



## Overview

---

- [Cisco Security Cloud Control overview, on page 1](#)
- [Signing in to Security Cloud Control, on page 4](#)

### Cisco Security Cloud Control overview

Security Cloud Control is a web application that provides centralized management of Cisco Secure product instances, user identity, and user access management across Cisco Security Cloud. Security Cloud Control administrators can create new Security Cloud enterprises, manage users in an enterprise, claim domains, and integrate their organization's SSO identity provider, among other tasks.

#### Overview tab

The **Overview** tab lists your currently activated Cisco product instances and those that are pending activation. You also can claim a subscription or attach an external product to Security Cloud from here. For details, see [Managing products and subscriptions](#).

The screenshot shows the Cisco Security Cloud Control interface. At the top, the Cisco logo and 'Security Cloud Control' are visible. The main header reads 'Overview - Example Corp.' with a 'Claim subscription' button. A left sidebar contains navigation options: Overview (selected), Users, Domains, and Identity Providers. The main content area is divided into two sections. The first section, 'Activation pending', shows three items: Cisco XDR, Cisco Secure Endpoint, and Cisco Secure Email Threat Defense, each with a start date of 06/27/2023 and an 'Activate' button. The second section, 'Products', shows 'Cisco XDR' in a trial state with an instance ID of 0299f560- followed by redacted characters. At the bottom, there is a copyright notice for © 2023 Cisco Systems, Inc. and links for Privacy Policy and Terms of Service.

## Users tab

The **Users** tab lists users that have been [invited](#) to the enterprise by an administrator. Administrator can also reset user passwords and MFA settings (for users in a [claimed and verified domain](#)) and deactivate user accounts. See [Managing users](#) for more information.



# Security Cloud Control



Overview



Users



Domains



Identity Providers

## Users

4 Current Accounts

### Email address

user1@example.

user2@example.

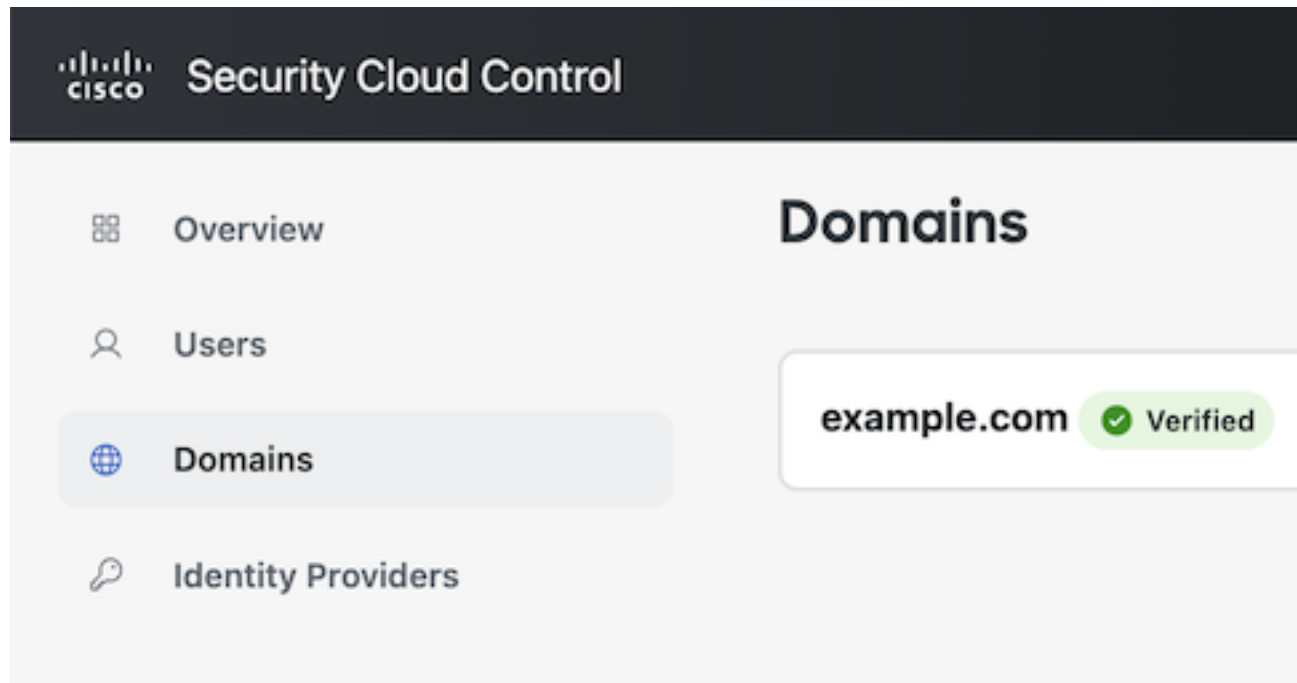
user3@example.

user4@example.

### Domains tab

The **Domains** tab lists email domains that have been claimed and verified for the enterprise. Verifying a domain is required to integrate an identity provider with Security Cloud Sign On. It also allows administrators

to reset passwords or MFA settings of users in the claimed domain. See [Managing domains](#) for more information.



#### Identity Providers tab

The **Identity Providers** tab lists any identity providers integrated with Security Cloud Sign On using SAML (Secure Assertion Markup Language) for the current enterprise. This allows enterprise users to access their Cisco Secure products with their identity provider's SSO credentials. See [Identity provider integration guide](#) for details.

## Signing in to Security Cloud Control

To sign in to Security Cloud Control you need a [Cisco Security Cloud Sign On](#) account. If you don't have an account, [create one](#) and configure multi-factor authentication with either Duo MFA or Google Authenticator. The first time you sign in to Security Cloud Control with your Security Cloud Sign On account, a new enterprise is created with your Security Cloud Sign On account as the sole [user](#) in the enterprise.

If you only have one enterprise associated with your Security Sign On account, that enterprise will always be [selected](#) when you sign in. If you have [created](#) multiple enterprises, the last enterprise that was selected will be selected after signing in.

---

**Step 1** Open [Security Cloud Control](#).

**Step 2** Sign in with your Security Cloud Sign On credentials and MFA options you established when creating your account.

If this is the first time signing in to Security Cloud Control, account, a new enterprise is created for you with a default name. You can [rename](#) the enterprise by clicking the pencil icon.

---