Managed Services Portal®

Version 23.41

Managed Services Portal Usage Guide

August 2023

38000-100-23.41

Legal Notices

The content in this documentation is provided for informational purposes only and is provided "as is," without warranty of any kind, expressed or implied of Illumio. The content in this documentation is subject to change without notice.

For legal information, see https://www.illumio.com/legal-information.

Standard versus LTS Releases

For information on Illumio software support for Standard and LTS releases, see Versions and Releases on the Illumio Support portal.

Tenant Management for MSPs and MSSPs

This section describes how to use the Illumio Managed Services Portal to onboard your customers in to Illumio Core, Illumio Xpress, and Illumio Edge in the Illumio Cloud and then manage and administer those Illumio products on their behalf.

For detailed information about using Illumio Core, Illumio Xpress, and Illumio Edge, see the following documentation:

Illumio Product	Product Documentation
Illumio Core	• Get started with Core • Use Core • Administer Core
Illumio Xpress	• Use Xpress • Adminster Xpress
Illumio Edge	• Usage Guide

Actions Available to MSPs/MSSPs Global Org Owners

Illumio Managed Services Portal organization owners with the Global Organization Owner role can:

- Invite MSP/MSSP users to your Illumio Managed Services Portal organization.
- If your organization uses an Idenity Provider (IdP) solution, you can configure SAML Single-Sign On Authentication (SSO) access to your Illumio Managed Services Portal organization.
- Add client tenants in Illumio for your customers.
- Navigate to your customer's Illumio tenant(s) from the Managed Services Portal My Managed Tenants page
- View all your customer tenants from the My Managed Tenants page.
- Create policy and install VENs in your managed tenants.
- View the Events generated by you and other users in your Illumio Managed Services Portal organization.
- Manage your Illumio Managed Services Portal subscription (payment methods, billing history, account updates, and more).
- Remove client tenants from Illumio.

For more information about roles in Managed Services Portal, see Manage RBAC for Your Illumio Managed Services Portal

Typical Workflow

Illumio suggests this typical workflow for getting started with your Illumio Managed Services Portal organization:

STEP 1: Accept the Invitation

Accept the invitation to your account and add a new tenant.

> NOTE:
> You must be a **Global Organization Owner** to add a customer tenant. For details, see Manage RBAC for Your Illumio Managed Services Portal.

1. In your email, find the **Your Invitation to Illumio** message and click **Create Account**.
2. In the **Welcome to Illumio Multi-tenant Portal** screen, click **Add New Tenant**.

   Once you've created a tenant for a customer, you can easily create other tenant types for the same customer by clicking their name in the **My Managed Tenants** page and then clicking the desired tenant type in the **Contract** section . A new details page launches, pre-populated with the customer's information. The type of tenant that you selected is indicated in the **Contract** section.

   When you add a tenant for a customer, an audit event is generated automatically. You can view these events from your portal at **Troubleshooting > Events**. The user ID of the logged-in MSP/MSSP user appears on the Events page in the **Generated By** field.
3. Choose the type of tenant you want to add:
   - Core Tenant
   - Xpress Tenant
   - Edge Tenant
4. Enter details:
   - **Name**: Enter a descriptive name for the new tenant.
   - **Customer Domain**: Enter a globally unique name in the form of a domain (example.com).
   - **Company URL**: Enter the customer's company website URL.
   - **Country**
   - **Address lines 1 & 2**

- City
- State
- Zip Code

5. Click **Save**.

STEP 2: Configure SAML

Configure SAML single sign-on access for your users (if applicable).

> NOTE:
> This step applies only if you use a third-party SAML-based identity provider (IdP) to manage user authentication in your organization. If you don't use an IdP to manage identities, skip to STEP 3: Add MSP/MSSP Users.

