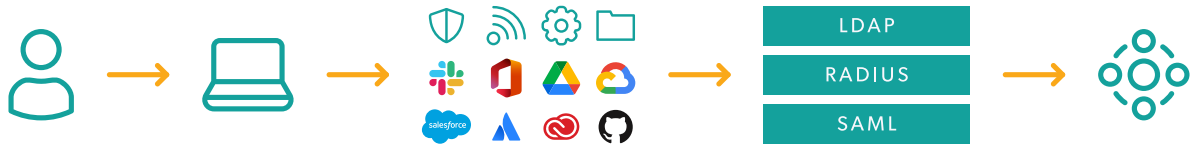
jumpcloud™

Guide

Implementation Guide
SSO & RADIUS

Get to Know JumpCloud

JumpCloud is a comprehensive and flexible cloud directory platform. From one pane of glass, manage user identities and resource access, secure macOS, Windows, and Linux devices, and get a full view of your environment.



As you implement JumpCloud into your organization it is important to understand the best practices related to getting your existing users onboarded, enrolling devices while taking over existing user accounts, integrating with existing IT tools, and enabling user access to all their resources. Implementing resources in piecemeal fashion without a cohesive plan could result in wasted time and a poor user experience. For example, users who come from a preexisting directory (e.g., Active Directory/Azure AD) or an MDM will have a different implementation pathway than organizations implementing a directory platform solution for the first time. Be sure to take advantage of the following resources to streamline your implementation.

Sign up for an account in JumpCloud University!

Check out this easy-to-follow infographic for the steps to register for a free account.

JCU gives you access to many resources including interactive courses, short tutorial videos, hands-on practice with guided simulations, and help from our experts. Plus, your progress is saved and tracked as you go.

This quick 30-minute course is a great introduction to JumpCloud and is designed to help familiarize you with JumpCloud University.

What is JumpCloud?

Become certified through JCU!

Why get certified:

- Feel more confident in your ability to use the JumpCloud platform.
- Be the go-to JumpCloud admin for your IT org.
- Showcase your skills by displaying your certification badge on your professional profiles.

Phase 4: SSO

Configure SAML App Integration (if applicable)

JumpCloud's Directory-as-a-Service gives your organization's employees access to supported applications using their JumpCloud credentials. This centralized method of identity uses one set of employee credentials to gain access to all applications, versus creating individual logins for each application. This single sign-on (SSO) workflow lets the JumpCloud-managed identity be asserted via the SAML protocol to an application.

Using SAML (SSO) Applications with JumpCloud

1. Select an App

Select an application you want to connect with JumpCloud through SAML 2.0-based SSO.

You may see some applications in the list with a beta flag. We're currently evaluating these connectors in various real-world environments so we can gather feedback to enhance their performance.

You may see some applications with a JIT provisioning label. This signals that you can provision users to that application using Just-In-Time provisioning. Learn about SAML-supported JIT provisioning.

Some applications use a shared login with the services they provide. For example, the Atlassian connector provides SSO to JIRA, Confluence, and Bitbucket. When you search for these applications, the Atlassian connector shows up in the search results because it's the connector the applications share a login with.

You can connect on-prem/legacy applications that use LDAP to JumpCloud's LDAP services. See Using JumpCloud's LDAP-as-a-Service.

