Get Started: Conditional Access Policies

Archived: 2026-04-05 13:31:35 UTC

Get Started: Conditional Access Policies

To implement Zero Trust security for your organization, create conditional access policies that secure access to resources based on conditions like a user's identity, their network, or the type of device they're on. For example, lock down your environment with policies that deny access when users are on unmanaged devices or unapproved networks. Alternatively, relax access and let users log in to the User Portal without Multi-factor Authentication (MFA) when they're using a VPN or managed device.

Considerations:

- Desktop access policies using Device Trust Certificates are only supported on the following browsers:
  - Windows: Google Chrome, Microsoft Edge
  - macOS: Google Chrome, Safari
  - Linux: Google Chrome
- When Device Trust Certificates are enabled and users use JumpCloud Go to log in to web applications, JumpCloud Go takes precedence over the certificate to verify the device's management status.
- Mobile devices are supported using Mobile Device Trust. See Get Started: Mobile Device Trust to learn more.
- An access policy becomes a conditional access policy when you add a condition. Adding a condition for the User Portal or SSO Applications is a Premium feature and is part of our Platform Prime plan.

Tip:

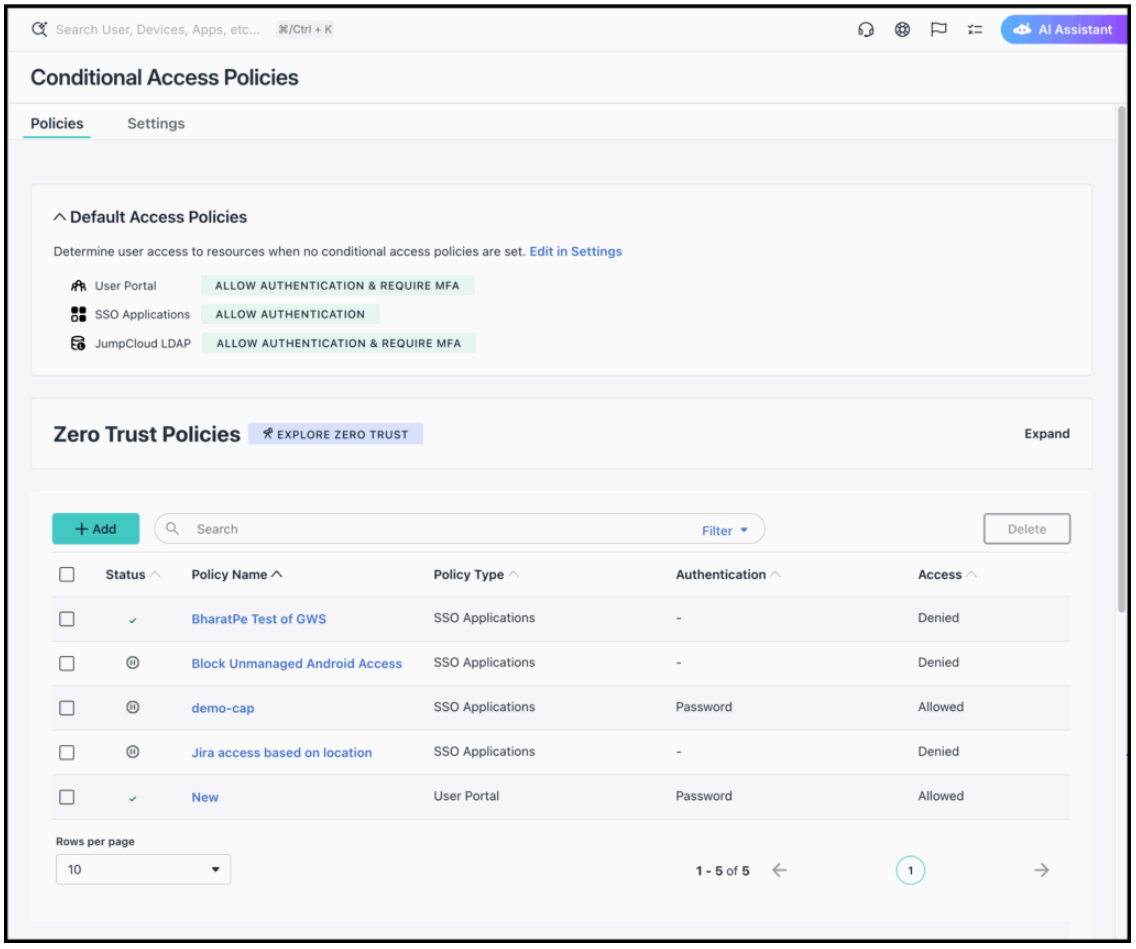
You can remotely apply policies that make your managed devices and third-party apps secure and meet compliance levels. See Get Started: Policies.