If you use a third-party SAML-based identity provider (IdP) to manage user authentication in your organization, you can configure that IdP as an external authentication method for your MSP/MSSP users to access your Illumio Managed Services Portal organization. SAML SSO allows login credentials to be validated against your own Identity Management solution instead of requiring your users to create additional user passwords managed by Illumio.

Illumio Managed Services Portal supports any IdP that supports SAML 2.0, including the following:

- Azure AD
- Microsoft Active Directory Federation Services (AD FS)
- Okta
- OneLogin
- Ping Identity

> IMPORTANT:
> While other SAML-based IdPs may work with Illumio Managed Services Portal, configuring them is the responsibility of Illumio customers.

Before configuring SSO in your Illumio Managed Services Portal organization, configure SSO on your chosen IdP and obtain the required SSO information. Once you've obtained that information, log in to your Illumio Managed Services Portal organization and complete the configuration. For details, see the following documentation:

Topic
General Information
Information Needed to Configure SAML SSO
Signing for SAML Requests
SSO Instructions
Active Directory Single Sign-on
Azure Single Sign-on
Okta Single Sign-on
OneLogin Single Sign-on
Ping Identity Single Sign-on

STEP 3: Add MSP/MSSP Users

Illumio Managed Services Portal organization owners can add other MSP/MSSP users to their organization and grant them roles with specific permissions.

Types of Users

For detailed information about user types, see the topic Setup for Role-Based Access Control in PCE documentation. For information about roles and permissions in the Managed Services Portal, see Manage RBAC for Your Illumio Managed Services Portal

> IMPORTANT:
> If you consult the topic Setup for Role-Based Access Control, ignore all references to "scopes" and "scoped roles." Illumio Managed Services Portal doesn't support scopes.

Local Users

- Local Users are created and managed by Illumio; they are not managed by an Identity Provider (IdP) solution. Illumio encrypts and stores their password.
- When Illumio creates your Managed Services Portal, the first user account it creates is a Local User. This means that all Illumio Managed Services Portal customers have at least one Local User.
- In organizations that don't use a third-party SAML-based identity provider (IdP) to manage user authentication in their organization, all users in the Managed Services Portal will be Local Users.
- When added as a Local User, MSP/MSSP users are sent an account invite link to the email address specified when they were added. The invite link is valid only

for 7 days. If a Local User doesn't receive an email or the link they received expired, you can send them a new link.

External Users (applicable only for customers who implement SAML IdP)

- An External User is externally authenticated by your corporate IdP solution (if you have one). Your IdP solution manages authentication so that when these users attempt to log in to the Illumio Managed Services Portal they're redirected to the IdP to authenticate and then back to Illumio.
- No login or Welcome email is sent to External Users. You must provide MSP/MSSP users a URL to your Illumio Managed Services Portal.
- To allow you to access your Illumio Managed Services Portal in case the external IdP goes offline or the SAML server is not accessible, you may want to consider creating more than one Local User.

External Groups (applicable only for customers who implement SAML IdP)

External Groups are user groups maintained in your corporate IdP solution. Members in an External Group are externally authenticated by your corporate IdP solution (if you have one). Groups allow you to manage user authentication centrally for the Illumio Managed Services Portal. You assign roles to the groups managed by your IdP to control the access that group members have to your Illumio Managed Services Portal organization. When a user who is a member of an external group logs in to the Managed Services Portal, the corporate IdP authenticates the user and returns the list of groups the user belongs to. For each of those groups, the Managed Services Portal determines what roles are assigned to the group. The user is granted access to the resources associated with the roles. A user can belong to multiple external groups. When a user belongs to multiple groups, the user is granted access to Illumio resources based on the most permissive role defined for each group.

Add a Local User

> NOTE:
> If your organization doesn't use a third-party SAML-based identity provider (IdP) to manage user authentication. In that case, you can only create Local Users. If your organization uses a third-party SAML-based identity provider (IdP) to manage user authentication (see STEP 2: Configure SAML above), you should create at least one Local User as a backup in case the external IdP goes offline or the SAML server is not accessible. Make sure the email address you enter when you add the Local User is not the same address configured for the user in your IdP solution

1. Click **Access > Local Users** in the left pane.
2. Click **Add**.
3. In the **Add Local User**dialog box:
   a. Enter a name and email address.

