Cisco Secure Access Documentation Changes

Cisco Secure Access
Updated September 22, 2026

Topics included

1 Change log overview

Topics:

Explains how the change log compares Secure Access Help snapshots and reports page counts, additions, removals, and links to changed content.

What the change log includes

Identifies the snapshot dates, page counts, added or removed pages, and content details included in each Secure Access Help change-log entry.

A change-log entry is a record of changes to the Cisco Secure Access Help (https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp.html). It compares the current snapshot with the previous snapshot and links to affected pages. The change log is generated weekly, except during holidays.

Each change-log entry includes:

- Generation date
- Previous snapshot date used as the comparison baseline
- Number of pages checked
- Number of pages changed since the previous snapshot
- Number of pages added since the previous snapshot
- Number of pages removed since the previous snapshot
- Added or removed text, with a link to each affected page

Access the legacy Secure Access Help change log

Provides access to the legacy Secure Access Help change log for documentation published before Secure Access Help moved to Cisco.com.

Cisco Secure Access Help has moved to Cisco.com. If you need to access the legacy change log, see https://securitydocs.cisco.com/docs/csa/changelog/170171.dita.

2 September 2026 updates

Topics:

Lists the Secure Access Help updates published during September 2026 and groups them by dated change-log entry.

Cisco Secure Access documentation changes 2026-09-21

Lists changes to Cisco Secure Access documentation published on September 21, 2026.

Summary

- Document URL: https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp.html
- Snapshot date: 2026-09-21
- Pages checked: 457
- Pages changed: 22
- Pages added: 0
- Pages removed: 0

Changed Pages

About this content

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp.html

- Removed: Endpoint Data Loss Prevention using Ciso Secure Client
- Added: Endpoint Data Loss Prevention using Cisco Secure Client

Endpoint Data Center Selection

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/introduction-secure-access-intro/Endpoint_Data_Center_Selection.html

- Removed: Secure Access - Local data residency deployments: With these deployments, data in the control, management, and data planes remains in a specific region rather than using a global cloud.
- Removed: The features are comparable to standard Secure Access.
- Added: Secure Access - Local data residency deployments: In these deployments, data in the control, management, and data planes remain within a specific region rather than in a global cloud.
- Added: The core security features are comparable to standard Secure Access.
- Added: For data processing details, see the Cisco Secure Access with Local Data Residency Offer Disclosure on the Cisco Trust Portal.

Network Tunnel Groups

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/manage-network-infrastructure-intro/manage-network-tunnel-groups.html

- Added: Step 1 - General Settings
- Added: Step 2 - Tunnel ID and Passphrase—Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.
- Added: If you opted to configure a backup primary or secondary region, you must also enter the IP addresses for both data centers within that region.
- Added: Step 3 - Routing — Configure routing options and network overlaps for this tunnel group.
- Added: Step 4 - Data for Tunnel Setup

Configure Tunnels with Cisco ISR

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/network-tunnels-by-device-intro/configure-tunnels-with-cisco-isr.html

- Added: Follow these steps to connect the Cisco ISR (G2, 4K) or CSR router to Secure Access.

Enroll Meraki SD-WAN Sites with Meraki Auto-VPN Tunnels

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/network-tunnels-by-device-intro/end-meraki-sd-wan-sites-with-meraki-auto-vpn-tunnels.html

- Added: Enrolling a Meraki Site
- Added: Perform the following steps to enroll a Meraki site.
- Added: For more information, refer to Cisco SASE: Sites Connectivity.

