



Secure Access DNS Onboarding Guide

Cisco Secure Access
Updated October 15, 2026

1 Welcome to Secure Access

Topics:

- [Getting Started](#)
- [Prerequisites and Network Requirements](#)

A general welcome to Secure Access with a guided overview on immediate action-items to ensure the Secure Access organization is prepared for devices and policy deployment.

You must create a Secure Access Organization. Follow the guide here for more information. Once you have created an organization, we recommend the following immediate steps:

Create a Secure Access Organization

Follow the guide to create a new [Secure Access Organization](#).

View Organization Details

In the Security Cloud Control platform menu, select your organization from the organization picker list. In the organization menu, select **Platform Service > Platform Management > Organization Details** to view this information:

- Organization name.
- Organization ID.
- Cloud Region.

Claim a subscription

An administrator uses a claim code to claim the subscription for the organization. For more information, see [Determine Your Current Package](#). If you encounter a feature here that you do not have access to, contact your sales representative for more information about your current package. For more information, see [Cisco Secure Access Packages](#) and [Claim a Subscription](#).

Manage Registered Networks

A Registered Network resource represents a single public static or dynamic IP address, or a range of IP addresses. Cisco Secure Access supports both IPv4 and IPv6 for static IP addresses and only IPv4 for dynamic IP addresses. In Secure Access, all traffic originating from the public IP space is identified as coming from that network. The public IP space or IP range defines the scope of the network resource.

A Registered Network resource represents a single public static or dynamic IP address, or a range of IP addresses. Cisco Secure Access supports both IPv4 and IPv6 for static IP addresses and only IPv4 for dynamic IP addresses. In Secure Access, all traffic originating from the public IP space is identified as coming from that network. The public IP space or IP range defines the scope of the network resource.

Point DNS to Cisco Secure Access

Configure your DNS to direct traffic from your network to the Cisco Secure Access global network. When a request to resolve a hostname on the internet is made from a network pointed at our DNS addresses, Secure Access applies the security settings configured in your policy rules. To have Secure Access protect your

networks, you need to explicitly change the DNS settings in your operating system or hardware firewall or router to Secure Access's name server IP addresses and turn off the automatic DNS servers provided by your ISP. Secure Access supports both IPv4 and IPv6 addresses. For more information, refer to [Point DNS to Secure Access](#) and [Configure Windows server to Secure Access DNS](#). Make sure [Cisco Secure Access Root Certificate](#) is installed.

Validate DNS Protection

Use Secure Access reports to monitor usage, identify blocked requests and sources, and track trends to improve threat detection and response. For more information on different types of reporting refer to [Available Reports](#).

Getting Started

Review how to get started with onboarding a device to Secure Access with the intent of focusing on DNS.

Cisco Secure Access provides flexible secure connectivity to the internet, Software-as-a Service (SaaS) applications, and your private digital and network resources. Secure Access enables you to connect seamlessly to on-premises data centers, public clouds, or private networks from both remote and on-network locations.

The **Get Started with Cisco Secure Access** workflow guides you through the initial setup of Secure Access. Sign in to Secure Access and navigate to **Workflows**. The first step in the Get Started workflow takes you through the setup of your organization's network connections. You can provision users and groups from your organization in Secure Access and set up integrations with Security Assertion Markup Language (SAML) identity providers (IdPs). From a DNS perspective, the following flow is a general guide on how to navigate through this guide and any affiliated documentation included here.

Before initiating the onboarding process, please ensure that all components are running supported software versions. You can verify the latest available version of the Cisco Secure Client via the Cisco Secure Access - Connect - Internet Security download page.

Traffic Redirection Methods

At the DNS level we recommend the following traffic redirection methods per deployment type. Review the table below and affirm the redirection method:

Table 1: Traffic Redirection Methods per Deployment Type

Deployment Type	Description
Registered Network	Register the branch public IP for DNS requests.
Cisco Secure Client- Roaming Module	DNS redirection from roaming endpoint.
VA- DNS Forwarders	Lightweight conditional DNS forwarders.
Network Device	Intercept DNS request going through device - ISR, MX, SDWAN.
Android/iOS App/Chromebook	Mobile DNS protection.