      > NOTE:
      > - If you configured/plan to configure SAML single sign-on access for your MSP/MSSP users and your organization uses a third-party SAML-based identity provider (IdP) to manage user authentication, the email address you enter here must not also be configured in your IdP solution.
      > - The email address must use the format xxxx@yyyy.zzzz and cannot exceed 255 characters.
      > - Email addresses with an apostrophe (') are permitted.
      > - Illumio Managed Services Provider allows duplicate names for local users but not duplicate email addresses.

   b. Select a **Role**. Options include:
      - None
      - Global Organization Owner
      - Global Administrator
      - Global Viewer

      For details about roles, see About Roles, Scopes, and Granted Access.

> IMPORTANT:
> If you consult the topic Setup for Role-Based Access Control, ignore all references to "scopes" and "scoped roles." The Illumio Managed Services Portal doesn't support scopes.

c. Click **Add**. A success message appears. Illumio sends an email to the specified email address with an account set-up link. The link is valid for 7 days.

Add an External User

This procedure is applicable only for customers who implement SAML IdP.

Perform these steps if your organization uses a third-party SAML-based identity provider (IdP) to manage user authentication. Additionally, you can create Local Users as a backup in case the external IdP goes offline or the SAML server is not accessible.

1. Click **Access > External Users** in the left pane.
2. Click **Add**.
3. In the **Add External User** dialog box:
   a. Enter a name and email address.

   > NOTE:
   > - The email address must use the format xxxx@yyyy.zzzz and cannot exceed 255 characters.
   > - Email addresses with an apostrophe (') are permitted.
   > - Illumio Managed Services Provider allows duplicate names for External Users but not duplicate email addresses.

   b. Select a **Role**:
      - None
      - Global Organization Owner
      - Global Administrator
      - Global Viewer

      For details about roles in the Managed Services Portal, see Manage RBAC for Your Illumio Managed Services Portal.

   c. Click **Add**.

Add an External Group

This procedure is applicable only for customers who implement SAML IdP.

Perform these steps if your organization uses a third-party SAML-based identity provider (IdP) to manage user authentication and you use groups to manage user authentication centrally.

1. Click **Access > External Groups** in the left pane.
2. Click **Add**.
3. In the **Add External Group** dialog box:
    a. **Name:** Enter a name (max. 225 alphanumeric or special characters).
    b. **External Group**: Enter the group name as it's configured in your IdP solution.

       In your IdP, the group is designated by a simple group name (for example "Sales") or by a group name in distinguished name (DN) format (for example "CN=Sales, OU=West"). To verify the correct format to enter in the PCE, check the `memberOf` attribute in the SAML assertion from your IdP. The `memberOf` attribute is a multiple-value attribute that contains the list of distinguished names for groups that contain the group as a member.
    c. Click **Add**.
    d. Assign a Global Role to the group. You must assign a role for newly-created External Groups because no role is assigned by default.
        i. In the External Groups page, click the new group that you just added.
        ii. Under Access Roles, click **Add Role > Add Global Role**.
        iii. Select the role you want to assign to the group.
        iv. Click **Grant Access** and then **Confirm** in the confirmation message.