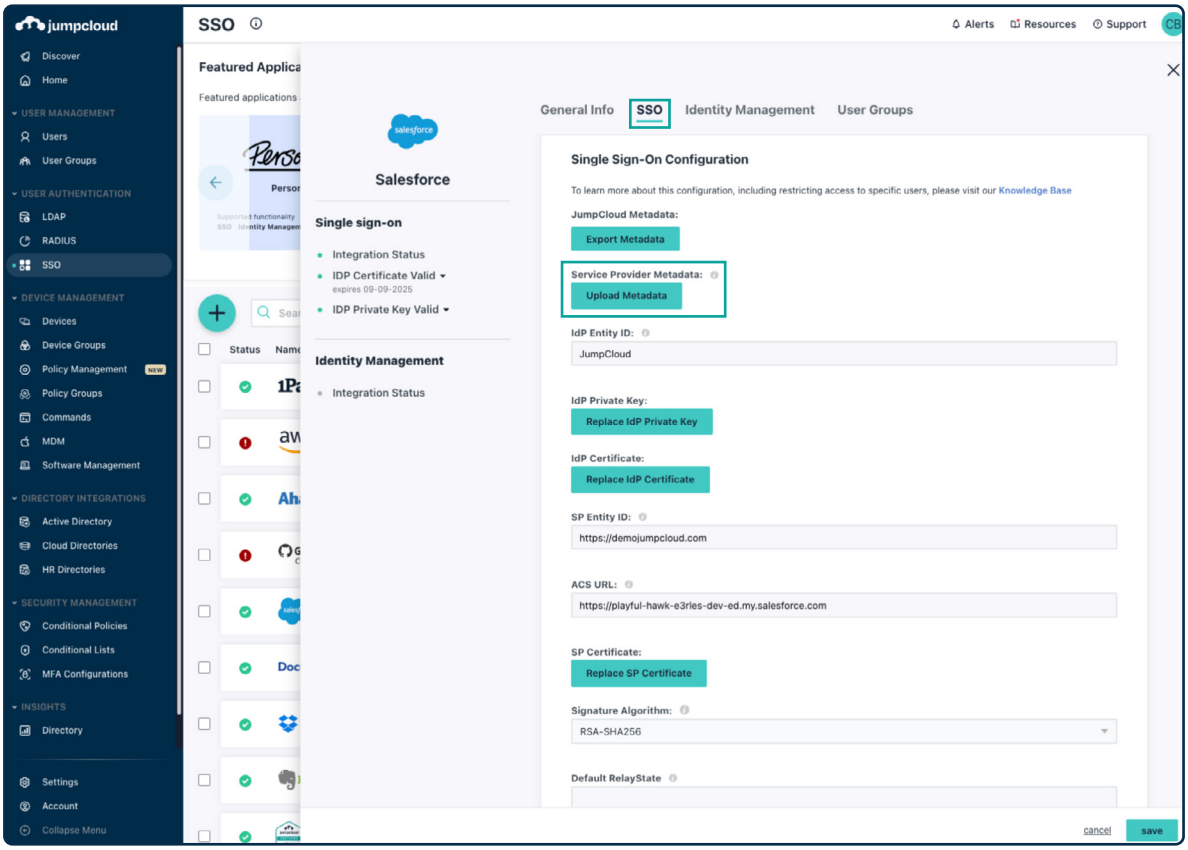
2. Configure Your App

You can set various SAML configurations with JumpCloud acting as the app's "IdP," or identity provider. Each application connector has explicit instructions required to establish the connection. Refer to an application's SAML/SSO connection documentation for information on setting up your application to integrate with JumpCloud.

3. Upload a Metadata File

You can upload service provider application XML metadata files to populate connector attributes for applications.

To apply a metadata file for an application you're connecting, select Upload Metadata. Navigate to the file you want to upload, then select Open. You'll see a confirmation of a successful upload.



Tip: Be aware that if you upload more than one metadata file, you'll overwrite the attribute values applied in the previously uploaded file.

