

Cisco Secure Access Service Edge (SASE)

With Meraki SD-WAN

Design Guide

September 2021

Contents

Scope	3
In scope	3
Out of scope	3
Introduction	4
Solution Overview	5
SASE Business Flows	5
SASE Design	7
Connect	7
Control	10
Converge	16
SASE Deployment	18
Connect - Branch Networks	18
Connect - Roaming Workforce	21
Control	36
Converge	63
Validation Tests	81
Remote Worker to Public Application (SaaS)	81
Remote Worker to Private Application (VPNless)	93
Remote Worker to Private Application (VPN)	100
Branch DIA	104
Branch to Data Center	120
Appendix	122
Appendix A - Meraki Remote Access VPN	122
Appendix B - Install the Cisco Umbrella Root Certificate	123
Appendix C - Umbrella Web Selective Decryption List	127
Appendix D - Acronyms Defined	129
Appendix E - References	130

Scope

In scope

Cisco SASE design guide with Meraki covers the following components:

- Cisco Meraki SD-WAN
- Cisco Umbrella Secure Internet Gateway
 - DNS Security
 - Secure Web Gateway
 - Cloud Delivered Firewall including IPS
 - Data Loss Prevention
 - Remote Browser Isolation
- Cisco Secure Access by Duo
 - Multi-factor authentication
 - VPNless access to private applications (Duo Network Gateway)
 - Single sign on
- Cisco Remote Access VPN
 - Cisco AnyConnect
 - Cisco Firepower Threat Defense
- Cisco Secure Endpoint
- Cisco ThousandEyes
- Cisco SecureX
 - Visibility Dashboard

Out of scope

Cisco SASE design guide with Meraki does not cover the following topics:

- The Meraki scope has been limited to basic WAN connectivity and the creation of IPsec tunnels to Umbrella from a high availability pair. Capabilities such as quality of service, TCP flow optimization or service chaining have not been evaluated in this design
- Cisco Meraki Systems Manager for cloud-based mobile device management
- Security has been assumed to exist in the Data Center, but the level of security, and the use of those tools have not been included in this design guide
- Cisco Secure Endpoint has been included in its most basic form. Creation of custom policies is out of scope for this guide
- Cisco Secure Malware Analytics, the file sandboxing engine used by Cisco Secure Endpoint, is not in scope for this design guide
- Laptops and desktop clients are the only sources of traffic. No smartphones or internet of things devices were used in the creation of this guide

Introduction

Today's workforce expects seamless access to applications wherever they are, on any device. It is now common practice to provide remote employees with direct access to cloud applications such as Office 365 and Salesforce with additional security. The need for cloud-delivered security service expands daily as contractors, partners, IoT devices and more each require network access. IT needs to protect users and devices as if they were located at a corporate office or branch. Each requires secure access to applications and must now be treated as a 'branch of one'.



Figure 1.
High level SASE Architecture

In this new paradigm, IT requires a simple and reliable approach to protect and connect with agility. This is forcing a convergence of network and security functions closer to users and devices, at the edge—and is best delivered as a cloud-based, as-a-service model called secure access service edge (SASE).

Solution Overview

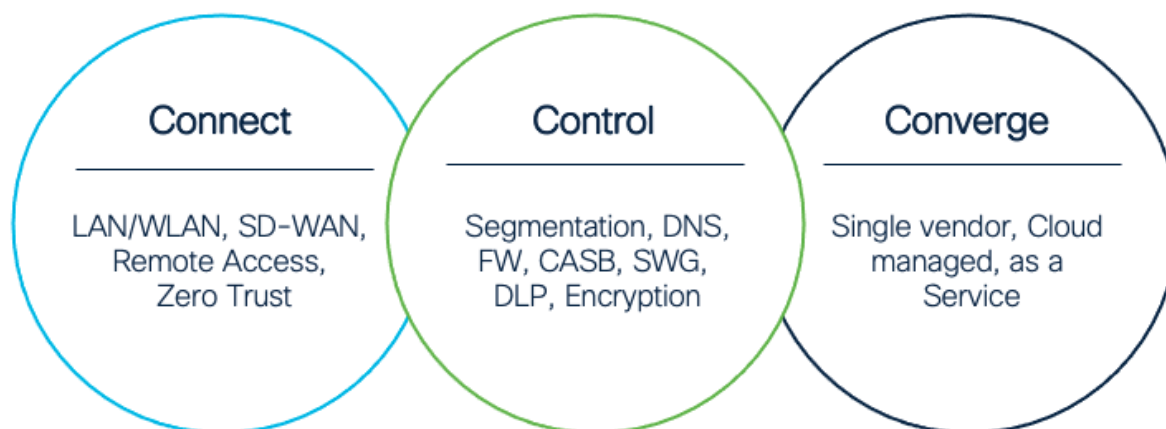


Figure 2.
Three C's for SASE

The SASE architecture has three core components:

- **Connect** – Unleash your workforce by delivering a seamless connection to applications in any environment from any location
- **Control** – Simplify security, streamline policy enforcement, and increase threat protection by combining multiple functions into a single, cloud-native service
- **Converge** – Unite security and networking through a flexible, integrated approach that meets multi-cloud demands at scale

For a full breakdown of the architecture, see the [Cisco SASE Architecture Guide](#).

SASE Business Flows

In the Cisco SASE Architecture guide, the concept of SAFE business flows was introduced. Cisco SAFE uses the concept of business flows to simplify the analysis and identification of threats, risks, and policy requirements for effective security. This enables the selection of very specific capabilities necessary to secure them.

This design guide addresses the following business flows for a SASE network:

- An unmanaged device accessing business critical SaaS applications
- A managed device browsing the public Internet, such as researching product information
- An unmanaged device accessing corporate applications that are publicly accessible
- A managed device accessing corporate applications that are not publicly accessible

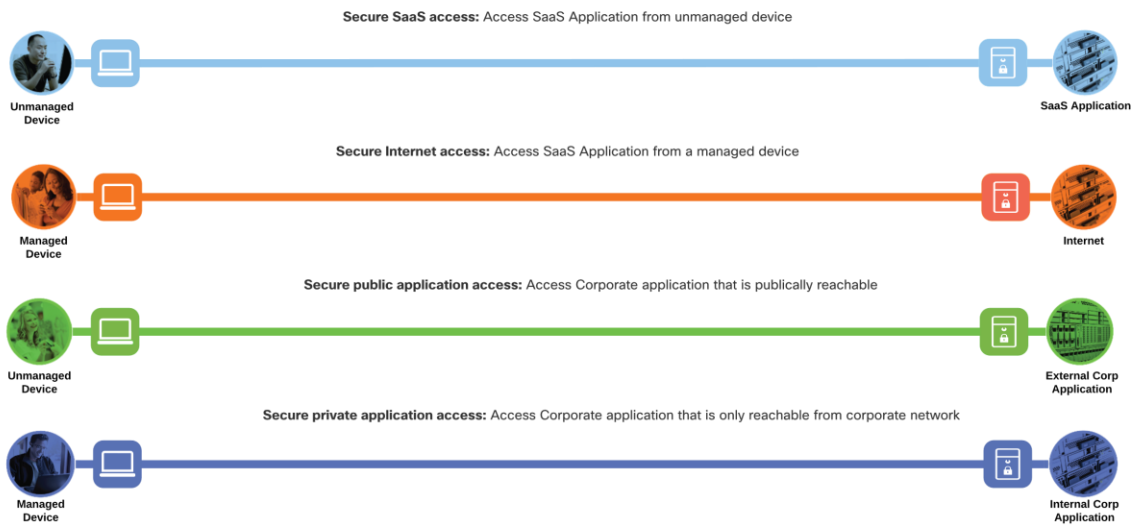


Figure 3.
SASE Business Flows

Not all business flows have the same requirements. Some use cases are subject to a smaller attack vector and therefore require less security to be applied. Some have larger and multiple vectors and require more. Evaluating the business flow by analyzing the attack surfaces provides the information needed to determine and apply the correct capabilities for flow specific and effective security. This process also allows for the application of capabilities to address risk and administrative policy requirements.

