Cortex Gateway Administrator Guide

Confidential - Copyright Â© Palo Alto Networks

1. Cortex Gateway

1 | Cortex Gateway

Cortex Gateway is a centralized portal for managing roles, user groups, and users for all tenants. Any roles and user groups created in Cortex Gateway are available for all tenants.

Only users with the Account Admin role can manage roles, tenants, and user groups in Cortex Gateway.

1.1 | Activate a tenant

Abstract

Learn how to activate your Cortex tenant.

Activate your tenant from Cortex Gateway and then log in to your tenant.

1.1.1 | Activate Cortex XDR tenant

Abstract

Learn how to activate your Cortex XDR tenant.

Watch the video here.

For more information about setting up 2FA in the Customer Support Portal, see Two Factor Authentication (2FA) Overview. You can also add an IdP, which is recommended. See How to Enable a Third Party IdP.

To activate a Cortex XDR tenant, you need to log into Cortex Gateway, which is a centralized portal for activating and managing tenants, users, roles, and user groups. After activating the tenant you can then access the tenant. If you have multiple Cortex XDR tenants, you will need to repeat this task for each tenant. The activation process includes accessing Cortex Gateway, activating the tenant, and then accessing the tenant.

> **PREREQUISITE:**
>
> Before you begin, make sure you have the following:

- Cortex XDR activation email.
- Customer Support Portal Super User role is assigned to your account.

  Before activating your Cortex XDR tenant, you need to set up your Customer Support Portal account. See How to Create Your Customer Support Portal User Account. When you create a Customer Support Portal account you can set up two-factor authentication (2FA) to log into the Customer Support Portal, by using one of the following:

  - Email
  - Okta Verify
  - Google Authenticator (non-FedRAMP accounts)

  Users who create the Customer Support Portal account are granted the Super User role. If you are the first user to access Cortex Gateway with the Customer Support Portal Super User role, you are automatically granted Account Admin permissions for the gateway.

  You can activate Cortex XDR new tenants, access existing tenants, and create and manage role-based access control (RBAC) for all of your tenants.

How to activate Cortex XDR

1. Enable and verify access to Cortex XDR communication servers, storage buckets, and various resources in your firewall configuration. For more information, see Enable access to required PANW resources.
2. Go to Cortex Gateway .

   You can also access the link from the activation email.
3. Enter your username and password or multi-factor authentication (if set up) by using your Customer Support Portal account credentials to sign in.

   Once signed in, you can view the following:

   - Tenants that are allocated to your Customer Support Portal account and ready for activation. After activation, you cannot move your tenant to a different Customer Support Portal account.
   - Tenant details such as license type, number of endpoints, and purchase date.
   - Tenants that were activated and are now available. If you have more than one Customer Support Portal account, the tenants are displayed according to the Customer Support Portal account name.
4. In the Available for Activation section, use the serial number to locate the tenant that needs activation, and then click Activate.
5. On the Tenant Activation page, define the following:

- Tenant Name: Enter a name for the tenant. Use a name that is unique across your company account and up to 59 characters long.
- Region: Geographic location where your tenant will be hosted. For more information, see supported regions.
- Tenant Subdomain: DNS record associated with your tenant. Enter a name that will be used to access the tenant directly using the full URL:
- Directory Sync: Select the active directory for connecting your tenant when activated.

6. Select I agree to the terms and conditions of the Privacy policy.
7. Click Activate.

   The activation process can take about an hour.
8. After activation, from Cortex Gateway, in the Available Tenants when hovering over the activated tenant, do the following:
   - Ensure that you can successfully access the tenant by clicking the Cortex XDR tenant name (when the tenant is active).
   - In the dialog box, view the tenant status, region, serial number, and license details.
   - Activation in Progressindicates that the tenant's activation is still in process.
   - Click the menu icon to Change Tenant Subdomain.

     Before changing your tenant subdomain, first complete the necessary preparations, including updating your Cortex XDR agent to the latest version, configuring your firewalls and Single Sign-On (SSO).

     You can only change the tenant subdomain only once.
   - Click the menu icon to Change Tenant Name.

1.1.2 | Activate Cortex XSIAM tenant

Abstract

Learn how to activate your Cortex XSIAM tenant.

For more information about setting up 2FA in the Customer Support Portal, see Two Factor Authentication (2FA) Overview. You can also add an IdP, which is recommended. See How to Enable a Third Party IdP.

To activate a Cortex XSIAM tenant, you need to log into Cortex Gateway, which is a centralized portal for activating and managing tenants, users, roles, and user groups. After activating the tenant you can then access the tenant. If you have multiple Cortex XSIAM tenants, you will need to

repeat this task for each tenant. The activation process includes accessing Cortex Gateway, activating the tenant, and then accessing the tenant.

> **PREREQUISITE:**
>
> Before you begin, make sure you have the following:
>
> - Cortex XSIAM activation email.
> - Customer Support Portal Super User role is assigned to your account.
>
>   Before activating your Cortex XSIAM tenant, you need to set up your Customer Support Portal account. See How to Create Your Customer Support Portal User Account. When you create a Customer Support Portal account you can set up two-factor authentication (2FA) to log into the Customer Support Portal, by using one of the following:
>
>   - Email
>   - Okta Verify
>   - Google Authenticator (non-FedRAMP accounts)
>
>   Users who create the Customer Support Portal account are granted the Super User role. If you are the first user to access Cortex Gateway with the Customer Support Portal Super User role, you are automatically granted Account Admin permissions for the gateway.
>
>   You can activate Cortex XSIAM new tenants, access existing tenants, and create and manage role-based access control (RBAC) for all of your tenants.

How to activate Cortex XSIAM

1. Enable and verify access to Cortex XSIAM communication servers, storage buckets, and various resources in your firewall configuration. For more information, see Enable access to required PANW resources.
2. Go to Cortex Gateway .

   You can also access the link from the activation email.
3. Enter your username and password or multi-factor authentication (if set up) by using your Customer Support Portal account credentials to sign in.

   Once signed in, you can view the following:

   - Tenants that are allocated to your Customer Support Portal account and ready for activation. After activation, you cannot move your tenant to a different Customer Support Portal account.
   - Tenant details such as license type, number of endpoints, and purchase date.
   - Tenants that were activated and are now available. If you have more than one Customer Support Portal account, the tenants are displayed according to the Customer Support Portal account name.

4. In the Available for Activation section, use the serial number to locate the tenant that needs activation, and then click Activate.

   > **NOTE:**
   >
   > When you activate, a production tenant is first activated. After activation, you can set up a development tenant (subject to your license).

5. On the Tenant Activation page, define the following:

   - Tenant Name: Enter a name for the tenant. Use a name that is unique across your company account and up to 59 characters long.
   - Region: Geographic location where your tenant will be hosted. For more information, see supported regions.
   - Tenant Subdomain: DNS record associated with your tenant. Enter a name that will be used to access the tenant directly using the full URL:
   - Directory Sync: Select the active directory for connecting your tenant when activated.

