



# Quest<sup>®</sup> Security Management Platform Global Settings

## **User Guide**



© 2026 Quest Software Inc.

**ALL RIGHTS RESERVED.**

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.  
Attn: LEGAL Dept.  
20 Enterprise, Suite 100, Aliso Viejo, CA 92656

Refer to our website (<https://www.quest.com>) for regional and international office information.


**Patents**

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

**Trademarks**

Quest and the Quest logo are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. All other trademarks and registered trademarks are property of their respective owners.

**Legend**

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

 **IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

# Contents

<b>Working with Security Management Platform Global Settings</b> .....	<b>6</b>
<b>Overview of Security Management Platform Global Settings</b> .....	<b>7</b>
Organizations .....	7
Microsoft Entra tenants .....	8
<b>Signing up for Security Management Platform Global Settings</b> .....	<b>9</b>
Organizations and regions .....	9
Signing in to Security Management Platform .....	10
Quest Security Management Platform Cookie Policy .....	11
Modifying Your Consent .....	12
Security Management Platform subscriptions .....	12
<b>Managing organizations and regions</b> .....	<b>13</b>
Geographic regions .....	13
Multiple organizations .....	14
Creating a new organization .....	14
Displaying the organization ID and deployment region .....	15
Switching organizations .....	16
Editing organization settings .....	16
Restricting access to organizations .....	16
Renaming organizations .....	17
Deleting organizations .....	17
Security Management Platform endpoint requirements .....	18
<b>Adding users and groups to an organization</b> .....	<b>20</b>
Users, groups, and roles .....	20
Default roles and permissions .....	20
Access Control: Roles .....	21
Viewing role permissions .....	21
Creating a custom role .....	22
Editing a custom role .....	22
Assigning a role to a user .....	23
Deleting a custom role .....	23
Organization access for Microsoft Entra users .....	23
Adding a user to your organization and assigning a role .....	24
Editing user roles .....	24
Removing a user from the organization .....	25
Organization access through Microsoft Entra group membership .....	25
Adding a group to your organization and assigning a role .....	25
Filtering the groups displayed .....	26
Editing group roles .....	26
Removing groups from the organization .....	26
Joining an organization prerequisites .....	26

<b>Managing your Microsoft Entra tenants and on-premises domains</b> .....	<b>28</b>
Tenants overview .....	28
Adding tenants .....	29
GCC and GCC High tenants .....	29
Prerequisites for adding tenants .....	29
Managing admin consent permissions .....	30
About admin consent status .....	31
Granting and regranting admin consent .....	31
About the Status and Actions column .....	32
About the Microsoft Authentication Library (MSAL) .....	32
About revoking admin consent .....	33
Removing a tenant .....	33
Managing your on-premises domains .....	34
On-premises agent prerequisites .....	34
On-premises agent supported operating systems .....	35
On-premises agent system configuration requirements .....	35
On-premises agent endpoint requirements .....	36
Adding an on-premises agent .....	37
About agent installation .....	39
Agent service account configuration .....	39
Secure LDAP configuration and deployment .....	39
Installing the agent using the command shell .....	40
Configuring an agent .....	41
Editing an agent configuration .....	41
Automatic updates for on-premises agents .....	42
Removing an agent .....	42
Adding an Active Directory domain .....	43
Editing a domain configuration .....	43
Removing a domain .....	43
<b>Security Management Platform Home page</b> .....	<b>44</b>
Masthead .....	44
Masthead drop-down menu .....	45
AI Assistant .....	45
Announcements and global notifications .....	46
Managing global notifications .....	46
Information window .....	47
Security Management Platform Status page .....	47
Side navigation panel .....	47
Dashboard .....	48
Tenant filter .....	48
Needs your attention! .....	49
Product tiles .....	49
<b>Configuring settings</b> .....	<b>50</b>
Organization .....	50
Access Control .....	50

Subscriptions .....	51
Subscription details .....	51
Managing subscriptions .....	52
Subscription expiry .....	54
Activity trail .....	55
Notifications .....	56
Managing Notification Templates: Required Permissions .....	57
Configuring Audit Notification Templates .....	57
Configuring Security Management Platform Notification Templates .....	58
Configuring Identity Recovery for Active Directory Notification Templates .....	59
Configuring Identity Recovery for Microsoft Entra ID Notification Templates .....	59
Configuring Migration - Self-Service Notification Templates .....	60
<b>Documentation roadmap .....</b>	<b>62</b>
Global settings .....	62
Release Notes .....	62
More resources .....	63
<b>Technical Support .....</b>	<b>64</b>
Current operational status .....	64
Contact support .....	64
Module product support pages .....	64
Information and discussion: Quest community forums .....	64

# Working with Security Management Platform Global Settings

Welcome to Security Management Platform Global Settings. For an overview of the application, see [Overview of Security Management Platform Global Settings](#). Use the links below for information on using Security Management Platform.

<a href="#">Signing up for Security Management Platform Global Settings</a>	<p>Security Management Platform is hosted in the cloud by Quest Software and made available to users through the internet. This section contains information regarding signing up for the Security Management Platform service.</p> <p>Security Management Platform management is based on the concept of organizations. A Security Management Platform organization can subscribe to modules. Organization administrators can use the tools provided by the modules to perform administrative actions on Microsoft Entra tenants.</p> <p><b>IMPORTANT:</b> To use the features of a module after you sign up, you must have a subscription.</p> <p>Trial licenses are available. See "Product Licensing" in the Global Settings Release Notes.</p>
<a href="#">Managing your Microsoft Entra tenants and on-premises domains</a>	<p>A tenant houses the users in a company and the information about them. You must add a Microsoft 365 tenant to Security Management Platform to manage the tenant properties using a Security Management Platform product. For the U.S. region, in addition to commercial tenants, you can add GCC and GCC High tenants if needed,</p> <p>In addition to managing your Microsoft Entra tenants, Security Management Platform provides support for connecting to on-premises domains in hybrid environments to perform data collection and management activities.</p>
<a href="#">Managing organizations and regions</a>	<p>Security Management Platform management is based on the concept of organizations. You can create a Security Management Platform organization and specify the region in which the organization data is to be stored.</p>
<a href="#">Adding users and groups to an organization</a>	<p>Once you have created an organization, you can add additional users and groups and determine what tasks they can perform.</p>
<a href="#">Security Management Platform Home page</a>	<p>After signing in, users see the Dashboard. In addition to a tile for each module, the Dashboard displays statistics and operational data for your tenant.</p>
<a href="#">Configuring settings</a>	<p>Use settings to configure Security Management Platform for your organization.</p>
<a href="#">Documentation roadmap</a>	<p>Links to the User Guide and Release Notes for each module.</p>
<a href="#">Technical Support</a>	<p>Resources for Security Management Platform technical support.</p>

---

# Overview of Security Management Platform Global Settings

Security Management Platform is a cloud-based management platform that provides access to multiple Quest Software tools for Microsoft product management through a unified interface. Cloud-based is a term that refers to applications, services, or resources that are made available to users and groups on demand through the Internet. Quest Security Management Platform is a Software as a Service (SaaS) application where application software is hosted in the cloud and made available through [quest-on-demand.com](https://quest-on-demand.com).

Security Management Platform management is based on the concepts of organizations, modules, and Microsoft Entra tenants. When you sign up for the Security Management Platform service, you create an organization. The organization can subscribe to products. Organization administrators can use the tools provided by the products to perform administrative actions on Microsoft Entra tenants.

! | **NOTE:** Azure Active Directory is now Microsoft Entra ID.

## Products

Currently, the following management products are available:

- Migration
- Identity Recovery
- Identity Defense

## Global Settings

Security Management Platform Global Settings refers to management tools and configuration settings that apply to all Security Management Platform products. This includes tenant and domain management tasks, adding users, groups, and roles, configuring notifications, and downloading activity trail logs.

## Organizations

Security Management Platform administration is based on organizations. When a user signs up for Security Management Platform, an organization is created.

For information about how to add users and groups to an organization, see [Joining an organization prerequisites](#) and [Adding a group to your organization and assigning a role](#).

For details on managing organizations, see [Managing organizations and regions](#).

# Microsoft Entra tenants

Microsoft Entra ID also uses the concept of an organization and a tenant. A tenant is representative of an organization and is a dedicated instance of the Microsoft Entra service that an organization receives and owns when it signs up for a Microsoft cloud service such as Microsoft Intune or Microsoft 365. Each tenant is distinct and separate from other tenants.

A tenant houses the users in a company and the information about them - their passwords, user profile data, permissions, and so on. It also contains groups, applications, and other information pertaining to an organization and its security. For more information see this [Microsoft help page](#).

# Signing up for Security Management Platform Global Settings

Security Management Platform is a Software as a Service (SaaS) application. SaaS is a software licensing and delivery model in which application software is licensed on a subscription basis. The Security Management Platform software is hosted in the cloud by Quest Software and made available to users through the internet. This section contains information regarding signing up for the Security Management Platform service.

<a href="#">Organizations and regions</a>	An overview of organizations and regions. For details on configuring organizations and regions after you sign up, see <a href="#">Managing organizations and regions</a> .
<a href="#">Signing in to Security Management Platform</a>	Information on how to sign up for Security Management Platform and enable multi-factor authentication.
<a href="#">Quest Security Management Platform Cookie Policy</a>	Information on managing your cookie policies.
<a href="#">Security Management Platform subscriptions</a>	You must start a trial or purchase a subscription to begin using Security Management Platform Global Settings services.

## Organizations and regions

Security Management Platform management is based on the concepts of organizations. When you sign up for the Security Management Platform service, you create an organization and you become the organization administrator. The organization can then subscribe to modules. Organization administrators can use the tools provided by the modules to perform administrative actions on Microsoft Entra tenants. You can add additional organization administrators and module administrators that have access to specific modules.

For most Security Management Platform use cases, a customer creates a single organization. Multiple administrators and multiple tenants can be added to the organization.

### **NOTE: Recovery account recommendation**

Quest recommends having an external account added to an organization that could be used in case access is lost. This external account should be a Microsoft Entra account from a tenant that is different from any user accounts normally used to access a Security Management Platform organization. For details see Microsoft's documentation [Manage emergency access accounts in Microsoft Entra ID](#).

### **CAUTION: Adding a tenant to multiple organizations.**

Adding the same tenant to multiple organizations can result in conflicting application of policies and settings. When using multiple organizations to manage a tenant, the organization administrators must coordinate their management activities.

An Azure region is a set of data centers deployed within a geographic area. Selecting the correct region for your organization lets you achieve higher performance and supports your requirements regarding data location. Specifying the region for your organization determines the geographical region where your data is stored.

During sign up, you can choose the region where your Security Management Platform data will be hosted. The following regions are currently supported:

- Australia
- Canada
- Europe
- United Kingdom
- United States

For more information, see [Geographic regions](#).

# Signing in to Security Management Platform

Signing into Security Management Platform is done through Microsoft Entra ID. Authenticating through Microsoft Entra ID provides native granular control and allows you to manage your configuration from a central location. It allows configuring advanced security layers through your own conditional access policies, such as MFA, integration with OKTA and other applications that work with the Microsoft Authentication Library (MSAL).

A Microsoft Entra ID access token (constrained to the Quest Security Management Platform application) is obtained when the user navigates through the authentication process. This Microsoft Entra ID access token has a lifetime limit of 10 minutes after which it is automatically refreshed if the user is actively using the application. The user is automatically logged out following a period of inactivity. If the user token is revoked in Microsoft Entra ID, the user will continue to have access to Security Management Platform until the token expiry, for a maximum of 10 minutes. User access to Security Management Platform organization can be also revoked within Security Management Platform by a Security Management Platform Organization Administrator, resulting in access loss after token expiry.

## To enable multi-factor authentication (MFA) when signing in to Security Management Platform

**NOTE:** Multi-factor authentication (MFA) increases the security of the sign in process. With MFA, a user is granted access only after presenting two or more pieces of evidence (or factors) to an authentication mechanism.

- 1 Go to the web page [quest-on-demand.com](https://quest-on-demand.com).
- 2 On the Welcome to Quest Security Management Platform page, click **Sign in with Microsoft**.
- 3 Sign in using your Microsoft MFA-enabled account.

As part of the login process with Microsoft Entra ID, users must consent to the set of minimal permissions required by the Quest Security Management Platform application.

Permission	Description
View your basic profile	Permission required for Quest to access users name and email to display the logged in user.
Maintain access to data you have given it access to	Permission is automatically included and required by Microsoft for Single Page Applications as it gives access to critical refresh tokens for proper functionality.  This permission scope is required for single sign on (SSO) and allows a refresh token to be returned from the authentication flow to avoid Security Management Platform prompting the user every time their primary authentication token times out.

By default, all users are allowed to consent to applications for permissions that do not require administrator consent. This behavior might be disabled in some Microsoft Entra tenants and may require tenant administrators to enable user consent flow for the Quest Security Management Platform application.

**i | NOTE:**

- The ability to consent on behalf of your organization is available if logging in as the global administrator in the tenant.
- The ability to request consents will only be available if the global administrator has enabled the admin consent workflow. See [Microsoft documentation](#).

- 4 Click **Create New Organization**.
- 5 Enter a name for your Security Management Platform organization.
- 6 Select the deployment region where you want your data to reside.
- 7 Click **Create New Organization**.

You are signed in as the Security Management Platform administrator for the new organization.

# Quest Security Management Platform Cookie Policy

Our website requires certain cookies to function properly (these are essential). In addition, we may use other cookies—with your consent—to:

- Enhance your experience
- Analyze website performance and traffic

**i | NOTE:** We also share information about your use of our site with social media, advertising, and analytics providers, as described in our [Cookie Use Policy](#).