Site-to-Site VPN tunnels with Microsoft Azure

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/network-tunnels-by-device-intro/configure-site-to-site-vpn-azure.html

- Added: Component 1: Create a VPN Gateway in Microsoft Azure
- Added: Note The Azure S2S IPsec tunnel is sourced from the VPN Gateway.
- Added: If you have already deployed a VPN Gateway in your Azure environment, skip ahead to Component 2.
- Added: Component 2: Create a network tunnel group in Secure Access
- Added: Create a network tunnel group in Secure Access with the following configuration.
- Added: For a more detailed procedure, see Add a Network Tunnel Group.
- Added: Component 3: Create two local network gateways in Azure with S2S connections
- Added: Create and configure two local network gateways in Azure, then connect them to Secure Access.
- Added: The local network gateway acts as the remote site connected by tunnel to the Secure Access DC.
- Added: Component 4: Create a static route table in Azure
- Added: Add a table of branch routes and internet routes to the primary VPN gateway and associate the route table with any required subnets.
- Added: For more information, see Azure: Create, change, or delete a route table.
- Added: Component 1: Create a VPN Gateway in Microsoft Azure
- Added: Note The Azure S2S IPsec tunnel is sourced from the VPN Gateway.
- Added: If you have already deployed a VPN Gateway in your Azure environment, you can skip this section.
- Added: Component 2: Create a network tunnel group in Secure Access.
- Added: Configure a network tunnel group in Secure Access.
- Added: For a more detailed procedure, see Add a Network Tunnel Group.
- Added: Component 3: Create two local network gateways in Azure with S2S connections.
- Added: Create and configure two local network gateways in Azure, then connect them to Secure Access.
- Added: The local network gateway acts as the remote site connected by tunnel to the Secure Access DC.
- Added: Component 4: Verify tunnel status in Azure and Secure Access.

Configure a Site-to-Site VPN tunnel with Amazon Web Services

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/network-tunnels-by-device-intro/configure-site-to-site-vpn-aws.html

- Added: Component 1: Create a VPC with two subnets in AWS—In your AWS dashboard, create a VPC with two subnets.
- Added: Skip this step if you already have a VPC.
- Added: For more information, refer to Create a VPC
- Added: Component 2: Create a Transit Gateway in AWS—Create a transit gateway in AWS with an attachment to your Amazon VPC.
- Added: For more information, refer to Connect your VPC to other VPCs and networks using a transit gateway, Create a transit gateway using Amazon VPC Transit Gateways, and Create a VPC attachment using Amazon VPC Transit Gateways.
- Added: Component 3: Create two placeholder Customer Gateways in AWS—Create two customer gateways with S2S connections.
- Added: For more information, refer to Get started with AWS Site-to-Site VPN, Step 1: Create a customer gateway and Step 5: Create a VPN connection.
- Added: Note These gateways will act as temporary placeholders that provide outside IP addresses required by the Secure Access network tunnel group configuration in the next step.
- Added: The network tunnel group will provide the Secure Access BGP ASN and public IP addresses for the Secure Access Peer IP address DCs that you will use to create two new customer gateways in AWS.
- Added: Component 4: Create a Site-to-Site VPN connection for each customer gateway
- Added: Component 5: Create a network tunnel group in Secure Access—For a more detailed procedure, refer to Add a Network Tunnel Group.
- Added: Component 6: Replace the placeholder customer gateways in AWS—Configure two more customer gateways in AWS to connect to the Secure Access DC IPs.
- Added: These will replace the placeholder customer gateways that you created for Component 3.
- Added: Note It is not possible to update the placeholder customer gateways.
- Added: You must create new customer gateways with the DC IPs from Secure Access, then modify the VPN connection in AWS to target the new customer gateways.
- Added: Before you begin, you will need this information from Secure Access:
- Added: The DC IP addresses for the primary and secondary tunnel from Component 4.
- Added: You can also find this information in Secure Access by navigating to Connect> Network Connections> Network Tunnel Groups and clicking the network tunnel group name for details.
- Added: The Peer (Secure Access) BGP AS number for the network tunnel group.
- Added: Find this information in Secure Access by navigating to Connect> Network Connections> Network Tunnel Groups and clicking the network tunnel group name for details.
- Added: Component 7: Verify tunnel status in AWS and Secure Access—In the left navigation menu of the AWS VPC dashboard, navigate to Virtual private network (VPN) and click Site-to-Site VPN connections.
- Added: Click the VPN ID of each VPN connection to confirm that the State is Available and that the Status of both tunnels is Up.
- Added: This example shows VPN connection 1 is Available and both tunnels are Up:
- Added: VPN connection 2 is also Available and both tunnels are Up.