6. Select I agree to the terms and conditions of the Privacy policy.

7. Click Activate.

   The activation process can take about an hour.

8. After activation, from Cortex Gateway, in the Available Tenants when hovering over the activated tenant, do the following:

   - Ensure that you can successfully access the tenant by clicking the Cortex XSIAM tenant name (when the tenant is active).
   - In the dialog box, view the tenant status, region, serial number, and license details.

9. Subject to your license, activate your development tenant.

   a. Hover over the activated tenant, and on the right-hand side, click the ellipsis and then click Activate Dev Tenant.

   b. Define the development tenant name, region, and subdomain.

      After the development tenant is activated, you can set up your remote repository. For more information, see development tenant.

1.1.3 | Activate Cortex XSOAR tenant

Abstract

Learn how to activate your Cortex XSOAR tenant.

To activate a Cortex XSOAR tenant, you need to log into Cortex Gateway, which is a centralized portal for activating and managing tenants, users, roles, and user groups. After activating the tenant you can then access the tenant. You must repeat this task for each tenant if you have multiple tenants. The activation process includes accessing the Cortex Gateway, activating the tenant, and then accessing the tenant.

Before you begin, ensure that you have the following:

- The Cortex XSOAR activation email.
- A Customer Support Portal (CSP) account.

  You need to set up your CSP account. For more information, see How to Create Your CSP User Account.

  When you create a CSP account, you can set up two-factor authentication (2FA) to log into the CSP by using an Email, Okta Verify, or Google Authenticator (non-FedRAMP accounts). For more information, see How to Enable a Third Party IdP.
- You have one of the following roles assigned:

Role	Description
CSP role	The Super User role is assigned to your CSP account. The user who creates the CSP account is granted the Super User role.
Cortex role	You must have the Account Admin role. If you are the first user to access Cortex Gateway with the CSP Super User role, you are automatically granted Account Admin permissions for the Cortex Gateway. You can also add Account Admin users as required. In the Cortex Gateway, you can activate new tenants, access existing tenants, and create and manage role-based access control (RBAC) for all of your tenants.

How to activate Cortex XSOAR

1. Log in to Cortex Gateway.

   You can also access the link from the activation email.
2. Enter your username and password or multi-factor authentication (if set up) by using your CSP account credentials to sign in.

After you are signed in, you can view the following:

- If you are a CSP Account Admin, you can see tenants allocated to your CSP account and ready for activation. After activation, you cannot move your tenant to a different CSP account.
- Tenant details such as license type, status, and serial number.
- Tenants that were activated and are now available. If you have more than one CSP account, the tenants are displayed according to the CSP account name.

3. In the Available for Activation section, use the serial number to locate the tenant that needs activation, and then click Activate as SAAS.

   If you want to install On-prem instead, download the install package. For more information, see Cortex XSOAR installation.

   > **NOTE:**
   >
   > When you activate, a production tenant is first activated. After activation, you can set up a development tenant (subject to your license).

4. In the Activate XSOAR 8 dialog box, select Start Fresh.

   If you are migrating from Cortex XSOAR 6, select Migrate your tenant. When activated, this option starts the migration process. For more information, see Migrate XSOAR 6 to 8 Using the Migration Wizard.

5. On the Tenant Activation page, define the following:

Parameter	Description
Tenant Name	Enter the name of the tenant. Use a unique name across your company account up to 59 characters long.
Region	Geographic location where your tenant will be hosted. For more information about supported regions, see Supported host regions.
Tenant Subdomain	DNS record associated with your tenant. Enter a name that will be used to access the tenant directly using the full URL: `https://<subdomain>crtx.<region>.paloaltonetworks.com`

6. Review and agree to the terms and conditions of the Privacy policy, Terms of Use, and EULA , and then Activate your tenant.

   > **NOTE:**
   >
   > Activation can take about an hour and does not require that you remain on the activation page. Cortex XSOAR sends a notification to your email when the process is complete.

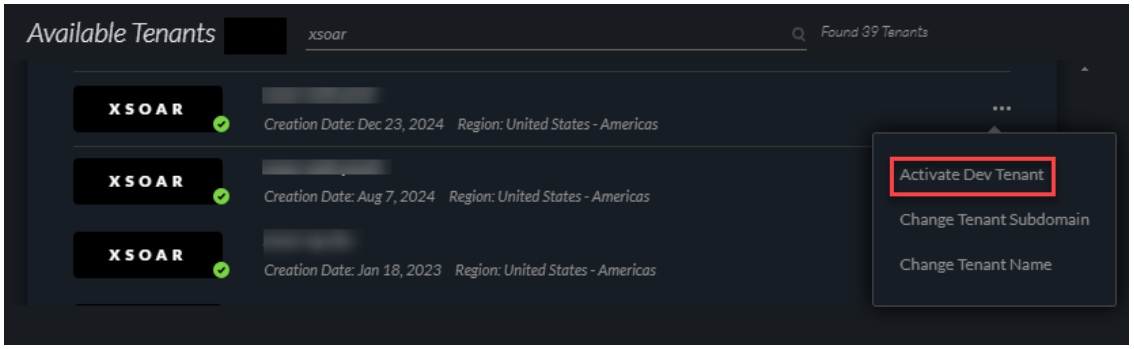
7. When the tenant is active, ensure you can access the tenant by clicking the Cortex XSOAR tenant name.

   When hovering over the activated tenant, you can see the tenant's status, region, serial number, and license details.

   > **NOTE:**
   >
   > If you want to change your tenant's name, the subdomain, or activate a development tenant (subject to license), on the right-hand side, click the ellipsis.

8. Subject to your license, activate your development tenant.

   a. Hover over the activated tenant, and on the right-hand side, click the ellipsis and then click Activate Dev Tenant.

   b. Define the development tenant name, region, and subdomain.

      After the development tenant is activated, you can set up a remote repository. For more information, see Set up a remote repository.

9. Enable access to Palo Alto Network resources in your firewall. See Enable access to Palo Alto Networks resources.

1.2 | Users and roles in Cortex

Abstract

Set up and configure roles and user groups in the Cortex tenant and Cortex Gateway. Configure authentication and manage users.

Cortex uses role-based access control (RBAC) to manage roles with specific permissions for controlling user access. RBAC helps manage access to components, so that users, based on

their roles, are granted the minimal access required to accomplish their tasks.

You can create or configure roles, users, and user groups in Cortex Gateway, the tenant, or both. For example, create a Manager role in Cortex Gateway, which enables you to maintain the Manager role in a central place with the same level of access for all tenants. If you are using SSO, you create a user group in the Cortex tenant that includes the Manager role, assign tenant users to this group, and map the user group to your SAML group.