STEP 4: Create Policy in Managed Tenants

Conceptual information about Illumio products that you'll manage on behalf of your customers, as well as procedures on how to administer them, is beyond the scope of this document. For this type of information, see the relevant information from these sources:

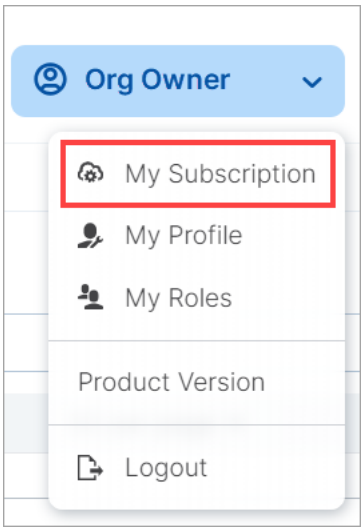
Illumio Product	Product Documentation
Illumio Core	• Get started with Core • Use Core • Administer Core
Illumio Xpress	• Use Xpress • Adminster Xpress

Illumio Product	Product Documentation
Illumio Edge	• Usage Guide

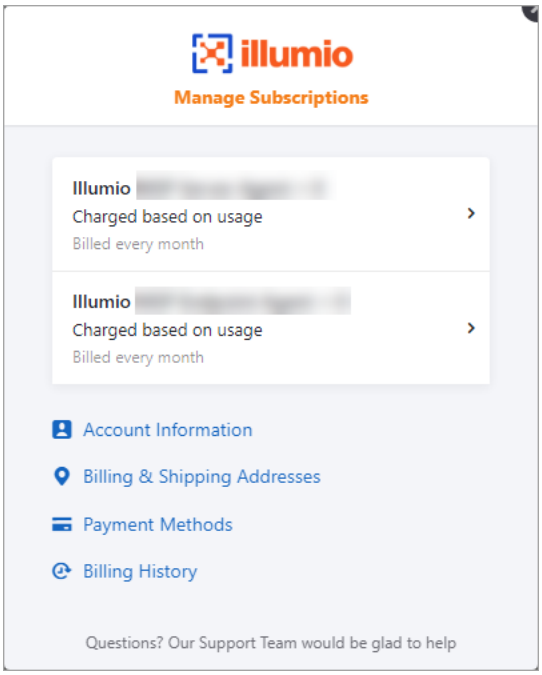
STEP 5: Manage Your Subscription

The Illumio Managed Services Portal integrates with a third-party payment management provider to handle usage-based billing for your Managed Services Portal organization. Illumio has created a subscription to that provider for your organization. You can manage your subscription as described in these steps.

1. In the upper right-hand corner of the console, click your username, and then select **My Subscription** from the drop-down menu.



2. In the **Manage Subscriptions** dialog box, follow the prompts to enter your credentials and log in.



3. You can view and manage the following areas of your subscription:
    - Subscription details. To view, click **Charged based on usage** for the subscription you want to investigate.
    - Account information
    - Billing and Shipping addresses
    - Payment methods
    - Billing history

Illumio Managed Services PortalProcedures

This section includes the procedures for setting up and using the Illumio Managed Services Portal.

For a recommended workflow of tasks, see Typical Workflow.

For detailed information about using Illumio Core, Illumio Xpress, and Illumio Edge, see the following documentation:

Illumio Product	Product Documentation
Illumio Core	• Get started with Core • Use Core • Administer Core
Illumio Xpress	• Use Xpress • Adminster Xpress
Illumio Edge	• Usage Guide

Add a Managed Tenant

> NOTE:
> You must be a **Global Organization Owner** to add a customer tenant. For details, see Manage RBAC for Your Illumio Managed Services Portal.

When you add a tenant:

- An Illumio organization is created automatically for your customer.
- An audit event is generated automatically. You can view these events from your Illumio organization in **Troubleshoot > Events**. The user ID of the logged-in MSSP user appears on the Events page in the **Generated By** field.

1. Log in to your Managed Services Portal organization.
2. On the My Managed Tenants page, click **Add**, and then select the type of tenant you want to add:
    - Core Tenant
    - Express Tenant
    - Edge Tenant
3. Enter details:

- **Name**: Enter a descriptive name for the new tenant.
- **Customer Domain**: Enter a globally unique name in the form of a domain (example.com).
- **Company URL**: Enter the customer's company website URL.
- **Country**
- **Address lines 1 & 2**
- **City**
- **State**
- **Zip Code**

4. Click **Save**.

Remove a Managed Tenant

> NOTE:
> You must be a **Global Organization Owner** to add a customer tenant. For details, see Manage RBAC for Your Illumio Managed Services Portal.