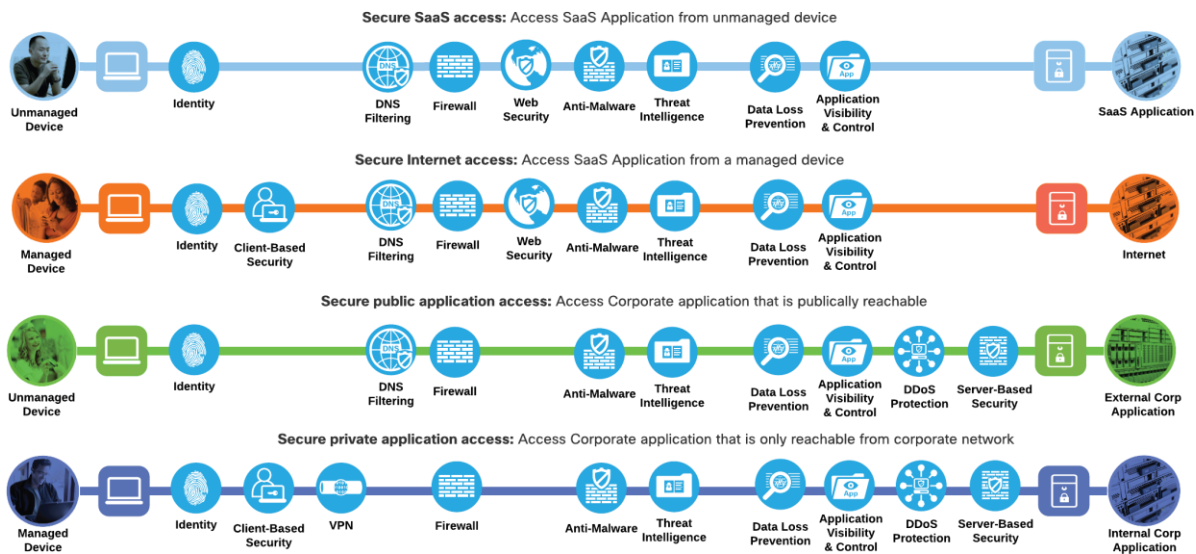


Figure 4.
SASE Business Flows with required capabilities

SASE Design

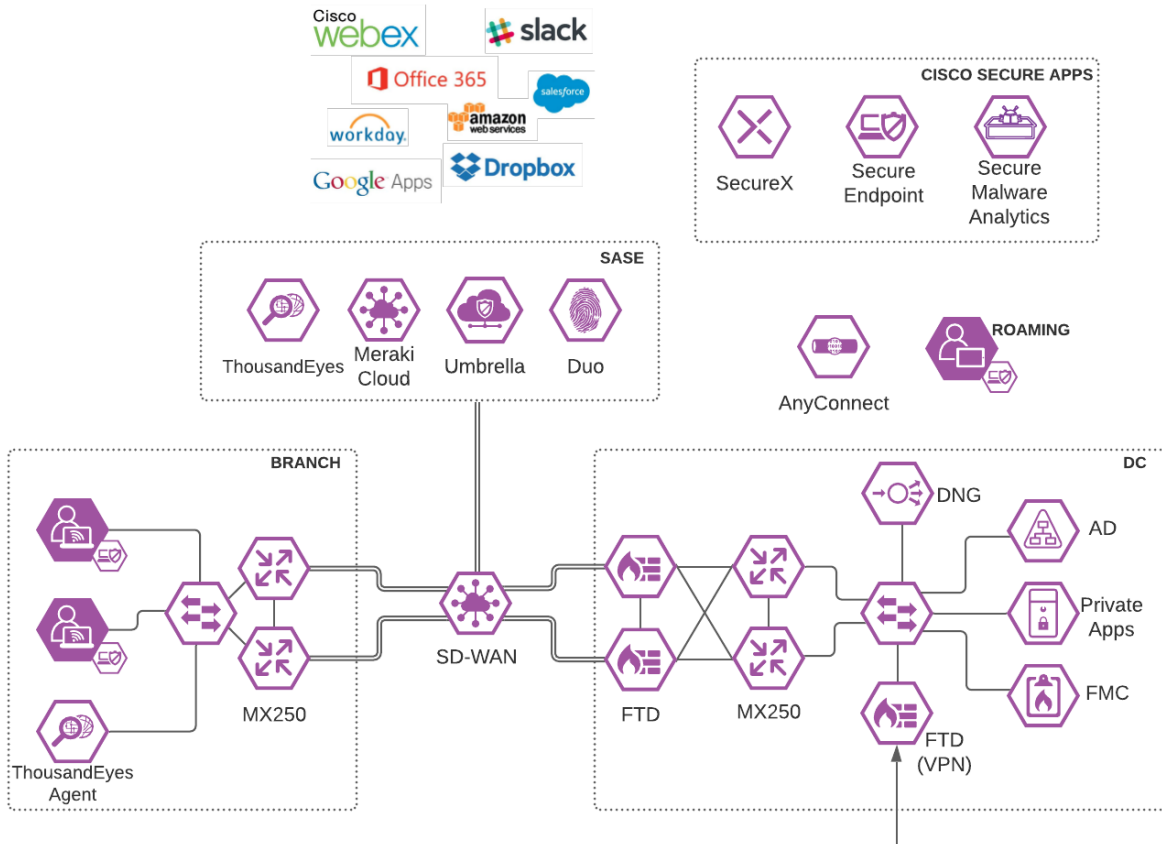


Figure 5.
Cisco SASE Architecture

Connect

Meraki SD-WAN with Umbrella SIG

Software-defined WAN (SD-WAN) is a suite of features designed to allow the network to dynamically adjust to changing WAN conditions without the need for manual intervention by the network administrator. By providing granular control over how certain traffic types respond to changes in WAN availability and performance, SD-WAN can ensure optimal performance for critical applications and help to avoid disruptions of highly performance-sensitive traffic, such as VoIP. Additionally, SD-WAN can be a scalable and often much cheaper alternative to traditional WAN circuits like multiprotocol label switching (MPLS) lines. All Cisco Meraki security appliances are equipped with SD-WAN capabilities that enable administrators to maximize network resiliency and bandwidth efficiency.



Cisco Secure SD-WAN



Figure 6.
Meraki SD-WAN

Enabling direct internet access (DIA) from the branch is simplified with Cisco SD-WAN technology. The Cisco SD-WAN and Umbrella integration enables you to infuse effective cloud security throughout your SD-WAN fabric. Cloud security can be deployed to thousands of branches in a matter of minutes, instantly gaining protection against threats on the internet.

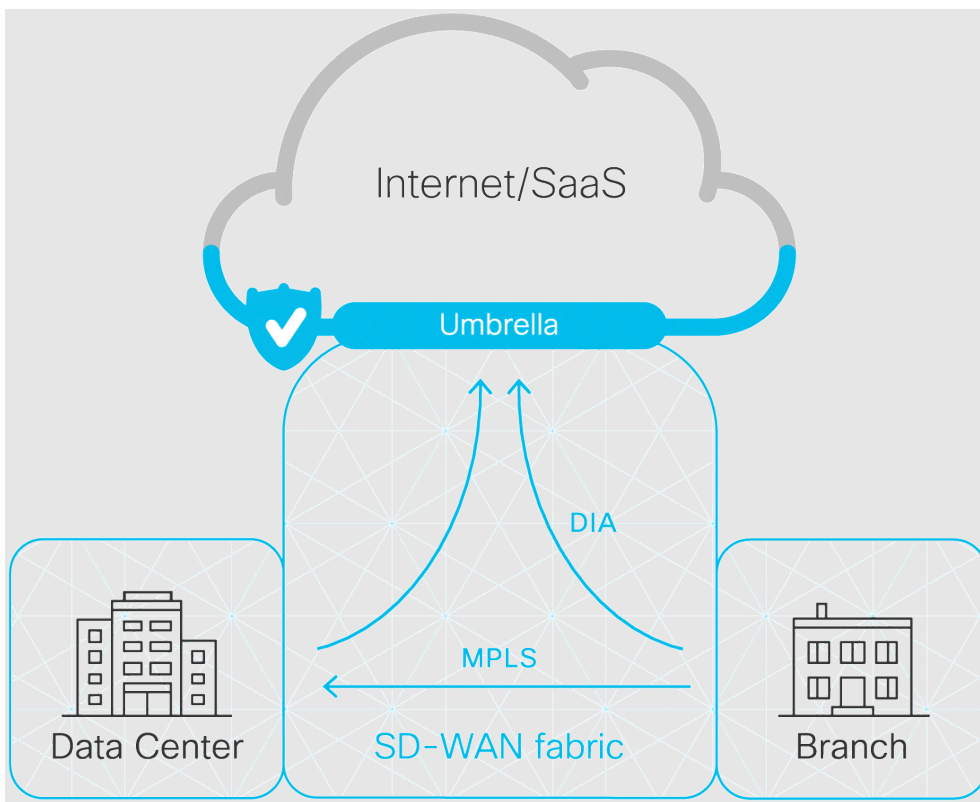


Figure 7.
Meraki/Umbrella Integration

AnyConnect

Cisco AnyConnect is unified security endpoint agent that delivers multiple security services to the roaming workforce.



Figure 8.

Cisco AnyConnect Secure Mobility Client

Cisco AnyConnect not only provides VPN access through Secure Sockets Layer (SSL) and IPsec IKEv2 but also offers enhanced security through various built-in modules. Modules used in this guide include:

- **Off-Network Protection** – Cisco Umbrella Roaming module protects devices while not connected to a trusted network. This module forces all traffic through Umbrella SIG, enabling consistent policies to be applied to users on and off net
- **AMP Enabler** – Cisco AnyConnect AMP Enabler is used as a medium for deploying Cisco Secure Endpoint, formerly Advanced Malware Protection (AMP). This approach provides the roaming workforce with an additional security agent that detects potential malware threats, allowing for removal of said malware and the quarantine of devices from doing further harm in the network when they try to connect back to the enterprise

For information on additional AnyConnect features, such as the ability to do NetFlow analysis for the roaming workforce, see [Cisco AnyConnect Secure Mobility Client](#).

Duo Network Gateway

Duo Network Gateway (DNG) allows users to access on-premises websites, web applications, and SSH servers without having to worry about managing VPN credentials, while also adding security with Duo MFA (discussed in the Control section below).

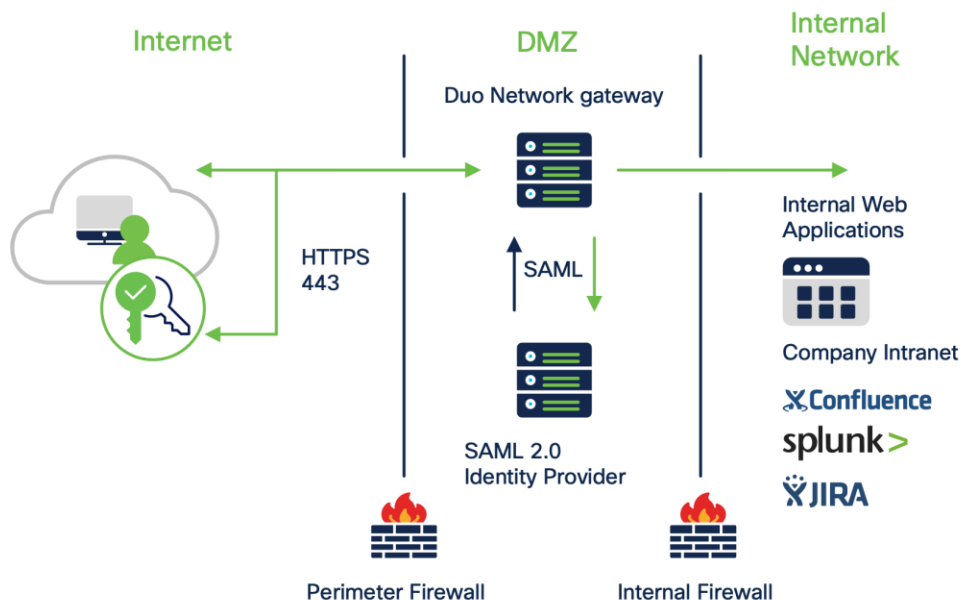


Figure 9.
Cisco Duo Network Gateway

DNG gives you granular access control per web application, set of SSH servers, and user groups. You can specify different policies to make sure only trusted users and endpoints are able to access your internal services. For example, you can require that SharePoint users complete two-factor authentication at every login, but only once every seven days when accessing Confluence. Duo checks the user, device, and network against an application's policy before allowing access to the application.