When you open Security Management Platform, you'll see options to review the cookie policy and manage your preferences. You can choose to:

- Accept cookies
- Reject all cookies
- Manage my cookies

## **To customize your cookie settings:**

- 1 Select **Manage my Cookies**.

You can choose which types of cookies to allow. Click the category headings to learn more and adjust settings. Blocking some cookies may affect site functionality and available services.

- **Strictly Necessary Cookies** (Always active.) These cookies are required for the website to function and cannot be disabled in our system. They are typically set in response to actions you take, such as setting privacy preferences, logging in, or completing forms. You can block or receive alerts about these cookies through your browser settings, but some parts of the site may not work properly. These cookies do not store personally identifiable information.
- **Performance Cookies** (Disabled by default). You can enable these cookies to help us measure and improve site performance. They show which pages are popular and how visitors navigate the site. All data is aggregated and anonymous. If you disable them, we will know when you visit the Security Management Platform site or be able to monitor performance.

Confirm your selections by clicking **Confirm my choices**.

## Modifying Your Consent

If you have previously accepted cookies (such as Performance Cookies) and wish to change your settings, you can return to the **Manage my Cookies** section. By disabling a category or selecting **Reject all cookies**, you revoke consent and those optional cookies are removed from your browser. In this state, only **Strictly Necessary Cookies** will remain active.

## Security Management Platform subscriptions

Once you have signed in to and created an organization, you have the option to begin a trial or purchase a subscription for modules. In the side navigation panel, click Services to open a page with module information and Learn More links that take you to the appropriate Quest web site.

# Managing organizations and regions

Security Management Platform management is based on the concept of organizations. An organization can subscribe to modules. Organization administrators can use the tools provided by the modules to perform administrative actions on Microsoft Entra tenants.

When a user signs up for Security Management Platform, an organization is created and the user becomes an administrator for the organization. For most Security Management Platform use cases, a customer creates a single organization. Multiple administrators and multiple tenants can be added to the organization. See [Signing up for Security Management Platform Global Settings](#).

Use the links below for more information on managing organizations and regions.

- [Geographic regions](#)
- [Multiple organizations](#)
- [Creating a new organization](#)
- [Displaying the organization ID and deployment region](#)
- [Switching organizations](#)
- [Editing organization settings](#)
- [Deleting organizations](#)
- [Security Management Platform endpoint requirements](#)

## Geographic regions

An Azure region is a set of data centers deployed within a geographic area. Selecting the correct region for your Security Management Platform organization enables you to achieve higher performance and supports your requirements and preferences regarding data location. Specifying the region for your organization determines the geographical region where your data is stored. For more information, see [Microsoft documentation](#).

During sign up, you can choose the region where your Security Management Platform data will be hosted. The following regions are currently supported:

- United States
- Europe
- United Kingdom
- Canada
- Australia

## Regional availability of modules

Microsoft continues to deploy services across Azure regions. However, at this time, not all services are available in all regions. As a result, not all Security Management Platform modules are available in all regions. The table below lists current module availability by region. When you create an organization in a region, only the available module tiles are displayed on your home page.

Region	Available Products
U.S.	<ul style="list-style-type: none"> <li>• Identity Defense</li> <li>• Migration</li> <li>• Identity Recovery</li> </ul>
Europe	<ul style="list-style-type: none"> <li>• Identity Defense</li> <li>• Migration</li> <li>• Identity Recovery</li> </ul>
U.K.	<ul style="list-style-type: none"> <li>• Identity Defense</li> <li>• Migration</li> <li>• Identity Recovery</li> </ul>
Canada	<ul style="list-style-type: none"> <li>• Identity Defense</li> <li>• Migration</li> <li>• Identity Recovery</li> </ul>
Australia	<ul style="list-style-type: none"> <li>• Identity Defense</li> <li>• Migration</li> <li>• Identity Recovery</li> </ul>

For the most up-to-date information, see <https://regions.quest-on-demand.com/>.

## Multiple organizations

Some customers may want to create multiple organizations. For example:

- A managed service provider (MSP) can create an organization for each client.
- A global company can create separate organizations for employees by geographic region.

When you sign up for Security Management Platform, you are prompted to name your organization. Users with multiple organizations associated with their email address are prompted to select an organization during sign in.

### **CAUTION:** Adding a tenant to multiple organizations.

Adding the same tenant to multiple organizations can result in conflicting application of policies and settings. When using multiple organizations to manage a tenant, the organization administrators must coordinate their management activities.

## Creating a new organization

As an Security Management Platform user, there may be no organizations associated with your account. This can happen if this is the first time that you have used Security Management Platform and have not yet been invited to an organization or if you have been removed from all organizations. In this case, after you sign in, the Welcome to Security Management Platform page opens where you can create a new organization. Use the following steps to create an organization.

If you are currently signed in, you can create a new organization by clicking your email address in the menu bar at the top of the page and selecting **Create Organization**. Follow the steps that follow to create an organization.

- TIP:** On the Create Organization page, if you decide not to create a new organization, click on your browser back button to return to your original organization.

### **To create a new organization:**

- 1 Enter an organization name.

- 2 Select a region.
- 3 Click **Create Organization**.

## Best practices when selecting a region for a new organization

If you are creating an organization for use with a Security Management Platform product, first determine the data location for your Microsoft 365 tenants.

You can view tenant-specific data location information in your Microsoft 365 Admin Center in **Settings | Org settings | Organization Profile | Data location**. For details about where your data is stored, see the Microsoft article: <https://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations?view=o365-worldwide>

For most Security Management Platform products, select the Security Management Platform deployment region that contains the data location of your Microsoft 365 tenant, if none of the available deployment regions match your Microsoft 365 tenant data location, select the deployment region that is closest to your Microsoft 365 tenant. For the On Demand Migration product see the section that follows.

## Considerations when you create a Security Management Platform organization for migration

The following points should be considered when selecting a region for a new organization:

- Select the Security Management Platform deployment region that contains at least one data location for your source and target Microsoft 365 tenancies.
- If the source and target Microsoft 365 tenant data locations are in different deployment regions, select the region closest to the target tenant data location.
- If neither the source nor target Microsoft 365 tenant data locations are in a Security Management Platform deployment region, select a region that provides the shortest migration path **from** source tenant **to** Security Management Platform deployment region **to** target tenant.
- If the Microsoft 365 tenancies have Multi-Geo capability enabled, you might need to create separate Security Management Platform organizations in different deployment regions. Consider the locations of each source and target combination and create Security Management Platform organizations in a suitable deployment region.

## Displaying the organization ID and deployment region

Each organization has a unique organization ID. This ID may be required by technical support to troubleshoot issues. You can display the organization to which you are currently signed in and its region by clicking on your email address in the top menu bar.

In the menu list, if you have only one tenant, the organization is shown under the Organization Name title. Click the organization to open the **Settings | Organization** page where you can see the organization ID, deployment region, name, and the domains authorized to access it.

If you have more than one tenant, the Manage Tenants option is shown under Organization Name. Click **Manage Tenants** to see the list of your tenants with the tenant to which you are connected indicated. The organization ID is displayed on the tile for each tenant.

### ***To display the organization basic information:***

- 1 In the top menu bar, on the right hand side, click on your user email address.  
-OR-
- 2 In the navigation panel on the left, click **Settings | Organization**.  
The Organization ID and deployment region are found under **Basic Information**.

## Switching organizations

If you have multiple organizations associated with your email address, you are prompted to select an organization when you sign in. Once you are signed in, you can switch to another organization.

### ***To switch to another organization:***

- 1 In the top menu bar, on the right hand side, click on your user email address.
- 2 Select **Switch Organization**.  
The Choose an Organizations page opens.
- 3 Locate the row that contains the organization to which you want to switch.
- 4 Click **Select**.

## Editing organization settings

Once an organization has been created, you can edit the organization name and the domains that are authorized to access it and delete organizations that are no longer needed.

You must be an Security Management Platform organization administrator to edit an organization.

- [Restricting access to organizations](#)
- [Renaming organizations](#)

## Restricting access to organizations

By default, users from all domains have access to an organization. If required, you can restrict access to only users from authorized domains.

### ***To add authorized domains:***

- 1 Sign in to the organization that you want to change.
- 2 In the top menu bar, on the right side, click on your user email address, and select your organization under the **Organization Name**.  
-OR-  
In the navigation panel on the left, click **Settings | Organization**, and select **Edit**.
- 3 Under **Authorized Domains**, add the Fully Qualified Domain Name of the domains (and associated users) that you want to have access to the organization.
- 4 Click **Save**.
- 5 Click **Yes** to confirm.

# Renaming organizations

## **To rename an organization:**

- 1 Sign in to the organization that you want to change.
  - 2 In the top menu bar, on the right side, click on your user email address, and select your organization under the **Organization Name**.
- OR-
- In the navigation panel on the left, click **Settings | Organization**, and select **Edit**.
- 3 Under **Basic Information**, enter the new name in the **Organization Name** field.
  - 4 Click **Save**.
  - 5 Click **Yes** to confirm.

# Deleting organizations

When you delete an organization, all data configured for the organization (such as custom roles and role assignments), associated tenants, consents, and module-specific configurations are also removed.



## **IMPORTANT:**

- This operation can only be restored through Quest Support within 30 days of the deletion.
- You must be an Security Management Platform organization administrator to delete an organization.

## **To delete an organization:**

- 1 Sign in to the organization that you want to change.
  - 2 In the top menu bar, on the right side, click on your user email address, and select your organization under the **Organization Name**.
- OR-
- In the navigation panel on the left, click **Settings | Organization**, and select **Delete Organization**.

# Security Management Platform endpoint requirements

Table 1. Endpoints required for "base" Security Management Platform access

Region	Endpoints
United States	<a href="https://www.quest.com">https://www.quest.com</a> <a href="https://quest-on-demand.com/">https://quest-on-demand.com/</a> <a href="https://support.quest.com">https://support.quest.com</a> <a href="https://status.quest-on-demand.com">https://status.quest-on-demand.com</a> <a href="https://us.notification.quest-on-demand.com">https://us.notification.quest-on-demand.com</a> <a href="https://us.core.api.quest-on-demand.com/">https://us.core.api.quest-on-demand.com/</a> <a href="https://odatprodcomputeusw2.blob.core.windows.net">https://odatprodcomputeusw2.blob.core.windows.net</a> <a href="https://login.microsoftonline.com/">https://login.microsoftonline.com/</a> <a href="https://browser.events.data.microsoft.com">https://browser.events.data.microsoft.com</a> <a href="https://login.microsoftonline.com/">https://login.microsoftonline.com/</a> <a href="https://browser.events.data.microsoft.com">https://browser.events.data.microsoft.com</a> <a href="https://login.live.com/">https://login.live.com/</a> <a href="https://aadcdn.msftauth.net/">https://aadcdn.msftauth.net/</a> <a href="https://logincdn.msauth.net">https://logincdn.msauth.net</a> <a href="https://7j6bxwtnrppf.statuspage.io/api/v2/summary.json">https://7j6bxwtnrppf.statuspage.io/api/v2/summary.json</a>
Canada	<a href="https://www.quest.com">https://www.quest.com</a> <a href="https://quest-on-demand.com/">https://quest-on-demand.com/</a> <a href="https://support.quest.com">https://support.quest.com</a> <a href="https://status.quest-on-demand.com">https://status.quest-on-demand.com</a> <a href="https://canada.notification.quest-on-demand.com">https://canada.notification.quest-on-demand.com</a> <a href="https://canada.core.api.quest-on-demand.com/">https://canada.core.api.quest-on-demand.com/</a> <a href="https://odatprodcomputeecac.blob.core.windows.net">https://odatprodcomputeecac.blob.core.windows.net</a> <a href="https://login.microsoftonline.com/">https://login.microsoftonline.com/</a> <a href="https://browser.events.data.microsoft.com">https://browser.events.data.microsoft.com</a> <a href="https://login.live.com/">https://login.live.com/</a> <a href="https://aadcdn.msftauth.net/">https://aadcdn.msftauth.net/</a> <a href="https://logincdn.msauth.net">https://logincdn.msauth.net</a> <a href="https://7j6bxwtnrppf.statuspage.io/api/v2/summary.json">https://7j6bxwtnrppf.statuspage.io/api/v2/summary.json</a>
Europe	<a href="https://www.quest.com">https://www.quest.com</a> <a href="https://quest-on-demand.com/">https://quest-on-demand.com/</a> <a href="https://support.quest.com">https://support.quest.com</a> <a href="https://status.quest-on-demand.com">https://status.quest-on-demand.com</a> <a href="https://eu.notification.quest-on-demand.com">https://eu.notification.quest-on-demand.com</a> <a href="https://eu.core.api.quest-on-demand.com/">https://eu.core.api.quest-on-demand.com/</a> <a href="https://odatprodcomputeun.blob.core.windows.net">https://odatprodcomputeun.blob.core.windows.net</a> <a href="https://login.microsoftonline.com/">https://login.microsoftonline.com/</a> <a href="https://browser.events.data.microsoft.com">https://browser.events.data.microsoft.com</a> <a href="https://login.live.com/">https://login.live.com/</a> <a href="https://aadcdn.msftauth.net/">https://aadcdn.msftauth.net/</a> <a href="https://logincdn.msauth.net">https://logincdn.msauth.net</a> <a href="https://7j6bxwtnrppf.statuspage.io/api/v2/summary.json">https://7j6bxwtnrppf.statuspage.io/api/v2/summary.json</a>