Conditional Access Policies List View

To find the list view, log in to the JumpCloud Admin Portal and go to **Security** > **Conditional Access Policies**.

Important:

If your data is stored outside of the US, check which login URL you should be using depending on your region, see JumpCloud Data Centers to learn more.



From the list view you can:

- See a list of the access policies that you've configured.
- To make changes to the default access policies, click **Edit in Settings** under **Default Access Policies**.
- See Set a Default Access Policy
- Configure (or delete) new access policies for the User Portal, SSO Applications, or JumpCloud LDAP.
    - See Configure a Conditional Access Policy
- Access the Conditional Policy Settings page, where you can enable Certificate Distribution, manage Default Access Policies, and customize conditional access deny message displayed to users.
    - To create a custom deny message for users, click the **Custom** tab, and enter the message as required. You can also give a hyperlink to a help article by clicking the **Link** toggle key.

Understanding Policy Precedence

Tip:

Conditional Access Policies work in conjunction with Default Access Policies. If none of the set access policies apply to a user, the Default Access Policies are enforced as fallback policies.

Before you create several access policies, it's important to understand policy precedence so that you don't accidentally lock out your users. When you have several policies enabled, the policy precedence is the following:

- A policy set to deny access is first priority.
- A policy set to allow access with MFA is second priority.
- A policy set to allow access without MFA is third priority.

This means if several policies with different actions apply to a single user, the policy that denies access takes effect over policies that allow access with or without MFA.

For example: consider these two policies:

- One policy denies access to the User Portal if a user isn't on an approved network (conditional). You include a specific user group with this policy.
- Another policy allows access to the user portal with MFA. You include all your users with this policy.

Result: If a user is included in both policies and they try to log in to the User Portal from an unapproved network, they're denied access.

With that in mind, we recommend being very specific when you create a policy that denies access. If you're not careful, you could prevent your users from being able to access resources.

When no conditional access policies apply to a user, the Default Access Policy takes effect. For example, say you have:

- An access policy that allows access without MFA.
- A user who isn't included in the policy.
- The Default Access Policy set to allow access with MFA.

In this case, the user is required to authenticate with MFA.

Supported Resources

You can create access policies for the User Portal, SSO applications, and LDAP applications. An access policy becomes a conditional access policy when you add a condition. Adding a condition for the User Portal or SSO Applications is a Premium feature and is part of our Platform Prime plan.

A policy can only have one resource type associated with it, so you can't have one policy that applies to both the User Portal and SSO Applications.

- User Portal: Configure a policy that relaxes, restricts, or denies access to the User Portal.
    - For example, use a device condition to let users log in to the User Portal without MFA when they're on a JumpCloud-managed device, or set a policy across all your users that requires MFA to access the User Portal.

Important:

To avoid account lockout and password reset failure issues, we recommend informing your users to set up an MFA factor in their User Portal **before** you apply a conditional access policy to the User Portal. For user instructions on how to do this, see Set up an Authenticator App.

You can also enable your users to reset their password when MFA is enforced for the User Portal but they have not yet enrolled. See Manage Password and Security Settings.