Consider the following pros and cons for DNS forwarders in regards to how they could affect redirection.

DNS Forwarders

Lightweight VM that works as a recursive DNS resolver for your endpoints. Provides domain-based protection only Best deployed on IoT, Servers, Guest Networks

Network Devices

API-based integration with certain network devices (Meraki, FTD, etc) for domain level inspection. Network device intercepts DNS request and rewrites headers to Cisco DNS resolvers Best deployed on IoT, Servers, Guest Networks Make sure it doesn't conflict with other methods.

Android/iOS/Chromebook

Mobile devices leverage QUIC for better performance. Note that Chromebook uses DoH and an extension for DNS redirection.

Prerequisites and Network Requirements

Review the required networking, port, and service configurations or settings. These must be commuted prior to onboarding your device to a Secure access organization.

Before initiating the onboarding process, please ensure that all components are running supported software versions. You can verify the latest available version of the Cisco Secure Client via the Cisco Secure Access - Connect - Internet Security download page.

Ensure your firewall allows these outbound and inbound connections for proper functioning of Secure Access components.

Table 2: Table of Network Requirements

Component or Service	Port and Protocol	Source	Destination	Purpose or Notes
AD Connector - Umbrella Cloud	443/TCP	AD Connector	api.umbrella.com disthost.umbrella.com	Initial registration, automatic updates. health status reporting.
AD Connector - Certificate Validation	80/TCP	AD Connector	ocsp.digicert.com crl3.digicert.com crl4.digicert.com commercial.ocsponder.com validation.identrust.com	Certificate revocation check (OCSP/ CRL validation).
AD Connector - LDAP Sync	389/TCP, 636/TCP	AD Connector	Domain - Controller/Domain	LDAP syncing with Active Directory.
AD Connector - RPC Communication (outbound)	135/TCP 49152-65535/TCP	AD Connector	Domain - Controllers and Events Domain - Log Collector	RPC communication to fetch.
AD Connector - RPC Response (Inbound)	135/TCP	Domain Controllers/Event Log Collector	AD Connector	RPC response for login event data
AD Connector - Virtual Appliance Communication	443/TCP	AD Connector	Virtual Appliances	Send login events and IP addressing info. This is non-SSL by default.
Roaming Client / Cisco Secure Client - DNS (Standard)	53/UDP	Client Machine	208.67.222.222 208.67.220.220 2620:119:53::53 2620:119:35::35	DNS query resolution. This is standard unencrypted.
Roaming Client / Cisco Secure Client - DNS (TCP)	53/TCP	Client Machine	208.67.222.222 208.67.220.220 2620:119:53::53 2620:119:35::35	DNS query resolution . This is TCP fallback.
Roaming Client / Cisco Secure Client - Encrypted DNS	443/UDP	Client Machine	208.67.222.222 208.67.220.220 2620:119:53::53 2620:119:35::35	Encrypted DNS queries. This is optional, however it is automatic if port open).

Component or Service	Port and Protocol	Source	Destination	Purpose or Notes
Roaming Client / Cisco Secure Client - API	443/TCP	Client Machine	146.112.255.101 67.215.71.201 67.215.92.210 146.112.255.152/29 sync.hydra.opendns.com 2620:0:cc1:115::210 2a04:e4c7:ffff::20/125	Initial registration, version updates, status reporting, internal domains.
Virtual Appliance - Umbrella Cloud	443/TCP	Virtual Appliance	api.umbrella.com disthost.umbrella.com	Core communication with Umbrella Cloud services.
Virtual Appliance - DNS Queries	53/UDP 53/TCP	Client Machines (on protected network)	Virtual Appliance IP	DNS query forwarding to Umbrella.
Virtual Appliance - Internal DNS	53/UDP	Virtual Appliance	Local DNS Servers	Forward internal DNS queries to corporate DNS.
Virtual Appliance - AD Connector	443/TCP	Virtual Appliance	AD Connector	Receive login events and user or group information.

