Getting Started

Version: 8.4

Revised: September 2023

Copyright and Trademark Notices

Contents

Getting Started with IdentityIQ

How you log in to IdentityIQ is based on how your system is configured. The following login options may be available:

- Custom login
- New User Registration
- QuickLinks
- Password Recovery – Account Unlock

> Note: Based on your role and individual privileges, and how your system is configured some options in this section could be unavailable.

After you log in to IdentityIQ, the Home page displays. For more information, see IdentityIQ Home Page and Navigation

> Note: Do not open multiple tabs or browsers. Opening multiple tabs might overwrite changes made in the other.

New User Registration

Self service registration enables new users to request an IdentityIQ user account the first time they access the product. When this option is enabled, the **New User Registration** link displays below the **Password** field on the Welcome screen.

> Note: To use this feature, enable self-service registration on the Lifecycle Manager Configuration page. See the **Lifecycle Manager** documentation.

> Note: You can also access the New User Registration page through a direct link that bypasses the login page and simplifies the registration process.

1. Click the **New User Registration** link to launch the New User Registration page.
2. Fill in the required fields, which include the requested IdentityIQ user name and password.
3. Click **Register.**

After the request is authorized, you receive an email notification and you can use the name and password submitted to log on to IdentityIQ.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) adds an additional layer of security by requiring you to use multiple methods to authenticate your identity before you can log in to IdentityIQ. When MFA is configured for your system:

1. Log in to IdentityIQ from the default login page and then your MFA provider's login page displays. If your password is expired or you are required to change your password, you must complete the MFA process first.
2. Follow the login prompts for your provider.
3. After you are authenticated, you are logged in to IdentityIQ and the **Home** page displays.

> Note: If you are assigned to multiple providers, you must select a provider from the provider list before you can proceed to the provider's login page.

Password Recovery – Account Unlock

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

- **Forgot Password** – your password is reset and you are automatically logged in to IdentityIQ
- **Account Unlock** – your account is unlocked and you can log in

When an Administrator sets up password recovery and account unlock options, the following verification methods are configured:

- Answer Authentication Questions
- Send a Text Message with a Verification Code

Answer Authentication Questions

To use this feature, your administrator must activate this option and you must provide answers to authentication questions in your IdentityIQ User Preferences before this feature is available.

Your administrator can set the following items that determine how the feature works:

- Number of answers you must define in your IdentityIQ User Preferences
- Number of correct answers you must provide to authentication questions

- Maximum number of wrong answers you can enter before IdentityIQ locks you out
- Number of minutes you are locked out

To unlock the account before the lockout time ends, an administrator with the appropriate system capabilities can click **Unlock Identity** on the Identity Cube Attributes tab.

How to Recover Your Password Using Authentication Questions

If you have not set up and answered the authentication questions and do not know your password, you must contact your help desk or your IdentityIQ administrator to reset your password.

Complete the following steps:

1. Click the **Forgot Password?** link.
2. Enter your username and click **OK**.
3. Enter the correct answers to the questions you previously set up and click **Done**.

   > Note: The responses entered on this window are compared to the recorded answers. If you provided the required number of correct answers, IdentityIQ can authenticate you. The authentication process ignores case when comparing the your answers to the stored answers.

4. On the next window, enter your new authentication password in the **New Password** and **Confirm Password** boxes and click **Change**.

The new password must meet the requirements of the password policy that your IdentityIQ administrator set up.

Send a Text Message with a Verification Code

To use this feature, your administrator must activate this option and a mobile telephone number must be configured for your IdentityIQ account. Your mobile phone number must contain a complete number including the area code.

This option is configured in **Login Configuration**. See the **IdentityIQ System Configuration** documentation for more details.

IdentityIQ Home Page and Navigation

The IdentityIQ Home page is a web-based console that enables you to review and act on compliance-related data and activities across the enterprise. The Home page displays after you log into the IdentityIQ or when you click the **Home** icon. The Home page functions as a dashboard with convenient links to specific areas IdentityIQ. These links are defined when IdentityIQ is deployed and are based on the needs of your enterprise.

The Home Page includes:

- QuickLinks
- Home Page Widgets
- Navigation Menu Bar

> Note: Lifecycle Manager must be installed to access the Lifecycle features. Contact your SailPoint representative for more information.

> Note: Based on your role and individual privileges, the availability of IdentityIQ components may be limited.

QuickLinks

QuickLinks are tasked-based links to frequently-used areas of IdentityIQ. Your administrator determines the behavior and availability of these links. QuickLinks are displayed as cards on the IdentityIQ Home page and as links in the QuickLink Menu, which is available throughout the product.