- Added: Note that each tunnel has a unique Outside IP Address.
- Added: Tunnel 1 has the same Inside IPv4 CIDR range for each VPN connection, and Tunnel 2 has the same Inside IPv4 CIDR range for each VPN connection.
- Added: Component 8: Modify subnet routing tables to send traffic to the AWS Transit Gateway—To send traffic from the AWS VPC to the AWS transit gateway, modify the routing table of each subnet to target the Transit gateway ID.
- Added: For more information, refer to Change a subnet route table.

Manage Resource Connectors and Connector Groups

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/resource-connectors-groups-intro/manage_resource_connectors_and_connector_groups.html

- Added: 208.67.222.222 Note The Resource Connector uses the Cisco OpenDNS resolver (208.67.222.222) as a fallback mechanism.
- Added: This is optional and is only utilized if your configured DNS server becomes non-functional.
- Added: If you do not wish to use this fallback, it is not required for standard operations.
- Added: 208.67.222.222
- Added: TCP/53, UDP/53

Provision Users, Groups, and Endpoint Devices from Active Directory

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/provisioning-active-directory-intro/provision_users_groups_and_endpoint_devices_from_active_directory.html

- Added: Delete one AD component
- Added: Delete all AD components

Manage Destination Lists

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/internet-saas-resource-intro/manage_destination_lists.html

- Removed: Table 1.

Manage Virtual Private Networks

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/vpns-and-proxies-intro/manage-virtual-private-networks.html

- Added: Note Proxy Override Settings manage proxy behavior once the VPN tunnel is active.
- Added: These settings are independent of the Cisco Secure Client proxy settings configured in Step 4 of the Add VPN Profiles Step 4 – Cisco Secure Client Configuration procedure, which specifically govern the client's VPN connection.

Manage Notification Pages

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/notification-pages-intro/manage_notification_pages.html

- Added: Note You can pin a specific column or re-arrange columns in your desired layout by clicking on the Settings gear icon.
- Added: Note You can View or Edit the Default Settings End User Notification Page, but you cannot Delete it.
- Removed: Click +Add, or expand the setting you want to edit.
- Added: Click + Add notification page, or expand the setting you want to edit.

- Removed: If this is a new configuration, name this set of notification pages.
- Removed: Click Allow blocked users to contact an admin from the block page.
- Added: If this is a new configuration, name this set of notification pages using a maximum of 128 characters.
- Added: Enable Show diagnostic information that Cisco TAC may need for troubleshooting, such as organization ID, origin ID, query string, and server name.
- Added: Disabling diagnostic fields may limit support effectiveness..
- Removed: Images larger than 125 x 70 pixels will be cropped and resized.
- Added: Images larger than 600 x 200 pixels will be cropped and resized.
- Added: You can select your desired logo position.
- Removed: Specify your custom message.
- Removed: You can adjust the size of text, as well as bold, italicize, underline, or strikethrough it.
- Removed: You can also add hyperlinks, numbered lists, and bulleted lists.
- Removed: You can also use the following variables within your message.
- Removed: [domain]—Substitutes the domain name that the end-user tried to browse to.
- Removed: [client_ip]—Substitutes the external IP address of the client that is hitting the block page.
- Added: Enter your custom message.
- Added: You can change the size and formatting of your text.
- Added: Add bold, italic, underline, and strikethrough styles.
- Added: You can also include hyperlinks, numbered lists, and bulleted lists.
- Added: You can include the following variables within your message.
- Added: [domain]—Displays the domain that triggered the block and warn page.
- Added: [rule_name]—Displays the name of the rule that triggered the block or warn page.
- Added: [url_category]—Displays the URL category associated with the blocked or warned destination.
- Added: [client_ip]—Displays the client IP address associated with the request.
- Added: [public_ip]—Displays the public source IP address of the client.
- Added: [user_agent]—Displays information about the browser or client that made the request.
- Added: You can redirect users to the URL of your choice by clicking on the radio button and entering the URL.
- Added: Note: You can allow users to directly contact their administrators by enabling Allow blocked users to contact an adminstrator.
- Added: You can change the size and formatting of your text.
- Added: Add bold, italic, underline, and strikethrough styles.
- Added: You can also include hyperlinks, numbered lists, and bulleted lists.
- Added: You can include the following variables within your message.
- Added: [domain]—Displays the domain that triggered the block and warn page.
- Added: [rule_name]—Displays the name of the rule that triggered the block or warn page.