**Table 1. Endpoints required for "base" Security Management Platform access**

<b>Region</b>	<b>Endpoints</b>
United Kingdom	<a href="https://www.quest.com">https://www.quest.com</a> <a href="https://quest-on-demand.com/">https://quest-on-demand.com/</a> <a href="https://support.quest.com">https://support.quest.com</a> <a href="https://status.quest-on-demand.com">https://status.quest-on-demand.com</a> <a href="https://uk.notification.quest-on-demand.com">https://uk.notification.quest-on-demand.com</a> <a href="https://uk.core.api.quest-on-demand.com/">https://uk.core.api.quest-on-demand.com/</a> <a href="https://odatprodcomputeuks.blob.core.windows.net">https://odatprodcomputeuks.blob.core.windows.net</a> <a href="https://login.microsoftonline.com/">https://login.microsoftonline.com/</a> <a href="https://browser.events.data.microsoft.com">https://browser.events.data.microsoft.com</a> <a href="https://login.live.com/">https://login.live.com/</a> <a href="https://aadcdn.msftauth.net/">https://aadcdn.msftauth.net/</a> <a href="https://logincdn.msauth.net">https://logincdn.msauth.net</a> <a href="https://7j6bxwtnrppf.statuspage.io/api/v2/summary.json">https://7j6bxwtnrppf.statuspage.io/api/v2/summary.json</a>
Australia	<a href="https://www.quest.com">https://www.quest.com</a> <a href="https://quest-on-demand.com/">https://quest-on-demand.com/</a> <a href="https://support.quest.com">https://support.quest.com</a> <a href="https://status.quest-on-demand.com">https://status.quest-on-demand.com</a> <a href="https://au.notification.quest-on-demand.com">https://au.notification.quest-on-demand.com</a> <a href="https://au.core.api.quest-on-demand.com/">https://au.core.api.quest-on-demand.com/</a> <a href="https://odatprodcomputeaue.blob.core.windows.net">https://odatprodcomputeaue.blob.core.windows.net</a> <a href="https://login.microsoftonline.com/">https://login.microsoftonline.com/</a> <a href="https://browser.events.data.microsoft.com">https://browser.events.data.microsoft.com</a> <a href="https://login.live.com/">https://login.live.com/</a> <a href="https://aadcdn.msftauth.net/">https://aadcdn.msftauth.net/</a> <a href="https://logincdn.msauth.net">https://logincdn.msauth.net</a> <a href="https://7j6bxwtnrppf.statuspage.io/api/v2/summary.json">https://7j6bxwtnrppf.statuspage.io/api/v2/summary.json</a>
Optional (analytics / opt-in)	To collect Security Management Platform analytics if opted-in: <a href="https://edge.fullstory.com">https://edge.fullstory.com</a> <a href="https://rs.fullstory.com">https://rs.fullstory.com</a>

# Adding users and groups to an organization

Once you have created an organization, you can add additional users and groups and determine what tasks each can perform. To perform these activities, select **Settings | Access Control** in the left navigation bar.

Quest Security Management Platform uses the Role-based Access Control (RBAC) security policy that restricts information system access to authorized users. In Security Management Platform, you can grant authenticated users and groups access to specific resources based on your company requirements and assigned permission levels. You can also create new custom roles to provide specific access to the different modules and features.

## Users, groups, and roles

When you add a user or group to an organization, you also assign one or more roles. The role assignment determines what permission level they have and what tasks they can perform.

Security Management Platform is configured with a number of default roles. The default role permission settings cannot be changed, but you can create custom roles with specific permission settings to align with your company policies. You can assign multiple roles to each user or group to combine permission sets.

**i** | **NOTE:** Every user and group must be assigned to at least one role. You cannot remove all roles from a user or group.

Access Control provides the following options:

- For information about configuring roles, see [Access Control: Roles](#)
- For information about managing user access, see [Organization access for Microsoft Entra users](#)
- For information about managing group access, see [Organization access through Microsoft Entra group membership](#)

## Default roles and permissions

Security Management Platform is configured with default roles that cannot be edited or deleted. You can, however, duplicate default roles to create custom roles.

For the complete list of module default roles and permissions, refer to your module-specific User Guide.

### Default Roles

- Platform administrator  
Platform administrators have full access to global settings and all modules. The user who signed up for the platform and created the organization is automatically assigned the Platform Administrator role.
- Module administrator  
Module administrators only have access to the specific module where they have been added as an administrator. Module administrators do not have access to global settings or tenants.

## Security Management Platform Organization Role Permissions

Permission	Description
Can Add and Remove Tenants	Users with this permission can add new tenants or remove existing tenants from the organization.
Can Configure Agents	Users with this permission can add or modify the actions and domains of an agent in the organization.
Can Create and Delete, and Assign Access Control Roles	Users with this permission can create, assign user to, and delete access control roles for the organization.
Can Export Data	Users with this permission can export data from the selected services within the organization.
Can Read Access Control Roles	Users with this permission are able to view specific permissions within an access control role in the organization.
Can Read Activity Trail	Users with this permission can access the activity trail and view detailed information regarding user and system activity that has occurred within the organization associated to the selected services.
Can Manage the Organization	Users with this permissions can delete or edit the organization (modify name and authorized domains list).

### To view the current list of permissions available for each default role:

- 1 Select **Settings**, expand **Access Control**, and select **Roles**.
- 2 Click a row in the list of default roles to expand the table to see the individual role permissions.

# Access Control: Roles

Each access control role has a specific set of permissions that determines what tasks a user assigned to the role can perform. Your Security Management Platform organization comes configured with a number of default roles. The default role permissions settings cannot be changed, but you can create custom roles with specific permission settings to align with your company policies.

**i** | **NOTE:** To manage access control roles, you must have the permission "Can create, delete, and assign access control roles".

Perform the following tasks from the **Setting | Access Control | Roles** page:

- [Viewing role permissions](#)
- [Creating a custom role](#)
- [Editing a custom role](#)
- [Assigning a role to a user](#)
- [Deleting a custom role](#)

## Viewing role permissions

Use the Roles page to view the list of roles defined for your organization. You can also view the users assigned to each role.

### To view roles and permissions

- 1 In the left side navigation panel, click **Settings**, expand **Access control** and select **Roles**.
- 2 Click on a role name to open a read only page that displays the **Role Permissions**.

The panel on the right is a list of users assigned to the role.

- 3 To add users to the role, see [Adding a user to your organization and assigning a role.](#)
- 4 To add groups to the role, see [Adding a group to your organization and assigning a role.](#)

## Creating a custom role

You can create roles with a custom set of permissions. Default roles cannot be edited. You must create a custom role to enable editing.

### To create a role

- 1 In the left side navigation panel, click **Settings**, expand **Access control** and select **Roles**.
- 2 At the top right of the Roles page, click **Create Role**.  
**NOTE:** You can define a role based on an existing role. In the Roles list, click on the **Action** menu for a role and select **Duplicate**.
- 3 On the Create Role page, enter a **Role Name** and **Description**.
- 4 Under Role Permissions, select the check boxes for the permissions you want to assign to the role.  
Some role permissions are partitioned into services. If available, you can configure access to a service using the **Selected Services** field.
- 5 At the top right of the page, click **Create Role**.  
You are returned to the Roles page and there is a prompt to **Assign Users**.
- 6 To add a user to the role, click **Assign Users**.
- 7 In the **Add User to <custom\_role>** field, enter the email address of the user you want to add.
- 8 Click **Add User**.  
If the user is not currently a member, they are added to the organization.

## Editing a custom role

Note that you cannot edit a default role. You can duplicate a default role and edit it to create a custom role.

### To edit a role

- 1 In the left side navigation panel, click **Settings**, expand **Access control** and select **Roles**.
- 2 In the **Roles** list, click on the **Action** menu for a role and select **Edit**.
- 3 On the Edit Role page, you can edit:  
**Name**  
**Description**  
**Role Permissions**.  
Some role permissions are partitioned into services. If available, you can configure access to a service using the **Selected Services** field.
- 4 Click **Save**.  
You are returned to the Roles page and there is a prompt to **Assign Users**.
- 5 To add a user to the role, click **Assign Users**.
- 6 In the **Add User to <custom\_role>** field, enter the email address of the user you want to add.
- 7 Click **Add User**.

If the user is not currently a member, they are added to the organization.

## Assigning a role to a user

### **i** | **NOTE: Email notification**

When a user is added to a role, the user receives an email informing them of the action.

#### **To add a user to a role**

- 1 In the left side navigation panel, click **Settings**, expand **Access control** and select **Roles**.
- 2 In the **Roles** list, click on the **Action** menu for a role and select **Assign Users**.  
The Assign Role page opens.
- 3 In the **Add a user to this role** field, enter the email address of the user you want to add.  
The user name must use the email address format *username@domain*.
- 4 Click **Add User**.  
The user is assigned to the role and has the permission set defined by the role.

## Deleting a custom role

You cannot delete a default role.

Before deleting a role, you must remove all users from the role and either assign them a new role or remove them from the organization.

#### **To delete a role**

- 1 In the left side navigation panel, click **Settings**, expand **Access control** and select **Roles**.
- 2 In the **Roles** list, click on the **Action** menu for a role and select **Delete**.
- 3 In the confirmation window, click **Delete**.  
You are returned to the Roles page.

## Organization access for Microsoft Entra users

Organization user credentials are based on email addresses. To log in to Security Management Platform using the email address, the user must create a Security Management Platform Global Settings account with the email address.

Once you have added a user, inform them that they have been added to an organization and specify the email address or Microsoft Entra account used. Direct the new users to sign in to the organization using the procedures under [Joining an organization prerequisites](#).

For details on managing user access see:

- [Adding a user to your organization and assigning a role](#)
- [Editing user roles](#)
- [Removing a user from the organization](#)

# Adding a user to your organization and assigning a role

Before adding users to an organization, review the default role permissions settings. If required, you can create custom roles with specific permission settings to align with your company policies.

To create a custom role, see [Access Control: Roles](#).

## **i** | **NOTE: Email notification**

When a user is assigned a role in an organization, the user receives an email informing them of the action.

### **To add a user**

- 1 In the left side navigation panel, click **Settings**, expand **Access control** and select **Entra Users**.
- 2 In the **User Name** field, enter the email address of the user you want to add.  
The user name must use the email address format <local\_part>@<domain>.
- 3 In the **Assigned Role** field, enter the role name. An auto-complete list offers suggestions based on your input.
- 4 Select a role to enable the **Add** button.
- 5 Click **Add User**.

## Editing user roles

Security Management Platform is configured with default roles. To create a custom role, see [Access Control: Roles](#).

## **i** | **NOTE: Email notification**

When a user is added to a role, the user receives an email informing them of the action.

### **To assign a new role**

- 1 In the left side navigation panel, click **Settings**, expand **Access control** and select **Entra Users**.
- 2 In the list of users, locate the user you want to edit in the **User Name** column.
- 3 On the right side of the **Role** field for the user, click the edit icon to make the **Role** field editable.
- 4 Click inside the editable **Role** field and begin typing the name of the role you want to add. An auto-complete list offers suggestions based on your input.
- 5 Enter the role name you want to add. An auto-complete list offers suggestions based on your input.
- 6 Select the role from the list.
- 7 Add additional roles or remove assigned roles as required.
- 8 Select the check mark to confirm the role assignment.

### **To remove a new role**

- 1 In the left side navigation panel, click **Settings**, expand **Access control** and select **Entra Users**.
- 2 In the list of users, locate the user you want to edit in the **User Name** column.
- 3 On the right side of the **Role** field for the user, click the edit icon to make the **Role** field editable.
- 4 Click inside the editable **Role** field and begin typing the name of the role you want to add. An auto-complete list offers suggestions based on your input.

- 5 Click the **X** next to the role to remove it.
- 6 Click the checkmark to confirm.

## Removing a user from the organization

### To remove a user



#### **NOTE: Email notification**

When a user is removed from the organization, they receive an email informing them that they no longer have access to the organization.

- 1 In the left side navigation panel, click **Settings**, expand **Access control** and select **Entra Users**.
- 2 In the list of users, locate the user you want to delete in the User **Name** column.
- 3 In the **Action** field for the user, click the delete icon.
- 4 In the confirmation window, click **Remove**.

## Organization access through Microsoft Entra group membership

To login to Security Management Platform using their email address, the user must be a member of a group granted access.

Once you have added a group, inform the group members that they have been added to an organization and specify the email address or Microsoft Entra account used. Direct the users to sign in to the organization using the procedures under [Joining an organization prerequisites](#).



**NOTE:** Only groups with the Security feature enabled are supported. These include Security Groups, Mail-enabled Security Groups, and Microsoft 365 Groups with the Security feature enabled.

For details on managing group access see:

- [Adding a group to your organization and assigning a role](#)
- [Filtering the groups displayed](#)
- [Editing group roles](#)
- [Removing groups from the organization](#)

## Adding a group to your organization and assigning a role

Before adding groups to an organization, review the default role permissions settings. If required, you can create custom roles with specific permission settings to align with your company policies.

To create a custom role, see [Access Control: Roles](#).

### To add a group

- 1 In the left side navigation panel, click **Settings**, expand **Access control** and select **Entra Groups**.
- 2 Select the required tenant from the dropdown list.

- 3 In the **Group Name** field, enter the group to add.
- 4 Click **Add Group**.
- 5 In the **Assigned Role** field, enter the role name. An auto-complete list offers suggestions based on your input.
- 6 Select a role to enable the **Select** button.

## Filtering the groups displayed

You can select to filter the display by name, tenant, or role.

### *To filter the display*

- 1 In the left side navigation panel, click **Settings**, expand **Access control** and select **Entra Groups**.
- 2 Select the **Filter** tab and choose to display based on a specific tenant and/or role.  
Expand the **Tenant Name** option and check the required tenant.
- 3 Expand the **Role** option, check the required role, and click **Select**.

## Editing group roles

Security Management Platform is configured with default roles. To create a custom role, see [Access Control: Roles](#).