- QuickLink Menu – Lists all of the QuickLinks that are available to the user. The menu is displayed on every IdentityIQ page. Your administrator can configure these links.
- QuickLink Cards – Displays task-oriented based on available QuickLinks. Cards are available only on the Home page. Users can add or delete cards from their Home page.

QuickLink Menu

The QuickLinks menu is available from any IdentityIQ page and provides access to frequently-used items. To view the QuickLinks menu, click the **QuickLinks icon**, the three-bar icon located on the Navigation menu.

For a QuickLinks menu item to be available, a QuickLink must be configured. Based on your role and individual privileges, the availability of IdentityIQ QuickLinks can be limited.

By default, IdentityIQ ships with the following configuration in the QuickLinks menu:

My Tasks

Access Reviews: Links to the **Certifications > My Reviews** page that lists your current access reviews. Click an access review in the list to display the Access Review Details page.

Approvals: Links to the **Manage Work Items** page where you can view and manage approvals that are assigned to you or to a work group of which you are a member. You can also view approvals assigned by you.

Forms: Links to the **Manage Work Items** page where you can view and provide needed information for form work items.

Signoff Reports: Links to the **Manage Work Items** page where you can view and manage sign off report work items.

Policy Violations: Links to the **Policy Violations** page where you can view and manage policy violations outside of certifications.

Manage Access

> Note: This feature requires Lifecycle Manager.

Manage User Access: Links to the **Manage My Access** page where you can request to add access based on roles or entitlements or remove access. If you can request access for others, the Manage User Access page displays.

Manage Accounts: Links to the **Manage Accounts** page for yourself where you can double-click on a current account to make changes. If you can manage accounts for others, this option links to a page that lists identities. Double-click on an identity and select the account you want to manage.

Change Password: Links to the **Manage Password**s page for yourself where you can manage passwords for your current application accounts. If you can change passwords for others, this option links to a page that lists identities. Double-click on an identity to manage passwords for the identity's application accounts.

Track My Requests: Links to the **Access Request** page that lists your open access requests. to view details about a specific request double-click a listing.

Manage Identity

> Note: This feature requires Lifecycle Manager.

Create Identity: Links to the Create New page where you can create a new identity to be stored in the Identity Warehouse.

Edit Identity: Links to the Edit Identity Attributes page for yourself where you can specify and request changes to your identity attributes. If you can edit identity attributes for others, this option links to a page that lists identities. Double-click on an identity to specify and request changes for the identity's attributes.

View Identity: Links to the View identity page for yourself where you can view identity information. If you can view identity information for others, this option links to a page that lists identities. Double-click on an identity to view the identity's information. The View Identity page contains information about an identity's attributes, entitlements, and application accounts.

See **How to Manage Identities.**

Those who have the Privileged Account Management module also have a Quicklink to the **Privileged Account Management** page. The SailPoint IdentityIQ Privileged Account Management Module (PAM) extends identity governance processes and controls to highly privileged access, enabling you to centrally manage access to privileged and non-privileged accounts.

Talk to your SailPoint representative or refer to the SailPoint IdentityIQ Privileged Account Management documentation for more information.

QuickLink Cards

QuickLink cards are based on the QuickLinks that are set up when IdentityIQ is deployed. You can rearrange, move, and add QuickLink cards on your Home page.

For a QuickLink card to be available, a QuickLink must be configured by the Administrator. Additionally, Lifecycle Manager must be installed to use to use the QuickLink cards for the Access Request component.

By default, IdentityIQ ships with the following cards set up on the Home page:

- Policy Violations
- Access Reviews
- Approvals
- Manage User Access
- Track My Requests

To use the the QuickLink cards for the Access Request component Lifecycle Manager must be installed and a QuickLink must be configured.

See QuickLink Menu for more information for information about default QuickLinks.

How to Manage QuickLink Cards on Your Home Page

To make changes to your Home page, click **Edit** and make any of the following changes:

- Rearrange cards – Click and hold **Drag** and then move the card to the new location.
- Remove a card – Click **Remove**.
- Add a card – Click **Add Card** and select one or items from the list of available cards and then click **Save**. to close the selection window.

You can also set the type of cards to display in the top row of the Home page, QuickLink cards or Widgets.

When your changes are complete, click **Save**.

Home Page Widgets

> Note: Based on your role and individual privileges, the availability of IdentityIQ Widgets may be limited.

Homepage Widgets use bite-size visualizations and data grids to present information of interest to the logged-in user. You can rearrange, move, and add widgets on your Home page. See How to Manage Widgets on Your Home Page. Click any item in the Widget card to go to the stand-alone page associated with the card. Click **All** to view the stand-alone page with all the listings associated with the card.

By default, IdentityIQ ships with the following predefined Widgets:

Work Item

Latest Approvals displays the five most recent approvals that the logged-in user or one of their work groups.