When you remove a tenant:

- The tenant is deleted and can't be restored. (The ability to restore a deleted tenant is planned for a future release.)
- The active VEN count for the tenant is reduced to zero.
- An audit event is generated automatically. You can view these events from your Illumio organization in **Troubleshoot > Events**. The user ID of the logged-in MS/MSSP user appears on the Events page in the **Generated By** field.

To remove a tenant:

1. Log in to your Managed Services Portal organization.
2. Select the tenant you want to remove.
3. Click **Remove**.

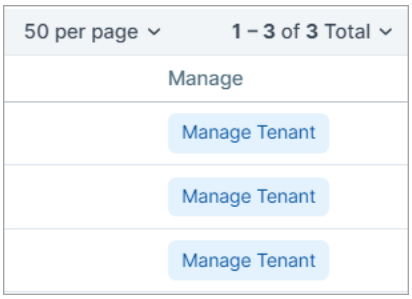
Access Your Managed Tenants

> NOTE:
> You must be a **Global Organization Owner** to add a customer tenant. For details, see Manage RBAC for Your Illumio Managed Services Portal.

1. Log in to your Managed Services Portal organization.

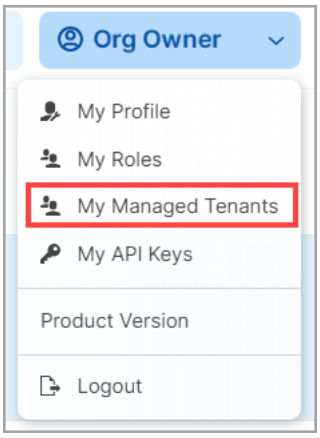
   The Managed Services Portal Home screen lists up to 500 of the tenants you're currently managing.

2. In the list, find the tenant that you want to access, and then click **Manage Tenant** for that tenant.



   You're redirected to the customer's tenant in the Illumio product where it resides (Core, Xpress, Edge).

3. To return to your Managed Services Portal organization, click the upper right-hand corner of the console, click your username, and then select My Managed Tenants from the drop-down menu.



For Illumio product details, see the links in the following table:

Illumio Product	Product Documentation
Illumio Core	• Get started with Core • Use Core • Administer Core
Illumio Xpress	• Use Xpress • Adminster Xpress

Illumio Product	Product Documentation
Illumio Edge	• Usage Guide

Customize the Managed Tenants List

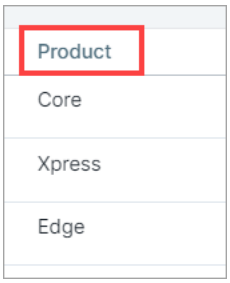
You can change the appearance of the managed tenants list in several ways:

Refresh the list

Click to update the number of VENs in the list.

Re-order the list

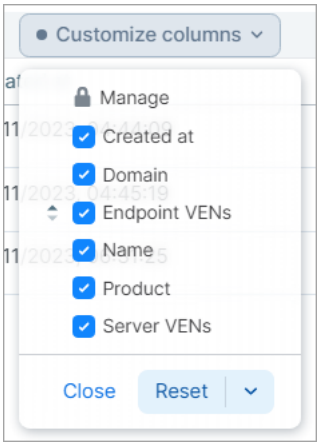
To reorder the Managed Tenants list according to the contents of a given column, click the appropriate column heading. For example, if you want to order the list by Illumio product, click the Product column heading.



Add or remove columns; reset to default sorting

By default, all columns appear in the list, sorted by tenant name.

- To add or remove columns from the Managed Tenants list, click **Customize Columns** and select the columns you want to appear.
- To reset the entire list page to the default order by Name, click **Reset**.