### *To assign a new role*

- 1 In the left side navigation panel, click **Settings**, expand **Access control** and select **Entra Groups**.
- 2 Locate the group you want to edit.
- 3 Add additional roles or remove assigned roles as required.
- 4 Click **Save** to confirm the role assignment.

## Removing groups from the organization

Removing the group will remove access from its members to Security Management Platform. Any explicit access the group members have assigned will continue.

### *To remove a group*

- 1 In the left side navigation panel, click **Settings**, expand **Access control** and select **Entra Groups**.
- 2 In the list of users, locate the user you want to delete in the **User Name** column.
- 3 Locate the group and select the **Remove** button.
- 4 In the confirmation window, click **Remove**.

## Joining an organization prerequisites

Once you have added a user or group, you must invite the user and group members to sign in to the organization, inform them that they have been added to an organization, and specify the email address or Microsoft Entra account used.

- An administrator for the organization must have added you to the organization.
- If multiple Security Management Platform organizations are associated with your email account, you must know the name of the organization you want to sign in to. After sign in, the Select Organization page is displayed where you must select the organization that you want to sign in to.
  - **NOTE:** Users do not need a Quest account to join an Security Management Platform organization. However, creating a Quest account allows you to access Security Management Platform resources such as the support site.

### ***To join an organization with a Microsoft Entra account***

- 1 Go to the web page [quest-on-demand.com](https://quest-on-demand.com).
- 2 On the Welcome to Quest Security Management Platform page, click **Sign in with Microsoft**.
  - If only one organization is associated with your email account, the Security Management Platform home page opens. You are signed in to the organization that you were added to.
  - If there are multiple organizations associated with your email account, the Multiple Organizations Found page opens with a list of organizations. Click the organization you want and click **Select Organization**.

# Managing your Microsoft Entra tenants and on-premises domains

A tenant is a dedicated instance of Microsoft Entra ID that your Microsoft organization receives and owns when it signs up for a Microsoft cloud service such as Microsoft 365. For more information, see this [Microsoft help page](#).

This section contains information about the following activities involved in setting up your Security Management Platform environment to manage your Microsoft Entra tenants and on-premises domains:

- [Tenants overview](#)
- [Adding tenants](#)
- [Managing admin consent permissions](#)
- [Removing a tenant](#)
- [Managing your on-premises domains](#)
- [Adding an on-premises agent](#)
- [Configuring an agent](#)
- [Automatic updates for on-premises agents](#)
- [Removing an agent](#)
- [Adding an Active Directory domain](#)
- [Removing a domain](#)

## Tenants overview

A tenant houses the users in a company and the information about them. You must add a tenant to manage its properties using a Security Management Platform product.

Applications used to manage tenant properties must participate in the consent flow provided by Microsoft Entra ID. This means a Global Administrator must provide admin consent when adding a tenant to Security Management Platform. Admin consent is granted on behalf of the Microsoft Entra ID organization.

The Tenants page provides an overview of all your tenants. It shows the number of users, consent status, and provides access to admin consent for the different Security Management Platform products.

**i** | **NOTE:** At present, authentication for Security Management Platform is supported only with Azure Commercial tenants.

## B2C tenants

In addition to the standard Microsoft Entra tenant, you can also add a B2C tenant. On the Tenant page, B2C tenants can be distinguished by the following icon next to the tenant name:



For more information on B2C tenants, see Microsoft documentation.

## Adding tenants

When you add a tenant, you must have Microsoft Entra ID Global Administrator credentials in Microsoft Entra ID since part of the process of adding a tenant is done in the Microsoft Azure portal.

The Microsoft Entra ID Global Administrator role is the top level administrator role and has access to all features. By default, the person who signs up for a Microsoft Entra ID subscription is assigned the Global Administrator role for the tenant. Additional users can be assigned to the Global administrator role.

If you are in the U.S. region, once you select **Tenants** and click **Add Tenant**, you must select the type of tenant you are adding, whether commercial, GCC, or GCC High. When you click **Add Commercial or GCC Tenant** (or **Add GCC High Tenant**) you are redirected to the Microsoft tenant administration login page where you must log in with the Global Administrator credentials for the tenant.

If you are in any other region, you select **Add Tenant** and are immediately redirected to the Microsoft tenant administration login page where you must log in with the Microsoft Entra ID Global Administrator credentials for the tenant. After successful authentication, the Consent Grant dialog is displayed. You must confirm the consent grant.

## GCC and GCC High tenants

GCC or a GCC High tenants are available only for deployments in the U.S. region.

Microsoft 365 GCC tenants are typically used by US public sector organizations and the contractor organizations that service them. GCC High tenants provide Microsoft 365 services that adhere to additional US Department of Defense security requirements. Customer eligibility to GCC High tenants is restricted.

- On Demand Migration supports GCC and GCC High tenants.
- Audit supports GCC tenants.

For more information about U.S. Government GCC High endpoints, see [Microsoft 365 U.S. Government GCC High endpoints](#).

For more information about commercial and GCC worldwide endpoints, see [Microsoft 365 worldwide endpoints](#).

**i** | **NOTE:** Commercial tenants are hosted and managed by Microsoft.

## Prerequisites for adding tenants

Admin consent is required to add a tenant to Security Management Platform. Since only a Microsoft Entra ID Global Administrator can grant admin consent, you must be able to provide Microsoft Entra Global ID administrator credentials for the tenant you are adding.

### **To add a tenant**

- 1 Log in to Security Management Platform using the credentials you used to sign up for Security Management Platform.
- 2 In the navigation panel on the left, click **Tenants**.  
The Office 365 Tenants page is displayed by default.

3 Click **Add Tenant**.

If you are in any region other than the U.S. region, such as Europe, United Kingdom, Canada, or Australia, you are immediately redirected to the Microsoft login page.

4 If you are in the U.S. region, you must select the type of tenant that you are adding:

- Click **Add Commercial or GCC Tenant**

- OR -

Click **Add GCC High Tenant**

 | **NOTE:** See [GCC and GCC High tenants](#) for details.

You are redirected to the Microsoft login page.

5 Enter your Global Administrator credentials and click **Next**.

A page opens with the list of permissions that you are granting.

6 Click **Accept**.

The Office 365 Tenants page is displayed.

7 On the Office 365 Tenants page, at the bottom of the tile for the newly added tenant, click **Edit Consents**.

The Admin Consent status page opens.

8 If the minimum permission settings granted when the tenant was added are sufficient for a module, the Status for the module is **Uses Base**. If the module requires additional permissions, the **Status is Not Granted**.

If you need to have additional permissions for a module, click **Grant Consent**. You are redirected to the Microsoft login page.

9 Enter the Global Administrator credentials and click **Next**.

A page opens with the list of permissions settings you are granting.


10 Click **Accept**.

The Office 365 Tenants page is displayed. GCC or GCC High tenants are identified with a GCC or GCC High tag in the right corner of the tenant tile.

If you click **Edit Consents** on a GCC or GCC High tenant tile, in addition to the domain name and the tenant ID, you will also see the country code for the tenant.

## Displaying a tenant name change

At a later date, if you change the display name of the tenant or the default domain name in Microsoft Entra ID, you can refresh the tenant in Security Management Platform to immediately update the name. When you refresh the tenant, Security Management Platform rereads the tenant information from your Microsoft Entra tenant to synchronize with the Security Management Platform stored data.

To refresh the tenant, display the Tenants page and click the refresh icon  that displays beside the tenant name on the tenant tile.

## Managing admin consent permissions

Once you add a tenant, you are redirected to a page that lists the permissions that will be granted. You must click **Accept** and provide admin consent for the Security Management Platform application. Once the Global Administrator adds a tenant to Security Management Platform, an application record is created in the tenant indicating that admin consent has been provided.

**i** | **NOTE:** Global Admin credentials are only required to grant admin consent for the minimal list of permissions required by Security Management Platform. Global Admin credentials are not stored, shared, or used for any other purpose.

When you first add a tenant, only the minimum permission settings are granted. Some modules require additional permissions for specific activities. Once a tenant has been added to Security Management Platform, you can grant additional permissions on the Tenant Consents page.

To open the Tenant Consents page, click **Tenants** in the navigation page and click **Edit Consents** on the tenant tile.

You can view the specific permissions for each Security Management Platform application by clicking **View Details**. You can also see the last time that consent was granted and which Security Management Platform user granted the consent.

- [About admin consent status](#)
- [Granting and regranting admin consent](#)
- [About revoking admin consent](#)

## About admin consent status

On the Tenant Consents page, you can view admin consent status for various applications used by Security Management Platform products for each tenant that you have added. The process of granting access to the customer Microsoft Entra tenant by the tenant global administrator is referred to as admin consent. A Microsoft Entra tenant global administrator must provide consent to any application listed on the page. Each application on this page defines the set of permissions required to provide a specific module functionality.

When a tenant is first added, the user is requested to grant admin consent for the Basic application. Other modules require a higher level of permissions.

Following best practices for SaaS applications, Security Management Platform applications use OAuth 2.0 and OpenId Connect protocol and authentication library for the Microsoft Identity Platform to configure and request access to protected resources in customer tenants. All Security Management Platform applications described on the Tenant Admin Page are configured in Microsoft Entra ID as multi-tenant confidential applications (<https://learn.microsoft.com/en-us/entra/identity-platform/application-model#multitenant-apps>).

Some Security Management Platform products require that a role be assigned to the service principal in addition to admin consent grant. The role is needed to support specific module functionality. For example, after granting consent for the Exchange Online PowerShell consent type, you must assign the Exchange Admin Role. This role is needed to perform Exchange tasks such as linking mailboxes to users and deleting mail-enabled groups.

## Granting and regranting admin consent

You must grant specific admin consents for each Security Management Platform tenant. For example, if you grant access for MyCompany tenant in organization A, and add the MyCompany tenant to organization B, you must grant consent for organization B. In some situations, you might have to regrant consent for an application used by your tenant.

For some consent types, you might also have to assign a role after you grant consent.

### **To grant admin consent for a tenant**

- 1 Click **Tenants** in the navigation panel on the left.
- 2 At the bottom of a tenant tile, click **Edit Consents**.

The Tenant Consents page for the tenant opens.

In the Status and Actions column, the status information indicates whether admin consent has been granted for the module consent type.

- 3 If the current status is **Not Granted**, you can enable the module consent type for this tenant by clicking **Grant Consent**.

If the current status is **Regrant Consent**, a change in the required permissions or new functionality might mean that you must regrant consent for a previously granted consent.

- 4 For the Exchange Online PowerShell consent type, the Exchange Admin Role must be assigned. After you grant consent for Exchange Online PowerShell, click **Assign Role**.

**i** | **NOTE:** If you assign a role and immediately refresh the page, the Assignment state might be displayed as "Not Assigned" for a short time until you refresh the page again.

- 5 To view the permissions that are granted for each consent type, click **View Details**.

**i** | **NOTE:** If additional admin consent permissions are required to perform specific tasks within a module, these consent types are listed below the core or basic consent type for the module.

## About the Status and Actions column

For the following scenarios, you would click **Grant Consent** or **Regrant Consent** in the Status and Actions column.

- The admin consent token for the module expired, resulting in a status of **Consent Required**. The status of Consent Required indicates that Security Management Platform cannot obtain a token with delegated permissions based on a previously granted admin consent. To restore the interrupted services, you must regrant consent.

The Consent Required status can be caused if the Microsoft Entra ID Global Administrator account used to grant consent has been changed such as: password change, user role change in the organization, user account was disabled or removed, or all tokens were invalidated for a tenant after a tenant policy update.

- A new feature in a Security Management Platform product can require that additional permissions be granted. In this scenario, you would click **Regrant Consent**. For example, when Security Management Platform implemented the new Microsoft Authentication Library (MSAL) in June 2022, admin consents had to be regranted for products that use delegated permissions.

The following Security Management Platform application registrations use delegated permissions:

- Quest Security Management Platform - Identity Recovery - Basic
- Quest Security Management Platform - Identity Recovery - Restore
- Quest Security Management Platform - Migration - Teams

For more information, see [About the Microsoft Authentication Library \(MSAL\)](#).

- Admin consent has been revoked in the Microsoft Azure portal, resulting in a status of **Revoked**. If you revoke the Core Basic admin consent in the tenant you will see **Revoked** status for Core Basic and **Not Available** for all other modules. The Core Basic application is used to determine the consent status for your tenant. If that consent is revoked, Security Management Platform cannot determine consent status for the rest of the modules. Consent might be granted for the modules, but Security Management Platform cannot verify it.

For this reason, it is strongly recommended that you do not revoke Core Basic consent.

## About the Microsoft Authentication Library (MSAL)

The Microsoft Authentication Library (MSAL) provides improved security, is resilient, and allows tokens to be generated with a very granular scope. Since MSAL supports generated tokens with a granular scope, Security Management Platform can use tokens with a narrowed scope when accessing your tenant.

This feature provides a more secure and granular approach for accessing your data. For more information, see [Permissions and consent in the Microsoft identity platform](#).

## About revoking admin consent

Completely revoking admin consent removes all permissions granted for the Security Management Platform application. Revoking admin consent is a manual process that must be performed in the Microsoft Azure portal.

**NOTE:** You can revoke or disable consent in the Microsoft Azure Portal.

## Revoking admin consent in the Azure Portal

Revoking admin consent removes all permissions granted for the Security Management Platform application.

### *To revoke admin consent*

- 1 Log in to the Azure Resource Manager with the credentials for the Microsoft Entra tenant.
- 2 Click on the **Microsoft Entra ID** icon in the left menu.
- 3 In the Active Directory panel, select **Enterprise applications**.
- 4 In the Enterprise applications panel, select **All applications**.
- 5 Search for and select the Quest Security Management Platform application.
- 6 In the Manage section of the left menu, select **Properties**.
- 7 At the top of the Properties pane, select **Delete**, and then select **Yes** to confirm you want to delete the application from your Microsoft Entra tenant.