- Added: [url_category]—Displays the URL category associated with the blocked or warned destination.
- Added: [client_ip]—Displays the client IP address associated with the request.
- Added: [public_ip]—Displays the public source IP address of the client.
- Added: [user_agent]—Displays information about the browser or client that made the request.
- Removed: Navigate to a notification page and expand the setting.
- Added: Navigate to a notification page and click Edit.

Built-in Data Identifiers

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/built-in-data-identifiers-intro/built-in_data_identifiers.html

- Removed: The built-in data identifiers are available as an Excel table here.
- Removed: The table is updated frequently, so be sure to download the most recent version.
- Added: The built in data identifiers are available as a PDF document here.

Set up the Zero Trust Access App for iOS Devices

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/client-based-za-mobile-intro/set_up_the_zero_trust_access_app_for_ios_devices.html

- Removed: We strongly recommend consulting your MDM documentation for setting options and configurable components.
- Added: We strongly recommend configuring the following settings in your Mobile Device Manager (MDM) to support the full range of functionality and features that Secure Access has to offer.
- Added: For information on how to implement these changes in your particular MDM, consult your MDM documentation.
- Added: ”enrollment_choice”: <enrollment choice file content>.
- Added: This allows you to deploy a different enrollment choice file instead of the default file.
- Added: ”DeviceUniqueIdentifier”: <device UDID>.
- Added: This allows the admin to set a unique device ID to the enrolled device into each connection request to the private resource to assist in identify the user's device.

Set up the Zero Trust Access App for Android on Samsung Devices

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/client-based-za-mobile-intro/set_up_the_zero_trust_access_app_for_android_on_samsung_devices.html

- Removed: Configure Android Settings in Seucre Access
- Added: Configure Android Settings in Sucre Access

Manage Zero Trust Access using Cisco Secure Client

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/za-secure-client-intro/manage_zero_trust_access_using_cisco_secure_client.html

- Removed: C:\\ProgramData\\Cisco\\Cisco Secure Client\\ZTA\\enrollments
- Added: C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment_choices

Endpoint Data Loss Prevention using Cisco Secure Client

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/edlp-secure-client-intro.html

- Removed: Endpoint Data Loss Prevention using Ciso Secure Client
- Added: Endpoint Data Loss Prevention using Cisco Secure Client

Onboard Experience Insights

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/experience-insights-intro/onboard-experience-insights.html

- Added: Step 1: ThousandEyes integration
- Added: Experience Insights requires the integration of your ThousandEyes account.
- Added: Note OAuth 2.0 with ThousandEyes
- Added: ThousandEyes uses the OAuth 2.0 protocol to grant Secure Access limited access to your ThousandEyes data.
- Added: For more information, see OAuth 2.0 with ThousandEyes.
- Added: Step 2: Account group configuration
- Added: Step 3: Default test target
- Added: Step 4: Unified collaboration application
- Added: Step 5: ThousandEyes agent
- Added: Endpoints must be registered to your Secure Access organization to be monitored for performance.
- Added: When you deployed Cisco Secure Client to your endpoints, the ThousandEyes Endpoint Agent was installed.
- Added: The ThousandEyes Endpoint Agent will register to your Secure Access organization automatically once your endpoints have connected to VPN, ZTA, or Roaming Module.