> **NOTE:**
>
> All users must have at least one role or belong to at least one user group to be saved in the Cortex Gateway.

Cortex Gateway and the tenant have different options and requirements.

Location	Details
Cortex Gateway	A centralized portal for managing roles, user groups, and users for all tenants. Any roles and user groups created in Cortex Gateway are available for all tenants. Only users with the Account Admin role can manage roles, tenants, and user groups in Cortex Gateway.
Cortex tenant	(Recommended) All permissions and roles are specific to the tenant and exist only at the tenant level. Advanced settings such as default dashboards, queries, and shift management can only be defined per role at the tenant level. Only user groups created on the tenant can be mapped to SAML groups when using SAML SSO. You need the Account Admin or Instance Administrator role to manage roles, users, and user groups.

Roles

Roles enable you to define permissions for specific components, such as incident data, playbooks, scripts, and jobs. For example, you can create a role that allows users to edit the properties of incidents, but not delete incidents. You can create new roles or customize out-of-the-box roles.

If you assign one or more roles to an incident, only users with those roles can view and interact with the incident. For example, you might have an incident with sensitive data that should only be accessible to Tier-1 analysts and managers.

Roles can also be used to define permissions for integration commands. On the Integration Permissions page, you can assign roles to specific integration instances (all commands for that instance) or specific integration instance commands. For example, you could assign the Generic Export Indicators Service integration instance the Account Admin role, or you could restrict certain commands in the Core Rest API to a specific role. For more information, see Integration Permissions.

User groups

While roles can be assigned directly to users, we recommend instead creating user groups. Each user group has a single role associated with it, but each user group can contain multiple users, and user groups can be nested within each other, enabling you to further refine your RBAC requirements. Users can belong to multiple user groups.

Nested roles

Cortex uses group nesting, where the group with higher permissions includes the permissions of the group with lower permissions, but as a subset of the group with lower permissions. For example, the Admin user group is included as a subset of the Analyst user group, as shown in the following graphic. The Admin role includes the permissions of the Analyst role.

For example, Content Developer and Analyst user groups include Employee user group permissions, and are nested in the Employee user group.

Authentication

You can create users in the Customer Support Portal or by using SAML Single Sign-On (SSO) in the tenant. After you create users, they authenticate by doing the following:

- Authenticate through the Customer Support Portal
- Authenticate by using SAML Single Sign-On (SSO) in the Cortex tenant

Manage users

In Cortex Gateway, you can manage users who have been created in the Customer Support Portal or view users who have been created using SSO. In the Cortex tenant, you can manage both sets of users.

By default, users do not have roles assigned and do not automatically have access to tenant data until you assign them a role or add them as members of a user group that has an assigned role.

1.3 | User management

Abstract

Manage users in Cortex Gateway or the Cortex tenant.

You can manage users in Cortex Gateway or the Cortex tenant. At the Users tab in the Permissions page (Cortex Gateway â Permission Management+Permissions) or the Users page (Settings & Info â Settings â Access Management â Users) in the tenant, you can see user information, including:

Name	Description
User Type	Indicates whether the user was defined in Cortex using the CSP, SSO using your organizationâ€ s IdP, or both CSP/SSO. **NOTE:** If you have migrated local users from Cortex XSOAR 6 to Cortex XSOAR 8 and these users are in the Customer Support Portal, these users are designated the PANW IDP user type. For more information, see Migrating users and roles.

Name	Description
Direct Role	Displays the name of the role assigned specifically to the user not inherited from somewhere else, such as a user group. In Cortex Gateway, select the arrow next to the name of the user to see the user roles and the tenants the user has access to. In the Cortex tenant, the direct role is the role assigned to the user in the tenant. When the user has no access permissions assigned specifically to them, the field displays No-Role. **NOTE:** If a user does not have a direct role or user group assigned, the user is revoked and is not saved in the Cortex Gateway.
Groups	Lists the user groups to which the user belongs. If a user is assigned to multiple user groups, which are mapped to different roles, or if the user is assigned to nested user groups, the user inherits the permissions of parent user groups and has the highest level of privileges based on the combination of roles. Any group imported from Active Directory has the letters AD added beside the group name. **NOTE:** If a user does not have a direct role or user group assigned, the user is revoked and is not saved in the Cortex Gateway.
Group Roles	Lists the different group roles based on the groups the user belongs to. When you hover over the group role, the group associated with this role is displayed.

Name	Description
Last Login Time	Last date and time the user accessed the Cortex tenant.
Status	Displays whether the user is Active or Inactive.
Phone number	Relevant only in the Cortex tenant. Displays the user's phone number. Including the user's phone number enables playbooks and scripts to trigger direct analyst communication by phone.

Considerations for managing users in Cortex Gateway or tenant

Option	Cortex Gateway	Cortex Tenant
SSO	Limited to viewing SSO users. You cannot edit SSO users in Cortex Gateway.	Full management of SSO users
Update user details option	N/a	View the user's details and add the user's telephone number.
User Permissions	Global user role management including assigning the Account Admin role, or limiting the user role to the relevant Cortex product/tenant, and adding/removing roles in the Tenant/Gateway. **NOTE:** You must have an Account Admin role to manage users in Cortex Gateway.	Management of predefined and custom user roles on the tenant. **NOTE:** You must have an Account Admin or Instance Administrator role.

Option	Cortex Gateway	Cortex Tenant
Hide users	Users are hidden from the list of users in Cortex Gateway, but can still be viewed in the tenants. By default, the Show User Subset field is selected, which displays the users not designated as Hidden users. This is useful when you have users not related to your Cortex tenant and who will not be designated with a Cortex tenant role, such as Customer Support Portal Super Users, and you want to hide them from the list. **NOTE:** Users without an assigned role or user group are not saved in the Cortex Gateway. However, there is an exception for users who did not have an assigned role or user group and who were hidden before the following product releases: • Cortex XSIAM 2.7 (legacy) • Cortex XSIAM 3.2 (platform) • Cortex XSOAR 8.11 • Cortex XDR 3.15 (legacy) • Cortex XDR 4.2 (platform) Users who were hidden before the release remain saved in the Cortex Gateway and are not revoked, even if they do not have an assigned role or user group.	The user is hidden in the list of users in the tenant, but can still be viewed in other tenants and Cortex Gateway. In the Cortex tenant under the Actions button, select Hide Hidden Users. When you hide users in the tenant, they are hidden in the tenant and not in Cortex Gateway.
Deactivate/activate users	Deactivate the user for one or more tenants.	Deactivate the user for the tenant only.

1.3.1 | Manage users in Cortex Gateway

Abstract

Add user roles, disable users, hide users, and deactivate users in Cortex Gateway.

In Cortex Gateway, on the Permissions page (Cortex Gateway â Permission Management), you can manage users that have been added to your Customer Support Portal account or view users that have been created in the tenant using SSO (you cannot edit SSO users in Cortex Gateway). All users must have at least one role or belong to at least one user group to be saved in the Cortex Gateway.