Alternately, to disable consent, you can disable a user from signing in.

### *To disable a user from signing in*

- 1 Sign in to the Azure portal as the global administrator for your directory.
- 2 Search for and select **Microsoft Entra ID**.
- 3 Select **Enterprise applications**.
- 4 Search for and select the Quest Security Management Platform application.
- 5 Select **Properties**.
- 6 Select **No** for Enabled for users to sign-in?.
- 7 Select **Save**.

## Removing a tenant

By removing a tenant, you are beginning the process of disabling all module functions related to the tenant. When you remove a tenant, you are removing the tenant from the Security Management Platform organization for all users and this action cannot be undone.

All module operations will stop after 30 days. At that point, the following operations are halted:

- Active backups and provisioning actions will be cancelled.
- Migration project and status information will be lost.
- Audit event data will no longer be collected.
- License and cost data will no longer be collected.

- Assessment data will no longer be collected.

**i** **NOTE:** If a tenant was inadvertently removed, it might be possible to restore a tenant and all the associated Security Management Platform configuration for up to 30 days after it was removed from Security Management Platform. In this situation, contact [Technical Support](#).

You must provide the tenant name, your organization ID, and the tenant region.

### To remove a tenant

- 1 Click **Tenants** in the navigation panel on the left.
- 2 On the tenant tile for the tenant you want to remove, click **Remove**.
- 3 Review the list of results from the remove action and select each check box.
- 4 Click **Remove Tenant**.

When you previously added the tenant, a Service Principal was created in your tenant, under Enterprise applications, for each consent that you granted for this tenant. To permanently remove the consents, log in to the Microsoft Azure portal and go to the Microsoft Entra Admin Center. Browse to Enterprise Applications, search for *Quest Security Management Platform*, and delete all the application records that you do not need.

## Managing your on-premises domains

In addition to managing your Microsoft Entra tenants, Security Management Platform provides support for connecting to on-premises domains in hybrid environments to perform data collection and management activities.

By installing an agent with a unique key and specifying domains to which the agent is connected, you can review information and perform actions in your hybrid environment. You start the process to install and configure an agent by selecting **Tenants** in the left navigation bar and selecting **Hybrid Agents**.

You can add on-premises domains to Security Management Platform selecting **Tenants** in the left navigation bar and selecting **Active Directory Domains**. You can also add domains as part of the agent configuration process.

## On-premises agent prerequisites

You must meet the following prerequisites to download and install an agent for on-premises data collection from specified domains:

- You must have the Security Management Platform Organization Admin role and specifically must have the Can Configure Agents (`core.configureAgents`) permission.
- You must have a passphrase, which you create on the How to Add an Agent page, that you enter when installing the agent.
- You must have a valid paid subscription for the Security Management Platform product with which you are using the agent.
- The login account that you use to run the agent setup program must have local administrator rights.

The agent setup program will prompt you for service account credentials (username and password) that are used to run the agent service. The agent service account must have local administrator rights on the computer on which the agent is being installed.

- You must be able to download the agent setup package from the storage location associated with your Security Management Platform Organization region:
  - Australia
    - <https://odjrsauprodaugrsto.blob.core.windows.net>
    - HTTPS - TCP 443

- Canada
  - <https://odjrscaprodcahrssto.blob.core.windows.net>
  - HTTPS - TCP 443
- Europe:
  - <https://odjrseuprodeugrssto.blob.core.windows.net>
  - HTTPS - TCP 443
- UK
  - <https://odjrsukprodukgrrssto.blob.core.windows.net>
  - HTTPS - TCP 443
- US:
  - <https://odjrsusprodusgrssto.blob.core.windows.net>
  - HTTPS - TCP 443

## On-premises agent supported operating systems

Installation platforms (x64) supported for the following versions:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

## On-premises agent system configuration requirements

The agent requires:

- LDAP (TCP 389) connectivity to all domain controllers in the local domain.
- SMB TCP port 445 open on the domain controllers.
- The following Windows services running:
  - DNS client
  - Remote Procedure Call (RPC)
  - Windows event log

The agent uses:

- The Windows (Internet Explorer) Proxy Server settings applied to the service account or computer where it is installed.
- MQTT over WebSockets - TCP 443 for IoT Hub communication.
- HTTPS - TCP 443 for upload/download of files.

- The login account that you use to run the agent setup program must have the Windows (Internet Explorer) Proxy Server settings configured if your environment requires a Proxy Server to access the Internet.

The agent footprint:

- Estimated hard disk space used: 160 MB + log size.
- By default, up to 10 MB of log files are retained.
- Estimated physical memory (RAM) used: 25 to 50 MB.

## On-premises agent endpoint requirements

The agent must be able to access the following endpoints associated with the region where your Security Management Platform organization resides.

- Australia:
  - Agent updates: [odjrсаuprodauiotinst--odjrсаuprodauiotacct.b.nlu.dl.adu.microsoft.com](https://odjrсаuprodauiotinst--odjrсаuprodauiotacct.b.nlu.dl.adu.microsoft.com)
    - HTTP - TCP 80
  - Agent connection to Security Management Platform: [odjrса-uprod-au-iothub.azure-devices.net](https://odjrса-uprod-au-iothub.azure-devices.net)
    - MQTT over WebSockets - TCP 443
  - Agent and package download: <https://odjrсаuprodaugrssto.blob.core.windows.net>
    - HTTPS - TCP 443
  - Agent data upload: <https://odjrсаuprodausto.blob.core.windows.net>
    - HTTPS - TCP 443
- Canada:
  - Agent updates: [odjrсаprodcaiotinst--odjrсаprodcaiotacct.b.nlu.dl.adu.microsoft.com](https://odjrсаprodcaiotinst--odjrсаprodcaiotacct.b.nlu.dl.adu.microsoft.com)
    - HTTP - TCP 80
  - Agent connection to Security Management Platform: [odjrса-prod-ca-iothub.azure-devices.net](https://odjrса-prod-ca-iothub.azure-devices.net)
    - MQTT over WebSockets (TCP 443)
  - Agent and package download: <https://odjrсаprodсagrsto.blob.core.windows.net>
    - HTTPS - TCP 443
  - Agent data upload: <https://odjrсаprodсasto.blob.core.windows.net>
    - HTTPS - TCP 443
- Europe:
  - Agent updates: [odjrсеuprodeuiotinst--odjrсеuprodeuiotacct.b.nlu.dl.adu.microsoft.com](https://odjrсеuprodeuiotinst--odjrсеuprodeuiotacct.b.nlu.dl.adu.microsoft.com)
    - HTTP - TCP 80
  - Agent connection to Security Management Platform: [odjrсе-uprod-eu-iothub.azure-devices.net](https://odjrсе-uprod-eu-iothub.azure-devices.net)
    - MQTT over WebSockets (TCP 443)
  - Agent and package download: <https://odjrсеuprodeugrssto.blob.core.windows.net>
    - HTTPS - TCP 443
  - Agent data upload: <https://odjrсеuprodeusto.blob.core.windows.net>
    - HTTPS - TCP 443

- UK:
  - Agent updates: [odjrsukprodukiotinst--odjrsukprodukiotacct.b.nlu.dl.adu.microsoft.com](https://odjrsukprodukiotinst--odjrsukprodukiotacct.b.nlu.dl.adu.microsoft.com)
    - HTTP - TCP 80
  - Agent connection to Security Management Platform: [odjrs-ukprod-uk-iothub.azure-devices.net](https://odjrs-ukprod-uk-iothub.azure-devices.net)
    - MQTT over WebSockets (TCP 443)
  - Agent and package download: <https://odjrsukprodukgrssto.blob.core.windows.net>
    - HTTPS - TCP 443
  - Agent data upload: <https://odjrsukproduksto.blob.core.windows.net>
    - HTTPS - TCP 443
- US:
  - Agent updates: [odjrsusprodusiotinst--odjrsusprodusiotacct.b.nlu.dl.adu.microsoft.com](https://odjrsusprodusiotinst--odjrsusprodusiotacct.b.nlu.dl.adu.microsoft.com)
    - HTTP - TCP 80
  - Agent connection to Security Management Platform: [odjrs-usprod-us-iothub.azure-devices.net](https://odjrs-usprod-us-iothub.azure-devices.net)
    - MQTT over WebSockets (TCP 443)
  - Agent and package download: <https://odjrsusprodusgrssto.blob.core.windows.net>
    - HTTPS - TCP 443
  - Agent data uploads: <https://odjrsusprodussto.blob.core.windows.net>
    - HTTPS - TCP 443

## Adding an on-premises agent

The following steps describe the general process for installing and configuring the Security Management Platform on-premises agent. For the detailed procedures, see [To add an agent](#) and [To configure an agent](#).

For information about the permissions required to install an agent and the permissions needed by the agent service account, see [On-premises agent prerequisites](#).

- 1 Generate a passphrase on the How to Add an Agent page. Take note of the passphrase.
- 2 Add the agent to Security Management Platform.
 

An agent package is generated with a unique key.
- 3 Download the agent package and copy it to the member server on which you want to run the agent.
- 4 Install the agent, specifying the required information including the passphrase.
 

Once the agent is installed it connects to the Security Management Platform organization.
- 5 Configure the agent specifying the actions it can perform and domains with which it works.

### **i** **NOTE: On-premises hybrid agent support**

Installation platforms (x64) supported for the following versions:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

### **To add an agent**

- 1 Log in to Security Management Platform using the credentials you used to sign up for Security Management Platform.

2 In the navigation panel on the left, click **Tenants**.

3 Click **Hybrid Agents**.

4 Click **Add Agent**,

When you click Add Agent, the How to Add an Agent page is displayed. You must create a passphrase that will be used when you install the agent.

5 To create a passphrase, use one of the following options:

- Click **Generate New** to get a new passphrase.
- Enter a passphrase manually. The passphrase can be from 4 to 100 words (32 to 1024 characters long).
- Edit a displayed passphrase to make it more complex (such as adding numbers or characters).
- Enter a passphrase word count (from 4 to 100 words) and click **Generate New** to get a passphrase of the specified word count. **NOTE:** The passphrase must be from 32 to 1024 characters long.

6 When you decide to use the displayed passphrase, click **Copy and Continue**.

The passphrase is copied to your clipboard. Ideally, you should paste it into a Notepad or Word document to keep for future reference.

7 Once the installation package is ready, click **Download**.

The agent package with a unique key is downloaded to your computer.

**i** | **IMPORTANT:** You must install the agent within 10 days or the unique key will expire. Also, you cannot re-use an agent package, even if you have removed the agent from a previous installation. You must download and install a separate agent on each server.

8 Copy the agent package to the server and double-click the **AgentSetup.exe** file.

The installer is packaged as a self-extracting executable. If you run the installer without arguments, it prompts you for the required installation parameters, including the folder where the agent should be installed. You also are asked for the passphrase that was copied to your clipboard.

For information about the available arguments, see [Installing the agent using the command shell](#).

**i** | **IMPORTANT:** The maximum number of agents is limited to 10 per organization. If you need a higher number of agents, contact Quest Support.

9 In the command line console, enter the following information in response to the prompts:

- Agent installation path: The folder to which the agent files will be extracted. If you do not specify the path, the default path is set to C:\QuestAgent.
- Enter Y when you are prompted to install Quest Security Management Platform On-Premises Agent.
- Agent name - optional. If you do not specify an agent name, the NETBIOS name of the computer is used.
- Secure LDAP - optional. Enter Y to use TLS encrypted LDAP. **IMPORTANT:** Domain controllers in the forest must be properly configured to enable this feature. See [Secure LDAP configuration and deployment](#) for more information.
- Credentials (user name and password) of the account that is used to run the agent service. The account specified must have local administrator rights on the computer where the agent is being installed. Other required rights depend on the modules with which the agent will be used.
- Passphrase - The generated passphrase that you generated on the How to Add an Agent page.

# About agent installation

Depending on your browser and the download options that you configured, when you click Download, the AgentSetup.exe file is downloaded to the location you specify. In most cases the AgentSetup.exe file is downloaded to your Downloads folder.

The setup program is a console application. If you double-click the AgentSetup.exe file, a console window is opened and you are prompted for information such as installation folder and service user name and password. Optionally, you can open a command shell and manually execute the installer from the command line which allows you to specify arguments

The file name of the downloaded file is AgentSetup.exe. The installer is packaged as a self-extracting executable. If you run the installer without arguments, it prompts you for all required installation parameters, including the folder where the agent should be installed.

You can run the AgentSetup.exe from any directory (as long as you run the program on the computer on which it is to be installed). The self-extracting executable prompts you for the folder to which the agent files will be extracted. The self-extracting installation package extracts the files to the specified target folder and runs the setup program (Setup.exe) from the target folder.

Once an agent installation package is used to install the agent on a computer, you cannot use the same package to install the agent on another computer.

- IMPORTANT:** The installation key included in the installer is a unique one-time key that cannot be used again to install the agent elsewhere, even if you uninstall the agent from the current computer.

After you have installed the agent, it is recommended that you delete the file containing the passphrase (if you saved it to a file) and the downloaded agent installation package. However, do not delete the AgentSetup.exe file that was extracted.

## Agent service account configuration

When specifying a service account, the following options are supported:

- Group Managed Service Account (gMSA) and Standalone Managed Service Account (sMSA) types. When this account type is used, a password will not be requested. Specify the account using domain\account\$ format.
- Local System account. When this account type is used, a password will not be requested. Specify the account using one of the following formats:
  - .\LocalSystem
  - LocalSystem
  - NT Authority\Local System
- Local user accounts. When this account type is used, specify the account using one of the following formats:
  - .\Username
  - Username
  - computername\Username

Consult your module documentation for any additional pre-requisites.