- SSO Applications: Use a policy to relax, restrict or deny access to SSO applications when users access them from the User Portal or through service provider-initiated authentication.
    - For example, enable a policy for your software engineer user groups that requires them to use MFA when they access AWS and GitHub applications.
- LDAP Applications: Use a policy to relax, restrict or deny access to LDAP applications when users access them from the User Portal.
    - For example, enable a policy for your users that requires them to use MFA when accessing the VPN.
    - Note that conditions are not applicable for LDAP access policies.

Note:

If you plan to create policies that require MFA, you need to set up MFA in **SECURITY MANAGEMENT** > **MFA Policies**. See MFA Guide for Admins to decide which type of MFA to set up.

When you create an access policy that requires MFA, users who are included in the policy but don't have MFA set up will be required to enroll in MFA the next time they log in to the User Portal.

- Admin Portal: Use a policy to relax, restrict or deny access to Admin portal when Admins access it. See Configuring Conditional Access Policies For Admin Portal to learn more.

Supported Conditions

Configure your access policies with conditions to control level of access to the User Portal, SSO Applications, and Admin Portal. Conditions are a premium feature and are part of the Platform Prime plan.

Examples of ways to leverage conditions to support your security posture include:

- **Device Management**

    - Block access to work applications from unmanaged devices.
    - Require users to use MFA when they access work applications on managed devices.
- **Disk Encryption**
    - Deny access to resources when the device does not have disk encryption enabled.
- **Location**
    - Block access to secure resources when the authentication request is coming from an unknown or untrusted country.
- **IP Address**
    - Relax MFA requirements if the request to authenticate is coming from inside the corporate network.
    - Require step-up authentication when the request to authenticate is coming from outside a trusted network.
- **Operating System**
    - Enable granular control and target specific device types by operating system in a policy. For example:
        - Configure a policy with the Device Management condition to block devices not managed by JumpCloud, but add the Operating System condition for macOS, Windows, and Linux. This allows access for mobile devices, while preventing access from unmanaged desktop devices.
        - Or configure a policy with the Device Management condition and use the Operating System condition to target mobile devices specifically (iOS/iPad OS and Android).

Was this information helpful?

Still Have Questions?

If you cannot find an answer to your question in our FAQ, you can always contact us.

Submit a Case

- **Functional Cookies**
- **Targeting Cookies**

Your Privacy

When you visit any website, it may store or retrieve information on your browser, mostly in the form of cookies. This information might be about you, your preferences or your device and is mostly used to make the site work as you expect it to. The information does not usually directly identify you, but it can give you a more personalized web experience. Because we respect your right to privacy, you can choose not to allow some types of cookies. Click on the different category headings to find out more and change our default settings. However, blocking some types of cookies may impact your experience of the site and the services we are able to offer.
More information

Strictly Necessary Cookies

These cookies are necessary for the website to function and cannot be switched off in our systems. They are usually only set in response to actions made by you which amount to a request for services, such as setting your privacy preferences, logging in or filling in forms. You can set your browser to block or alert you about these cookies, but some parts of the site will not then work. These cookies do not store any personally identifiable information.

Performance Cookies

These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us to know which pages are the most and least popular and see how visitors move around the site. All information these cookies collect is aggregated and therefore anonymous. If you do not allow these cookies we will not know when you have visited our site, and will not be able to monitor its performance.

Functional Cookies

These cookies enable the website to provide enhanced functionality and personalisation. They may be set by us or by third party providers whose services we have added to our pages. If you do not allow these cookies then some or all of these services may not function properly.

Targeting Cookies

These cookies may be set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant adverts on other sites. They do not store directly personal information, but are based on uniquely identifying your browser and internet device. If you do not allow these cookies, you will experience less targeted advertising.

Your Privacy [`dialog closed`]

Source: https://jumpcloud.com/support/get-started-conditional-access-policies