2 Manage Roaming Devices

Topics:

- [Deploy Roaming Devices](#)
- [Internet Security Settings](#)
- [Traffic Steering](#)
- [Endpoint Diagnostic Tool](#)

Discover where and how to download the Cisco Secure Client, known limitations, recommended security settings and traffic steering.

Cisco Secure Access Roaming Devices represent user devices that have deployed the Cisco Secure Client with the Umbrella Roaming Security module. The Cisco Secure Client syncs with Secure Access to manage the DNS and Web security on the device. As part of the sync, a Roaming Device resource is added to Secure Access. An administrator of the organization can apply policy rules to the Roaming Device resource. For more information about the Cisco Secure Client with the Umbrella Roaming Security module, see [Manage Internet Security on Cisco Secure Client](#).

In Secure Access, you can view **Roaming Devices** in the organization. You can edit the Internet Security settings for certain devices or all devices. You can override the Internet Security settings for the devices or delete a Roaming Device.

Deploy Roaming Devices

This chapter explains how to deploy one or multiple roaming devices to Secure Access for complete protection regardless of network type. Install and use the Anyconnect client to deploy and manage your devices.

Installs Cisco Secure Client with the roaming security module on end-user devices, so they're protected by Secure Access policy no matter what network they're connected to.

Customers utilizing the Secure Client VPN functionality can deploy the Umbrella module directly from their VPN headend, a method known as web deployment. This configuration is performed on the VPN server. Be aware of the following limitations:

- Clients with existing AnyConnect Secure Client deployments can automatically download the Umbrella module and profile when they initiate a connection to the VPN.
- Cisco Secure Client can also be installed through a self-service workflow, where each user visits the HTTP web portal hosted on the VPN headend.
- This web deployment method allow you to update Cisco Secure Client and the Umbrella module software versions by centrally uploading new versions to the VPN server.

For more information about roaming devices across different platforms, see the following documents:

- [Download and Install Cisco Secure Client](#)
- [Mass Deployment \(Windows\)](#)
- [Mass Deployment \(macOS\)](#)
- [VPN Headend Deployment](#)
- [Cloud Management](#)

Internet Security Settings

Read through what internet security settings are available for roaming devices and how to manage the settings through the Secure Access dashboard.

Decides which traffic from a roaming device actually gets sent to Secure Access for inspection, versus which traffic goes directly to the local DNS resolver for resolution.

See the following documentation for more information:

- [Manage Internet Settings](#)
- [View Internet Security Settings for Roaming Devices](#)
- [Edit Internet Security Settings for Roaming Devices](#)
- [Delete a Roaming Device](#)

Traffic Steering

Read through the following description to understand what traffic steering provides for your organization and how to manage the security bypass action.

Internet Security Bypass lets you exclude specific IPs, CIDRs, or domains from Secure Access security inspection. You can bypass the **DNS resolvers and SWG** or **SWG only**, typically for internal or trusted destinations. See [Manage Internet Security Bypass](#).

Endpoint Diagnostic Tool

Review how to operate the endpoint diagnostic tool to troubleshoot roamin clients if you experience issues in connection, policy deployment, or general reporting.

Cisco's Endpoint Diagnostics Tool, referred to in Cisco support documentation by the abbreviation CEDT, is the standard way to troubleshoot a roaming client that isn't behaving as expected; connectivity failures, policy not applying, or the client not reporting into the dashboard. For more information, see [How to use Endpoint Diagnostic Tool](#).

3 Manage Identities

Topics:

- [Active Directory Integration](#)
- [User and Identity Management](#)
- [Get Started with User Configuration Management](#)
- [Get Started with Endpoint Device Management](#)
- [Provisioned Users and Groups](#)
- [Manage User Directory Integrations](#)
- [Authentication Properties and Preferences](#)

Review how Secure Access uses identities to support users or user groups and endpoint devices. Monitor your connections to ensure your environment remains protected.