View user activity

You can view a list of user activity through the Access menu.

1. Log in to your Managed Services Portal organization.
2. Select **Access** and then select **User Activity**. Session details for each user appear.
3. Click a user to view the role assigned to that user. The User Activity page also displays users who were removed and are offline.

Manage Your Profile

Your Managed Services Portal profile is created automatically when Illumio creates your Managed Services Portal organization.

You can edit the following fields in your profile:

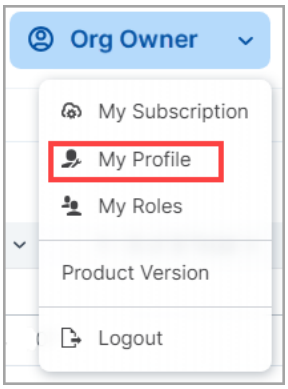
- Name
- Time Zone
- Color Mode
- Password

The following fields cannot be edited:

- Email address/Username
- My Organization name
- My Organization ID

To edit your profile:

1. Log in to your Managed Services Portal organization.
2. In the upper right-hand corner of the console, click your username, and then select **My Profile** from the drop-down menu.



3. Make your edits.
4. Click **Save**.

Manage RBAC for Your Illumio Managed Services Portal

This section briefly describes how to configure and manage role-based access (RBAC) for the users in your Managed Services Portal organization.

Types of Roles

- **Global Organization Owner**:
  - Manage all aspects of the Managed Services Portal organization, including management of the users they invite to their MSP/MSSP organization (Access Management page)
  - View and manage existing tenants including create policy for tenants
  - Manage the Managed Services Portal subscription
- **Global Administrator**: This role has limited capabilities in the Managed Services Portal. However, in the managed PCE tenants themselves, Global Administrators have the same capabilities as Global Organization Owners.

  > NOTE:
  > Given the mix of capabilities across separate environments (Managed Services Portal vs. managed PCEs), note that the role of Global Administrator differs from the role of the same name in the PCE.

  - Capabilities within managed PCE tenants
    - View and manage PCE tenants just like a Global Organization Owner
  - Capabilities within the Managed Services Portal
    - View the Events page for the Managed Services Portal
    - View the product version of the Managed Services Portal
    - View their profile and edit some areas of it
    - Access Support for the Managed Services Portal
  - Limitations within the Managed Services Portal
    - Cannot create, delete, or update a managed PCE tenant in the Managed Services Portal

    - Cannot create, update, or delete Managed Services Portal users (the Access Management option does not appear for Global Administrators.)
    - Cannot manage the Managed Services Portal subscription
- **Global Viewer**: Currently, users with this role can:
    - View almost everything within managed PCE tenants
    - View and modify their profile the Managed Services Portal
    - View, add, modify, and delete My API Keys
- **Global Policy Object Provisioner:** Currently, users with this role can:
    - View almost everything within managed PCE tenants
    - Provision Services, IP Lists, Label Groups, and Security Settings
    - View and modify their profile the Managed Services Portal
    - View, add, modify, and delete My API Keys

View or change the Global Role for a user or group

> NOTE:
> You must be a **Global Organization Owner** to view or change the role for a user or a group.

You specify a Global Role when you add users to your Illumio Managed Services Portal organization as either a Local User or an External User.