Control

Umbrella

With the advent of the cloud era, network architectures designed to provide robust connectivity to a corporate data center is increasingly inefficient and must evolve. Most of the network traffic today occurs either within the data center itself (East-West traffic) or from an organization's various locations to the cloud via the Internet (North-South traffic). As a result, backhauling network traffic from remote or branch locations over MPLS wide-area network (WAN) links, or roaming user traffic over virtual private network (VPN) connections, is no longer an efficient or viable option. Organizations are increasingly providing DIA broadband links for their remote, branch, and roaming users to access their SaaS applications without the slow performance and latency associated with backhauling traffic to a corporate office with a single security stack. To alleviate the inconvenience of separately managing security settings at each branch location, Umbrella Secure Internet Gateway (SIG) provides a cloud managed solution.

Cisco Umbrella SIG unifies multiple functions in a single solution that traditionally required a set of on-premises security appliances (firewalls, proxies, gateways) or single function cloud-based security solutions. Umbrella combines secure web gateway (SWG), firewall, DNS-layer security, cloud access security broker (CASB)

functionality, remote browser isolation (RBI), data loss prevention (DLP), plus interactive threat intelligence in one cloud-delivered service.

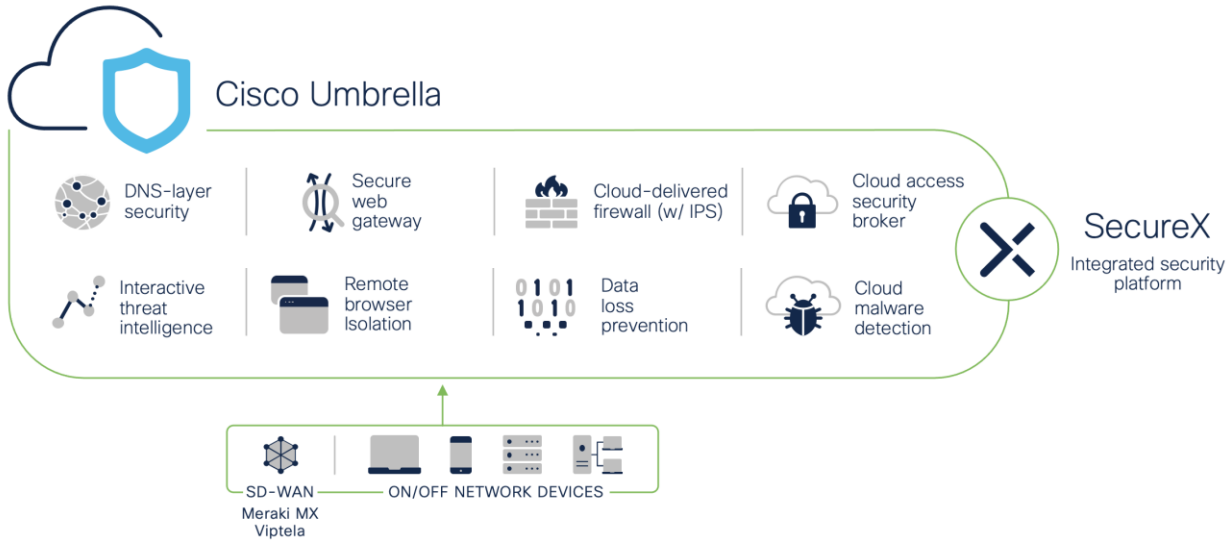


Figure 10.
Umbrella

Brief summaries of key Cisco Umbrella functions:

DNS Security



Figure 11.
SAFE Capability - DNS Filtering

By enforcing security at the DNS and IP layers, Umbrella blocks requests to malicious and unwanted destinations before a connection is even established – stopping threats over any port or protocol before they reach your network or endpoints. Highlights include:

- The visibility needed to protect internet access across all network devices, office locations, and roaming users
- Detailed reporting for DNS activity by type of security threat or web content and the action taken
- Ability to retain logs of all activity for as long as needed
- Fast rollout to thousands of locations and users to provide immediate return on investment

Secure Web Gateway (SWG)



Figure 12.
SAFE Capability - Web Security

Umbrella includes a cloud-based full proxy that can log and inspect all your web traffic for greater transparency, control, and protection. IPsec tunnels, PAC files and proxy chaining can be used to forward traffic for full visibility, URL and application-level controls, and advanced threat protection. Highlights include:

- Content filtering by category or specific URLs to block destinations that violate policies or compliance regulations
- The ability to efficiently scan all uploaded and downloaded files for malware and other threats using the Cisco Secure Endpoint (formerly Cisco AMP) engine and third-party resources
- Cisco Secure Malware Analytics (formerly Threat Grid) rapidly analyzes suspicious files
- File type blocking (e.g., block download of .exe files)
- Full or selective SSL decryption to further protect your organization from hidden attacks and time-consuming infections
- Granular app controls to block specific user activities in select apps (e.g., file uploads to Dropbox, attachments to Gmail, post/shares on Facebook)
- Detailed reporting with full URL addresses, network identity, allow or block actions, plus the external IP address

Cloud-Delivered Firewall (CDFW)



Figure 13.
Web Capability - Firewall

The Umbrella CDFW provides visibility and control for traffic that originated from requests going to the internet, across all ports and protocols. Highlights include:

- Deployment, management and reporting through the Umbrella single, unified dashboard
- Customizable policies (IP, port, protocol, application and IPS policies)
- Layer 3 / 4 firewall to log all activity and block unwanted traffic using IP, port, and protocol rules
- Layer 7 application visibility and control to identify and control access to thousands of applications
- Intrusion Prevention System (IPS) to examine network traffic flows and prevent vulnerability exploits with an added layer of threat prevention using SNORT 3 technology

- Detection and blocking of vulnerability exploitation
- Scalable cloud compute resources eliminate appliance capacity concerns Cisco Talos threat intelligence to detect and block more threats

Cloud Access Security Broker (CASB)



Figure 14.
SAFE Capability - Application Visibility & Control

Umbrella helps expose shadow IT by detecting and reporting on cloud applications in use across your environment. Insights can help manage cloud adoption, reduce risk and block the use of offensive or inappropriate cloud applications. Highlights include:

- Reports on vendor category, application name, and volume of activity for each discovered app
- App details and risk information such as web reputation score, financial viability, and relevant compliance certifications
- Cloud malware detection to detect and remove malware from cloud-based applications and ensure that applications remain malware-free
- Ability to block/allow specific apps
- Tenant restrictions to control the instance(s) of SaaS applications that all users or specific groups/individuals can access.

Data Loss Prevention (DLP)



Figure 15.
SAFE Capability - Data Loss Prevention

As more companies move toward cloud-based services, company data becomes more vulnerable to both malicious exfiltration and unintentional misuse by inexperienced users. Umbrella DLP analyzes data in-line to provide visibility and control over sensitive data leaving your organization. Highlights include:

- Easy enablement as part of Umbrella secure web gateway
- 80+ built-in content classifiers including personally identifiable information (PII), payment card industry (PCI), and personal health information (PHI)
- Content classifiers are customizable with threshold and proximity to tune and reduce false positives
- Create user-defined dictionaries with custom phrases (such as project code names)

- Detection and reporting on sensitive data usage and drill-down reports to help identify misuse
- Inspection of cloud application and web traffic content and enforcement of data policies

Remote Browser Isolation (RBI)



Figure 16.
SAFE Capability - Remote Browser Isolation as a feature of Web Security

By isolating web traffic from the user device and the threat, Umbrella Remote Browser Isolation (RBI) delivers an extra layer of protection to the Umbrella secure web gateway so that users can safely access risky websites. Highlights include:

- Isolation of web traffic between user device and browser-based threats
- No performance impact on end users
- Protection from zero-day threats
- Granular controls for different risk profiles
- Rapid deployment without changing existing browser configuration
- On-demand scale to easily protect additional users on all devices, browsers, and operating systems

Cisco Secure Access by Duo



Figure 17.
SAFE Capability - Identity

Multi-factor authentication (MFA) from Cisco's Duo protects your applications by using a second source of validation, like a phone or token, to verify user identity before granting access. The modern workforce is more mobile than ever before. Users and devices can connect from anywhere – so companies must protect them everywhere. A zero-trust security model establishes trust in users and devices through authentication and continuous monitoring of each access attempt, with custom security policies that protect every application.



Figure 18.
Cisco Secure Access by Duo

Zero trust can be summed up as “never trust; always verify.” This security approach treats every access attempt as if it originates from an untrusted network – so access won’t be allowed until trust is demonstrated. Once users and devices have been deemed trustworthy, zero trust ensures that they have access only to the resources they absolutely need, to prevent any unauthorized lateral movement through an environment. Highlights of Cisco Secure Access by Duo include:

- **MFA** - Enforce secure identity verification methods, like Duo Push
- **User Access Policies** - Options to set policies for specific user groups either globally or by application
- **Cloud Based Single Sign-On (SSO)** - Enable SSO for any SAML2-enabled app, to consolidate users’ login workflows under a single set of credentials protected by strong MFA
- **Duo Device Health** - Monitor laptop and desktop devices to ensure they have the right security protocols in place
- **Secure Endpoint integration** - When Duo and Cisco Secure Endpoint have shared visibility into a Windows or macOS endpoint, user access can be blocked to applications protected by Duo from endpoints deemed compromised by Cisco Secure Endpoint

Cisco Secure Endpoint with Secure Malware Analytics



Figure 19.
SAFE Capability - Client-Based Security & Network Anti-Malware

Cisco Secure Endpoint offers cloud-delivered endpoint protection and advanced endpoint detection and response across multi-domain control points. Capabilities include:

- **Prevention** - Block known malware automatically leveraging the best global threat intelligence and enforce Zero Trust by blocking risky endpoints from gaining access to applications
- **Detection** - Run complex queries and advanced investigations across all endpoints, and continuously monitor all file activity to detect stealthy malware

- **Response** – Rapidly contain the attack by isolating an infected endpoint and remediating malware across PCs, Macs, Linux, servers, and mobile devices (Android and iOS)

For files that have unknown disposition to Cisco Secure Endpoint, Secure Malware Analytics (formerly Threat Grid) combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware. With a robust, context-rich malware knowledge base, you will understand what malware is doing, or attempting to do, how large a threat it poses, and how to defend against it.