Latest Policy Violations displays the five most recent forms that the logged-in user or one of their work groups

Latest Forms displays the five most recent forms that the logged-in user or one of their work groups.

Certification

Certification Campaigns displays as a chart that indicates the completion status as a percentage.The color of the chart and message displayed under the title change based on the proximity to the due date.
Today – text indicates Due Today and chart is red.
Week – text indicates Due This Week and chart is orange.
Other – text indicates Due X where X is the due date and chart is green.

To view this widget, user must have compliance officer, certification admin, or auditor capabilities.

My Access Requests displays as a pie chart that indicates the completion status as with the number of items completed out of total items. The color of the chart and message displayed under the title change based on the proximity to the due date.
Today – text indicates Due Today and chart is red.

Week – text indicates Due This Week and chart is orange.
Other – text indicates Due X where X is the due date and chart is green.

Risk

Risk Scores: Applications and Identities displays risk scores for applications and identities. By default, the Applications panel displays the top five applications with the highest risk scores. To view the top five identities with the highest risk score, click the forward arrow. To switch between the panels, click the forward or back arrow.

Productivity

Direct Report Actions displays a list of the direct reports for the logged-in manager. Based on the manager's rights and capabilities, the manager can perform actions such as request access, change password, manager accounts, and view identity details. Click and identity name to view information about the identity.

Data Governance

Requires the File Access Manager integration

Sensitive Data Exposure shows the number of overexposed resources, and the overall compliance score. The compliance score is color coded to indicate risk (0-5 is considered high risk, 5.1-7.5 medium risk, and 7.6-10 low risk).

Sensitive Resources Missing Owners shows the number of resources with classified data that are missing an assigned data owner, and the overall compliance score. The compliance score is color coded to indicate risk (0-5 is considered high risk, 5.1-7.5 medium risk, and 7.6-10 low risk).

How to Manage Widgets on Your Home Page

To make changes to your Home page, click **Edit** and make any of the following changes:

- Rearrange cards – click and hold **Drag** and then move the card to the new location.
- Remove a card – click **Remove**.
- Add a card – click **Add Card** and select one or items from the list of available cards and then click **Save** to close the selection window.

You can also set the type of cards to display in the top row of the Home page, QuickLink cards or Widgets.

When your changes are complete, click **Save**.

Navigation Menu Bar

The Navigation bar can be accessed from any IdentityIQ page and provides a convenient way to access areas of IdentityIQ. By default, IdentityIQ ships with the following top-level headings in the Navigation bar:

- Home
- My Work
- Identities
- Applications
- Intelligence
- Data Governance
- Setup
- Gear Icon – Administration Menu
- Bell Icon - Work Item Menu
- User Name – User Menu

> Note: Based on your role and individual privileges, the availability of IdentityIQ navigation menu bar items can be limited. Additionally, some options require IdentityIQ administrative capabilities. For information about setting up administrative capabilities, contact your IdentityIQ administrator.

Home

Your Home page functions as a dashboard with convenient QuickLink cards that link directly to frequently-used areas in IdentityIQ. Click **Home** in the Navigation menu bar from any IdentityIQ page to refresh or return to the Home page.

You can rearrange, add, or delete QuickLink cards based on available QuickLinks. See How to Manage QuickLink Cards on Your Home Page.

My Work

This menu item links to the Manage Work Items page where your can view and manage open items that require your input, such as Access Reviews, Access Requests, Policy Violations, and Work Items.

Identities

This menu item links to the Identities page, which contains links to pages related to user identities, such as:

- **Identity Warehouse** – links to the Identity Warehouse page where you can create, view, and edit information for individual identities in your enterprise.
- **Identity Correlation** – links to the Identity Correlation page where you can correlate one or more accounts with an identity.
- **Identity Risk Model** – links to the Risk Scoring Configuration page where you can configure risk scoring identities.

Applications

The Applications menu bar item contains links to pages related to applications and entitlements, such as:

- **Application Definition** – links to the Application Definition page where you can specify the connection properties, relevant attributes, targets and aggregation rules for each application in your enterprise to work with IdentityIQ.
- **Entitlement Catalog** – links to the Entitlement Catalog page where you can view and manage managed attributes including entitlements, account groups/application objects and permissions.
- **Application Risk Model** – links to the Application Risk Scoring Configuration page where you can configure risk scoring for applications in your organization.
- **Activity Target Categories** – links to the Activity Target Categories page where you can view, add or edit the defined categories to use with the Activity Search page.

Intelligence

The Intelligence menu bar item contains links to pages related to analytics, such as:

- **Advanced Analytics** – links to the Advanced Analytics page where you can create specific queries based on identities, certifications, activity and audit logs.
- **Reports** – links to the Reports page where you can use standard or custom reports to collect information you need to manage the compliance process.
- **Identity Risk Scores** – links to the Identity Risk Score page where you can view individual risk scores for users. The page displays one tab for each risk level defined in IdentityIQ.
- **Application Risk Scores** – links to the Application Risk Scores page where you can view risk scores associated with each application. The page displays a table summarizing all of the applications score cards.