View

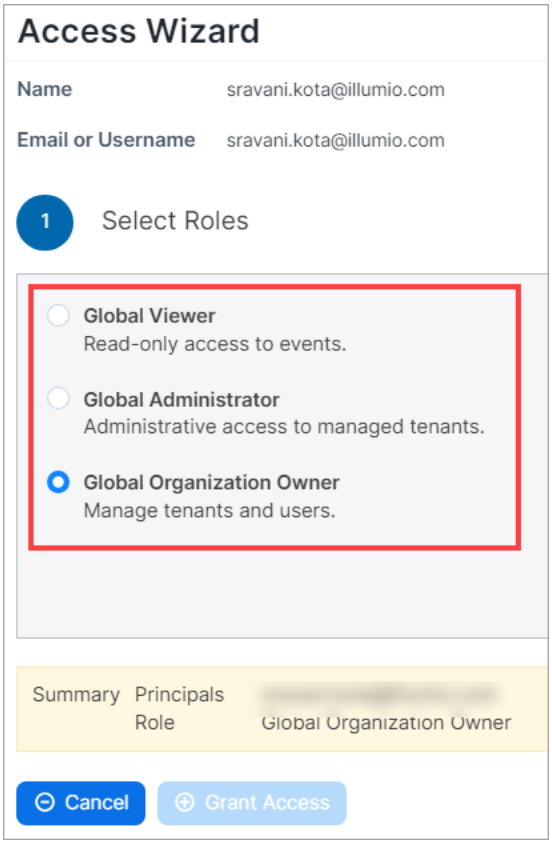
1. Select **Access**.
2. Click **Global Roles**.
3. Click the desired tab.
4. Click the group or user whose Global Role you want to view.

Change

> NOTE:
> The role descriptions that appear in the **Access Wizard - Select Roles** dialog box may be inaccurate. Refer to the role descriptions above.

1. Select **Access**.
2. Click a user type (Local or External).
3. Click the pencil icon.

4. In the Access Wizard, select a role.
5. Click **Grant Access**.



View and Export Events

The Illumio Managed Services Portal web console provides an ongoing log of all Organization events that occur in your Illumio Managed Services Portal organization. For example, Organization events capture actions such as users logging in and logging out, tenant creation, failed login attempts, and so on.

From the platform and API perspective, Organization events are referred to internally as `auditable_events` and are generated by the `auditable_events_service`.

View Events

> TIP:
> A wealth of information about Events is available in the Core PCE documentation in the Events Administration Guide. However, please note that not all of the information in that guide pertains to your Illumio Managed Services Portal organization. For assistance, please send a message to **ms@illumio.com**.

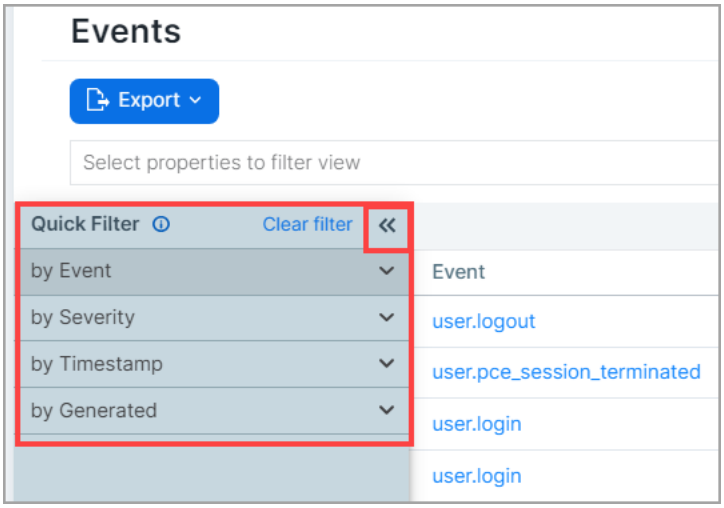
1. Select **Troubleshoot > Events**.
2. Use the filters to search for events by type of event, event severity level, and when the event occurred.
3. Once you've defined a filter, click Go to run the query.

Export Events

You can export all Organization events or a filtered list of events to a CSV file.

1. Select **Troubleshoot > Events**.
   - To export all Organization events, click **Export** and then select **Export All**.
   - To export a filtered list of events, filter the list, click Export, and then select **Export Filtered**.
   - To search for events based on event type, severity, status, timestamp, and who generated them, use the search filter.

- To use **Quick Filters**, click the double arrows.



