User Accounts and Roles

Cloud Insights

Tony Lavoie
August 31, 2021

Table of Contents

User Accounts and Roles

Cloud Insights provides up to four user account roles: Account Owner, Administrator, User, and Guest. Each account is assigned specific permission levels as noted in the table below. (Note that *User* and *Guest* roles are not available in the Cloud Secure feature.). Users are either invited to Cloud Insights and assigned a specific role, or can sign in via Single Sign-On (SSO) Authorization with a default role. SSO Authorization is available as a feature in Cloud Insights Premium Edition.

Permission levels

You use an account that has Administrator privileges to create or modify user accounts. Each user account is assigned a role for each Cloud Insights feature from the following permission levels.

Role	Monitoring	Cloud Secure	Reporting
Account Owner	Can modify subscriptions, view billing and usage information, and perform all Administrator functions for Monitoring & Optimization, Cloud Secure, and Reporting. Owners can also invite and manage users, as well as manage SSO Authentication and Identity Federation settings. The first Account Owner is created when you register for Cloud Insights. It is strongly recommended to have at least two Account Owners for each Cloud Insights environment.		
Administrator	Can perform all Monitoring & Optimization functions, all user functions, as well as management of data collectors, API keys, and notifications. An Administrator can also invite other users but can only assign Monitor and Optimize roles.	Can perform all Cloud Secure functions, including those for Alerts, Forensics, data collectors, automated response policies, and APIs for Cloud Secure. An Administrator can also invite other users but can only assign Cloud Secure roles.	Can perform all User/Author functions, as well as all administrative tasks such as configuration of reports, and the shutdown and restart of reporting tasks. An Administrator can also invite other users but can only assign Reporting roles.
User	Can view and modify dashboards, queries, alerts, annotations, annotation rules, and applications, and manage device resolution.	n/a	Can perform all Guest/Consumer functions as well as create and manage reports and dashboards.

Role	Monitoring	Cloud Secure	Reporting
Guest	Has read-only access to asset pages, dashboards, alerts, and can view and run queries.	n/a	Can view, schedule, and run reports and set personal preferences such as those for languages and time zones. Guests/Consumers cannot create reports or perform administrative tasks.

Best practice is to limit the number of users with Administrator permissions. The greatest number of accounts should be user or guest accounts.

Cloud Insights Permissions by User Role

The following table shows the Cloud Insights permissions granted to each user role.

Feature	Administrator/ Account Owner	User	Guest
Acquisition Units: Add/Modify/Delete	Y	N	N
Alerts*/Policies: Create/Modify/Delete	Y	Y	N
Alerts*/Policies: View	Y	Y	Y
Annotation Rules: Create/Run/Modify/Delete	Y	Y	N
Annotations: Create/Modify/Assign/View/Remove/Delete	Y	Y	N
API Access*: Create/Rename/Disable/Revoke	Y	N	N
Applications: Create/View/Modify/Delete	Y	Y	N
Asset Pages: Modify	Y	Y	N
Asset Pages: View	Y	Y	Y
Audit: View	Y	N	N
Cloud Cost	Y	N	N
Cloud Secure*	Y	N	N
Dashboards: Create/Modify/Delete	Y	Y	N
Dashboards: View	Y	Y	Y

Data Collectors: Add/Modify/Poll/Delete	Y	N	N
Notifications: View/Modify	Y	N	N
Queries: Create/Modify/Delete	Y	Y	N
Queries: View/Run	Y	Y	Y
Device Resolution	Y	Y	N
Reports*: View/Run	Y	Y	Y
Reports*: Create/Modify/Delete/Schedule	Y	Y	N
Subscription: View/Modify	Y	N	N
User Management: Invite/Add/Modify/Deactivate	Y	N	N

*Requires Premium Edition

Creating Accounts by Inviting Users

Creating a new user account is achieved through Cloud Central. A user can respond to the invitation sent through email, but if the user does not have an account with Cloud Central, the user needs to sign up with Cloud Central so that they can accept the invitation.

Before you begin

- The user name is the email address of the invitation.
- Understand the user roles you will be assigning.
- Passwords are defined by the user during the sign up process.

Steps

1. Log into Cloud Insights
2. In the menu, click **Admin > User Management**

   The User Management screen is displayed. The screen contains a list of all of the accounts on the system.