Cisco Secure Access supports the integration of users, groups, and endpoint devices through various identity providers (IdPs). Once integrated with Secure Access, you can protect and monitor the connections for the users and devices to internet and private destinations by configuring Access rules in the organization's policy. This complete section refers to the identity management for users and groups and different from dashboard SAML login. For dashboard SAML refers to the section [Secure Access Single Sign-On Authentication - Dashboard Login](#).



Note

You can integrate multiple cloud IdPs with Secure Access.

Active Directory Integration

Review how to integrate the Active Directory (AD) to Secure Access, how AD is used as part of the communication flow, troubleshooting, and integration with virtual appliances.

The following information is about the Active Directory (AD) and how communication between Secure Access and the AD connector occur.

AD and the AD Connector

Endpoint device integration requires devices provisioned by an on-premise AD domain controller (DC) and Cisco AD Connector version 1.14.4 or newer. For more information, see [Connect Active Directory to Secure Access](#) and [Configure Updates on AD Connectors](#).

AD Connector Communication Flow and Troubleshooting

The AD Connector is a Windows application and service that communicates with Cisco Secure Access and AD domain controllers. The AD Connector only syncs the required AD **User** and **Group** attributes with Secure Access.

For more information see [AD Connector Communication Flow and Troubleshooting](#).

AD Integration with Virtual Appliances

The integration of Microsoft AD with Cisco Secure Access Virtual Appliances (VAs) provides AD user, group, or computer name information for each applicable DNS request. Secure Access VAs forward DNS requests at the site. Please refer to [AD Integration with Virtual Appliances](#) for more information.

User and Identity Management

Review this short description of users, user groups, and endpoint devices as part of the Identity management implemented in Secure Access.

After provisioning users, groups, and endpoint devices in Secure Access, you can view information about these identities.

Get Started with User Configuration Management

Review this short section on how to get started with user configuration management in Secure Access. This does encourage users to implement a user directory integrated with Secure Access.

First, configure a user directory integration with Secure Access. The directory integration provisions users and groups into Secure Access.

Get Started with Endpoint Device Management

Review the following to manage the integration of the Active Directory (AD) of your choice as an endpoint. This allows you to discovery, configure, and monitor the devices connected to your network.

Configure your on-premise Active Directory integration and provision your identity endpoints in Secure Access, see [Manage Active Directory Integration](#).

Provisioned Users and Groups

Review the following details on how to provision users and user groups, see user details and endpoint device details in the Secure Access dashboard.

After you provision users, group, and endpoint devices in Secure Access, you can view the information about these identities.

- [View User Details](#)
- [View Group and Organizational Unit Details](#)
- [View Endpoint Device Details](#)

Manage User Directory Integrations

Read this section to understand user directories, how to integrate a user directory to Secure Access, and how to manage third-party providers as directories.

Manage the integrated user directories. For more information, see [Manage User Directories](#). Provision the organization's users and groups into Secure Access. For more information, see [Configure User Directory Integrations](#).

Integration Methods

The integration of a user directory in Secure Access manages the provisioning of the organization's users and groups from the identity provider (IdP) to Secure Access. You can integrate multiple cloud IdPs with Secure Access. For more information, see [Add a Cloud Identity Provider](#).

Configure User Directory Integrations

Add the user directory integrations for the organization and configure advanced settings for the directories.

- [Configure User Directory Integrations](#)
- [Manage Advanced Configuration Settings](#)

Manage User Directory Integrations

After you add the user directory integrations for the organization, you can view, edit, or delete a user directory.

- [Manage Cloud Identity Providers](#)
- [Manage Active Directory Integration](#)
- [Manage Google Workspace Integration](#)
- [Import Users and Groups from CSV File](#)

Authentication Properties and Preferences

This chapter addresses authentication properties, preferences, and how to implement both a network device and a network device integration.

User Principal Name (UPN) is the primary authentication attribute.