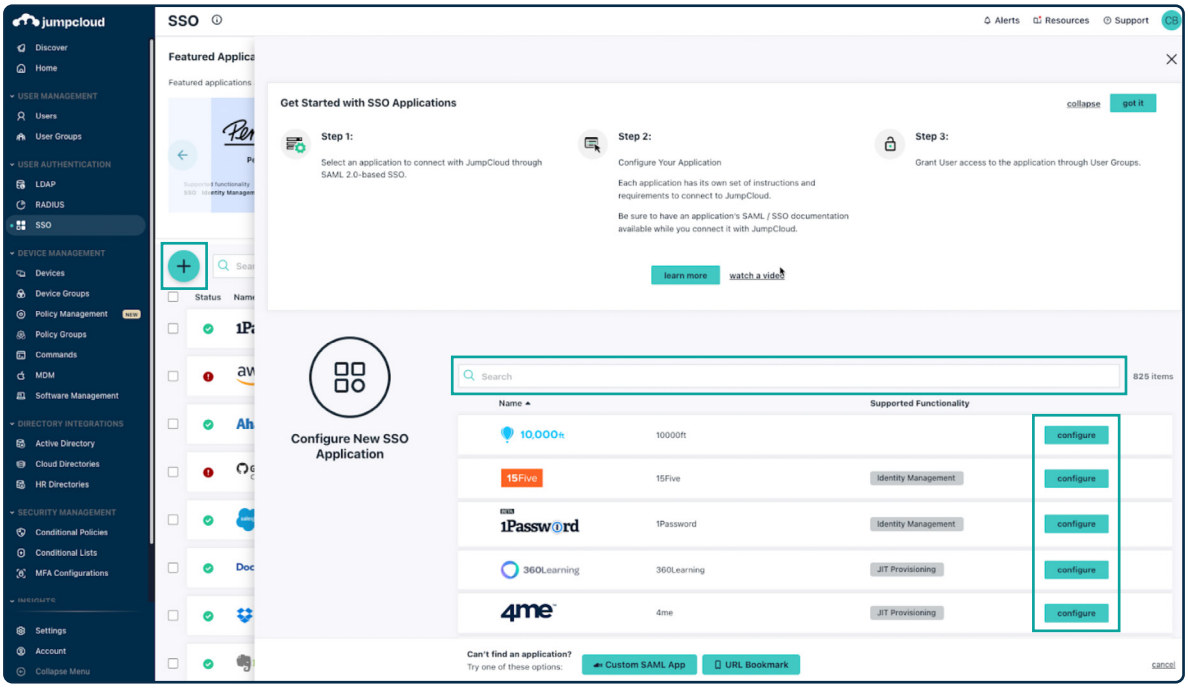
4. Connect Your App to a User Group

After you connect the application to JumpCloud, you can connect it to user groups. Members of connected groups gain access to the application through SAML. They see the application icon in the User Portal in Applications. Many service provider applications allow users to log in from their application. If users log in from the application, they are redirected to JumpCloud for SAML authentication.

Setting Up SAML-Based SSO with an Application

To connect an application to JumpCloud:

1. Log in to the JumpCloud Admin Portal.
2. Go to User Authentication > SSO, then select (+). The Configure New Application panel appears.
3. Search for an application by name using the search bar at the top of the panel.
4. When you find the application you want to connect, select configure.



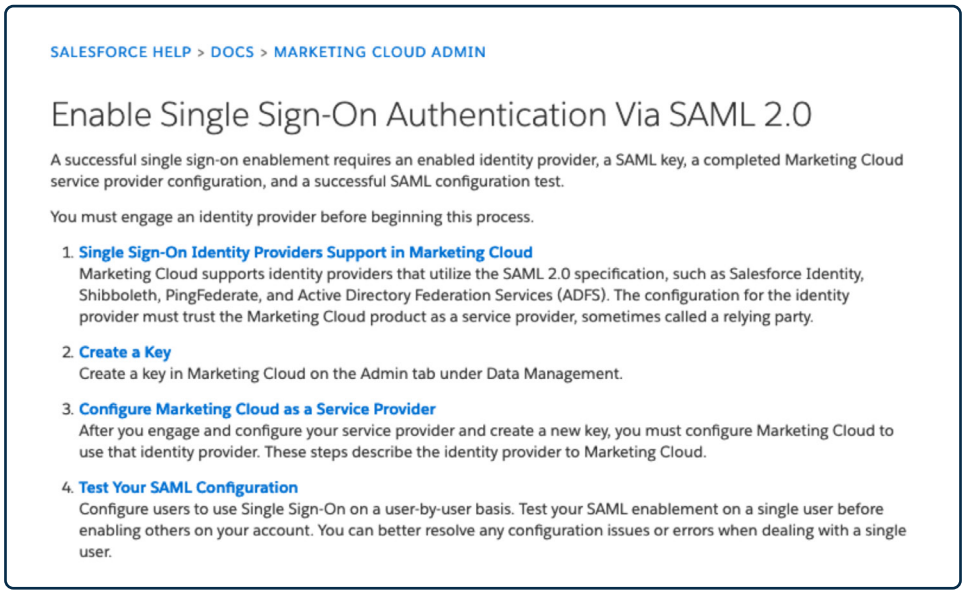
If there isn't a connector for an application you want to connect to JumpCloud, check out this Knowledge Base article to learn how to connect that app to JumpCloud using the SAML 2.0 Connector:

Single Sign On (SSO) with SAML 2.0 Connector (Custom SAML App)

Configuring Authentication from the Application Service Provider

The service provider (SP) typically provides SAML configuration parameters to set up SSO from a compatible IdP like JumpCloud.