Cisco Secure Malware Analytics is out of scope for this guide. For more information, see the [Cisco Breach Defense Design Guide](#).

Converge

Seamless integration between Umbrella and Meraki

While both products have their own separate management clouds, the integration between Umbrella (security as a service) and Meraki (networking as a service) is done in minutes to instantly gain protection against threats like malware, ransomware, and C2 callbacks. For additional control and convenience, you can apply Umbrella DNS policies directly in the Meraki dashboard.

This integration ensures that all devices and users on the network are protected by Umbrella. Meraki access points will automatically redirect DNS traffic to Umbrella resolvers, while all network tunnels will terminate in the Umbrella Secure Internet Gateway as discussed above.

Cisco SecureX

Cisco has been on a mission for several years to simplify security. That mission culminated in the launch of the Cisco SecureX platform, which integrates the entire Cisco security portfolio as well as additional security, networking, and IT technologies from both Cisco and third parties. It is included with all the Cisco security products, so once you have one, you can begin using SecureX.



Figure 20.
Cisco SecureX

Cisco SecureX brings together key security technologies considered fundamental for SASE with unified visibility and control through one console. Highlights include:

- **Unified visibility** – Experience simplicity with a customizable dashboard that included operational metrics, visibility into emerging threats, and access to new products in a single click
- **Threat Response** – Accelerate threat investigations and incident management by aggregating and correlating global intelligence and local context in one view

- **Orchestration** – Automate routine tasks using prebuilt workflows that align to common use cases, or build your own workflows with a no-to-low code, drag-and-drop canvas
- **Ribbon and single sign-on** – Use the dashboard ribbon for quick access to Cisco SecureX features. SSO helps share and maintain context around incidents in one location
- **SSO across all Cisco platforms** – Easily access all your Cisco Security products, with one set of credentials, from any device.

Cisco ThousandEyes

With the increased reliance on the internet and cloud services, more networks are outside your ownership or direct control. Organizations need to ensure the performance and integrity of the underlying transport, even when you don't own the infrastructure or control how service providers route traffic.

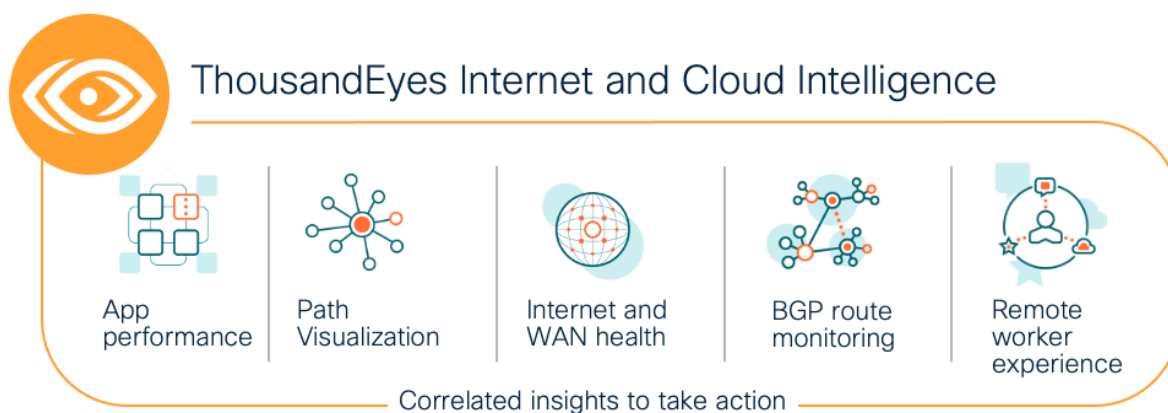


Figure 21.
Cisco ThousandEyes

Cisco ThousandEyes is a network intelligence SaaS platform that allows users to run a variety of tests using global vantage points to monitor DNS resolution, browser response characteristics, detailed aspects of network pathing and connectivity, the status of network routing, and VoIP streaming connection quality. Highlights include:

- Reduce Mean Time to Identify and resolve by immediately pinpointing the source of issues across internal network, ISPs, and cloud and application providers
- Gain successful escalations with service providers based on data that can be easily shared across internal and external stakeholders
- Eliminate wasteful finger pointing and effectively manage OLAs/SLAs across internal teams and external providers

SASE Deployment

Connect - Branch Networks

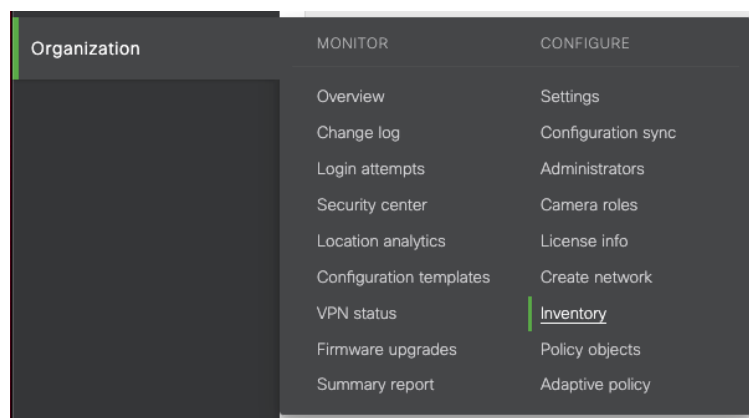
Meraki SD-WAN

This design guide consists of an MX250 pair in both the branch site and data center. The hardware installation for these appliances, along with the initial network configuration for internet connectivity can be found in the [MX250 Installation Guide](#).

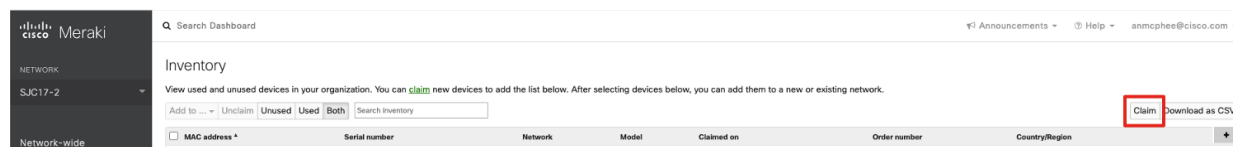
Add devices to inventory

For this design guide, appliances were added to the Meraki dashboard using individual serial numbers after they were installed in the lab. An alternate approach is to claim your devices with an order number.

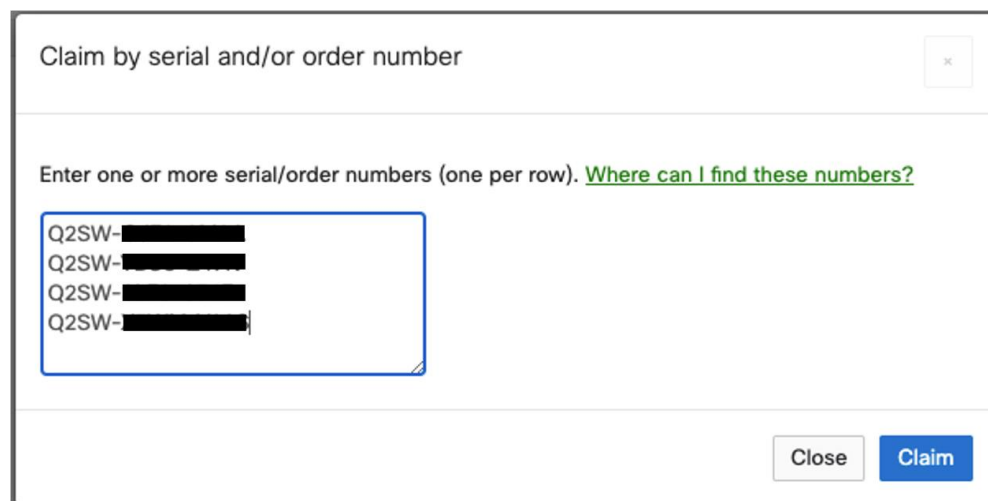
Step 1. In the Meraki Dashboard, navigate to **Organization > Configure > Inventory**.



Step 2. Click **Claim**.



Step 3. Enter all the serial numbers for the devices you wish to add to the Meraki Dashboard. *Note: You can also use an order number to avoid having to add individual serial numbers.*

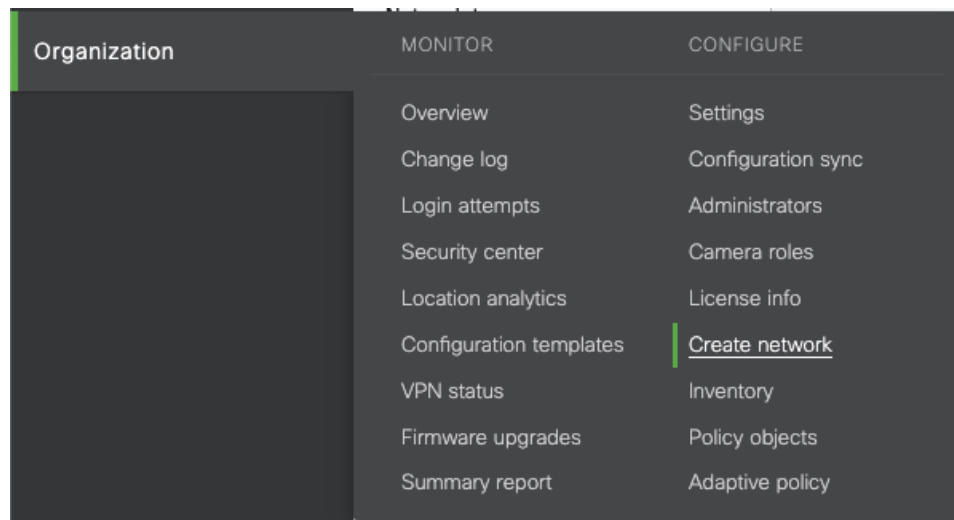


Step 4. Click **Claim**.

Group devices by network

The devices are now available to be added to a network. Dashboard networks provide a way to logically group and configure Meraki devices within an organization and to separate physically distinct sites within an organization.