Authentication Name (authName) can be enabled as an additional authentication attribute [Authentication Properties](#).

See the following links for more information:

- [Manage Network Devices](#)
- Network Device Integrations
 - A network device is any hardware device—for example, a router, switch, or access point—that can encrypt and route DNS traffic to Secure Access's recursive DNS servers. Some network devices provide these additional features:
 - Adding internal IP addresses to DNS requests.
 - Policy by network segment or service set identifier (SSID).

4 Manage Network Devices

Topics:

- [Network Device Integrations](#)

Read through the integration instructions for the device types that support DNS. The hardware of the device type facilitates how DNS traffic is moved through Secure Access.

A network device is any hardware device—for example, a router, switch, or access point—that can encrypt and route DNS traffic to Secure Access's recursive DNS servers. Some network devices provide these additional features:

- Adding internal IP addresses to DNS requests.
- Policy by network segment or service set identifier (SSID).

Network Device Integrations

Review this chapter and discover how to integrate a network device to Secure Access. Below are examples and information on how to integrate some of the more common device types.

To integrate a network device with Secure Access, you must add your username and password, or Secure Access Network Devices API key and secret to the device and register the device. After you register your network device with Secure Access, the network device becomes a Secure Access identity that you can manage and set policies for. There is no need for any client device configuration.

DNS supports the following device types; review the prerequisites and limitations for the device type in question:

- [Meraki Integration](#)
- [SDWAN Integration](#)
- [ISR Integration](#)

5 Manage Access Policies for DNS

Topics:

- [About the Access Policy](#)

Explore how to configure the system-provided Access policy with rules and settings to finesse the control on your environment security and protect your organization.

Secure Access has a single unified policy, which consists of policy rules and settings. Your private access rules and the default policy rules control the access and security of your resources and protect the traffic in your organization. For more information about [managing the access policy](#).

About the Access Policy

Read about the system-provided Access policy that comes with every Secure access organization. This one policy contains all of the rules and guidelines on how traffic is handled; read about priority, rule organization, and settings that are applied across the tenant.

The Cisco Secure Access policy is the collection of your internet and private access rules, rule defaults, and global settings. The policy displays your configured rule data and allows you to choose how to prioritize the rules in your policy. Once you add a rule, you can edit various components on the rule. You decide how to view and manage your rules that best meets your organization's access controls to resources. For more information, please see the sections below.

- [Best Practices of Access Policy](#)
- [Default Rule Data](#)
- [Edit the order of the rules in Access Policy](#)

Policy Precedence

You can design any number of access policies to protect your identities and manage access to destinations. When you create a policy, you choose which identities to add to a certain policy. Then, you order the policy listing the highest priority policy first. Secure Access evaluates your policies to match an identity and destination using the order which you set. If a match is not found, Secure Access applies to the Default “For all internet Rules” policy for internet access rules. “For Private access rules” the default rule is set to block

Several Umbrella identities integrate with Active Directory (AD). Within the highest ranked access policy, Secure Access first checks for a matching AD user identity. If a match is not found, then Secure Access continues to check for a matching identity and destination. Secure Access considers the AD identities higher priority within a list of identities.

Secure Access checks for known identities in this order:

- Active Directory (AD) user – AD integration provided by a Virtual Appliance or Roaming Client.
- Active Directory (AD) computer – AD integration provided by a Virtual Appliance.
- Internal Network (Site) – AD integration provided by a Virtual Appliance.
- Umbrella Site – Virtual Appliance with no other identity deployed.
- Roaming Client – Roaming Client.
- Network – Uses source IP of the DNS request.

Default Access Rules in your Policy

If your traffic does not match any of the rules in your policy, Secure Access applies the settings on the Default Access rules. For more information, see [Edit the Default Access Rules](#).

Rule Defaults and Global Settings

- For more information, see [Global Settings for Access Rules](#).
- For more information, see [Rule Defaults: Default Settings for Access Rules](#).