3. Click **+ User**

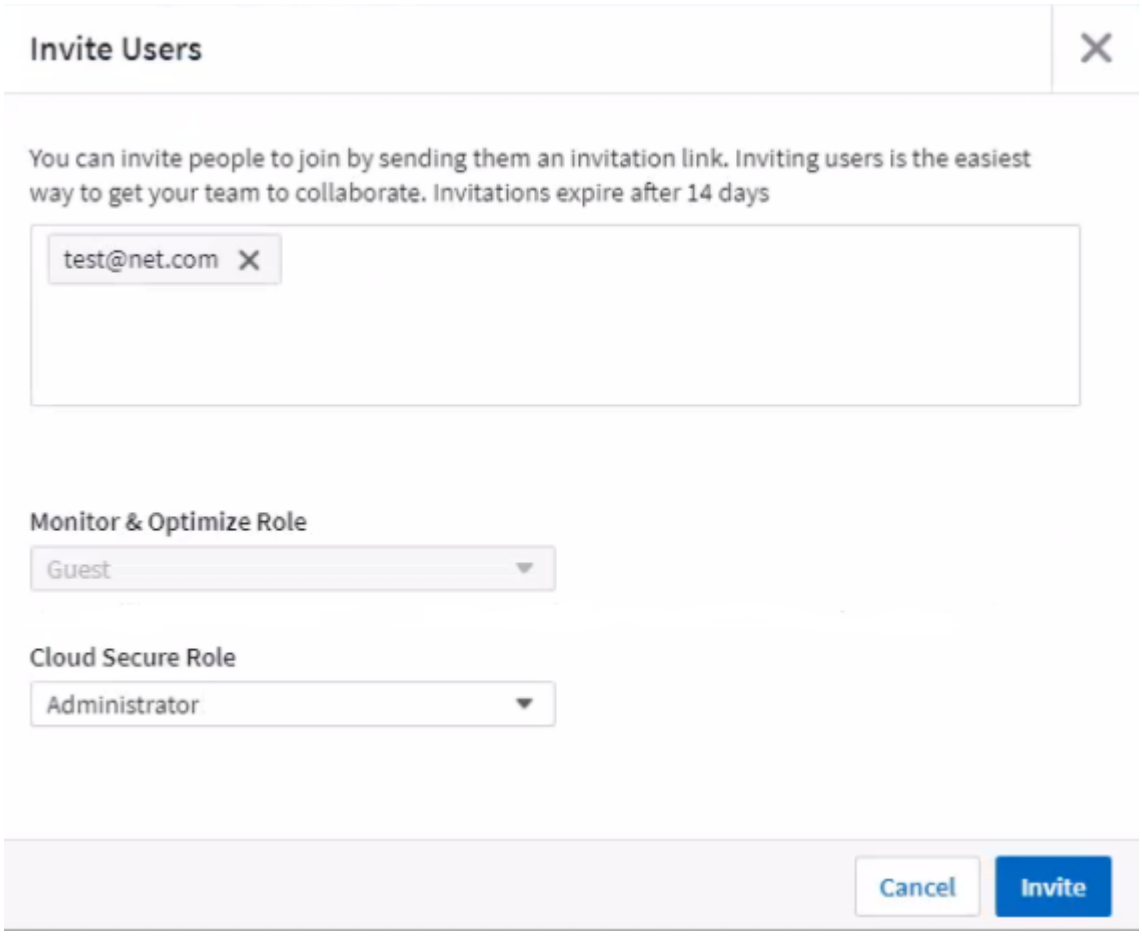
   The **Invite User** screen is displayed.

4. Enter an email address or multiple addresses for invitations.

   Note: When you enter multiple addresses, they are all created with the same role. You can only set multiple users to the same role.

1. Select the user's role for each feature of Cloud Insights.

The features and roles you can choose from depend on which features you have access to in your particular Administrator role. For example, if you have Admin role only for Reporting, you will be able to assign users to any role in Reporting, but will not be able to assign roles for Monitor and Optimize or Cloud Secure.



2. Click **Invite**

   The invitation is sent to the user. Users will have 14 days to accept the invitation. Once a user accepts the invitation, they will be taken to the NetApp Cloud Portal, where they will sign up using the email address in the invitation. If they have an existing account for that email address, they can simply sign in and will then be able to access their Cloud Insights environment.