Step 1. In the Meraki Dashboard, navigate to **Organization > Configure > Create Network**.



Step 2. Give a meaningful name to the network and under the **Network Type** dropdown list click **Combined hardware**.

Note: A network can contain any number of access points or switches, but only a single security appliance. For this design guide, two security appliances have been deployed at each location, however, they have been configured as a high availability pair. For more information see [MX Warm Spare – High Availability Pair](#).

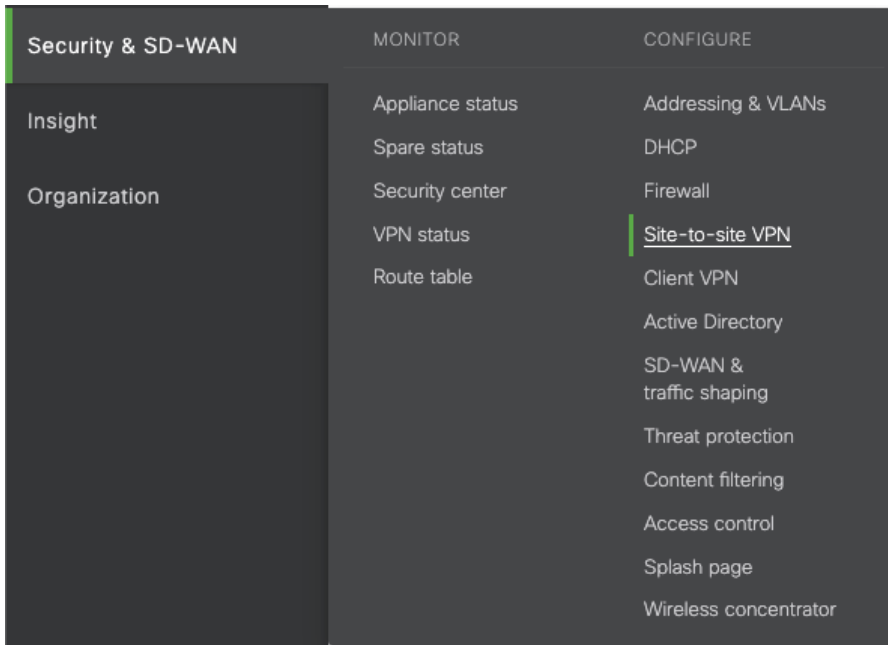
Step 3. Under **Inventory**, check the box for any device that should be added to the network. *Note: This is an optional step as devices can be added/removed after network has been created.*

Step 4. Click **Create Network**.

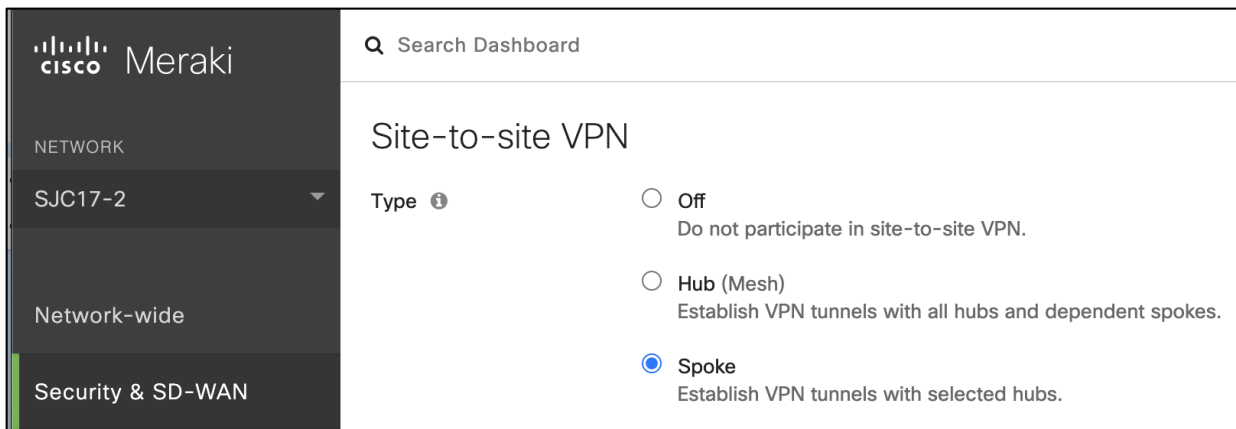
Create routing policies

After the networks have been established, they need to be connected through the SD-WAN network. Meraki Auto VPN is a proprietary technology developed by Meraki that allows you to quickly and easily build VPN tunnels between Meraki MX devices at your separate network branches with just a few clicks.

Step 1. In the Meraki Dashboard, navigate to **Security & SD-WAN > Configure > Site-to-Site VPN**.



Step 2. Select **Hub** or **Spoke**.



Step 3. Click **Save Changes**.

Step 4. Repeat for each network. This design guide is configured to use the data center as a hub and branch as a spoke so that branch networks will establish VPN tunnels to the data center.

Create IPsec tunnel(s) to Umbrella

With Cisco Umbrella being at the center of the Cisco SASE approach, cloud delivered security will be used to protect direct internet breakouts from branch locations. To automatically create a tunnel between branch sites and the Umbrella cloud, see [MX and Umbrella SIG IPsec Tunnel](#).



Connect - Roaming Workforce

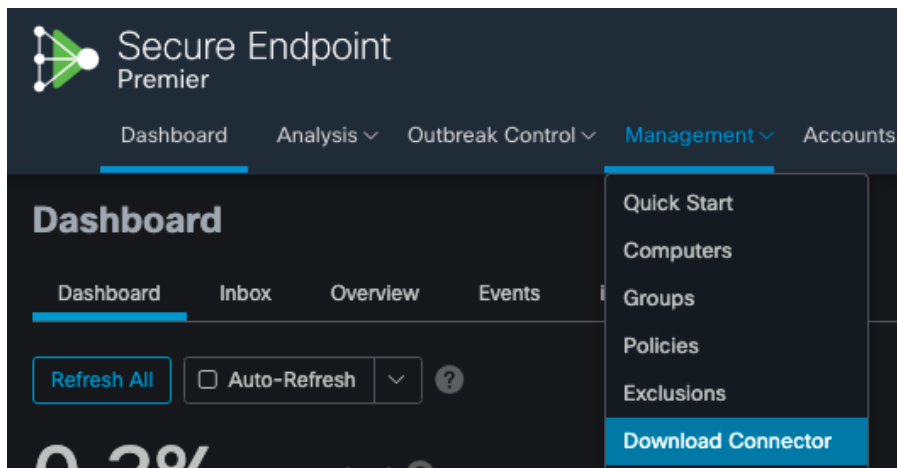
This design guide makes use of Cisco Firepower Threat Defense (FTD) devices to terminate VPN connections. Other deployment options include the use of the Cisco Adaptive Security Appliance (ASA) or natively on the Meraki MX security appliance. A deployment guide for Meraki remote access VPN can be found in Appendix A, which when using RADIUS authentication, offers the same Duo protections that will be shown below.

AnyConnect

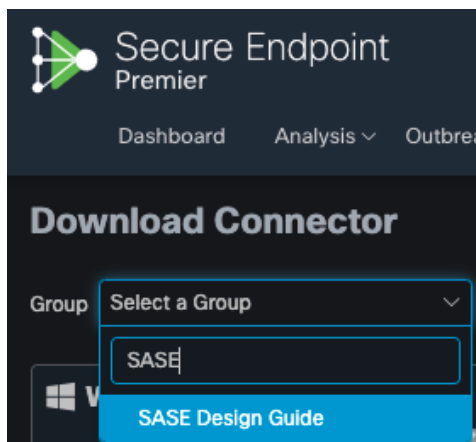
The Cisco AnyConnect Secure Mobility Client software package contains a profile editor for all operating systems. The only profile editor that will be configured for this guide is the AMP Enabler. For details on the other editors, including creating Always On VPN profiles for users in untrusted networks, see the [Cisco AnyConnect Secure Mobility Client Administrator Guide](#).

Step 1. Download and install the stand-alone AnyConnect Profile Editor for Windows. *Note: When using a Cisco ASA as the VPN headend, the Cisco Adaptive Security Device Manager (ASDM) activates the profile editor when you load the AnyConnect client image on the ASA. This design guide is using an FTD, which has no native support for the profile editor.*

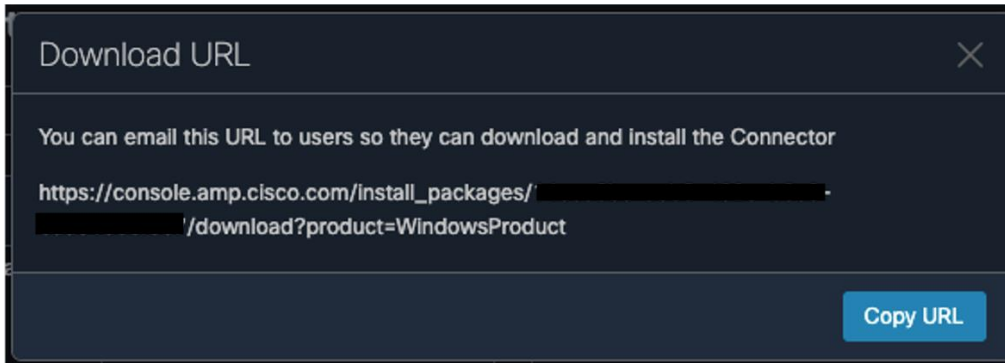
Step 2. In Secure Endpoint cloud, navigate to **Management > Download Connector**.



Step 3. Select the group that this policy applies. *Note: If no group exists, navigate to **Management > Groups** and click **Create Group**.*

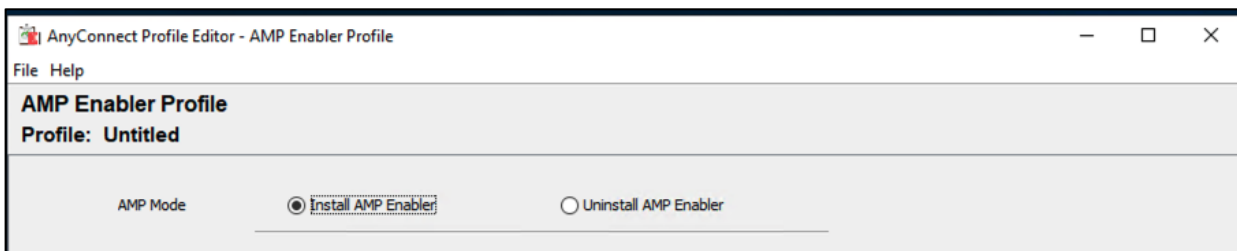


Step 4. For both Windows and Mac, click on **Show URL** and copy them for use in further steps.