## Secure LDAP configuration and deployment

When selecting to use Secure LDAP, ensure that you adhere to the following guidelines:

- A valid certificate must be provisioned.

- A public-key certificate for the domain controller is required on the host of each Hybrid Agent that makes Active Directory requests to a domain controller.
- Secure LDAP settings are global. Once enabled, domain controllers from all domains known to Actions assigned to the Hybrid Agent which support Secure LDAP must be configured to support this method. Domains which do not support Secure LDAP will not be searchable by assigned Actions which respect the Hybrid Agent Secure LDAP configuration setting.
- Actions assigned to the Hybrid Agent may or may not support Secure LDAP or may require additional configuration from the corresponding Security Management Platform product. Consult your module documentation for more information.

## Installing the agent using the command shell

If you open a command shell, you must open it with elevated permissions (such as “Run as administrator”). The setup program requires admin rights.

You can provide the parameters for agent installation through command line switches. This method allows the agent to be installed without any prompts. The supported switches are as follows:

`--outdir <output_directory>`

Provides the target directory where the agent files will be extracted. This is the only switch that is handled directly by the self-extracting executable. All other switches are forwarded to the agent setup program that is executed after the files are extracted.

`--quiet`

Prevents prompting. When you use this switch, you must also specify all parameters that do not have default values through the command line. If any parameters are missing, the installation will fail.

`--name <name>`

The name used to identify the agent. The agent name is displayed in the Security Management Platform Agent configuration page once the agent installation is completed. If no name is provided, the NETBIOS name of the computer is used as a default value.

`--user <username>`

The account under which the agent service is run. This is a required parameter. The account specified must have local administrator rights on the computer where the agent is being installed.

Additional permissions depend on the workload being performed by the agent. Refer to the documentation for the specific Security Management Platform product for more information.

The account is granted Log On As Service rights on the local system during installation.

`--password <password>`

The password of the account under which the agent service is run. This password is not stored anywhere within Security Management Platform. The password is only used to configure the startup properties of the Windows service.

`--passphrase "<passphrase>"`

The generated passphrase that was created on the How to Add an Agent page. The passphrase is required to install the agent. Since the passphrase will contain spaces, you must use quotation marks to enclose the passphrase.

`--enableldaps`

Enables TLS/SSL encryption on LDAP connections.

# Configuring an agent

After you have installed the agent, you must assign the actions it can perform. Some actions require on-premises domains be specified in the Connected Domains section.

## To configure an agent

- 1 Click **Tenants** in the left navigation bar and select **Hybrid Agents**.  
A tile for the newly installed agent is displayed. The text under the headings for Domains and Agents shows Not Configured.
- 2 Click **Edit Configuration**.
- 3 In the Actions section, view the list of actions and select the actions that the agent is allowed to perform.  
Consult your Security Management Platform product documentation for Actions you might need to enable and other Action related requirements.
- 4 In the Connected Domains section, do one of the following steps:
  - Click **Add New** and add an on-premises domain to Security Management Platform that will be connected to this agent. For information about adding a domain, see [Adding an Active Directory domain](#).
  - OR -
  - Click **Select Existing** and select a domain that has already been added to Security Management Platform.
- 5 Click **Save**.

# Editing an agent configuration

After an agent is configured, you can update the agent configuration at any time. When you view an agent tile for a configured agent, you can see the computer on which the agent is installed and the number of allowed actions and the number of connected agents.

**i** | **NOTE:** The main Hybrid Agents tab displays an “Updates pending” label when either the Hybrid Agent itself has an automatic update waiting to be applied or any of its assigned actions have automatic updates pending.

## To update an agent configuration

- 1 On the agent tile, click **Edit Configuration**.  
**General Information** provides basic information about the agent such as the agent name, the name of the computer on which the agent is installed, last agent sync date, agent status, connection status, installed version, latest version available, installation status, and the version installation date.  
**Actions** provides configuration details including the allowed actions for the agent, the Installed version with the installation date, the most recent version available and when it became available and whether the assigned actions are up to date or have an update pending.  
**Connected Domains** lists the domains to which the agent is connected.
- 2 You can update the agent configuration as follows:
  - For General Information, select **Diagnostic Access** to allow Quest to review the hybrid agent log files for troubleshooting purposes. This option can be turned on and off as needed.
  - For actions, you can click **Select Actions** to update the allowed actions.
  - For connected domains, you can click either **Add Domain** or **Select Existing** to add a new domain for the agent or to connect the agent to an existing domain.

- 3 When you have made your changes, click **Save**.

When viewing the information for the configured agent, you also have the option of removing an action or a connected domain.

To remove the action or domain from the displayed agent configuration, click  beside the action or domain.

## Automatic updates for on-premises agents

If you have an agent installed and running and Quest has released a new version, the agent is automatically upgraded in your environment. When a new version of the agent is available, Quest will generate a package to be distributed to all organizations. Each installed agent will be updated. Updates do not require any manual intervention and the upgrade does not require a system reboot.

## Removing an agent

There are two stages in removing an agent:

- You remove the agent from Security Management Platform.
- You uninstall the agent from the server on which it was installed.

### **To remove an agent**

- 1 Log in to Security Management Platform using the credentials you used to sign up for Security Management Platform.
- 2 In the navigation panel on the left, click **Tenants**.
- 3 Click **Hybrid Agents**.
- 4 Select the tile for the agent you want to remove and click **Remove**.
- 5 Review the list of results from the remove action and select each check box.
- 6 Click **Remove Agent**.

At this point, the agent will be disconnected from Security Management Platform cloud services. The agent is no longer linked to any Security Management Platform domains and cannot perform any configured allowed actions.

### **Uninstalling the agent**

After the agent is removed from Security Management Platform, you can uninstall it from the command line using the following steps:

Option A:

- From Programs and Features click **Uninstall/Change** on the "Quest Security Management Platform On-Premises Agent", and follow the resulting command prompt.

Option B:

- 1 Open a command prompt with administrative privileges (such as Run as Administrator).
- 2 Switch to the folder in which you installed the agent. By default, the path is C:\QuestAgent unless otherwise specified.
- 3 Type the following command: **setup --uninstall**

# Adding an Active Directory domain

When you select **Tenants** in the navigation panel on the left, a tab titled **Active Directory Domains** is shown. Select the tab to view information about your domains and to add new domains. You add domains to Security Management Platform by specifying the FQDN (Fully Qualified Domain Name) for each domain that you want to add. In an Active Directory multi-domain forest, you must add each parent and child domain with which you want to work.

Optionally, if you add your agents first, you can add a domain when you are configuring an agent.

## **To add a domain**

- 1 In the navigation panel on the left, click **Tenants**.
- 2 Click **Active Directory Domains**.
- 3 Click **Add Domain**.
- 4 Enter the FQDN (Fully Qualified Domain Name) for the on-premises domain you want to add.
- 5 If there is a preferred domain controller that you want to use, enter the name for the domain controller. This is optional.
- 6 Click **Save**.

After you have added your domains, you can install and configure the agents that will work with those domains.

## Editing a domain configuration

You cannot change the FQDN (Fully Qualified Domain Name) for a domain in Security Management Platform. If the FQDN for an on-premises domain has changed, or if you accidentally entered the FQDN incorrectly, you must remove the domain from Security Management Platform and add a new domain with the new FQDN.

You can modify the preferred domain controller for a domain.

## Removing a domain

You can remove a domain from Security Management Platform. When you remove a domain, the association with your on-premises domain is removed and the domain is removed from all linked agents. Active Directory group membership will not be updated and Active Directory data is no longer collected.

## **To remove a domain**

- 1 In the navigation panel on the left, click **Tenants**.
- 2 Click **Active Directory Domains**.
- 3 On the tile for the domain that you want to remove, click **Remove**.
- 4 Review the list of results from the remove action and select each check box.
- 5 Click **Remove Domain**.

# Security Management Platform Home page

The Home page contains the following components.

- [Masthead](#)
- [AI Assistant](#)
- [Announcements and global notifications](#)
- [Information window](#)
- [Security Management Platform Status page](#)
- [Side navigation panel](#)
- [Dashboard](#)

## Masthead

The masthead displays your current user ID and provides information about your organization. It displays the Security Management Platform name on the left and on the right side shows the following:

- Your user ID with a drop down menu arrow.
- An information icon (**i**) that opens the Security Management Platform information window.
- A status icon and a message that indicates the system status for the modules in your organization. You can expand the status to view the individual modules that might be affected. You can click the **Status Overview** link to view the Security Management Platform Status page.
  - If all your modules are operational, the icon is green and displays **All Systems Operational**. If you click the status text, you can see the individual modules with green icons indicating systems are operational.
  - If one or more modules has a status of degraded performance or partial outage, the icon is yellow and displays **Partial System Outage**. When you click the status text, yellow icons appear beside the affected modules.
  - If one or more modules has a status of major outage the icon is red and the text link displays **Major Service Outage** in red. When you click the status text, red icons appear beside the affected modules .

You can click the **Status Overview** link to display details about outages, past incidents, and all planned maintenance in the near future in the [Security Management Platform Status page](#).

If there is scheduled maintenance planned that will include system downtime, a blue banner is displayed at the top of the masthead that includes information about the scheduled outage. You can click **Read more** to view the maintenance details on the [Security Management Platform Status page](#).

# Masthead drop-down menu

Clicking anywhere on your user ID opens the drop-down menu to perform the following tasks:

- View your current **Region Name** and **Organization Name**.
- Perform organization management [Managing organizations and regions](#).
- Configure your user settings by clicking My Account.
  - **Use of Cookies:** You can enable or disable the use of a cookie for session monitoring. The initial state of this setting is determined by your response to the cookie notice when you join an organization. Note that this setting is by region. If you join an organization in a different region, you receive the cookie notice again.
- **Sign Out** from your current session. Note that you are automatically logged out after 120 minutes of inactivity.

# AI Assistant

The AI Assistant is embedded in Quest Security Management Platform to help you quickly find answers, guidance, and troubleshooting information—right when you need it.

Instead of manually searching across multiple documents, you can ask questions in natural language. The AI Assistant searches Quest product documentation and knowledge base articles to return relevant, trusted information directly within the platform.

The AI Assistant helps you:

- Understand how features work across Quest Security Management Platform products.
- Find guidance, recommendations, and best practices.
- Locate troubleshooting information and known solutions.
- Navigate product documentation and knowledge base content more efficiently.

The AI Assistant is designed to support both exploration—learning how products and features work—and problem resolution, such as identifying known issues, behaviors, and recommended actions.

## Where to Find It

The AI Assistant is available directly within the Security Management Platform interface and is accessible throughout your workflow, making help and guidance easy to reach whenever questions arise.

- 1 Select this icon to open the AI Assistant:



- 2 Select the required product from the drop-down list.
- 3 Enter your question, and click **Send**.

## Using Product Context to Refine Results

To improve accuracy and relevance, you can select a specific product before asking your question. Applying product context narrows the scope of the search and prioritizes documentation and knowledge base content related to the selected product.

For example, selecting Identity Defense ensures that responses focus on content specific to that product rather than broader, cross-platform information.

When you submit a question, the AI Assistant:

- Searches relevant Quest documentation and knowledge base articles.
- Presents answers with citations so you can see where the information came from.
- Suggests follow-up questions to help you explore related topics or investigate further.

This approach allows you to verify sources, gain confidence in the response, and continue researching without starting over.

## Announcements and global notifications

Notifications provide timely and valuable updates, making your experience within Security Management Platform easier and more intuitive. You'll find a centralized notification hub, represented by a bell icon in the top-right corner of the masthead. A small badge on the bell will show the number of unread notifications, so you can see new alerts at a glance.

Notifications are designed to be relevant to you, offering contextual information like a download being ready or an important alert about an expired subscription. They deliver information that's just-in-time, ensuring you receive key updates exactly when you need them.

Notifications within Security Management Platform are organized into three categories to help you quickly identify the importance and purpose of each message.

- **Needs Attention:** These are critical alerts that require your action or awareness, such as an expired subscription.
- **Notifications:** These are general updates that provide value, like a notification letting you know a file is ready for download.
- **Announcements:** These messages appear at the top of your notification hub and contain important news, such as feature release, system updates, significant announcements from Quest Product Management.

## Managing global notifications

Clicking the bell icon opens a flyout displaying your most recent notifications. You can easily manage them directly from this hub.

- **Read vs. Unread:** Notifications with a blue edge on the left are unread. Once you interact with one, the edge disappears, and the unread count on the bell icon adjusts automatically.
- **Dismiss:** To remove a notification from your hub, click the "X" in its top-right corner. Notifications which are considered significant may not provide the ability to dismiss and instead will auto-dismiss after a time-frame or expiry date controlled by Quest.
- **Actions:** Many notifications include specific actions such as **Learn More**, **View** and **Download** to help you take the next step.
- **Stacking:** To keep your hub from being cluttered, similar notifications are automatically stacked. For example, if you have multiple files ready to download from the same module, they'll appear as a single item with a hint like "+n similar" where n is the total number of similar notifications. Clicking this hint allows you to expand and view the full list. They will be stacked again the next time you open the hub.
- **Accessing Historical Notifications:** For a complete history of your alerts, access the full-page notification experience. This view provides a comprehensive record of all notifications from the last 30 days. You can filter and sort this page to find specific past alerts, giving you a full overview of your activity.
- To manage and view system alerts efficiently, you can apply filters to narrow down notifications by:
  - **Module:** Security Management Platform, Migration, Identity Recovery, and Identity Defense

- Severity:
  - Information – General updates or details.
  - Success – Completed actions or successful processes.
  - Warning – Potential issues that need attention.
  - Error – Problems that require corrective action.
  - Critical – High-priority issues needing immediate resolution.
  - Attention – Items flagged for review.