Data Governance

The Data Governance menu bar item is available only if the File Access Manager integration has been implemented, and is viewable only by users with an IdentityIQ capability that includes rights to see File Access Manager features. It contains links that provide direct access to the File Access Manager website.

For information about the Data Governance menu options, refer to the refer to the File Access Manager documentation.

Setup

The Setup menu bar item contains links to pages related to configuration items, such as:

- **Certifications** – links to the Certifications page where you can view and create the scheduled certifications that are required to maintain compliance in your enterprise.
- **Roles** – links to the Role Management page where you can create and maintain the roles that define your enterprise.
- **Policies** – links to the Policies page where you can define policies to monitor identities that are in violation of the policies.
- **Tasks** – links to the Task page where you can create tasks that automate the processes that build, update, and maintain the information contained within IdentityIQ.
- **Groups** – links to the Group Configuration page where you can work with groups and populations that track and monitor activity by membership and risk information.
- **Business Processes** – links to the Business Process Editor page where you can create a sequence of steps or activities and each step can perform one or more actions.
- **Lifecycle Events** – links to Lifecycle Events page where you can create new events or configure existing events in your enterprise to trigger business processes.
- **Batch Requests** – links to the Batch Requests page where you can work with batch requests that enable you to generate specific types of access requests for more than one user at a time.

Gear Icon – Administration Menu

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

The Administration menu bar item contains links to pages specific to system-wide configurations, such as:

- **Global Settings** – configure control and default settings for the entire IdentityIQ product.

  For more information, see the **System Configuration** documentation.

- **Lifecycle Manager** – adds tools, work items and reports related to Lifecycle Manager core functionality.

  For more information, see the **Lifecycle Manager** documentation.

- **Compliance Manager** – access certifications, policy management, and audit reporting.

  For more information, see the **System Configuration** documentation.

- **Administrative Console** – provides Task, Provisioning, and Environment monitoring tables.

  For more information, see the **System Administration** documentation.

- **Plugins** – displays the third-party plugins configured to work with IdentityIQ.

  For more information, see the **IdentityIQ Plugins** documentation.

Bell Icon - Work Item Menu

The Bell icon provides notifications and quick access to work items for a logged-in user and can include the following types of work items:

- Approvals
- Forms
- Violations
- Others

When you log in, a red badge displays on the Bell icon and indicates the total number of any work items you have. Click a work item to display the associated Work Item page. See the **Work Items** documentation for more information.

> Note: The count for work item types refreshes on a regular interval. By default, the refresh cycle is five minutes. Because your administrator can customize this setting, your refresh cycle can be different.

User Name – User Menu

The name of the logged-in user is displayed in the navigation menu bar and contains a link to the Preferences page specific to you where you can view or edit user preferences.

There is also a Logout option allowing you to log out of IdentityIQ.

Edit Preferences

Preferences includes settings that personalize how you use IdentityIQ. Depending on your level of access you may have options to:

- Set up a user to whom all work items assigned to you are to be forwarded.
- If a forwarding user is used, edit the start and end dates for all forwarded work items.
- Change the password you use to log in to IdentityIQ.
- Select security questions and provide answers.
- Specify your name and the email address to use for notifications.

> Note: Only system administrators can change the name and email information from this location.

The ability to edit some of the preferences on this page is determined during configuration. Consult your administrator if you have questions.

General

On the **Edit Preferences > General** tab, you may designate a Forwarding User who will receive all work items, as well as the associated reminders and notifications, that are assigned to you for the time period you determine.

1. Use the dropdown arrow or begin typing to locate and select the appropriate user.
2. Select the **Start Date** checkbox, then use the date picker to indicate the date to start forwarding items.
3. If you want forwarding to end at some point, select the **End Date** checkbox and use the date picker to indicate when forwarding should stop. Note that specifying a forwarding user without an end date will *permanently* enable the forwarding process as of the start date.

Password

Use the form on the **Edit Preferences > Password** tab to change your IdentityIQ password. See **Self-Service Password Reset**.

1. Enter your current password.
2. Enter your desired new password.
3. Re-enter the new password to confirm.

Security Question

If your System Administrator has set up the system to require security questions as part of a password reset, you will have a Preferences menu option for Security Questions. They may be configured by System Administrators in **gear > Global Settings > Login Configuration > User Reset tab > Questions**.

System Administrators, see **Configuring the Security Question Settings** in the *IdentityIQ Password Management guide.*

End users, see **Security Questions Tab** in the *IdentityIQ Password Management Guide*.