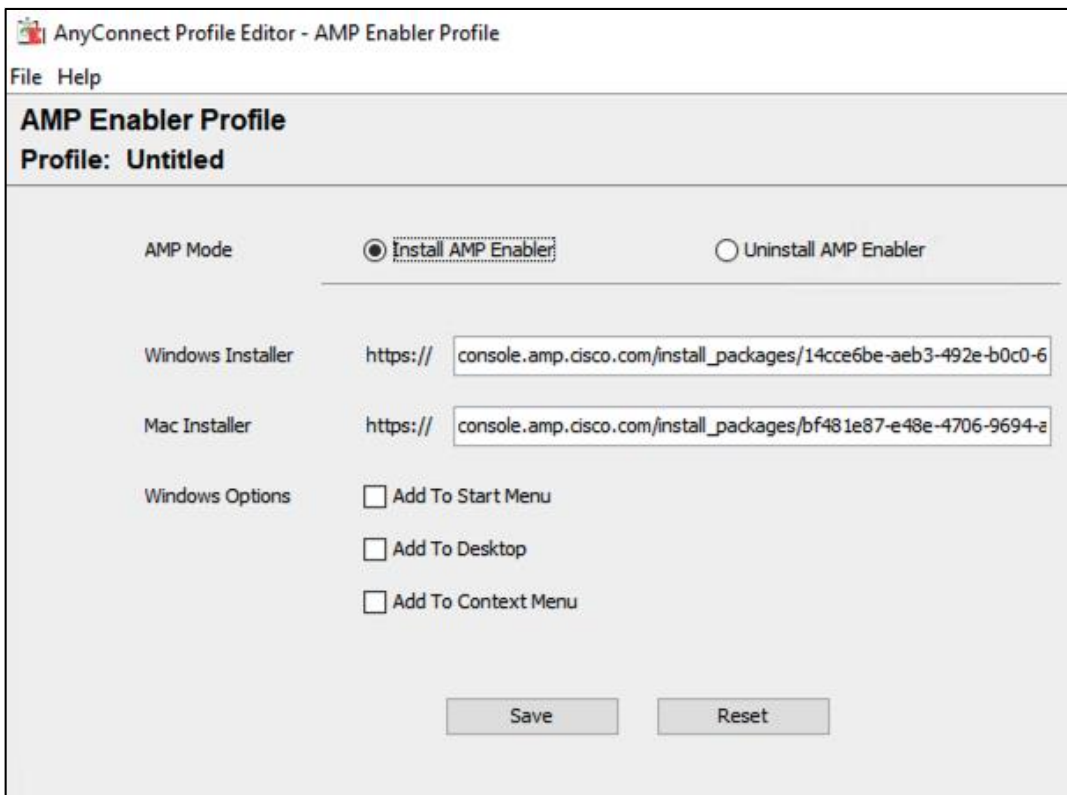


Step 5. On the windows machine that the AnyConnect profile editors have been installed, open the AnyConnect AMP Enable Standalone profile editor.

Step 6. Click **Install AMP Enabler**.



Step 7. Paste the URL for both Windows and Mac from step 4. *Note: Make sure to remove the Https:// from the copied URLs.*



Step 8. Click **Save**. *Note: If you press **Check** beside each URL and **Invalid entry** is returned, copy and paste the link into any browser and check if the file successfully downloads. There is an error with the tool.*

Duo Authentication Proxy

The Duo Authentication Proxy is an on-premises software service that receives authentication requests from local devices and applications via RADIUS or LDAP, optionally performs primary authentication against your existing LDAP directory or RADIUS authentication server, and then contacts Duo to perform secondary authentication. The Duo Authentication Proxy is used in this guide to facilitate MFA for VPN connectivity.

The configuration of the proxy may differ depending on the application you wish to protect and the environment that it is being run in. This design guide used [Cisco FTD VPN with AnyConnect – Install the Duo Authentication Proxy](#) when installing and configuring the proxy. The proxy is installed on an Ubuntu virtual machine and primary credentials are checked against Active Directory. The configuration can be seen below.

```
[ad_client]
host=ad.sasecampus.com
service_account_username=administrator
service_account_password=XXXXXXXXXXXXXXXXX
search_dn=DC=sasecampus,DC=com

[radius_server_auto]
ikey=DIXXXXXXXXXXXXXXXXXXXXXXXXX
skey=zS01XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
api_host=api-aXXXXXXXX.duosecurity.com
radius_ip_1=192.168.128.6
radius_secret_1=XXXXXXXXXXXXXXXXXXXXX
failmode=safe
client=ad_client
port=1812
```

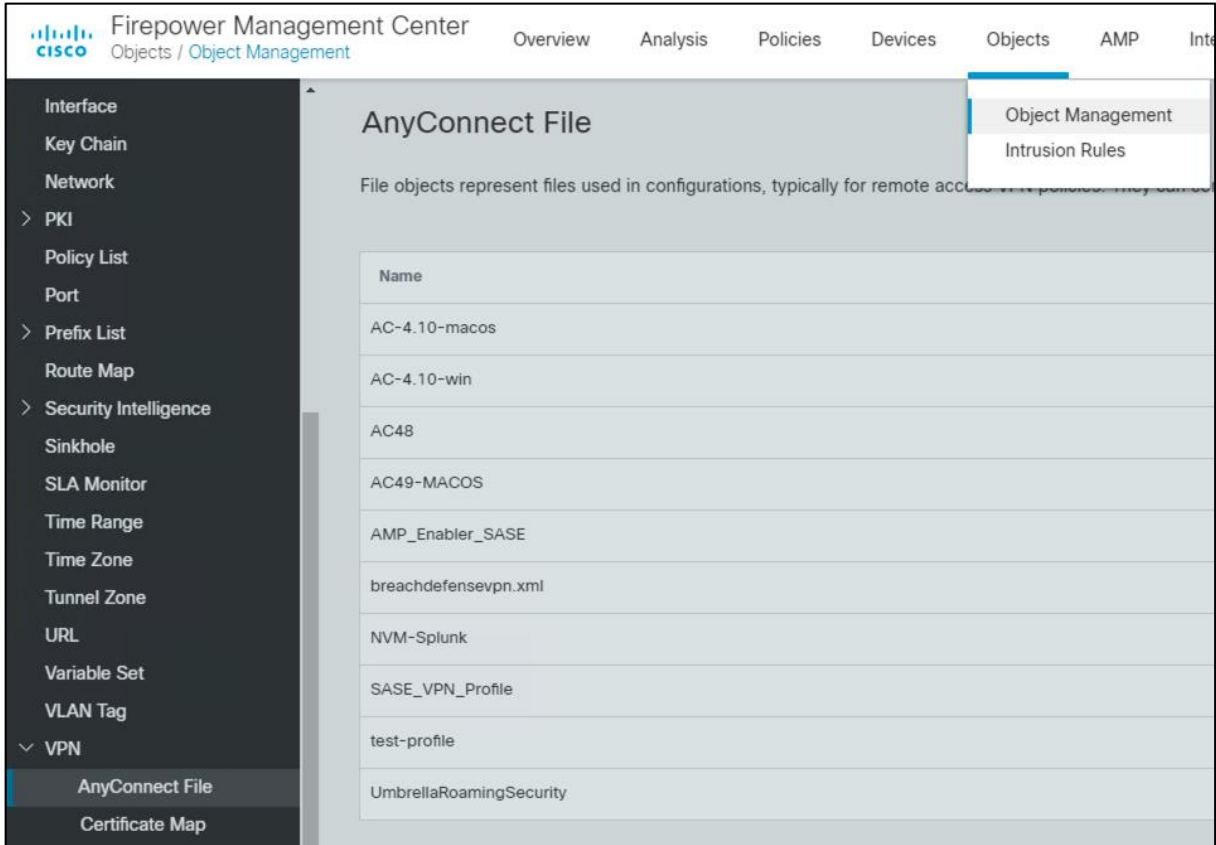
Cisco Secure Firewall - Firepower Threat Defense (FTD) VPN

Cisco Firepower Management Center (FMC) provides a remote access VPN policy wizard to guide you through the required minimal steps to configure the policy. Before you start, complete the following pre-requisites to ensure the configuration elements are in place for use in the policy wizard.

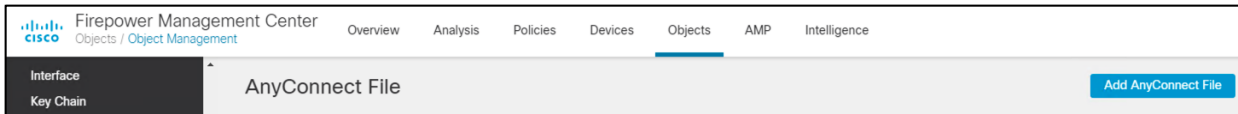
AnyConnect Client Package

Step 1. In Cisco Software Central, download the AnyConnect Headend package for Windows and Mac.

Step 2. In FMC, navigate to **Objects > Object Management > VPN > AnyConnect File**.



Step 3. Click Add AnyConnect File.



Step 4. Give a meaningful name to the AnyConnect File, add the headend package using the **Browse** button, and on the **File Type** dropdown menu click **AnyConnect Client Image**.