**i** | **NOTE:** Filters are temporary and only apply during your current session. They are not saved and will not carry over the next time you access the Security Management Platform portal.

## Information window

The Security Management Platform information window contains the following tabs:

- **About:** Version numbers and copyright information.
- **Third Party:** The list of third party components used in the product. This information is also contained in the Release Notes.
- **Contact:** Information on how to contact [Technical Support](#).

## Security Management Platform Status page

When you expand the system status on the masthead and click the **Status Overview** link, you can view the Security Management Platform Status page. The page provides detailed information about outages, past incidents, and planned maintenance. If there are partial outages or degraded performance for some modules, you can view an expanded list that indicates which geographic locations are affected.

If a blue banner displays at the top of the masthead, you can click **Read more** to see the scheduled maintenance list in the Security Management Platform Status page. The list provides the date for each scheduled maintenance activity and indicates whether downtime is expected during the maintenance activity.

You have the option to subscribe to updates through email notifications whenever Quest Security Management Platform creates, updates or resolves an incident.

## Side navigation panel

The side navigation panel is always available as you move through the Security Management Platform site. It provides access the following Security Management Platform functionality:

### Home

Click to return to the Home dashboard.

### Tenants

Opens the Tenants page where you can add Azure tenants and on-premises domains (using agents) to Security Management Platform. For details, see [Managing your Microsoft Entra tenants and on-premises domains](#).

## Migrate

Allows you to select the required Migration module, such as Projects, Active Directory, Directory Sync, Domain Rewrite, and Domain Move.

## Recover

Provides information on all available Identity Recovery products.

## Defend

Provides access to Identity Defense which is a solution that helps you keep the Active Directory domains and Entra ID tenants in your organization secure.

## Settings

Provides access to the following information:

- Organization page where you can see the organization details, edit the organization name and the domains that are authorized to access it and delete organizations that are no longer needed. See [Organization](#).
- Access Control page where you can manage users and their assigned roles. See [Adding users and groups to an organization](#).
- Subscriptions page where you can view and manage subscriptions. See [Subscriptions](#).
- Activity Trail page where you can view the complete activity trail history for an organization. See [Activity trail](#).
- Notifications page where you can configure email that will be sent to one or more recipients following an event. See [Notifications](#).

## Support

- Help opens an associated User Guide.
- Release Notes opens a document with information on the currently deployed software version and technical support information.

**i** | **NOTE:** When you are on the Security Management Platform Home page, the Global Settings documents open. When you are on a module page, these links open the documentation for the module.

# Dashboard

In addition to a tile for each module, the **Dashboard** displays statistics and operational data for your tenant. It includes the following components:






- [Tenant filter](#)
- [Needs your attention!](#)
- [Product tiles](#)

## Tenant filter

Located in the top right of the dashboard, the tenant filter determines what data is displayed on the dashboard. You can choose to display all tenants, a subset, or a single tenant.

# Needs your attention!

The Needs your attention! tile displays a summary of alerts and cautions from all of the modules you are currently subscribed to. It also displays information on the status of your subscription or trial if it is close to expiry.

Needs your attention!		
	Group modifications by Admin	<b>21</b> <a href="#">VIEW</a>
	Failed backups	<b>5</b> <a href="#">VIEW</a>
	Groups without owners	<b>4,568</b> <a href="#">ASSIGN</a>
	Something to warn you about	<b>2</b> <a href="#">VIEW</a>
	Something strange happened	<b>3</b> <a href="#">VIEW</a>

## Product tiles

If you have a subscription to a product, the product tile displays status information for your tenant.

**NOTE:** GCC High and GCC tenants are supported only by On Demand Migration and Identity Defense Audit and are only available in the US region. Totals shown for other Security Management Platform products do not include GCC High or GCC tenants.

---

# Configuring settings

- [Organization](#)
- [Access Control](#)
- [Subscriptions](#)
- [Activity trail](#)
- [Notifications](#)

## Organization

Once an organization has been created, you can select **Settings | Organization** in the left navigation to see the organization details, edit the organization name and the domains that are authorized to access it and delete organizations that are no longer needed.

For details, see [Editing organization settings](#) and [Deleting organizations](#).

## Access Control

Once you have created an organization, you can add additional users and determine what tasks each user can perform. To perform these activities, select **Settings | Access Control** in the left navigation bar.

Access control is a process by which users are granted access and certain privileges to systems, resources, or information. In Security Management Platform, you can grant authenticated users access to specific resources based on your company policies and the permission level assigned to the user.

The Access Control setting provides two options: Roles and Users

- For information about configuring roles, see [Access Control: Roles](#).
- For information about managing user access, see [Organization access for Microsoft Entra users](#).
- For information about managing group access, see [Organization access through Microsoft Entra group membership](#).

To see the task flow for access control procedures, see the task flow [Assigning a role to a user](#).

# Subscriptions

This section contains the following topics.

<a href="#">Subscription details</a>	The <b>Subscriptions</b> page contains the details of your current subscriptions.
<a href="#">Managing subscriptions</a>	Security Management Platform subscriptions are associated with an email address or a serial number.
<a href="#">Subscription expiry</a>	To prevent loss of data, subscription expiry takes place in stages.

## Subscription details

The Security Management Platform subscription page has been updated to a tiered format, displaying individual subscriptions by module, offering detailed information such as expiration dates and available licenses.

Some modules offer separate licenses for specific features. You can view the associated module features by hovering over the information icon.

Each module with a prepaid plan details individual subscriptions, and the top row provides a summary of these subscriptions, including details such as the total purchased, used, available, and expired.

Modules are categorized into two sections: those with active subscriptions and those with inactive subscriptions. For instance, if you have only Migration subscriptions, the Migration section will be prioritized at the top of the page, while inactive modules will be organized alphabetically below it.

Expand each module to view the associated subscription details.

### **i** NOTE: Using Filters

- You can select to filter the information displayed based on whether the subscription is Active, Not Subscribed, Expiring Soon, or Expired. By default, the Expired filter is not checked.
- When the filters are selected, the module tables will be updated to indicate a new summary row and associated subscriptions.

Table 1. Subscription detail descriptions

Field	Value	Description
Product	Feature name	A feature is the smallest subscription unit. Features can be bundled into Standard, Professional, and Advanced offerings.
Status	Current status	Shows whether the subscription is active, deactivated, not subscribed, expired, or expiring soon to provide insights into subscriptions that may require the administrators attention.
Type	Paid	The organization has purchased a subscription to features offered by this module. The specific subscription type depends on the number of features purchased.
	Evaluation	The organization has subscribed to an evaluation license. Module features maybe limited.
	Trial	The organization has subscribed to a trial license. Module features may be limited.  Note: When moving from Trial to Paid, the user associated with the paid subscription must be an organization administrator. See <a href="#">Changing Owner When Moving from Trial to Paid Subscription</a> .
Expiration Date	MMM/dd/yyyy	The date on which the subscription will expire. See <a href="#">Subscription expiry</a> .

Table 1. Subscription detail descriptions

Field	Value	Description
Purchased	####	The number of licenses that have been purchased (active and inactive).
Used	####	The number of licenses currently consumed.
Available	####	The number of licenses available.
Expired	####	The number of expired licenses. (Note: This is not the number of used licenses from expired subscriptions.)
Plan	Prepaid	The set number of licenses that have been purchased.
	Overages	The organization is billed for licenses as the are consumed.
Serial Number	####	The serial number associated with the subscription.
Subscription Owner	Organization identifier	The subscription owner.

## Managing subscriptions

Security Management Platform subscriptions are associated with the email address that was used to purchase the subscription. All valid email address formats are supported. The email address does not need to be associated with a Quest account to activate a subscription; the email address of the subscription owner must be added to the Subscription Owners list on the **Settings | Subscriptions** page.

- i** | **NOTE:** Adding a subscription owner to the Subscription Owners list does not add the user to the organization. A subscription owner does not have sign-in capability or any other permission settings. To add a user to an organization, see [Adding users and groups to an organization](#).

Depending on your deployment, subscriptions are shared using email addresses or activated through a serial number.

For details, see:

- [Sharing a subscription via email address](#)
- [Stop using a subscription shared through email](#)
- [Sharing a subscription via serial number](#)
- [Removing a subscription shared through a serial number](#)
- [Renewing a subscription shared through a serial number](#)

## Sharing a subscription via email address

To share a subscription, users request permission from the subscription owner by adding their email address to the Subscription Owners list. If the request is approved by the owner, all subscriptions associated with the email address are assigned to the organization.

- i** | **NOTE:**
- A subscription owner can share subscriptions with multiple organizations.
  - A Subscription sharing status of **Active** indicates that the user has consented to share subscriptions. It does not indicate that a valid subscription is associated with the email address.

### **To share a subscription:**

- 1 In the side navigation panel, click **Settings | Subscriptions**.
- 2 At the top right on the Subscriptions page, click **SHARED SUBSCRIPTIONS**.
- 3 On the Shared Subscriptions page, enter the email address of the subscription owner and click **Request**.  
The email address is added to the Subscription Owners lists with a Subscription sharing status of **Pending**.

- 4 The subscription owner receives an email with a request to share the subscriptions associated with the email address.

If the subscription owner approves the request, the Subscription sharing status changes to **Active** and any subscriptions associated with the email address are added to the Subscriptions page.

- 5 If Subscription sharing remains in the **Pending** state, you can choose to select **Cancel Request** from the Action menu.

## Stop using a subscription shared through email

You can stop subscription sharing by removing the subscription owner's email address from the Subscription Owners list.

- 1 In the side navigation panel, click **Settings | Subscriptions**.
- 2 At the top right on the Subscriptions page, click **SHARED SUBSCRIPTIONS**.
- 3 In the Subscription Owners list, locate the email address of the subscription owner that will no longer share subscriptions with the organization.
- 4 In the Action column for the subscription, select **Stop Using Subscription**.
- 5 The confirmation window lists the subscriptions that will be removed from the organization. Click **Stop Using Subscription**. The subscription owner receives an email informing them that the subscription is no longer assigned to the organization. All subscriptions associated with it are removed from the Subscriptions page.

## Sharing a subscription via serial number

Subscriptions shared with a serial number are linked to your organization and become active as soon as they're added.



### NOTE:

- The serial number cannot be reused between organizations.
- Select **View Subscription** from the Dashboard homepage to review the subscription in your organization.

### *To share a subscription:*

- 1 In the side navigation panel, click **Settings | Subscriptions**.
- 2 At the top right on the Subscriptions page, click **Add Subscription**.
- 3 Add the serial number, review the details and click **Add**.

## Removing a subscription shared through a serial number

### *To remove a subscription:*

- 1 In the side navigation panel, click **Settings | Subscriptions**.
- 2 Select the product, and under **Actions**, choose **Remove**.

## Renewing a subscription shared through a serial number

You can only renew subscriptions that were originally shared using a serial number. The Renew option becomes available when the subscription is close to expiring.

### *To renew a subscription:*

- 1 In the side navigation panel, click **Settings | Subscriptions**.
- 2 Select the product, and under **Actions**, choose **Renew subscription**.

You will be redirected to the Quest website where you can purchase additional subscriptions.

## Changing Owner When Moving from Trial to Paid Subscription

The user that signed up for a trial subscription is automatically an administrator for the organization. If a different user email address is used for purchasing a paid subscription, this user address must be added to the Subscription Owners list before the subscription status displays as **Paid**.

If you need assistance determining the email address used to purchase the subscription or, if you want to change the address associated with the subscription, contact [Technical Support](#).

## Subscription expiry

To prevent loss of data, subscription expiry takes place in stages.

### Stage 1: Your subscription expires in X days

Thirty days prior to expiry, the Security Management Platform organization administrator receives an email notification. From this time on, the module tile on the Security Management Platform home page displays the number of days before the subscription expires.

### Stage 2: Subscription expired. Access denied.

Once the subscription expires, members of the organization can no longer access the Security Management Platform product. The configuration settings have been preserved and module services continue for the next 30 days.

### Stage 3: Subscription expired. Service disabled.

After 30 days, module services are no longer operational for the tenants in the organization. Data is preserved for 30 days and then, it is permanently deleted.

### Stage 4: Subscription expired. Grace period ended.

After 30 days, module services are no longer operational for the tenants in the organization. Data is preserved for 30 days and then, it is permanently deleted.

### Stage 5: Subscription expired. Data deleted.

Your data has been deleted and cannot be restored

- i** **NOTE:** To receive email notifications related to stages 2-4 subscribe to the Subscription Lifecycle notification template located under Security Management Platform Notifications (See [Configuring Security Management Platform Notification Templates](#).) By default, Security Management Platform Admin role members are configured to receive these notifications.

# Activity trail

An activity trail is a set of records that provide documentary evidence of the sequence of activities that have affected a specific operation, procedure, or event at any time. The recorded information includes date and time, actor, a description and customized fields of the event. Security Management Platform retains the complete activity trail history for an organization.

The following activity trail logs are available:

**Security Management Platform:** Records the information for:

- adding and removing tenant events
- granting of admin consent for a tenant
- assigning and unassigning a user to Security Management Platform access control roles
- platform service related tasks
- notification events

**Identity Defense:** Records information about the audit module and related events.

**Identity Recovery:** Records information about backup enable and disable events.

**Migration:** Records information about migration process events.

## Filtering and exporting activity trail logs

You can filter for the events that you want to see using the **FILTERS** option. You can also use the **EDIT COLUMNS** option to add and remove columns. When you are displaying the activities that you want, you can export the results to a .csv file.