The following image shows Salesforce instructions for setting up the Marketing Cloud for SAML SSO.

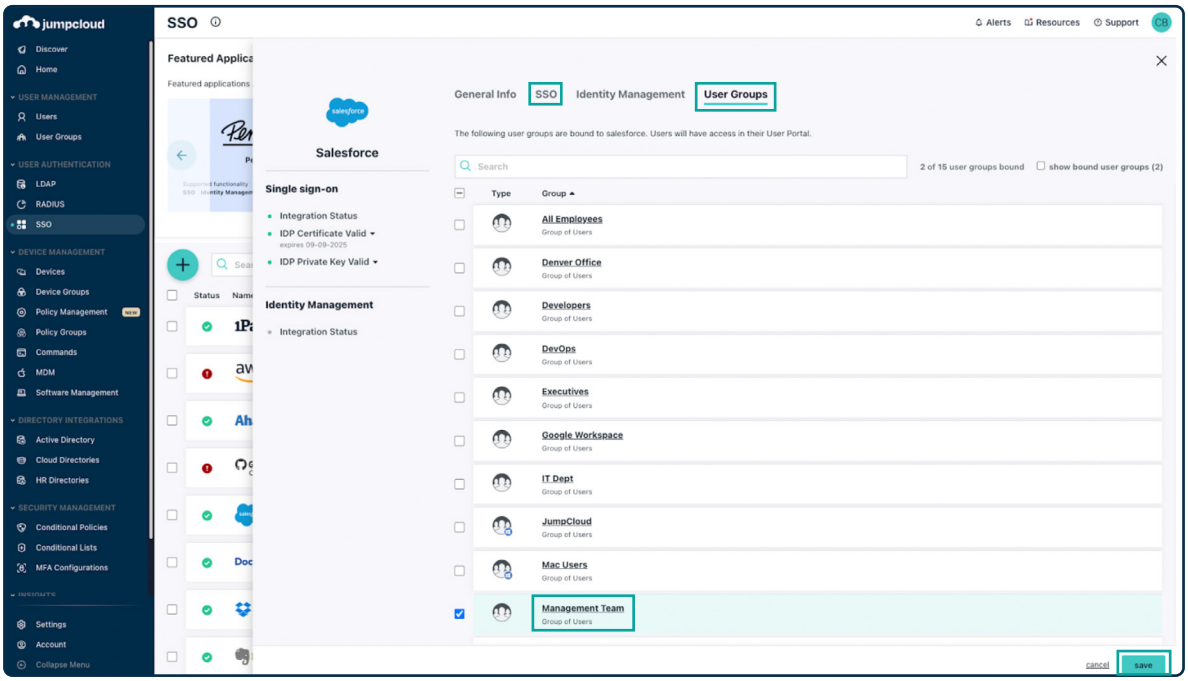


Managing Employee Access to Applications

Users are implicitly denied access to all JumpCloud resources, including applications. JumpCloud admins must explicitly grant access to SSO applications through the use of user groups.

To grant access to a user group:

1. Log in to the JumpCloud Admin Portal.
2. If you haven't already created a user group, create a new group.
3. If the group exists, in the Admin Portal, go to User Authentication > SSO.
4. Select the SSO application.
5. On the Application panel, select the User Groups tab.
6. Select the user group, then select save.



For more information on SSO, watch this tutorial:

Configuring an SSO Application

End-User Experience

To further understand the user experience, refer to the following Knowledge Base articles.

After you configure both the IdP and SP for SSO, employees can access the applications in two ways:

IdP-Initiated – Access from the JumpCloud User Portal

SP-Initiated – Access directly from the application

Configure JIT App Integration (if applicable)

Just-in-Time (JIT) provisioning lets you onboard new users to single sign-on (SSO) applications more efficiently. When JIT provisioning is in use, you don't have to manually create new user accounts in an application. Instead, a user account is created when a user authenticates into an application for the first time using SSO. JumpCloud supports the use of JIT provisioning by including the user attributes a service provider requires for account creation.

Benefits

JIT provisioning lets you automate user provisioning to SSO applications, giving you more time to focus on higher value projects. End users also benefit by gaining faster access to the SSO applications they need to do their jobs.