Log Formats and Versioning

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/logging-intro/log_formats_and_versioning.html

- Removed: v17—The same fields as version 16, but the v17 log format introduces Resource Connector logs and adds the following new fields to the existing logs:
- Added: v17—The same fields as version 16, but the v17 log format introduces Data Loss Prevention (DLP) logs and adds the following new fields to the existing logs:
- Removed: Data Loss Prevention (DLP) logs: taac tenant id, taac profile id, match excerpts, match violation starts, match violation ends, email sender, email recipients, email attachments, email id, email vendor id
- Added: DLP logs: taac tenant id, taac profile id, match excerpts, match violation starts, match violation ends, email sender, email recipients, email attachments, email id, and email vendor id.
- Removed: timestamp,policy identity label,internal client ip,external client ip,destination ip,content type,action,url,referer,user agent,status code,request size,response size,response body size,sha—sha256,categories,av detections,puas,amp disposition,AMP malware name,amp score,policy identity type,blocked categories,identities,identity types,request method,dlp status,certificate errors,file name,ruleset id,rule ID,destination list ids,isolate action,file action,warn status,forwarding method,producer,msp organization id,geo location of blocked destination countries,application ids,hostname,data center,egress,server name,time based rule,security overridden,detected response file type,warn categories,organization id,application entity name,application entity category, egress ip,ai model name,ai suply chain categories,event correlation id,isolation profile id,us
- Added: timestamp,policy identity label,internal client ip,external client ip,destination ip,content type,action,url,referer,user agent,status code,request size,response size,response body size,sha—sha256,categories,av detections,puas,amp disposition,AMP malware name,amp score,policy identity type,blocked categories,identities,identity types,request method,dlp status,certificate errors,file name,ruleset id,rule ID,destination

list ids,isolate action,file action,warn status,forwarding method,producer,msp organization id,geo location of blocked destination countries,application ids,hostname,data center,egress,server name,time based rule,security overridden,detected response file type,warn categories,organization id,application entity name,application entity category, egress ip,ai model name,ai suply chain categories,event correlation id,isolation profile id,source country

- Removed: It refers to the specific name of an application entity within a system.
- Removed: For example, the YouTube Channel "Cisco".
- Added: The specific name of an application entity within the system.
- Added: This field is currently used to identify YouTube channel names only.
- Removed: It represents the classification grouping of application entities based on shared characteristics or functions.
- Removed: For example, the YouTube Category "Networking".
- Added: The classification grouping of application entities based on shared characteristics.
- Added: This field is currently used to identify YouTube categories only.
- Removed: Reserved
- Removed: This field is currently not used.
- Added: egress port
- Added: The egress port number of the network where the request originated.
- Removed: Egress port
- Removed: The source port number used by Secure Access ZTA for a session as it exits the Secure Access ZTA infrastructure toward the destination application.
- Removed: For network tunnel backhauls, the destination network sees this port as the source port of the connection.
- Removed: For Resource Connector backhauls, this field does not represent the source port seen by the destination network.
- Added: zta source port
- Added: The port number used by the Zero Trust proxy service to connect to an unmanaged device requesting a connection to a private resource.

Monitor Secure Access with Reports

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/monitor-with-reports-intro/monitor_secure_access_with_reports.html

- Removed: However, the 'time out' is not reflected in the dashboard.
- Removed: Instead, status is set to "Generating..." and persists.
- Removed: The report remains in this state without resolution.
- Added: However, the timeout is not reflected in the dashboard.
- Added: Instead, status is set to Generating... and persists.
- Removed: If this situation occurs, re-run the report export with a shorter date range, or more filters applied.
- Added: If this situation occurs, rerun the report export with a shorter date range, fewer rows, or more detailed filters.
- Added: For Remote Access Logs, the selected time range and applied filters are used for the export, including filters selected from the filter menu or added from a table value.

