User accounts

Cloud Insights

Tony Lavoie, Dave Grace
March 27, 2020

NetApp®

Table of Contents

User accounts

Cloud Insights provides four user accounts: Account Owner, Administrator, User, and Guest. Each account is assigned specific permission levels. Users are either invited to Cloud Insights and assigned a specific role, or can sign in via Single Sign-On (SSO) with a default role. SSO 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 one of the following permission levels.
* **Guest** can view asset pages, dashboards, and queries, and run queries.
* **User** can perform all guest-level privileges as well as create, modify, or delete dashboards, queries, annotations, annotation rules, and applications.
* **Administrator** and **Account Owner** can perform all functions, as well as create, modify and delete policies, and manage all users and data collectors.

The Account Owner is created when you register for Cloud Insights.

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

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.

5. Enter the user's e-mail address.
6. Select the user role.
7. Click **Invite**

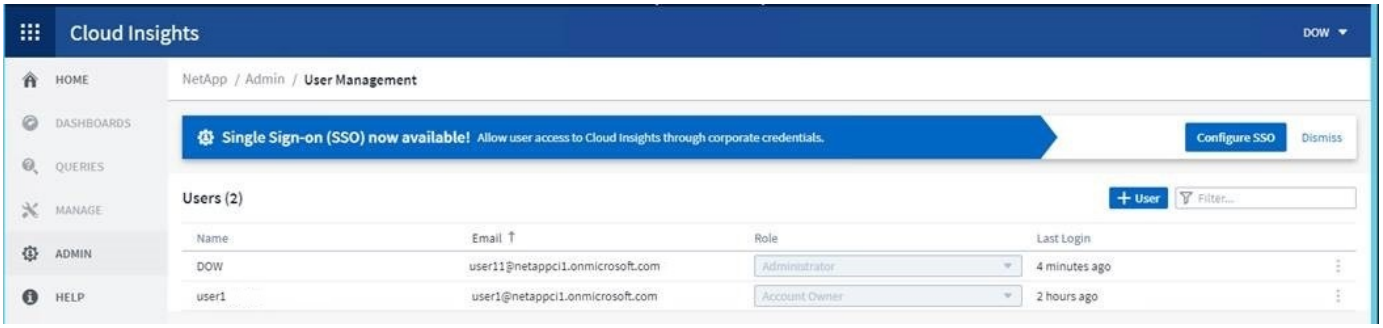
   The invitation is sent to the user. Users will have 14 days to accept the invitation. Once a user accepts the invitation, he or she will be taken to the NetApp Cloud Portal, where they will sign up using the email address in the invitation.
   If they have an existing account for that email address,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

Single Sign-On (SSO) Accounts

In addition to inviting users, administrators can enable **Single Sign-On** (SSO) 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 is available in Cloud Insights Premium Edition, and must be configured before it can be enabled for Cloud Insights. SSO configuration includes Identity Federation through NetApp Cloud Central. 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, on the **Admin** > **User Management** page, click the **Configure SSO** button. Once configured, administrators can then enable SSO user login. When an administrator enables SSO, 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 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 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.