How JIT Provisioning Works

The typical JIT provisional workflow looks like this:

1. Enable JIT provisioning in the service provider.
2. Configure the appropriate SAML SSO connector in the identity provider and service provider, making sure to set up the JIT required user attributes.
3. Authorize a user's access to the application in the identity provider.

To complete the provisioning process, a user logs in to the application using SSO. The SAML assertion passes from the identity provider to the service provider, and gives the service provider the information it needs to create the user account.

This Knowledge Base article will walk you through the steps of SAML supported JIT provisioning:

SAML Supported JIT Provisioning

Configure SCIM App Integration (if applicable)

JumpCloud Identity Management Connectors

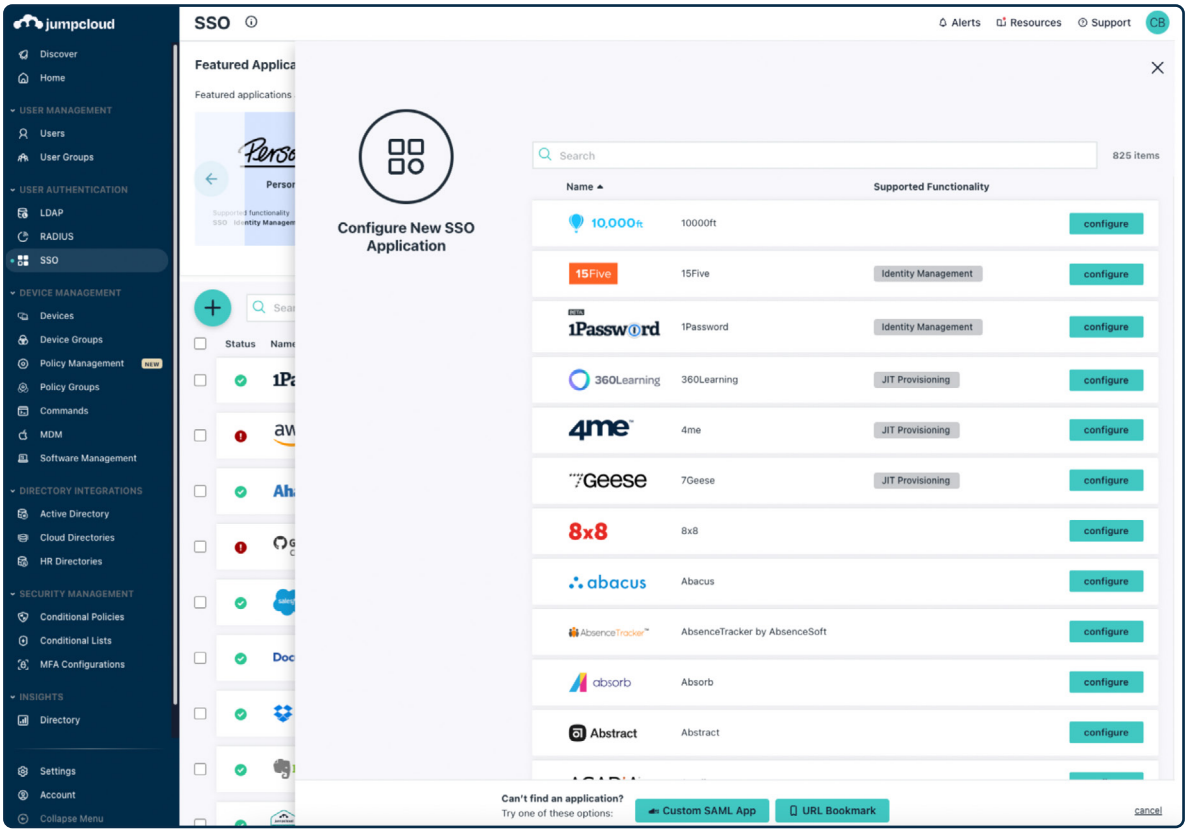
These integrations allow you to automate and centralize user and group management, depending on the application's group management support, through the full lifecycle from your JumpCloud Admin Portal. Connect the applications your organization uses with JumpCloud. Our Identity Management Connectors manage application user accounts through the Identity Management (SCIM) protocol.

As your company grows and experiences employee churn, you can easily manage application user accounts with Identity Management Connectors. After you integrate an application with JumpCloud, depending on an application's Identity Management action support, you can provision, update, and deprovision users.