> **NOTE:**
>
> To remove users added to your CSP account, you must do so in the CSP, not in Cortex Gateway.

The Permission page is split into the following:

- Users tab: View user information according to your Customer Support Portal account, including groups, roles, user types, and tenants assigned. When right-clicking a user, you can perform actions such as editing roles, deactivating users, and removing or adding roles.
- Tenants tab: View tenants according to the Cortex product and manage users who have access to each tenant.

Add/update user roles

Update a user's role if the user was added to the CSP. You can add the following roles:

- Pre-defined roles: Instance Administrator and Account Admin.
- Custom roles: Includes out-of-the-box roles and roles created in Cortex Gateway or the tenant.

You can add/update roles by either selecting the users in the Users tab or by tenants in the Tenants tab.

> **NOTE:**
>
> - To update the permissions associated with each role, you need to change them in the tenant or the Roles tab in Cortex Gateway.
> - If users have been created in the CSP, but you want them to access the tenant through SSO only, you should not assign a direct role. If you sign a direct role, users can access the tenant through both the CSP and SSO.
> - If no role is assigned either directly or through a user group, users cannot view or edit in the Cortex tenant, the user is revoked in the Cortex Gateway and their user information is no longer saved.

Update user roles according to each user

You can update user roles for one or multiple users.

1. From the Permissions page, in the Users tab, do one of the following:

- If editing one user, right-click the user's name and select Update Permissions or Add Permissions (if no role).
- If editing multiple users, select multiple users, and in the right-hand corner, outside the table, click the edit button.

2. In the Update user role window, if you want the user to have superuser permission across all tenants, select Apply the Account Admin role.

   We do not recommend creating additional Account Admins as the user has full access to all tenants across all Cortex products. Account Admin is a special role, automatically assigned to the Customer Support Portal Super User.

3. If you have multiple Cortex products, select the product for which you want to change permissions.
4. In the AVAILABLE TENANTS field, select the tenant where you want to add the user's role.
5. In the Role field, select one of the following:
   - Predefined role
   - Custom role
6. Save the user role.

Update user roles according to each tenant

You can update user roles according to each Cortex tenant or multiple tenants.

> **NOTE:**
>
> If you are updating multiple tenants at one time, you can only add predefined roles or roles created in Cortex Gateway (not custom roles created in the tenant).

1. In the Permissions page, select the Tenants tab.
2. If updating a single tenant, right-click the tenant and select Update Permissions.
3. If updating multiple tenants, select the multiple tenants, and in the right-hand corner, outside the table, click the edit button.
4. Select the role you want to add.

   If selecting multiple tenants, you can only add predefined and custom roles created in Cortex Gateway. If you want to add custom roles created in a tenant, you need to select only one tenant.

5. Select the users.
6. Save the role.

Remove permissions

If a user has a role in the tenant, you can remove their user permission to access each tenant. If no direct or user group role has been assigned, the user role displays No Role, and has no permission to view or edit the Cortex tenant.

1. From the Permissions page, in the Users tab, right-click the user's name and select Remote Permissions.
2. Do one of the following:
    - Remove permissions for all tenants, by clicking Select All Tenants.
    - To remove permissions for specific tenants, click the name field to select the tenants you want the user to be deactivated from.
3. Click Remove.

Deactivate users

Deactivate users for all or one or more tenants if they no longer need access, but may need it again at a later date. All user information is maintained for deactivated users. Users should be permanently removed if they no longer have access to the system through the CSP. The deactivated user appears grayed out. To reactivate, follow the same steps in this procedure.

> **NOTE:**
>
> You cannot deactivate a user who has an Account Admin role or who is not assigned access to a tenant. If you want to deactivate an Account Admin user role, right-click the user and select Remove User Permissions. You can then deactivate the user.

If the user is assigned to incidents or tasks or is the owner of a dashboard, these assignments do not automatically change when the user is removed or deactivated. We recommend changing incident and task assignments manually before removing or deactivating users.

Any reports the user has created remain available. Reports are not owned by specific users and can be edited or deleted by other users.

- Reassign open incidents to another user.

  Go to the Incidents page and search for `-status:closed owner:`*`user_name`* to find any incidents the user is assigned and reassign.

- Reassign tasks to another user.

  Go to the Incidents page and search for `-status:closed investigation.users:`*`user_name`* and reassign.

  When a user is assigned a task in an incident, the user is added to the incident. This search finds all incidents where the user is a participant.

How to deactivate users

1. From the Permissions page, in the Users tab, right-click the user's name and select Deactivate User.
2. Click Select All Tenants.
3. To select specific tenants, click the name field to select the tenants you want the user to be deactivated from.
4. Click Deactivate.

Hide users

Hides users from the user list in Cortex Gateway. This is useful when you have users who are not related to the Cortex tenant and will not be designated with a role, such as CSP Super Users, and you want to hide them from the list. When a user is designated as hidden, the user is no longer displayed when the table is configured to Show User Subset (default configuration).

You cannot view the user or search for the user when hidden. To show hidden users, deselect Show User Subset. To remove the hidden user tag, right-click the user and select unhide the user.

> **NOTE:**
>
> Users without an assigned role or user group are not saved in the Cortex Gateway. However, there is an exception for users who did not have an assigned role or user group and who were hidden before the following product releases:
>
> - Cortex XSIAM 2.7 (legacy)
> - Cortex XSIAM 3.2 (platform)
> - Cortex XSOAR 8.11
> - Cortex XDR 3.15 (legacy)
> - Cortex XDR 4.2 (platform)
>
> Users who were hidden before the release remain saved in the Cortex Gateway and are not revoked, even if they do not have an assigned role or user group.

1.4 | Roles management

Abstract

Configure roles in the Cortex tenant or Cortex Gateway.

You can assign the following permissions to various components in Cortex:

Permission	Description
None	No access to the specified component.
View	View, but not edit the specified component.
View/Edit	View and edit the specified component.

Next steps

Create roles or customize existing roles (recommended) in Cortex Gateway or the Cortex tenant.

Before you start creating or customizing roles, do the following:

- Review the Predefined roles in Cortex Gateway topic.
- Decide where you want to create roles (Cortex Gateway, the tenant, or both).

  Any roles and user groups created in Cortex Gateway are available for all tenants. In the Cortex tenant, all roles created in the tenant are specific to the tenant. Advanced settings such as default dashboards/queries and shifts can only be defined at the tenant level. Only user groups created on the tenant can be mapped to SAML groups when using SAML SSO.
- Decide whether you want to assign roles to users directly or through membership in user groups (recommended) in Cortex Gateway or the Cortex tenant.

1.4.1 | Predefined roles in Cortex Gateway

Abstract

Review the predefined roles in the Cortex Gateway.