Deleting Users

A user with the Administrator role can delete a user (for example, someone no longer with the company) by clicking on the user's name and clicking *Delete User* in the dialog. The user will be removed from the Cloud Insights environment.

Note that any dashboards, queries, etc. that were created by the user will remain available in the Cloud Insights environment even after the user is removed.

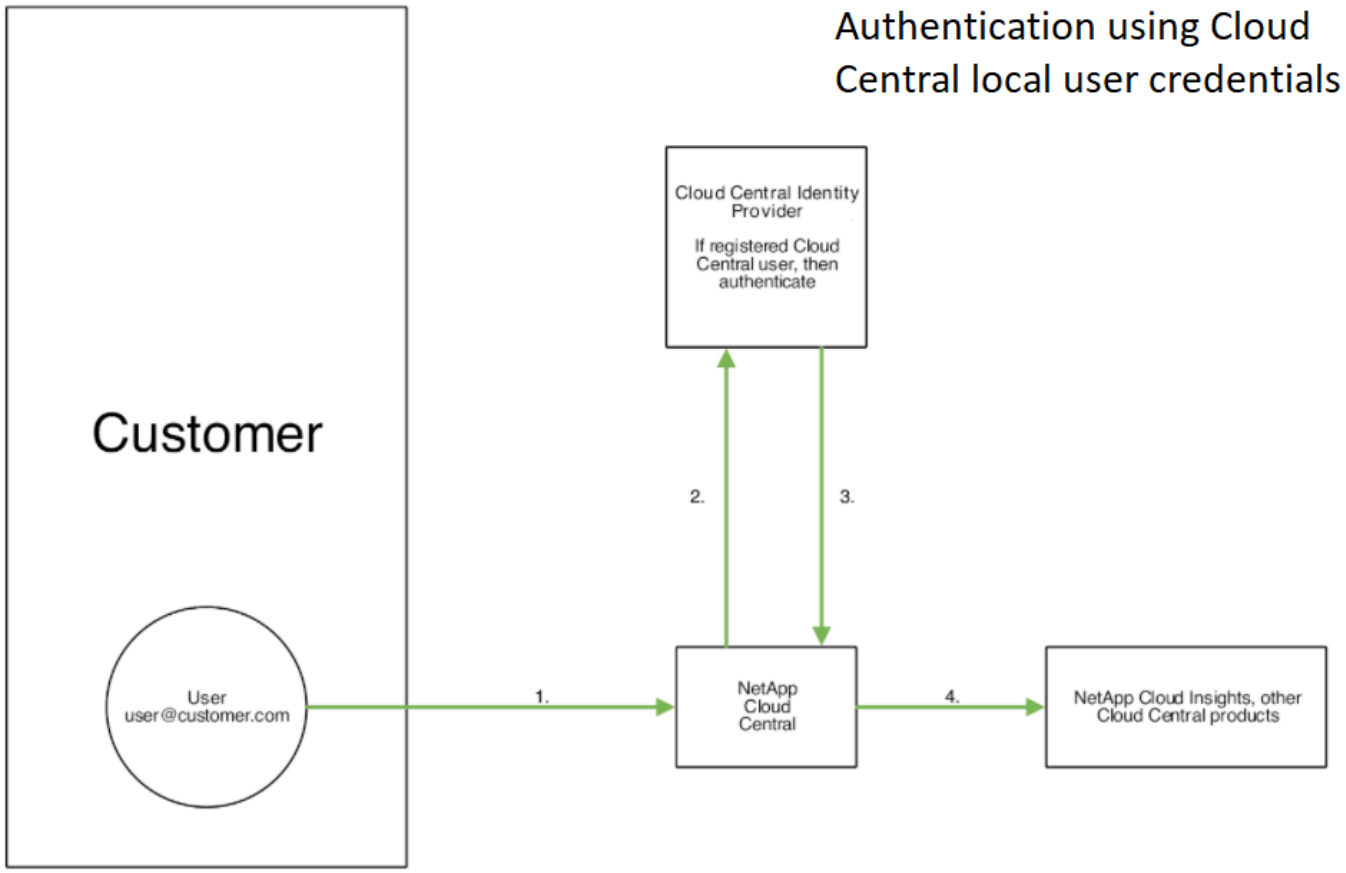
Single Sign-On (SSO) and Identity Federation