6 Manage Certificates and Block Pages

Topics:

- [Root Certificate Installation](#)
- [Manage Notification Pages](#)

Review how to set up your certificates for internet access, which are required for decryption and inspection, as well as how to set up any block or notification pages.

Certificates are required for secure internet access. Specifically, certificates are required to decrypt traffic to inspect it for threats, and to present notifications to end users when access is blocked or triggers a warning. Cisco provides trusted root store bundles, which contain information about certificates used by Cisco products. The Cisco Secure Access root certificate is essential for Cisco Secure Access to proxy and decrypt HTTPS traffic.

The Secure Access Root certificate is needed for two main functions, displaying block pages when a user visits a blocked HTTPS domain and enabling HTTPS decryption and inspection without causing browser errors.

Root Certificate Installation

This chapter addresses how to install a root certificate automatically or manually. Root certificates improve traffic decryption behavior to both private and internet resources for specific browser types.

Secure access root certificates enhance security and connectivity by enabling traffic decryption for threat detection to private and internet resources. SSE root certificate establishes trust for SAML authentication with identity providers. They also support user and device authentication in VPN connections, ensuring secure remote access. For detailed instructions, see [Manage the Secure Access Root Certificate](#)

Automatic or Manual Installation

Certificate installation can be done on a per-browser or per-machine basis. For larger deployments, you can perform an automatic installation through Group Policy Objects (GPO). Note that the automatic installation through GPO is only supported for the Edge or Chrome browsers on Windows systems. As such, for Firefox or Safari browsers, and for users on non-Windows operating systems, you must perform the [manual installation](#) procedure.

You can also install a [certificate automatically](#)—through Active Directory Group Policy Objects—for a group of users in Microsoft Windows Active Directory. This automatic installation of a certificate is only supported for Edge or Chrome browsers on Windows systems. For all other browsers and systems, you must perform the manual installation procedure.

Push the Cisco Root Certificate to Managed Devices

To support the display of block pages for HTTPS sites, HTTPS decryption if the Intelligent Proxy is used, and Trusted Network Detection if a VA is present, you must [push the Secure Access certificate to managed devices](#)

Manage Notification Pages

Read through this article to read what information is provided in the notification pages and how to navigate to the appropriate page in the Secure Access dashboard.

Secure Access displays notification pages to end users when users try to:

- Access a destination that is blocked by configurations in a security profile in an internet access rule. In this case, they see a Block page.
- You can display the default Secure Access notification or create one or more custom notifications to display in different situations.

Each security profile for internet access is associated with a single notification page configuration that includes Block pages.

View Notification Pages Displayed to End Users

You can view the default and any custom notification pages.

For more information, see [Preview Notification Pages](#).

To display customized block page or end user notification pages, please refer to this section [Display Custom Notification Pages for End Users](#).

To create your own notification pages, refer [Create Custom Block pages](#).

7 Manage Account, Users, and API Keys

Topics:

- [Add a New Account](#)
- [Secure Access API Keys](#)
- [Secure Access Single Sign-On Authentication](#)
- [Add Your Organization's Identity Provider in Security Cloud Sign On](#)
- [Single Sign-On De-Identification](#)

Learn how to manage users in your organization, how external or third-party system authenticate with Secure Access, and how to protect your privacy with monitoring and reporting.

This section covers who can access your Secure Access tenant, how external systems authenticate into it, and how to protect user privacy in reporting.

Add a New Account

Review on the recommended action on when and how to add a new account for a user that is new to your organization. Adding the user to your organization allows you to assign a permission level and access role.

You can add users to your instance of Cisco Secure Access by adding a new account. Each account is assigned a role that sets that account permissions to view, write, change, and delete Secure Access configurations.

Secure Access API Keys

Read the brief description of what Secure Access API Keys allow you to do and what aspects of the organization it can impact.

The Secure Access API enables you to create, manage, and protect the users, user devices, network connections, and private resources in your organization.

Secure Access Single Sign-On Authentication

This chapter describes what single-sign on SAML IdP authentication is and how this impacts Secure Access when you use the Security Cloud Sign On component.