The screenshot shows the 'Add AnyConnect File' dialog box. The form fields are:

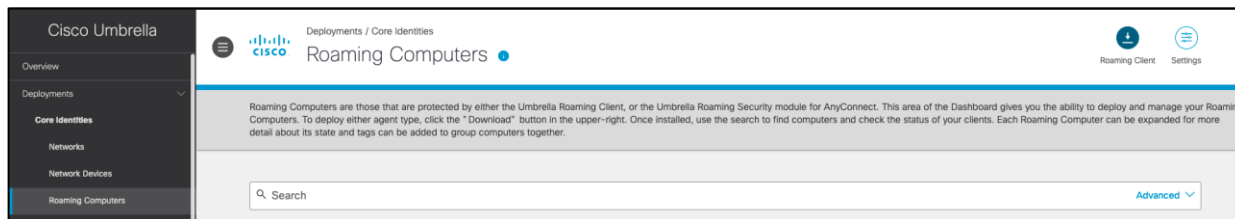
- Name: AC-4.10-win
- File Name: anyconnect-win-4.10.01075-webdeploy (with a 'Browse..' button next to it)
- File Type: AnyConnect Client Image (dropdown menu)
- Description: (empty text box)

The 'Cancel' and 'Save' buttons are at the bottom of the dialog box.

Step 5. Repeat for all headend packages that have been downloaded.

Umbrella Roaming Security Module


Step 1. In Umbrella, navigate to **Deployments > Roaming Computers** and click **Roaming Client**.



Step 2. Under **AnyConnect Umbrella Roaming Security Module**, click **Download Module Profile**.

AnyConnect Umbrella Roaming Security Module

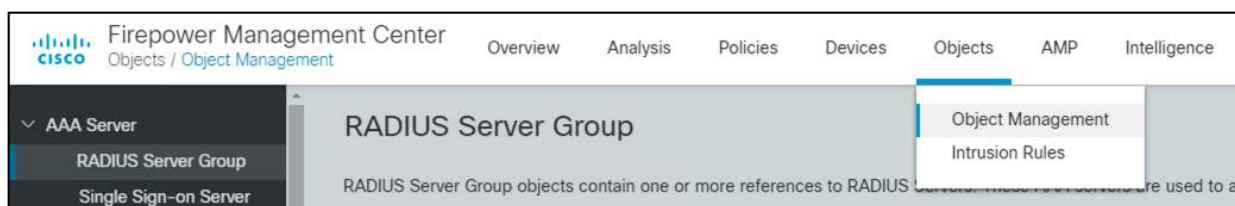
Cisco AnyConnect can be configured to enable an Umbrella Roaming Security module which provides similar functionality to the roaming client. There are many deployment options, and each requires the customized profile downloaded below. [For full documentation, read here.](#)

 **Download Module Profile**
The Umbrella module requires AnyConnect for Windows or macOS, version 4.3 MR1 minimum. 4.3 MR4+ is recommended.

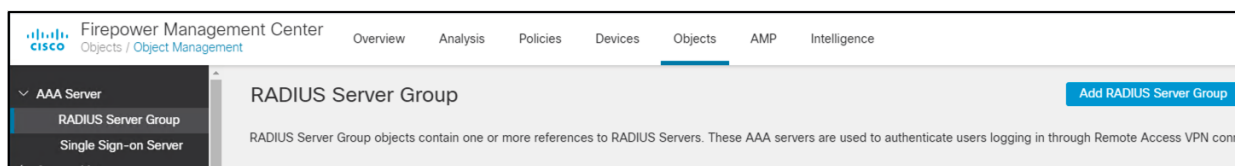
The AnyConnect 4.x client download can be found [here](#) (requires contract).

Duo Authentication Proxy

Step 1. In FMC, navigate to **Objects > Object Management > AAA Server > RADIUS Server Group**.



Step 2. Click **Add RADIUS Server Group**.



Step 3. Give a meaningful name to the server group and add the **IP Address/Hostname** where the Duo Authentication Proxy resides.

Edit RADIUS Server Group

Name:*

Description:

Group Accounting Mode:

Retry Interval:* (1-10) Seconds

Realms:

Enable authorize only

Enable interim account update

Interval:* (1-120) hours

Enable dynamic authorization

Port:* (1024-65535)

RADIUS Servers (Maximum 16 servers) +

IP Address/Hostname
192.168.128.4

Step 4. Click **Save**.

VPN Address Pool

Step 1. In FMC, navigate to **Objects > Object Management > Address Pools > IPv4 Pools**.

The screenshot shows the Firepower Management Center interface. The breadcrumb navigation is **Objects / Object Management**. The left sidebar shows a tree view with **Address Pools** expanded to **IPv4 Pools**. The main content area displays the title **IPv4 Pools** and a description: "IPv4 pool contains list of IPv4 addresses, it is used for diagnostic interface with clustering, or for VPN remote access profiles." A dropdown menu is open over the **Object Management** breadcrumb, showing **Object Management** and **Intrusion Rules**.

Step 2. Click **Add IPv4 Pools**.

The screenshot shows the same Firepower Management Center interface. The breadcrumb navigation is **Objects / Object Management**. The left sidebar shows **Address Pools** expanded to **IPv4 Pools**. The main content area displays the title **IPv4 Pools** and a description: "IPv4 pool contains list of IPv4 addresses, it is used for diagnostic interface with clustering, or for VPN remote access profiles." A blue button labeled **Add IPv4 Pools** is visible in the top right corner of the main content area.

Step 3. Give a meaningful name to the address pool and add the **IPv4 Address Range** you wish to assign to VPN users.

Edit IPv4 Pool ?

Name*

IPv4 Address Range*

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

Description

Allow Overrides

Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

▶ Override (0)

Step 4. Click **Save**.

VPN Split Tunnel List

Step 1. In FMC, navigate to **Objects > Object Management > Network**.

Firepower Management Center

Objects / Object Management

Overview
Analysis
Policies
Devices
Objects
AMP
Intell

- > AAA Server
- > Access List
- > Address Pools
- Application Filters
- AS Path
- Cipher Suite List
- Community List
- > Distinguished Name
- DNS Server Group
- > External Attributes
- File List
- > FlexConfig
- Geolocation
- Interface
- Key Chain
- Network

Network

A network object represents one or more IP addresses. Network objects are used in various places, including searches, reports, and so on.

Name
10_0_0_1
10_0_1_1
10_0_2_253
10_0_2_254
10_0_5_254
any
any-ipv4
any-ipv6

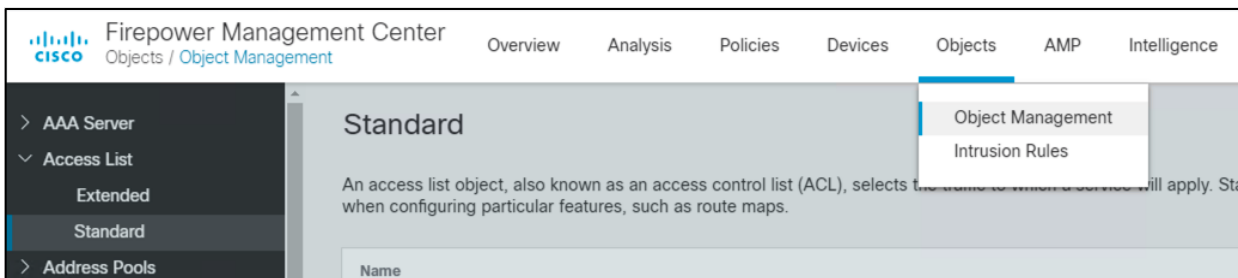
Step 2. In the **Add Network** drop down, click **Add Object**.



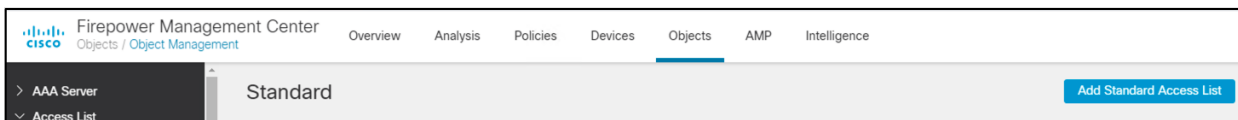
Step 3. Add the **Network** subnet that you would like roaming users to reach through the tunnel. In this design guide, roaming users will only use the VPN tunnel to access private applications, all other traffic will be sent through Umbrella.

Step 4. Repeat for each subnet or host that you would like to be reachable by roaming users.

Step 5. Navigate to **Objects > Object Management > Access List > Standard**.



Step 6. Click **Add Standard Access List**.



Step 7. Give a meaningful name to the split tunnel and add the network object(s) from the previous steps.

Edit Standard Access List Object ?

Name

▼ Entries (1) Add

Sequence No	Action	Network	
1	➔ Allow	SASE_Campus_Subnet	

Allow Overrides

Step 8. Click **Save**.

Remote Access VPN Policy Wizard

The Remote Access VPN Policy wizard in the Firepower Management Center can be used to quickly and easily set up SSL and IPsec-IKEv2 remote access VPNs with basic capabilities. Then, enhance the policy configuration if desired and deploy it to your Firepower Threat Defense secure gateway devices. For this deployment guide, it is assumed that all the above pre-requisites have been completed before getting to this point.

Step 1. In FMC, navigate to **Devices > VPN > Remote Access**.