About the Remote Access Log Report

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/remote-access-log-intro/remote-access-log-report.html

- Removed: The Remote Access Log report lists users that have remotely connected to Secure Access and requested access to destinations.
- Removed: Some relevant fields to aid debugging and trouble-shooting remote access sessions include:
- Removed: Display Username for Failed Events – Significantly improves how quickly issues can be tracked and addressed.
- Removed: ASA Syslog Message ID Extraction Support – Offers detailed insights by identifying the specific sys-log messages used in the remote access logs.
- Removed: Device ID – Includes the device ID with every event, providing critical help to network administrators in numerous ways.
- Removed: Failed Events for Posture – Provides vital information for effective triage during failed connection attempts.
- Added: The Remote Access Log report lists connection events for users who connect remotely to Secure Access.
- Added: Use the report to investigate connection activity, troubleshoot failed sessions, and identify access issues.
- Added: Some relevant fields include:
- Added: Display username for failed events – Helps you identify the affected user.
- Added: ASA syslog message ID – Helps you identify the syslog message associated with the event.
- Added: Device ID and device name – Helps you identify the endpoint.
- Added: Machine name – Identifies the client machine when the value is returned for the event.
- Added: Endpoint posture information – Provides posture details for failed events when posture data is returned.
- Added: Connection information – Includes the VPN profile, session type, IP addresses, operating system, and Secure Client version.
- Added: Use the time-range control and the filter menu to refine the report.
- Added: Depending on the selected time range and the data returned for that period, you can filter by user, country, region, posture profile, session type, device name, machine name, IP address, VPN profile, reason code, and Security Group Tag information.
- Added: Some filters provide fixed choices, some provide values found in the report data, and some accept a value that you enter.
- Added: You can also hover over a supported value in a table column and select the search control to add that value to the applied filters.
- Added: Use table settings to change the visible columns or table density.
- Added: The report supports sorting for supported columns, including User, Region, and VPN Profile.
- Added: Select a row to expand its details.
- Added: The expanded area can include Source, Endpoint Posture, Connection, and Tunnels information.
- Added: Endpoint Posture details can include the posture attributes evaluated for the event and the posture profile used for the evaluation.
- Added: If the posture profile is linked, select the link to open that posture profile.
- Removed: You can use filters to refine results and help identify security issues that require attention.
- Removed: Access Allowed

- Added: Status
- Added: Connected
- Added: Disconnected
- Added: Failed
- Added: Warning: User
- Added: Machine Name
- Added: Device Name
- Added: IP Address
- Added: Country
- Added: VPN Profile
- Added: Posture Profile
- Added: Region
- Added: Session Type
- Added: Reason Code
- Added: IKEv2 Check
- Added: Access Allowed Geocompliance Service Unavailable
- Added: IP Assignment Failed
- Added: Unknown
- Removed: DDNS Update Failed
- Removed: Geocompliance Service Unavailable
- Removed: IKEV2 Check
- Removed: Static IP Addr Assignment Fail
- Removed: Identities lets you filter by connection events with Security Group Tags (SGT) you have configured rules to traffic originating from IP addresses in network segments that include SGTs.
- Removed: When present, SGTs will be appended to the User column value.
- Added: DDNS update failed
- Added: OS Version
- Added: Client Version
- Added: Security group tag lets you filter by connection events with Security Group Tags (SGT) you have configured rules to traffic originating from IP addresses in network segments that include SGTs.
- Added: When present, SGTs are appended to the User column value.
- Removed: Note Each filter is dynamic, except for Identities, and will only display filter option values that are present in the connection data.
- Removed: If no option values are present in the data for a filter, that filter remains hidden.
- Added: Note Some filters provide fixed options, some display values found in the connection data, and some accept a value that you enter.