Cisco Secure Access supports Security Assertion Markup Language (SAML) for the authentication of administrators to the Secure Access console. An administrator signs in to Secure Access from Cisco Security Cloud Sign On (SCSO). Cisco Duo Security or the IdP that you integrated with Security Cloud Sign On provides single sign-on (SSO) authentication of Secure Access administrators through SCSO. Please refer to [Cisco Security Cloud Sign On Identity Provider Integration Guide](#).

To sign in to Secure Access, an administrator must have a Secure Access account and configure single sign-on authentication in SCSO. A Secure Access administrator signs in to SCSO authenticates to the IdP, and then automatically signs in to Secure Access.

Any changes made in your organization's SAML identity provider (IdP) are synced with Secure Access. If you update an account or change a password in the IdP, the changes are immediately reflected in your login. Only the username (email address) is stored in Secure Access. You must sign in to Secure Access with the same email address that you configured in your SCSO account. For more information, see [Getting Started Guide for New Customers of Security Cloud Control](#).

Add Your Organization's Identity Provider in Security Cloud Sign On

This chapter covers how to add a SAML IdP for the Security Cloud Sign On (SCSO) component of SEcure Access. Review the variety of third-party IdP services that are compatible with your organization.

You can add an SAML identity provider (IdP) in SCSO for Secure Access. Once you add an IdP and provision user accounts in Security Cloud Sign On, administrators in your organization are not required to complete the **Sign Up Now** steps. Please refer [Cisco Security Cloud Sign On Identity Provider Integration Guide](#) for different IDP integrations with Cisco Secure Access.

For instructions to integrate with specific identity service providers, see the following guides:

- [Auth0](#)
- [Microsoft Entra ID](#)
- [Duo](#)
- [Google Identity](#)

- [Okta](#)
- [Ping](#)

Single Sign-On De-Identification

Review what Single Sign-on De-Identification is and how impacts the information included in events; this does impact what data is generated in logs and other informational tables.

This action hides the hostname, internal IP address, and username of end users in Secure Access reports, replacing identity with a one-to-one hash.

- [Add a New Account](#)
- [Secure Access API Keys](#)
- [Secure Access Single Sign-On Authentication](#)
- [De-Identification](#)

The Security Activity report highlights security events generated by your organization's sources visiting destinations flagged—but not necessarily blocked—by Secure Access security researchers as a threat. Activities captured by this report include attempts to access sites hosting malware or phishing sites, botnet activity on infected machines on your local network, and attempts to download malicious files.

8 Manage Reports

Topics:

- [Report Types](#)

Learn how you can utilize Secure Access reports to monitor and improve the protection and activity of your organization. Learn patterns, types of attacks, and review blocked requests to further improve your tenant security.

Use reports to monitor your Secure Access deployment and to understand usage. Gain insights into request and block activity, determining which of your sources are generating blocked requests. Build actionable intelligence in addressing threats including changes in usage trends over time.

Report Types

Read through the variety of reports available in the Secure Access dashboard and what they provide, where to locate them, how to utilize them for troubleshooting events or failures, and more.

Activity Search –Search for activity from the sources in your environment over a selected time period. To learn more about the results of your activity search, click the View Actions icon for a result and choose an item from the menu. For more information see [View Activity Search Report Actions](#).

Security Activity –Lists security-related activity in your environment over a selected time period.

Total Requests - The Total Requests report displays traffic for a user-specified time period. View traffic trends using categories, traffic type, and responses.

Activity Volume - The Activity Volume report displays a summary of traffic by security categories and policies that are affected by content categories and destination lists. View allowed and blocked traffic and traffic percentage to identify activities that may pose risk.

App Discovery - Provides more information about the cloud applications in use in your environment.

Top Threats - The Top Threats report displays threats your organization may have been exposed to in a user-defined time period and whether the threats were blocked or allowed.

Top Destinations –Lists the top traffic-generating sources over the selected time period. Filterable by source and destination.