Review the predefined roles for the relevant Cortex product:

Predefined roles for XSOAR

Cortex XSOAR includes the following out-of-the-box roles:

Role	Type	Description
Account Admin	Predefined	A super user role that is assigned directly to the user in Cortex Gateway or tenant and has full access to all Cortex products in your account, including all tenants added in the future. In Cortex Gateway, the Account Admin can assign roles for Cortex instances, and can also activate Cortex tenants specific to the product. This user has the same view/edit permissions in the tenant as the Instance Administrator. **NOTE:** The user who activated the Cortex product is assigned the Account Admin role. You can add the role to a user in Cortex Gateway or the tenant. If you need to remove the Account Admin role from a user, this can only be done in Cortex Gateway. Only users with the Account Admin role can add or remove another Account Admin user role. You cannot edit this role. You can copy the role by saving it as a new role and then change permissions.
Instance Administrator	Predefined	View/edit permissions for all components and access to all pages in the Cortex tenant. The Instance Administrator can also assign the Instance Administrator role to other users on the tenant. If the application has predefined or custom roles, the Instance Administrator can assign those roles to other users. You cannot edit this role. You can copy the role by saving it as a new role and then change permissions.

Role	Type	Description
Analyst	Custom	A mix of view and view/edit permissions for all components and access to all pages in the Cortex tenant. Cortex products comes out-of-the-box with the following Analyst roles: •  Analyst role created in Cortex Gateway. This role applies to all tenants. In the Cortex tenant, you cannot edit this role, apart from changing advanced settings such as default dashboards. In Cortex Gateway, you can change permissions, apart from advanced settings. You can also delete the role (if not assigned to a user). •  Analyst role created in the tenant. This role is specific to the tenant. You can edit all permissions and delete the role (if not assigned to a user) in the tenant and Cortex Gateway. In Cortex Gateway, you cannot change advanced settings.

Role	Type	Description
Read-Only	Custom	Read permissions for all components and pages in the Cortex tenant. Cortex products comes out-of-the-box with the following Read-Only roles: •  Read-Only role created in Cortex Gateway. This role applies to all tenants. In the Cortex tenant, you cannot edit this role, apart from changing advanced settings such as default dashboards. In Cortex Gateway, you can change permissions, apart from advanced settings. You can also delete the role (if not assigned to a user). •  Read-Only role created in the tenant. This role is specific to the tenant. You can edit all permissions and delete the role (if not assigned to a user) in the tenant and Cortex Gateway. In Cortex Gateway, you cannot change advanced settings.

NOTE:

By default, users do not have roles assigned. If no direct or user group role has been assigned, users have no permission to view or edit data in the Cortex tenant.

Predefined roles for XDR/XSIAM

Role-based access control (RBAC) enables you to use predefined Cortex XDR/XSIAM roles to assign access rights to Cortex XDR/XSIAM users. You can manage roles for all Cortex XDR/XSIAM tenants and services in the Gateway or in the Cortex XDR/XSIAM tenant. By assigning roles, you enforce the separation of access among functional or regional areas of your organization.

Each role extends specific privileges to users. The way you configure administrative access depends on the security requirements of your organization. Use roles to assign specific access privileges to administrative user accounts.

You can manage role permissions in Cortex XDR/XSIAM, which are listed by the various components according to the sidebar navigation in Cortex XDR/XSIAM. Some components include additional action permissions, such as pivot (right-click) options, to which you can also

assign access, but only when youâ€ ve given the user View/Edit permissions to the applicable component.

The default Cortex XDR/XSIAM roles provide a specific set of access rights to each role. You cannot edit the default roles directly, but you can save them as new roles and edit the permissions of the new roles. To view the predefined permissions for each default role, go to Settings â Configurations â Access Management â Roles.

> **NOTE:**
>
> Some features are license-dependent. Accordingly, users may not see a specific feature if the feature is not supported by the license type or if they do not have access based on their assigned role.

Default Role	Description
Account Admin	A Super User role that is assigned directly to the user in Cortex Gateway and has full access to all Cortex products in your account, including all tenants added in the future. The Account Admin can assign roles for Cortex instances and activate Cortex tenants specific to the product. **NOTE:** The user who activated the Cortex product is assigned the Account Admin role. You cannot create additional Account Admin roles in the Cortex XDR/XSIAM tenant. If you do not want the user to have Account Admin permission, you need to remove the Account Admin role in Cortex Gateway.
Instance Administrator	View and edit permissions for all components and access all pages in the Cortex XDR/XSIAM tenant. The Instance Administrator can also make other users an Instance Administrator for the tenant. If the tenant has predefined or custom roles, the Instance Administrator can assign those roles to other users.
Deployment Admin	Manage and control endpoints and installations, and configure Broker VMs.

Default Role	Description
Investigator	View and triage alerts and incidents.
Investigation Admin	View and triage alerts and incidents, configure rules, view endpoint profiles and policies, and analytics management screens.
Responder	View and triage alerts, and access all response capabilities excluding Live Terminal.
Privileged Investigator	View and triage alerts, incidents, and rules, view endpoint profiles and policies, and analytics management screens.
Privileged Responder	View and triage alerts and incidents, access all response capabilities, and configure rules, policies, and profiles.
IT Admin	Manage and control endpoints and installations, configure Broker VMs, view endpoint profiles and policies, and view alerts.
Privileged IT Admin	Manage and control endpoints and installations, configure Broker VMs, create profiles and policies, view alerts, and initiate Live Terminal.
Privileged Security Admin	Triage and investigate alerts and incidents, and respond to and edit profiles and policies.

Default Role	Description
Viewer	View the majority of the features for this instance and can edit reports.
Scoped Endpoint Admin	Can only access product areas that support endpoint scoped-based access control (SBAC) - Endpoint Administration, Action Center, Response, Dashboards and Reports.
Security Admin	Can triage and investigate alerts and incidents, respond (excluding Live Terminal), and edit profiles and policies.

Predefined roles for XSIAM Platform

Role-based access control (RBAC) enables you to use predefined Cortex XSIAM Platform roles to assign access rights to Cortex XSIAM Platform users. You can manage roles for all tenants and services in the Gateway or directly in the tenant. By assigning roles, you enforce the separation of access among functional or regional areas of your organization.

Each role extends specific privileges to users. The way you configure administrative access depends on the security requirements of your organization. Use roles to assign specific access privileges to administrative user accounts.

You can manage role permissions in Cortex XSIAM Platform, which are listed by the various components according to the sidebar navigation in Cortex XSIAM Platform. Some components include additional action permissions, such as pivot (right-click) options, to which you can also assign access, but only when youâ€ ve given the user View/Edit permissions to the applicable component.

The default Cortex XSIAM Platform roles provide a specific set of access rights to each role. You cannot edit the default roles directly, but you can save them as new roles and edit the permissions of the new roles. To view the predefined permissions for each default role, in the tenant go to Settings â Configurations â Access Management â Roles.