List of Events

The following table provides the types of JSON events generated and their description. For each of these events, the CEF/LEEF success or failure events generated are the event name followed by `.success` or `.failure`.

For example, the CEF/LEEF success event for `auth_security_principal.create` is `auth_security_principal.create.success` and the failure event is `auth_security_principal.create.failure`.

Each event can generate a variety of notification messages. See Notification Messages in Events.

JSON Event Type	Description	Severity
`auth_security_principal.create`	RBAC auth security principal created	Informational
`auth_security_principal.delete`	RBAC auth security principal deleted	Informational
`auth_security_principal.update`	RBAC auth security principal updated	Informational
`authentication_settings.update`	Authentication settings updated	Informational
`org.create`	Organization created	Informational
`org.delete`	Organization deleted	Informational
`org.update`	Organization updated	Informational
`org.unpair_vens`	VENs unpaired	Informational
`orgs.ven_count`	Active VEN count for a list of orgs	Informational

JSON Event Type	Description	Severity
	obtained	
password_policy.create	Password policy created	Informational
password_policy.delete	Password policy deleted	Informational
password_policy.update	Password policy updated	Informational
permission.create	RBAC permission created	Informational
permission.delete	RBAC permission deleted	Informational
permission.update	RBAC permission updated	Informational
request.authentication_failed	API request authentication failed	Informational
request.authorization_failed	API request authorization failed	Informational
request.internal_server_error	API request failed due to internal server error	Informational
request.invalid	API request failed because it was invalid	Informational
request.service_unavailable	API request failed due to unavailable service	Informational
request.unknown_server_error	API request failed due to unknown server error	Informational
saml_acs.update	SAML assertion consumer services updated	Informational
saml_config.create	SAML configuration created	Informational
saml_config.delete	SAML configuration deleted	Informational
saml_config.pce_signing_cert	SAML signing certificate created or rotated	Informational
saml_config.update	SAML configuration updated	Informational
security_principal.create	RBAC security principal created	Informational
security_principal.delete	RBAC security principal deleted	Informational
security_principal.update	RBAC security principal updated	Informational
security_principals.bulk_create	RBAC security principals bulk created	Informational
system_task.prune_old_log_events	Event pruning completed	Informational
user.accept_invitation	User invitation accepted	Informational
user.authenticate	User authenticated	Informational
user.create	User created	Informational

JSON Event Type	Description	Severity
user.create_session	User session created	Informational
user.delete	User deleted	Informational
user.invite	User invited	Informational
user.login	User logged in	Informational
user.login_session_terminated	User login session terminated	Informational
user.logout	User logged out	Informational
user.pce_session_terminated	User session terminated	Informational
user.reset_password	User password reset	Informational
user.sign_in	User session created	Informational
user.sign_out	User session terminated	Informational
user.update	User session updated	Informational
user.update_password	User password updated	Informational
user.use_expired_password	User entered expired password	Informational
user_local_profile.create	User local profile created	Informational
user_local_profile.delete	User local profile deleted	Informational
user_local_profile.reinvite	User local profile reinvited	Informational
user_local_profile.update_password	User local password updated	Informational

Notification Messages in Events

Events can generate a variety of notifications that are appended after the event type:

- hard_limit.exceeded
- pce.application_started
- pce.application_stopped
- request.authentication_failed
- request.authorization_failed
- request.internal_server_error
- request.invalid
- request.service_unavailable
- request.unknown_server_error
- soft_limit.exceeded
- system_task.event_pruning_completed

- system_task.hard_limit_recovery_completed
- user.csrf_validation_failed
- user.login_failed
- user.login_failure_count_exceeded
- user.login_session_created
- user.login_session_terminated
- user.pce_session_created
- user.pce_session_terminated
- user.pw_change_failure
- user.pw_changed
- user.pw_complexity_not_met
- user.pw_reset_completed
- user.pw_reset_requested