma-delimited files and set parameters of the batch request.

Choose batch file

Click **Browse** and navigate the prepared comma-delimited file location.

Error handling

Determines the batch request process behavior in the event of an error. If a request item generates errors, you can continue the tasks or stop the task after a specified number of errors.

Policy Option

Determines the batch request process behavior for policy violations. You can include policy checking or to fail on any policy violation.

Schedule to run

Choose to run the batch request immediately or select a later date and time when the request runs.

Manual input

Determines the batch request process behavior when a request needs manual interaction. You can skip batch requests which require additional manual input or create any necessary provisioning forms.

Work items

Determines the batch request process behavior when a request results in the generation of a work item. You can skip the request or create any necessary work items.

Handle create identity as modify if identity exists

Select this check box to handle a create identity batch request line item as modify identity request if identity exists.

Generate identity requests

Select this check box to create an identity request that can be viewed **in Manage->Access Request**.