Enabling Identity Federation for SSO In Cloud Insights

With Identity Federation:

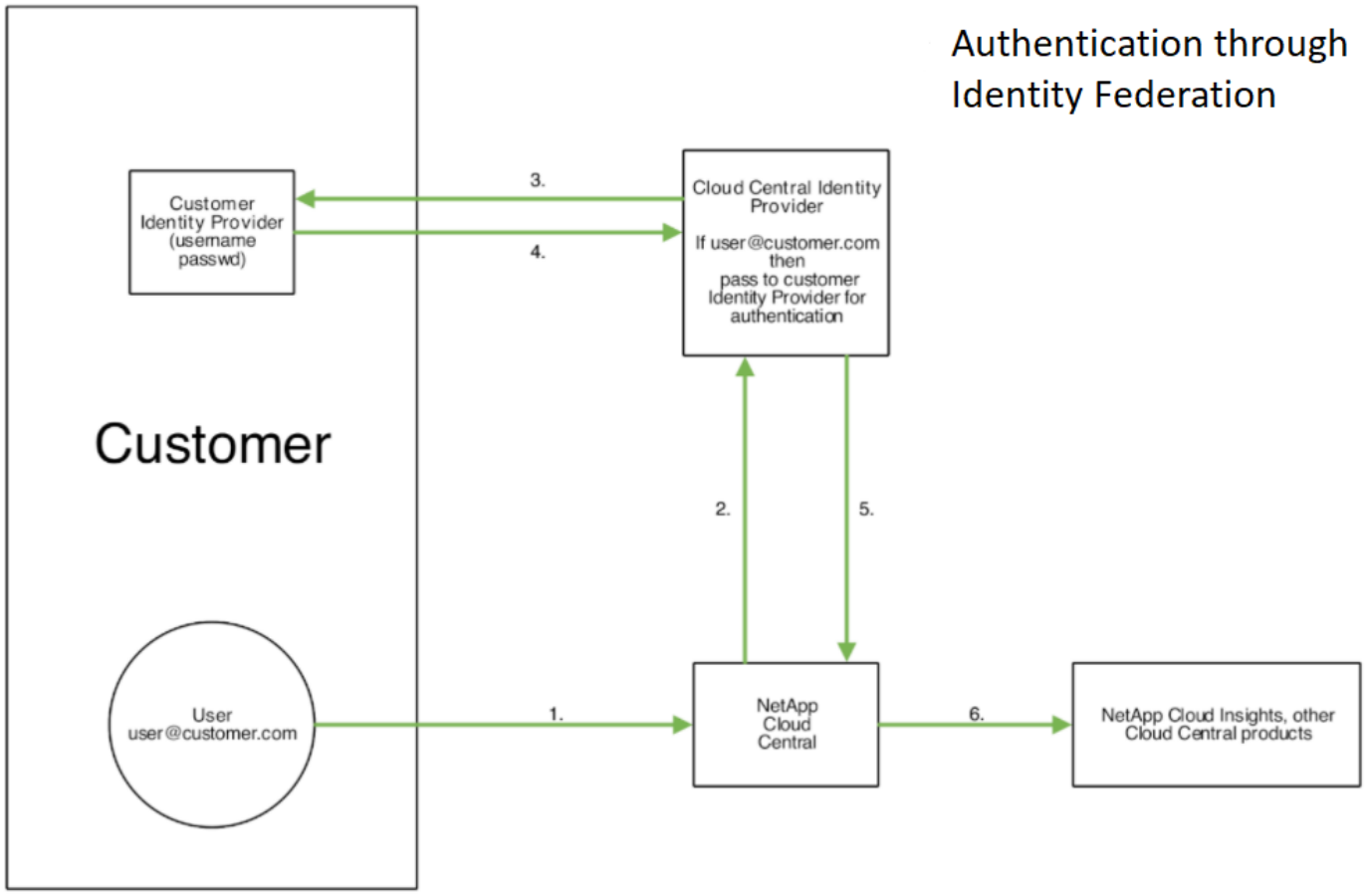
- Authentication is delegated to the customer's identity management system, using the customer's credentials from your corporate directory, and automatization policies such as Multi-Factor Authentication (MFA).
- Users log in once to all NetApp Cloud Services (Single Sign On).