> **NOTE:**
>
> Some features are license-dependent. Accordingly, users may not see a specific feature if the feature is not supported by the license type or if they do not have access based on their assigned role.

Default Role	Description
Account Admin	A Super User role that is assigned directly to the user in Cortex Gateway and has full access to all Cortex products in your account, including all tenants added in the future. The Account Admin can assign roles for Cortex instances and activate Cortex tenants specific to the product. **NOTE:** The user who activated the Cortex product is assigned the Account Admin role. You cannot create additional Account Admin roles in the Cortex tenant. If you do not want the user to have Account Admin permission, you need to remove the Account Admin role in Cortex Gateway.
Instance Administrator	View and edit permissions for all components and access all pages in the tenant. The Instance Administrator can also make other users an Instance Administrator for the tenant. If the tenant has predefined or custom roles, the Instance Administrator can assign those roles to other users.
Deployment Admin	Manage and control endpoints and installations, and configure Broker VMs.
Investigator	View and triage issues and cases.
Investigation Admin	View and triage issues and cases, configure rules, view endpoint profiles and policies, and analytics management screens.
Responder	View and triage issues, and access all response capabilities excluding Live Terminal.

Default Role	Description
Privileged Investigator	View and triage issues, cases, and rules, view endpoint profiles and policies, and analytics management screens.
Privileged Responder	View and triage issues and cases, access all response capabilities, and configure rules, policies, and profiles.
IT Admin	Manage and control endpoints and installations, configure Broker VMs, view endpoint profiles and policies, and view issues.
Privileged IT Admin	Manage and control endpoints and installations, configure Broker VMs, create profiles and policies, view issues, and initiate Live Terminal.
Privileged Security Admin	Triage and investigate issues and cases, and respond to and edit profiles and policies.
Viewer	View the majority of the features for this instance.
Compliance Administrator	
Developer	Have limited permissions primarily focused on viewing and monitoring security information. Access and analyze scan results, track progress, and collaborate with security teams. Does not include ability to modify detection rules, enforcements, or directly address security issues.

Default Role	Description
CLI Read Only Role	View scripts, playbooks, credentials, and CLI tool.
CLI Role	View scripts, playbooks, and credentials. View and edit permission for CLI tool.
AppSec Admin	Full permissions for all Cloud Application Security related activities. Create and modify detection rules within the Code/Build domain, track progress, and adjust enforcements as needed. Additionally, triage and investigate findings, issues, and cases spanning from code to cloud. The role also includes complete visibility into all cloud assets.
Scoped Agent Admin	Can only access product areas that support endpoint scoped-based access control (SBAC) - Agent Administration, Action Center, Response, Dashboards and Reports.
Security Admin	Can triage and investigate issues and cases, respond (excluding Live Terminal), and edit profiles and policies.
App Service Account	View and triage issues, cases, and rules, and support public APIs relevant for apps.

Predefined roles for Cortex Cloud

Role-based access control (RBAC) enables you to use predefined Cortex Cloud roles to assign access rights to Cortex Cloud users. You can manage roles for all tenants and services in the Gateway or directly in the tenant. By assigning roles, you enforce the separation of access among functional or regional areas of your organization.

Each role extends specific privileges to users. The way you configure administrative access depends on the security requirements of your organization. Use roles to assign specific access

privileges to administrative user accounts.

You can manage role permissions in Cortex Cloud, which are listed by the various components according to the sidebar navigation in Cortex Cloud. Some components include additional action permissions, such as pivot (right-click) options, to which you can also assign access, but only when youâ€ ve given the user View/Edit permissions to the applicable component.

The default Cortex Cloud roles provide a specific set of access rights to each role. You cannot edit the default roles directly, but you can save them as new roles and edit the permissions of the new roles. To view the predefined permissions for each default role, in the tenant go to Settings â Configurations â Access Management â Roles.

> **NOTE:**
>
> Some features are license-dependent. Accordingly, users may not see a specific feature if the feature is not supported by the license type or if they do not have access based on their assigned role.

Default Role	Description
Account Admin	A Super User role that is assigned directly to the user in Cortex Gateway and has full access to all Cortex products in your account, including all tenants added in the future. The Account Admin can assign roles for Cortex instances and activate Cortex tenants specific to the product. **NOTE:** The user who activated the Cortex product is assigned the Account Admin role. You cannot create additional Account Admin roles in the Cortex tenant. If you do not want the user to have Account Admin permission, you need to remove the Account Admin role in Cortex Gateway.
Instance Administrator	View and edit permissions for all components and access all pages in the tenant. The Instance Administrator can also make other users an Instance Administrator for the tenant. If the tenant has predefined or custom roles, the Instance Administrator can assign those roles to other users.

Default Role	Description
Viewer	View the majority of the features for this instance.
Developer	Have limited permissions primarily focused on viewing and monitoring security information. Access and analyze scan results, track progress, and collaborate with security teams. Does not include ability to modify detection rules, enforcements, or directly address security issues.
CLI Read Only Role	View scripts, playbooks, credentials, and CLI tool.
CLI Role	View scripts, playbooks, and credentials. View and edit permission for CLI tool.
AppSec Admin	Full permissions for all Cloud Application Security related activities. Create and modify detection rules within the Code/Build domain, track progress, and adjust enforcements as needed. Additionally, triage and investigate findings, issues, and cases spanning from code to cloud. The role also includes complete visibility into all cloud assets.
Security Admin	Can triage and investigate issues and cases, respond (excluding Live Terminal), and edit profiles and policies.

Role-based permission levels for Cortex XPANSE

Predefined User Roles for Cortex Xpanse

Abstract

Use predefined roles to easily assign user access to Cortex Xpanse views and actions.

Cortex Xpanse provides a set of predefined user roles that you can use to assign View and Edit permission to Cortex Xpanse users. Each predefined role extends a specific set of privileges to users. The permissions defined in the predefined roles cannot be changed, but you can save a predefined role as a new role and edit it as needed.

The following tables describe the permissions defined for each of the predefined roles.

Account Admin

The following table shows the permissions for the predefined role Account Admin.

Section	**Component**	**Permissions**		
		None	View	View/Edit
Dashboards & Reports	Dashboards	-	-	✓
	Reports	-	-	✓
Incident Response	Alerts & Incidents	-	-	✓
	Query Center	-	-	✓
	Personal Query Library	-	-	✓
	Playbooks	-	-	✓
	Remediation Path Rules	-	-	✓

Section	Component	Permissions		
	Attack Surface Rules	-	-	✓
Assets	Network Configuration	-	-	✓
	Asset Inventory	-	-	✓
	Business Unit Overrides	-	-	✓
	Websites	-	✓	-
Marketplace	Browse	-	-	✓
Configurations	Auditing	-	✓	-
	General Configuration	-	--	✓
	Alert Notifications	-	-	✓
	Integrations	-	-	✓
	Public API	-	-	✓

Instance Admin

The following table shows the permissions for the predefined role Instance Admin.