To find applications you can integrate with JumpCloud using Identity Management Connectors:

1. Log in to the JumpCloud Admin Portal.
2. Go to USER AUTHENTICATION > SSO. If you've connected any applications with JumpCloud, you will see them in this list.
3. To connect a new application, select (+).

Applications that you can integrate with JumpCloud through an Identity Management Connector can be found on the Configure New Applications panel. The supported ones have a User Export listed under the Supported Functionality column.



Phase 5: RADIUS

Create a RADIUS Endpoint in JumpCloud

JumpCloud's cloud-based RADIUS service extends your organization's user JumpCloud credentials to your Wi-Fi and other resources that support the RADIUS protocol. Each RADIUS server you add to JumpCloud can be connected to user groups, segmenting which users can access specific resources.

By leveraging your users' JumpCloud credentials for your network, you can ensure secure access and easy provisioning/deprovisioning to users. You'll also get access to prebuilt, preconfigured, and fully managed RADIUS servers.

You can proceed to the instructions below or follow along with this course that guides you through adding RADIUS as a Server:

Configuring RADIUS

Add a RADIUS Server

1. Log in to the JumpCloud Admin Portal.
2. Go to RADIUS.
3. Select (+). The New RADIUS server panel appears.
4. Configure the RADIUS server:
    - Enter a name for the server. This value is arbitrary.
    - Enter a public IP address from which your organization's traffic will originate.
    - Provide a shared secret. This value is shared with the device or service endpoint you're pairing with the RADIUS server.

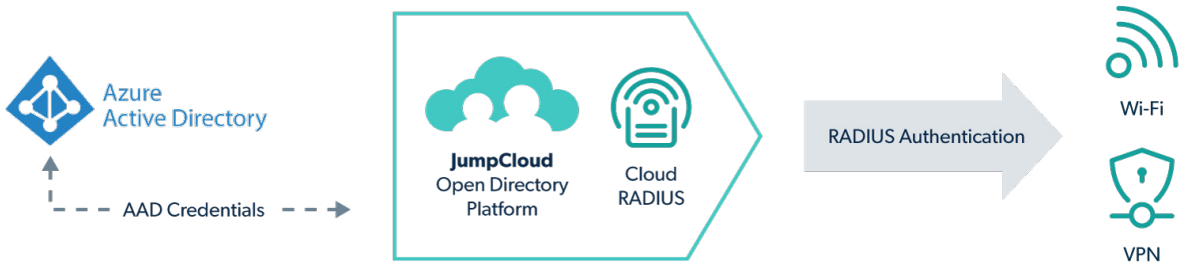
Set Up Primary Authentication

1. To select how your users will authenticate into this RADIUS server, select the Authentication tab and choose an Identity Provider from the dropdown menu.

    If the selection is Azure AD, users will be able to access this RADIUS server using their existing Azure AD credentials. MFA cannot be configured when Azure AD is the identity provider.

    Important:

    - Once Azure AD is selected and confirmed, this selection cannot be changed without deleting this RADIUS configuration and starting over.
    - Azure AD doesn't pass the user's password to JumpCloud, so the user remains in a Password Pending status. If an Azure AD organization is using JumpCloud exclusively for RADIUS, admins do not require users to create a password in JumpCloud, so the Password Pending status can be ignored.



2. If the selection is JumpCloud, the multi-factor authentication (MFA) configuration section will be available.

Configure Your Wireless Access Point (WAP)

Check out this Knowledge Base article to learn more about configuring your WAP.