User accounts are managed in NetApp Cloud Central for all Cloud Services. By default, authentication is done using Cloud Central local user profile. Below is a simplified overview of that process:



However, some customers would like to use their own identity provider to authenticate their users for Cloud Insights and their other NetApp Cloud Central Services. With Identity Federation, NetApp Cloud Central accounts are authenticated using credentials from your corporate directory.

The following is a simplified example of that process:



In the above diagram, when a user accesses Cloud Insights, that user is directed to the customer's identity management system for authentication. Once the account is authenticated, the user is directed to the Cloud Insights tenant URL.

Cloud Central uses Auth0 to implement Identity Federation and integrate with services like Active Directory Federation Services (ADFS) and Microsoft Azure Active Directory (AD). For more information on Identity Federation setup and configuration, see Cloud Central documentation on Identity Federation.

It is important to understand that changing identity federation in Cloud Central will apply not only to Cloud Insights but to all NetApp Cloud Services. The customer should discuss this change with the NetApp team of each Cloud Central product they own to make sure the configuration they are using will work with Identity Federation or if adjustments need to be made on any accounts. The customer will need to involve their internal SSO team in the change to identity federation as well.

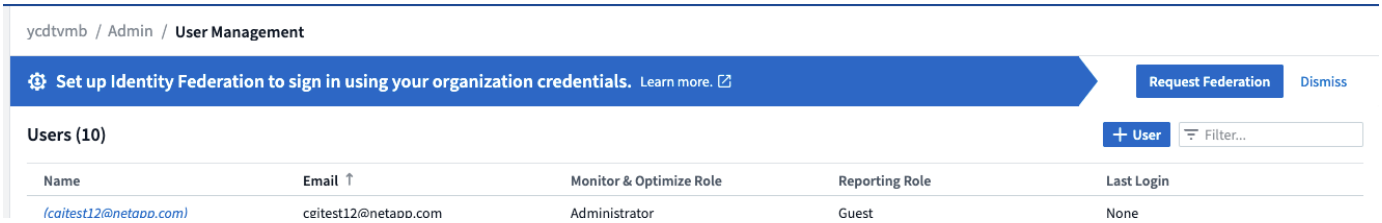
It is also important to realize that once identity federation is enabled, that any changes to the company's identity provider (such moving from SAML to Microsoft AD) will likely require troubleshooting/changes/attention in Cloud Central to update the profiles of the users.

Single Sign-On (SSO) User Auto-Provisioning

In addition to inviting users, administrators can enable **Single Sign-On (SSO) User Auto-Provisioning** access to Cloud Insights for all users in their corporate domain, without having to invite them individually. With SSO enabled, any user with the same domain email address can log into Cloud Insights using their corporate credentials.

SSO User Auto-Provisioning is available in Cloud Insights Premium Edition, and must be configured before it can be enabled for Cloud Insights. SSO User Auto-Provisining configuration includes Identity Federation through NetApp Cloud Central as described in the section above. Federation allows single sign-on users to access your NetApp Cloud Central accounts using credentials from your corporate directory, using open standards such as Security Assertion Markup Language 2.0 (SAML) and OpenID Connect (OIDC).

To configure *SSO User Auto-Provisioning*, on the **Admin > User Management** page, click the **Request Federation** button. Once configured, administrators can then enable SSO user login. When an administrator enables *SSO User Auto-Provisioning*, they choose a default role for all SSO users (such as Guest or User). Users who log in through SSO will have that default role.



Occasionally, an administrator will want to promote a single user out of the default SSO role (for example, to make them an administrator). They can accomplish this on the **Admin > User Management** page by clicking on the right-side menu for the user and selecting *Assign Role*. Users who are assigned an explicit role in this way continue to have access to Cloud Insights even if *SSO User Auto-Provisioning* is subsequently disabled.

If the user no longer requires the elevated role, you can click the menu to *Remove User*. The user will be removed from the list. If *SSO User Auto-Provisioning* is enabled, the user can continue log in to Cloud Insights through SSO, with the default role.

You can choose to hide SSO users by unchecking the **Show SSO Users** checkbox.

However, do not enable *SSO User Auto-Provisioning* if either of these are true:

- Your organization has more than one Cloud Insights tenant
- Your organization does not want any/every user in the federated domain to have some level of automatic access to the Cloud Insights tenant. *At this point in time, we do not have the ability to use groups to control role access with this option*.