Section	Component	Permissions		
		None	View	View/Edit
Dashboards & Reports	Dashboards	-	-	✓
	Reports	-	-	✓
Incident Response	Incidents and Alerts	-	-	✓
	Query Center	✓	-	-
	Personal Query Library	✓	-	-
	Playbooks	-	-	✓
Detection and Threat Intel	Attack Surface Rules	-	-	✓
Assets	Network Configuration	✓	-	-
	Compliance	✓	-	-
Assets	Websites	-	✓	-
	Asset Inventory	-	-	✓

Section	Component	Permissions		
Marketplace	Browse	-	-	✓
Settings	Auditing	-	✓	-
	General Configuration	-	-	✓
	Alert Notifications	-	-	✓
	Integrations	-	-	✓
	Public API	-	-	✓

Analyst

The following table shows the permissions for the predefined role Analyst.

Section	Component	Permissions		
		None	View	View/Edit
Dashboards & Reports	Dashboards	-	-	✓
	Reports	-	-	✓
Incident Response	Incidents and Alerts	-	-	✓

Section	Component	Permissions		
	Query Center	-	-	✓
	Personal Query Library	-	-	✓
Detection and Threat Intel	Attack Surface Rules	-	-	✓
Assets	Websites	-	✓	-
	Asset Inventory	-	-	✓
Marketplace	Browse	-	-	✓
Settings	Auditing	✓	-	-
	General Configuration	✓	-	-
	Alert Notifications	✓	-	
	Integrations	-	-	✓
	Public API	-	✓	-

Security Engineer

The following table shows the permissions for the predefined role Security Engineer.

Section	Component	Permissions		
		None	View	View/Edit
Dashboards & Reports	Dashboards	-	-	✓
	Reports	-	-	✓
Incident Response	Incidents and Alerts	-	-	✓
	Query Center	-	-	✓
	Personal Query Library	-	-	✓
	Playbooks	-	-	✓
Detection and Threat Intel	Attack Surface Rules	-	-	✓
Assets	Websites	-	✓	-
	Asset Inventory	-	✓	-
Marketplace	Browse	-	✓	
Settings	Auditing	✓	-	-

Section	Component	Permissions		
	General Configuration	-	✓	-
	Alert Notifications	✓	-	-
	Integrations	-	✓	-
	Public API	-	✓	-

Privileged IT Admin

The following table shows the permissions for the predefined role Privileged IT Admin.

Section	Component	Permissions		
		None	View	View/Edit
Dashboards & Reports	Dashboards	✓	-	-
	Reports	✓	-	-
Incident Response	Incidents and Alerts	✓	-	-
	Query Center	✓	-	-
	Personal Query Library	✓	-	-

Section	Component	Permissions		
	Playbooks	-	-	✓
Detection and Threat Intel	Attack Surface Rules	✓	-	-
Assets	Websites	✓	-	-
	Asset Inventory	✓	-	-
Marketplace	Browse	-	-	✓
Settings	Auditing	✓	-	-
	General Configuration	-	-	✓
	Alert Notifications	✓	-	-
	Integrations	-	-	✓
	Public API	-	-	✓

Viewer

The following table shows the permissions for the predefined role Viewer.

Section	Component	Permissions		
		None	View	View/Edit
Dashboards & Reports	Dashboards	-	✓	-
	Ingestion Monitoring	✓	-	-
	Reports	-	-	✓
Incident Response	Incidents and Alerts	-	✓	-
	Query Center	-	✓	-
	Personal Query Library	-	✓	-
	Playbooks	-	✓	-
Detection and Threat Intel	Attack Surface Rules	-	✓	-
	Threat Intel	✓	-	-
	Asset Inventory	-	✓	-
Marketplace	Browse	-	✓	-

Section	Component	Permissions		
Settings	Auditing	-	✓	-
	General Configuration	-	✓	-
	Alert Notifications	-	✓	-
	Integrations	-	✓	-
	Public API	-	✓	-

1.4.2 | Manage roles in Cortex Gateway

Abstract

View, create, edit, and delete roles in Cortex Gateway.

Cortex Gateway is a centralized portal for managing tenants, users, roles, and user groups.

> **NOTE:**
>
> You must have an Account Admin role to manage tenants, users, roles, and user groups in Cortex Gateway.

When you log into Cortex Gateway you can see the available tenants according to Cortex products, which you can manage according to your CSP account, including activation and licenses.

In the Permission Management page, in the Roles tab, you can manage roles created in Cortex Gateway or the tenant.

You can view, create, and edit roles and permissions that have been created in Cortex Gateway (All Tenants) or a tenant. If you create a new role, it applies to all tenants. For example, you may want a management role to have the same permissions across all tenants. To limit them to a specific tenant, create the role in the tenant.

When right-clicking a role, you can perform several actions, such as editing a role, saving it as a new role, and removing a role (deleting a role that is not assigned to a user).

Create a role

The roles you create provide more granular access control. You can add as many new roles as you need and combine them with user groups. You can set permission levels for viewing pages, limit potential actions, limit job actions, and limit scripts.

> **NOTE:**
>
> You must have an Account Admin role to create or edit a role.
>
> You cannot define advanced settings such as managing shifts or setting default dashboards in Cortex Gateway, as these are exclusive to the Cortex XSOAR tenant.
>
> We recommend copying and modifying out-of-the-box roles.

1. In Cortex Gateway, go to Permission Management â Roles â New Role.
2. Add the Role name and a meaningful Description.
3. In the Components tab, define the role-based permissions and save the role.

   > **NOTE:**
   >
   > In Cortex XDR/XSIAM, the Datasets tab is disabled in the Cortex Gateway as you can only set dataset access permissions in Cortex XDR/XSIAM Access Management. For more information in Cortex XSIAM, see Manage user roles. For more information in Cortex XDR, see Manage use roles.

4. You can create user groups and add roles to them (recommended), assign roles directly to users after they have been added, or both.

1.5 | User group management

Abstract

Create user groups, and assign roles and users to further refine your requirements,

Users are assigned roles and permissions either by being assigned a role directly or by being assigned membership in one or more user groups. A user group can only be assigned to a single role, but users can be added to multiple groups if they require multiple roles. You can also nest groups to achieve the same effect. Users who have multiple roles through either method will receive the highest level of access based on the combination of their roles.

For example:

- Joe has an Analyst role and is a member of the Tier-1 Analyst user group, which is assigned the Triage role. Joe has the permissions of the Analyst role and the Triage role. Joe is assigned 2 roles, and has the highest permission based on the combination of both roles.
- John is a member of two user groups - Tier-1 Analyst and Tier-2 Analyst. One group is configured to use the Triage role and the other group is configured to use the Incident Response role. John is assigned both roles and has the highest permissions based on the combination of all roles.
- Jack is a member of the Tier-2 user group which has an Incident response role. This user group is included in a Tier-3 user group (Threat Hunter role), added as a nested group. Jack is assigned both roles and has the highest permissions based on the combination of all roles.