Top Categories –Lists the most popular security and content categories for your organization over the selected time period.

Top Identities - View your organization's most active identities, based on DNS requests.

Third-Party Apps - View third-party cloud applications that have been authorized to access sanctioned tenant applications. Get visibility into the risks that your system is exposed to by the third-party app authorizations.

Cloud Malware –Lists malicious files detected within your organization and provides details of the potential risk and exposure these files present.

Admin Audit Log –Lists a record of any configuration changes made to your settings by any of your Secure Access administrators.

View and Customize the Activity Search Report

To learn more about the results of your activity search, click the View Actions icon for a result and choose an item from the menu. [View Activity Search Report Actions](#). To learn more about the report retention period [Report Retention](#).

9 Manage Logging

Topics:

- [Where Are Logs Stored](#)

Learn how to benefit from systematic logging and configure just where your logs are forwarded to. Where and how you store your logs is also addressed here.

Secure Access allows for the logging of events and traffic. You can configure Secure Access to save these logs to either the United States or Europe. Logs can be saved to your own or a Cisco Managed S3 bucket.

Only event data is stored in a data warehouse. This is any data that might appear in a Secure Access report. Configuration data, such as audit logs and policy settings, remain stored by Cisco in California regardless of a change to the data warehouse's location.

Secure Access logs are CSV-formatted, compressed (gzip), and saved every 10 minutes. For more information, see [Log Formats and Versioning](#).

Where Are Logs Stored

Review where logs generated by Secure Access are stored, what creates logs, and how to log to an S3 bucket, such as the Amazon S3 bucket.

When you create a policy, activity logs are by default saved to the North America – California, US location of the Secure Access data warehouse. You can change the location of the data warehouse to Europe at any time. For more information, see [Change the Location of Event Data Logs](#).

You can also optionally configure logging so that logs are also stored to an Amazon S3 bucket—either your own or one managed by Cisco.

Logging to the Secure Access Data Warehouse

The Secure Access data warehouse is the virtual location where your instance of Secure Access stores its event data logs. By default, Secure Access saves your event data logs to Cisco's California location; however, you can change the location of the data warehouse from North America to Europe at any time. For more information, see [Change the Location of Event Data Logs](#).

Logging to Amazon S3

As well as storing logs to one of its data warehouses, Secure Access can store logs to an Amazon S3 bucket.

By having your logs uploaded to an S3 bucket, you can then automatically download logs so that you can keep them in perpetuity in backup storage outside of the Secure Access data warehouse storage system. Saving to an S3 bucket also gives you the ability to ingest logs through your SIEM or another security tool. This can help you determine if any security events in your Secure Access logs coincide with events in other security tools.

Secure Access Amazon S3 options:

- [A self-managed bucket](#) - You own the Amazon S3 bucket, including its configuration and management.
- [A Cisco-managed bucket](#) - Cisco Secure Access owns the bucket and sets the configuration and management of it.

Advantages and Disadvantages of Configuring a Cisco-Managed Bucket

Review the following list of advantaged and disadvantages to consider if you opt to use a Cisco-managed bucket for logging:

- Secure Access supports the rotation of the S3 bucket key every 90 days.
- Included with your Secure Access license.
- You cannot add anything to your S3 bucket besides log files from Secure Access. You cannot use your Cisco-managed S3 bucket for any other application.
- Some SIEM integration types may require advanced privileges for the user accessing the S3 bucket (beyond the basic Read permissions) and as such, may not work with this feature.
- You cannot get support from Amazon directly for advanced configuration assistance, such as automation or help with the command line.
- Data can only be stored offline for a maximum of 30 days.

Additional Resources

If you discover that you need more information on logging and how Secure Access handles data in logging environments, review the following sources:

- [Enable Logging on a Rule in Access Policy](#)

- [Enable Logging to Your Own S3 Bucket](#)
- [Enable Logging to a Cisco-Managed S3 Bucket](#)
- [Migrate From Cisco S3 Bucket to Your Own S3 Bucket](#)