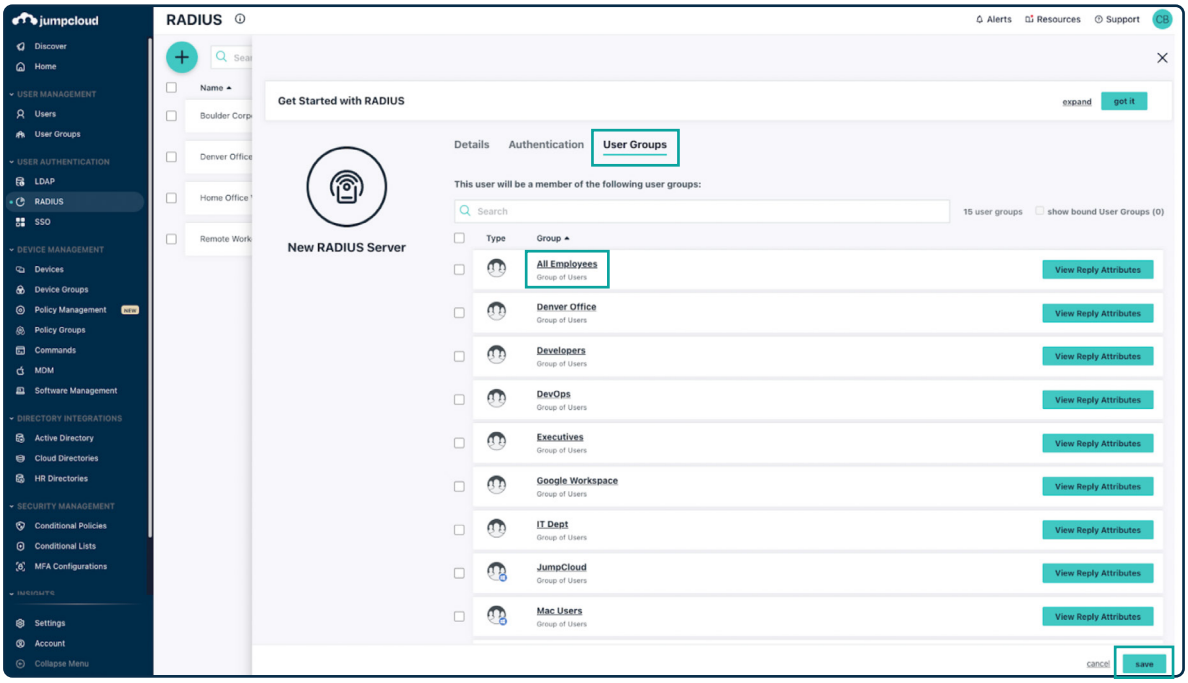
Configuring a Wireless Access Point (WAP), VPN, or Router for JumpCloud's RADIUS

Configure Multi-Factor Authentication for the RADIUS Server

1. Select the Authentication tab. If using JumpCloud as the identity provider, the MFA configuration section will be available.
2. Toggle the MFA requirement option to "On" for this server. This option is "Off" by default.
3. Select Require MFA on all users or only require MFA on users enrolled in MFA.
   - If selecting Require MFA on all users, a sub-bullet allows you to exclude users in a TOTP enrollment period, but this does not apply to JumpCloud Protect (users in a TOTP enrollment period who are successfully enrolled in Protect will still be required to complete MFA).
   - If JumpCloud Protect is not yet enabled, users can select the Enable Now link.

Grant User Groups Access to the RADIUS Server

1. To grant access to the RADIUS server, select the User Groups tab then select the appropriate groups of users you want to connect to the server.



2. Select save.

Note: Users who are granted access to a RADIUS server that will authenticate with the IdP of Azure AD must be imported into JumpCloud and then assigned to a User Group.

Enable MFA for RADIUS Networks (if applicable)

To configure RADIUS MFA for an existing server:

1. Log in to the JumpCloud Admin Portal.
2. Go to User Authentication > RADIUS.
3. Select an existing RADIUS server.
4. Configure TOTP multi-factor authentication for the RADIUS server:
    - Toggle the MFA requirement for this RADIUS server option to "On" to enable MFA for this server. This option is disabled by default.
    - Select Require MFA on all users or only require MFA on users enrolled in MFA. If selecting Require MFA on all users, a sub-bullet allows you to exclude users in a TOTP enrollment period.
5. Select save.

The RADIUS MFA settings have been updated from a previous version:

- Require MFA on all users (previously was Challenge all users, including during an enrollment period)
- Require MFA on all users, but exclude users in TOTP enrollment period (previously was Challenge all users, unless they are in an enrollment period)
- Only require MFA on users enrolled in MFA (previously was Challenge active TOTP MFA users)

Configure RADIUS Reply Attributes for User Groups (if applicable)

Get the strength and security of RADIUS without building, maintaining, or monitoring physical servers. It's quick to roll out managed RADIUS to your organization to authenticate users to Wi-Fi, VPNs, switches, and network devices securely. Read this article to learn how to use functions in the JumpCloud PowerShell module to configure RADIUS reply attributes like VLAN tagging for user groups.

Configure RADIUS Reply Attributes for User Groups in the API