On the User Groups page, you can create a new user group for several different system users or groups. You can see information including the details of all user groups, the roles, nested groups, IdP groups (SAML), and when the group was created/updated.

You can also right-click in the table to edit, save as a new group, remove (delete) a group, and copy text to the clipboard.

> **NOTE:**
>
> You can create user groups in the tenant or Cortex Gateway. User groups created in Cortex Gateway cannot be mapped to SAML groups. Only user groups that are created in the tenant support SAML group mapping. We recommend creating user groups in the Cortex tenant because user groups are available for all tenants and you may want different user groups in different tenants, such as dev/prod.

How to create a user group

1. If creating in Cortex Gateway, go to Permission Management â User Groups.
2. To create a new user group for several different system users or groups, click New Group, and add the following parameters:

Parameter	**Description**
Name	Name of the user group.
Description	Description of the user group.
Group for product	(Cortex Gateway only) If you have multiple products, select the relevant Cortex product.

Parameter	Description
Role	Select the group role associated with this user group. You can only have a single role designated per group. In Cortex Gateway, you can only select either Instance Administrator or a custom role created in the Gateway.
Users	Select the users you want to belong to this user group. **NOTE:** If users have been created in the CSP, but you want them to access the tenant through SSO only, skip this field and add only SAML group mapping after SSO is set up, otherwise, users can access the tenant through both the CSP and SSO. If you have not yet created any users, skip this field and add them later. See Set up authentication .
Nested Groups	Lists any nested groups associated with this user group. If you have an existing group you can add a nested group. User groups can include multiple users and nested groups, which inherit the permissions of parent user groups. The user group will have the highest level of permission. For example: • Group A has Tier-1 Analyst permissions • Group B has Tier-2 Analyst permissions If you add Group A as a nested group in Group B, Group A inherits Group B's permissions (Tier-1 and Tier-2 permissions). In Cortex Gateway, you can only add user groups that are created in Cortex Gateway.

Parameter	Description
SAML Group Mapping	(Relevant when creating a user group in the Cortex tenant only). Maps the SAML group membership to this user group. For example, you have defined a `Cortex XSOAR Admins` group. You need to name this group exactly how it appears in Okta. You can add multiple groups by separating them by a comma. **NOTE:** When using Azure AD for SSO, the SAML group mapping needs to be provided using the group object ID (GUID) and not the group name. If you have not set up SSO in your tenant, skip this field and add it later. After you have added it, follow the procedure relevant to your IdP. For example, see Set up Okta as the identity using SAML 2.0 .

3. Create a new user group.

1.6 | Egress configurations

The outgoing communication between tenants and external services is defined either by Cortex or by the user. Using the Egress Configurations feature in the Cortex Gateway, the user can define, manage and approve a tenant's outgoing communication flow, providing greater control over outgoing traffic. Refer to Flows/Path for detailed information on which flows are available for you to create a path for your tenant.

IMPORTANT:

Only Account Admin and Instance Admin can submit a request on behalf of a user. Only users with these roles can view the Egress Configurations option in the Gateway.

The Account Admin can view all the tenants from the account where requests have been submitted, and the Instance Admin can view all the requests that have been submitted for their tenant.

Egress configuration options

In Cortex Gateway, you can use the Egress Configurations for the following options:

- You can create a path.
- You can remove a request that's been approved.
- You can filter by flow.

Egress configuration parameters

After creating a path for your tenant, it is added to the Egress configurations table.

Parameter	Description
Requester	The user who is creating the path. Only Account Admin and Instance Admin can submit a request on behalf of a user.
Requester Email	The email of the requester.
Approver	The approver is the Account Admin or Instance Admin.
Approver Email	The email of the approver.
Route ID	A unique identifier associated with the path.
Status	The status of the egress path, which can be: • Approved • Removed
Date of Request	The date the path was created.
Updated	The date the path was updated.

Flows/Path

The table includes the list of flows that require egress configuration paths before enabling the outgoing traffic.

Flow	Path	Example
GitHub Server	<host> Enter the domain name or IP address of the GitHub instance.	`github.com`
GitHub (Code Scanning)	<repo_owner> Enter the owner or organization name of the repository in GitHub.	`alicesmith`
GitLab Self Managed	<host> Enter the domain name or IP address of the GitLab instance.	`gitlab.com`
GitLab (Code Scanning)	<project_name> Enter the project name within GitLab to allow access.	`myproject`
BitBucket (Code Scanning)	<workspace> Enter the workspace of your project or repository of the BitBucket application.	`engineering-team`

Flow	Path	Example
BitBucket Data Center	<host> Enter the server name of where the BitBucket application is running.	`bitbucket.com`
Azure DevOps (Code Scanning)	<org_name> Enter the name of the organization of the Azure Repos instance.	`myprojectteam`
TF Run Task Cloud	<host> Enter the domain name or IP address of the TF Run Task Cloud instance.	`tfruntask.com`
TF Run Task Enterprise	<host> Enter the domain name or IP address of the TF Run Task Enterprise instance.	`tfruntask.com`
External Storage: S3-compatible	<host> Enter the domain name or IP address of the External Storage: S3-compatible	`s3browser.com`
External Storage: AWS S3	<bucket_name> Enter the name of the AWS S3 bucket to allow access.	`my-example-bucket`

Flow	Path	Example
Snowflake	<host> Enter the host or domain name of the Snowflake account to which you are connecting.	`mycompany.snowflakecomputing.com`
SonarQube	<host> Enter the host address or domain of the SonarQube instance to which you are connecting.	`sonarqube.mycompany.com`
Webhook	<host> Enter the host name of the Webhook endpoint.	`webhook.mycompany.com`
External storage: AWS SQS	<queue_name> Enter the name of the AWS SQS queue.	`my-example-queue`
Splunk	<host> Enter the host or domain name of the Splunk instance.	`splunk.mycompany.com`

Submit a new path

Read more...

Follow the steps to submit a new path.

1. In the Gateway, in the Egress Configurations page, choose the TENANT for which to create a new path.
2. Click +Path:

- Select the Requester from the list of users.
- Select the Flow from the list of data service options:
- In Path, enter the egress configuration path.
- Click Add to create a new path.

3. The path is added to the Egress configuration table, showing the details.

Remove a path

Read more...

Follow the steps to remove a path.

1. In the Gateway, from the Egress configurations table, select a path that's been approved.
2. Right-click and select Remove.
3. In the Remove Path dialog box, click Continue.

   The selected row is greyed out and the Status changes to Removed. This is for auditing purposes.