- Added: A data-driven filter displays only option values that are present in the connection data for the selected time frame.
- Added: If no option values are present, the filter remains hidden.
- Removed: Option 1: Click the View Details icon (the blue ellipsis at the right end of each row).
- Removed: Option 2: Hover over an Event Details field in any row, then click Read More below the ASA syslog message ID.
- Added: Navigate to Monitor> Reports> Remote Access Logs.
- Added: Click the expand icon at the start of any row.
- Added: This expands the row and displays the event details.
- Removed: Result: The Event Details drawer displays detailed information about an individual event.
- Removed: Extra information is available in the Event Details window:
- Removed: Last Connected– The timestamp when this users was last connected to the machine.
- Removed: Posture profile information– The posture profile associated with the event.
- Added: Result: The event details display in the expanded row as Source, Endpoint Posture, and Connection cards.
- Added: Extra information is available in the event details:
- Added: Last Connected - The timestamp when this user was last connected to the machine.
- Added: Source - The Source card can include Date & Time, User, OS Type & Version, Device Name, Origin ID, Origin type, Country, Public IPv4 address, Public IPv6 address, and Security Group Tag.
- Added: Endpoint Posture - The Endpoint Posture card displays posture information.
- Added: It can show the posture profile applied to the event or indicate that no posture profile is applied.
- Removed: Reason Code– The reason code for VPN incompatibilities.
- Removed: Syslog Information–Syslog information related to the event you are examiningwith timestamps, syslog server IP, and indication of a logging message
- Removed: At the bottom of the Event Details window click View More Details to view VPN specific event details.
- Removed: The following categories is displayed:
- Removed: Duration– The duration of the event.
- Removed: Machine ID– The unique identifier assigned to the client machine.
- Removed: Redirect ACL– The redirect access control l (ACL) that originates from the user or device.
- Removed: Redirect URL–The URL where a user is automatically sent after attempting to access a different URL.
- Removed: Security group Tag– The unique identifier assigned to a device or user, representing their security role or access level within the network.
- Removed: Audit Session ID– The unique identifier generated and associated with a user's process when they successfully log in or connect.
- Removed: Tunnels– How many tunnels are contained within the VPN profile and tunnel information.
- Removed: From your search results, you can click an identity or destination and go to their respective detailed report.
- Added: Connection - The Connection card can include Connection Event, Reason Code, Syslog Info, Region, Internal IPv4 Address, Internal IPv6 Address, Last Connected, VPN Profile, Session Type, and Secure Client Version.

- Added: It can also display session duration, inactivity, redirect, security group tag, and audit session information.
- Added: Reason Code - The reason code for VPN incompatibilities.
- Added: Syslog Information - Syslog information related to the event you are examiningwith timestamps, syslog server IP, and indication of a logging message.
- Added: Review the following additional event details:
- Added: Duration - The duration of the session.
- Added: Inactivity - The amount of time that the session was inactive.
- Added: Redirect ACL - The redirect access control (ACL) that originates from the user or device.
- Added: Redirect URL - The URL where a user is automatically sent after attempting to access a different URL.
- Added: Security Group Tag - The unique identifier assigned to a device or user, representing their security role or access level within the network.
- Added: Audit Session ID - The unique identifier generated and associated with a user's process when they successfully log in or connect.
- Added: Tunnels - Select View tunnels to view tunnel information.
- Added: If the event includes more than one tunnel, select the corresponding tunnel tab to view each tunnel's details.
- Added: From your search results, you can click an identity or destination and go to its detailed report.

Integrate Cisco Identity Intelligence with Secure Access

https://www.cisco.com/c/en/us/td/docs/security/secure-access/secure-access-help/CiscoSecureAccessHelp/secure-access-integrations-intro/integrate-cisco-identity-intelligence.html

- Added: Onboarding