You can click **+** at the end of the first row and select **All of (and)** or **Any of (or)** to add an additional filter rule. To remove an individual filter rule, click **X** beside the rule.

**NOTE:** To see the detailed information for the event, click on a specific event.

### *To modify columns and filter activity trail logs*

- 1 In the side navigation panel, click **Settings**.
- 2 In the Activity Trail tab, click **FILTERS** to expand and specify your filter criteria.  
By default, a filter is set to show the logs for the last 7 days (**Date | during last | 7 | days**).
- 3 To change filter criteria, you can select attributes, operators, and values from the dropdown list.
  - To add an additional filter rule click **+** at the end of the first row and select **All of (and)** or **Any of (or)**.
  - To see all available logs for current organization, click **CLEAR ALL**.
  - To remove an individual filter rule, click **X** beside the rule.
- 4 To customize the displayed columns, click **EDIT COLUMNS**, select or clear the columns, and click **SELECT**.

Once you are displaying the activity trail information that you want, you can click **EXPORT TO .CSV** to download the information in a .csv (comma separated value) format file.

# Configuring a forwarding destination for Platform Activity Trail

If your organization uses Microsoft Sentinel, Splunk (Cloud Platform or Enterprise) as a SIEM solution, you can configure the platform to forward Activity Trail data to the appropriate tool for further analysis.

After configuration, the forwarding destination tile displays the configuration details and the timestamp of the most recently forwarded activity. You can also edit or remove a forwarding destination at any time.

## **To access the Forwarding configuration page;**

- 1 In the side navigation panel, choose **Settings | Activity Trail**.
- 2 Make sure the Forwarding tab is selected.

## **To configure Microsoft Sentinel as a forwarding destination:**

- 1 Click **Add Forwarding Destination**, select **Microsoft Sentinel**.
- 2 Enter the **Sentinel Workspace ID** and **Shared (Primary) Key**. Refer to the [Microsoft documentation](#) for instructions on Finding the Workspace ID and key.
- 3 Click **Send Test Event** to ensure that a connection can be made to Sentinel.  
A message will be returned indicating whether or not the test event was successfully sent. If the test event was not successful, ensure the Workspace ID and Shared Key were entered correctly.
- 4 Click **Save**.

## **To configure Splunk (Cloud Platform or Enterprise) as a forwarding destination:**

- 1 Click **Add Forwarding Destination**, select **Splunk**.
- 2 Enter the **Splunk HTTP Event Collector URL** (for example, <http or https>://<cloud or server address>:<port>) and **Token**. Refer to the [Splunk documentation](#) for instructions on Finding the HTTP Event Collector URL and Token.
- 3 Click **Send Test Event** to ensure that a connection can be made to Splunk.  
A message will be returned indicating whether or not the test event was successfully sent. If the test event was not successful, ensure the URL and Token were entered correctly.
- 4 Click **Save**.

## Notifications

Security Management Platform email notifications alert designated recipients when specific events occur. For example, if a backup fails, the configured recipients receive an email notification.

Notification templates allow you to configure who will receive notifications so that they can take the appropriate action to address the outlined risks to your environment.

- [Managing Notification Templates: Required Permissions](#)
- [Configuring Audit Notification Templates](#)
- [Configuring Security Management Platform Notification Templates](#)
- [Configuring Identity Recovery for Active Directory Notification Templates](#)
- [Configuring Identity Recovery for Microsoft Entra ID Notification Templates](#)
- [Configuring Migration - Self-Service Notification Templates](#)

# Managing Notification Templates: Required Permissions

To manage notification templates, your account must have the correct permissions. These permissions vary by module and alert type. Ensure your role includes the necessary access.

## Required Permissions

- Audit
  - Shared Alerts:  
Requires Can Manage Shared Alerts and Shared Notification Templates
  - Private Alerts:  
Requires Can Manage Private Alerts and Private Notification Templates
- Identity Recovery for Active Directory
  - Manage Access:  
Requires Can Manage Forests
  - View-Only Access:  
Can View All
- Identity Recovery for Microsoft Entra ID
  - Requires Can Manage Backup Settings
- Security Management Platform
  - Requires Can Manage the Organization

## Configuring Audit Notification Templates

### *To create an Audit notification template*

- 1 In the side navigation panel, click **Settings**.
- 2 In the main panel, click **Notification | Email Notifications**.
- 3 Expand **Audit**.
- 4 To create a new notification template, select **New Template**.
- 5 Enter a name for the template.
- 6 Specify whether you require the system to send email alerts. When the **Email Notifications** toggle is **On**, email notifications are enabled, and emails will be sent for relevant updates. To disable notifications, click the toggle so it switches to **Off**.
- 7 Select whether it is private (only visible to the individual who created it) or shared (visible to all Audit users allowing for collaboration with multiple users from the same organization).
- 8 Add recipients by role or by entering the required email addresses and click **Add Recipients** as needed. All recipients are listed under **Selected Recipients**.
- 9 Optionally, select recipients (all or specific recipients) and click **Send Test Email**.
- 10 Click **Save**.

Under the Linked Alerts column you can see the number of linked alerts. Selecting the number hyperlink allows you to see the list of linked alerts.

The template can only be removed if it does not have alerts associated with it. For more information on managing alerts, see the [Identity Defense User Guide](#).

### ***To edit an Audit notification template***

- 1 In the side navigation panel, click **Settings**.
- 2 In the main panel, click **Notification | Email Notifications**.
- 3 Expand **Audit**.
- 4 Click the notification template name to edit the template.
- 5 Optionally, specify whether you require the system to send email alerts. When the **Email Notifications** toggle is **On**, email notifications are enabled, and emails will be sent for relevant updates. To disable notifications, click the toggle so it switches to **Off**.
- 6 Update recipients as needed.
- 7 To add recipients, enter the required email addresses and/or select the required roles and click **Add Recipients**.
- 8 To remove recipients, select the required email addresses and/or unselect the required roles from the recipients listed under **Selected Recipients**, and click **Remove**.
- 9 Optionally, select recipients (all or specific recipients) and click **Send Test Email**.
- 10 Click **Save**.

The template can only be removed if it does not have alerts associated with it. For more information on managing alerts, see the [Identity Defense User Guide](#).

### ***To remove an Audit notification template***

- 1 In the side navigation panel, click **Settings**.
- 2 In the main panel, click **Notification | Email Notifications**.
- 3 Expand **Audit**.
- 4 Select the notification template to edit and click **Remove Template**.
- 5 Click **Remove** to confirm.

The template can only be removed if it does not have alerts associated with it. For more information on managing alerts, see the [Identity Defense User Guide](#).

## **Configuring Security Management Platform Notification Templates**

### ***To edit a Security Management Platform notification template***

- 1 In the side navigation panel, click **Settings**.
- 2 In the main panel, click **Notification | Email Notifications**.
- 3 Expand **Security Management Platform**.
- 4 Click the notification template name to edit the template.
- 5 [Specify whether you require the system to send email alerts. When the \*\*Email Notifications\*\* toggle is \*\*On\*\*, email notifications are enabled, and emails will be sent for relevant updates. To disable notifications, click the toggle so it switches to \*\*Off\*\*.](#) Update recipients as needed.
- 6 To add recipients, enter the required email addresses [and/or select the required roles](#) and click **Add Recipients**.
- 7 To remove recipients, select the required email addresses and/or unselect the required roles from the recipients listed under **Selected Recipients**, and click **Remove**.
- 8 Optionally, select recipients (all or specific recipients) and click **Send Test Email**.

- 9 Click **Save**.

The next time an event that is associated with this notification template occurs, all the listed recipients receive a notification email.

## Configuring Identity Recovery for Active Directory Notification Templates

### *To edit an Identity Recovery for Active Directory notification template*

- 1 In the side navigation panel, click **Settings**.
- 2 In the main panel, click **Notification | Email Notifications**.
- 3 Expand **Identity Recovery for Active Directory**.
- 4 Click the notification template name to edit the template.
- 5 Specify whether you require the system to send email alerts. When the **Email Notifications** toggle is **On**, email notifications are enabled, and emails will be sent for relevant updates. To disable notifications, click the toggle so it switches to **Off**.
- 6 Update recipients as needed.
- 7 To add recipients, enter the required email addresses and/or select the required roles and click **Add Recipients**.
- 8 To remove recipients, select the required email addresses and/or unselect the required roles from the recipients listed under **Selected Recipients**, and click **Remove**.
- 9 Optionally, select recipients (all or specific recipients) and click **Send Test Email**.
- 10 Click **Save**.

The next time an event that is associated with this notification template occurs, all the listed recipients receive a notification email.

## Configuring Identity Recovery for Microsoft Entra ID Notification Templates

### *To edit an Identity Recovery for Microsoft Entra ID notification template*

- 1 In the side navigation panel, click **Settings**.
- 2 In the main panel, click **Notification | Email Notifications**.
- 3 Expand **Identity Recovery for Microsoft Entra ID**.
- 4 Click the notification template name to edit the template.
- 5 Specify whether you require the system to send email alerts. When the **Email Notifications** toggle is **On**, email notifications are enabled, and emails will be sent for relevant updates. To disable notifications, click the toggle so it switches to **Off**.
- 6 Update recipients as needed.
- 7 To add recipients, enter the required email addresses and/or select the required roles and click **Add Recipients**.
- 8 To remove recipients, select the required email addresses and/or unselect the required roles from the recipients listed under **Selected Recipients**, and click **Remove**.

- 9 Optionally, select recipients (all or specific recipients) and click **Send Test Email**.
- 10 Click **Save**.

The next time an event that is associated with this notification template occurs, all the listed recipients receive a notification email. For more information on managing alerts, see [On Demand Recovery User Guide](#).

## Configuring Migration - Self-Service Notification Templates

### ***To create a Migration - Self-Service notification template***

- 1 In the side navigation panel, click **Settings**.
- 2 In the main panel, click **Notification | Email Notifications**.
- 3 Expand **Migrate - Self-Service**.
- 4 To create a new notification template, select **New Template**, enter a name for the template, enter an optional Sender Display Name (appears in the From field).

Optionally, modify the default Message Subject and corresponding Message Body. (You can choose bold, italic, underline text, use a custom link, and move the table/list of workstations and the link to the self-service portal to a specified position in the email body.)

Optionally attach a custom logo (JPEG, PNG, SVG formats are supported up to 100KB max file size).

- 5 Click **Save**.

At any time click **Revert to Default** to reset the template to the defaults. For more information on managing notifications, see [On Demand Migration User Guide](#).

### ***To edit a Migration - Self-Service notification template***

- 1 In the side navigation panel, click **Settings**.
- 2 In the main panel, click **Notification | Email Notifications**.
- 3 Expand **Migrate - Self-Service**.
- 4 Click the notification template name to edit the template.
- 5 Update any template properties as needed.
- 6 Click **Save**.

At any time click **Revert to Default** to reset the template to the defaults. For more information on managing notifications, see [On Demand Migration User Guide](#).

### ***To remove a Migration - Self-Service notification template***

- 1 In the side navigation panel, click **Settings**.
- 2 In the main panel, click **Notification | Email Notifications**.
- 3 Expand **Migrate - Self-Service**.
- 4 Select the notification template to edit and click **Remove Template**.
- 5 Click **Remove** to confirm.

### ***To duplicate a Migration - Self-Service notification template***

- 1 In the side navigation panel, click **Settings**.
- 2 In the main panel, click **Notification | Email Notifications**.

- 3 Expand **Migrate - Self-Service**.
- 4 Select the notification template to duplicate and click **Duplicate Template**.
- 5 Make adjustments as required.
- 6 Click Duplicate to confirm.

---

# Documentation roadmap

## Global settings

Security Management Platform global settings refers to management tools and configuration settings that apply to all Security Management Platform products. This includes tenant management tasks and downloading activity trail logs.

## Products

Currently, the following products are available:

- [Migration](#)
- [Identity Recovery](#)
- [Identity Defense](#)

## Documentation

For each product, and the global settings, there is a Release Notes document and a User Guide.

- The Release Notes contains a release history and details of new features, resolved issues, and known issues.
- User Guides contain descriptions and procedures for the management tasks you can perform with each module

Use the links below to navigate to the content you require.

## User Guides

Each product has its own user guide:

- [Global Settings](#)
- [Migration](#)
- [Identity Recovery](#)
- [Identity Defense](#)

## Release Notes

- [Global Settings](#)
- [Migration](#)

- [Identity Recovery](#)
- [Identity Defense](#)

## More resources

- For sales or other inquiries, visit <http://quest.com/company/contact-us.aspx>.
- To sign up for a trial or purchase a subscription, go to <https://www.quest.com/on-demand>.
- Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at <https://support.quest.com>.
- The [Quest On Demand Community](#) provides a space for blog posts and a forum to discuss the On Demand products.

---

# Technical Support

Quest provides numerous resources to support you with our products.

## Current operational status

### [Security Management Platform status](#)

Security Management Platform relies on Microsoft Azure and Amazon Web Services (AWS) infrastructure and as such, is subject to the possible disruption of these services. You can view the following status pages:

- [Microsoft Azure status](#)
- [AWS status](#)

## Contact support

The [Contact Support](#) page allows you to submit a Technical Service Request. It also provides the phone numbers to use when contacting the Quest support team.

## Module product support pages

Each Security Management Platform product has a dedicated support page with "getting started", troubleshooting, and other useful information.

- [Product Support - Identity Defense](#)
- [Product Support - Migration](#)
- [Product Support - Identity Recovery](#)

## Information and discussion: Quest community forums

Visit the [Security Management Platform community forum](#) to read current information or to post a forum topic.

## About us

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit [www.quest.com](http://www.quest.com) or follow Quest Software on [X \(formerly Twitter\)](#) and [LinkedIn](#).

## Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at <https://support.quest.com>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.