Firepower Management Center
 Devices / VPN / Remote Access

Overview Analysis Policies **Devices** Objects AMP Intelligence

- Device Management
- Device Upgrade
- NAT
- VPN
- Site To Site
- Remote Access**
- Dynamic Access Policy
- Troubleshooting
- QoS
- Platform Settings
- FlexConfig
- Certificates

Name	Status
RA_VPN	Targeting Up-to-date
SASE_Campus_RA_VPN	Targeting Up-to-date

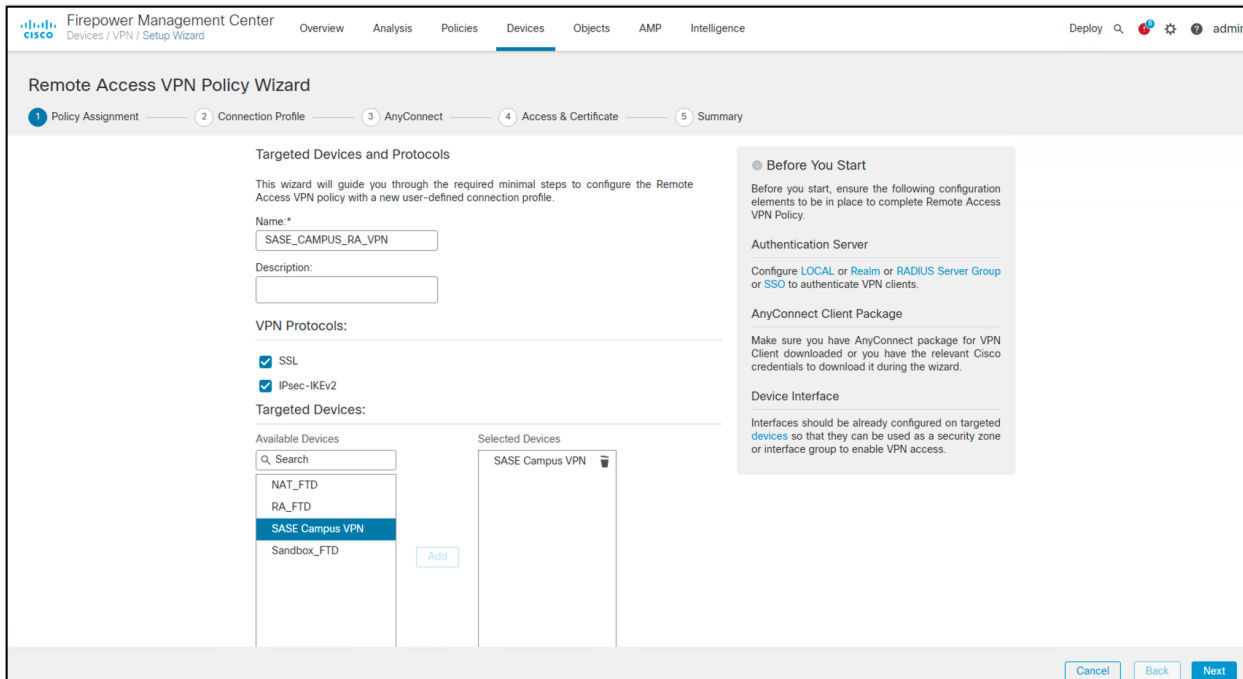
Step 2. Click **Add**.

Firepower Management Center
 Devices / VPN / Remote Access

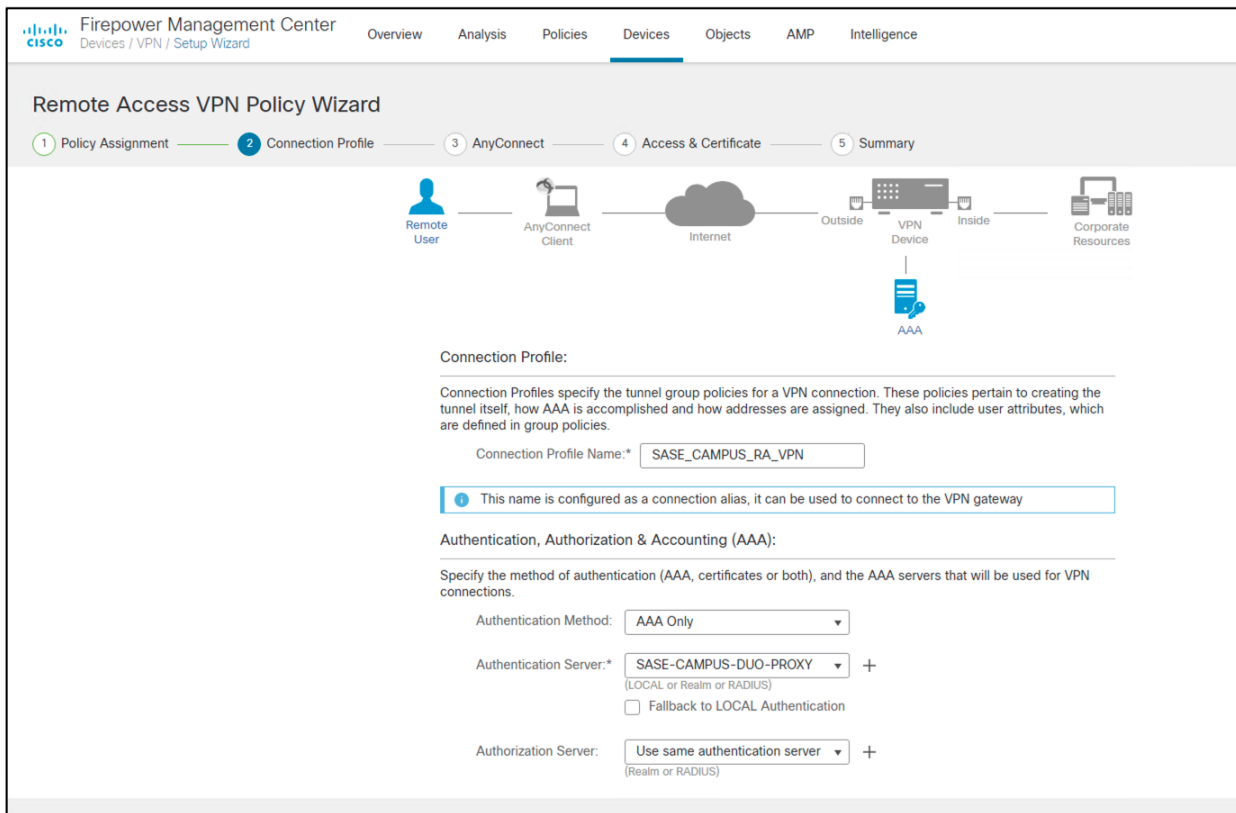
Overview Analysis Policies **Devices** Objects AMP Intelligence

Deploy 🔍 ⚙️ ⚙️ admin ▼

Step 3. Add a meaningful name and click the **FTD(s)** that this policy will apply. Click **Next**.



Step 4. Under **Authentication Server**, choose the **Duo Authentication Proxy** that was configured in a previous step.



Step 5. Add the **IPv4 Address Pool** that was created for VPN users.

Firepower Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects AMP Intelligence

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 **Connection Profile** — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Authorization Server: Use same authentication server (Realm or RADIUS) +

Accounting Server: (RADIUS) +

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ●

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: SASE-CAMPUS-VPN-POOL ✎

IPv6 Address Pools: ✎

Step 6. Under **Group Policy**, click **+**.

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* DfltGrpPolicy +

[Edit Group Policy](#)

Step 7. Give a meaningful name to the policy.

Step 8. In the **General > DNS/WINS** tab, add the DNS server for the internal network. *Note: If this network object does not already exist in FMC, it can be added using the **+** button.*

Step 9. In the **General > Split Tunneling** tab, click **IPv4 Split Tunneling** dropdown and choose **Tunnel networks specified below**. Repeat for IPv6 if applicable.

Step 10. Under **Standard Access List**, choose the Split Tunneling list that was created in a previous step. This will ensure that only the traffic that has been specified will use the tunnel.

General AnyConnect Advanced

VPN Protocols
IP Address Pools
Banner
DNS/WINS
Split Tunneling

IPv4 Split Tunneling:
Tunnel networks specified below ▼

IPv6 Split Tunneling:
Tunnel networks specified below ▼

Split Tunnel Network List Type:
 Standard Access List Extended Access List

Standard Access List:
 SASE_Campus_TunnelList ▼ +

Step 11. Under **DNS Request Split Tunneling**, click **DNS Requests** dropdown and choose **Send only specified domains over tunnel**.

Split Tunneling

Split Tunnel Network List Type:
 Standard Access List Extended Access List

Standard Access List:
 SASE_Campus_TunnelList ▼ +

DNS Request Split Tunneling

DNS Requests:
 Send only specified domains over tunnel ▼

Send DNS requests as per split tunnel policy

Always send DNS requests over tunnel

Send only specified domains over tunnel

Step 12. Enter the domain list for the internal network. All other DNS requests will be sent to Umbrella (when configured).

DNS Request Split Tunneling

DNS Requests:
 Send only specified domains over tunnel ▼

Domain List:
 sasecampus.com

Cancel Save

Step 13. Navigate to the **AnyConnect** tab.

Edit Group Policy

Name:*

Description:

General **AnyConnect** Advanced

Step 14. In the **Client Modules** tab, click the + button.

General **AnyConnect** Advanced

Profile
 Management Profile
Client Modules

Download optional client modules to the endpoint. AnyConnect client requests download from the FTD of only the modules that are configured here.

Step 15. Under **Client Module**, choose **AMP Enabler** and upload the AMP Enabler profile created in a previous step.

Edit Client Module ?

Client Module

Profile to download

Enable module download

Step 16. Click **Enable module download** and click **Add**.

Step 17. In the **Client Modules** tab, click the + button.

Step 18. Under **Client Module**, choose **Umbrella Roaming Security** and upload the **OrgInfo.json** file downloaded from Umbrella in a previous step.

Edit Client Module ?

Client Module

Umbrella Roaming Security ▼

Profile to download

UmbrellaRoamingSecurity ▼ +

Enable module download

Cancel
Save

Step 19. Click **Enable module download** and click **Add**.

Step 20. Click **Save** on the Group Policy.

Step 21. Click **Next** on the Remote Access VPN wizard.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 **Connection Profile** — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Authorization Server: Use same authentication server ▼ +
(Realm or RADIUS)

Accounting Server: ▼ +
(RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ●

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: SASE-CAMPUS-VPN-POOL ✎

IPv6 Address Pools: ✎

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* SASE_VPN_Group_Policy ▼ +
[Edit Group Policy](#)

Cancel
Back
Next

Step 22. Select the AnyConnect Client images that were uploaded in a previous step. Click **Next**.

AnyConnect Client Image

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

[Show Re-order buttons](#) +

	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	AC-4.10-macos	anyconnect-macos-4.10.01075-webdeploy...	Mac OS ▼
<input checked="" type="checkbox"/>	AC-4.10-win	anyconnect-win-4.10.01075-webdeploy-k9...	Windows ▼

Step 23. On the **Interface group/Security Zone** dropdown, choose the FTD interface that users will access for VPN connections.

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* +

Enable DTLS on member interfaces

Step 24. In the **Certificate Enrollment** dropdown, choose the device certificate that will be used to authenticate the VPN gateway. *Note: This design guide used a self-signed certificate that was created using the + button.*

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +

Enroll the selected certificate object on the target devices

Step 25. Click **Next**.

Step 26. Validate the policy information and click **Finish**.

Step 27. Click **Deploy** to send remote access policy to the FTD.

Note: While out of scope for this design guide, it is recommended to create access control rules on the firewall to limit access to VPN users. This can be achieved by using the IPv4 address pool reserved for VPN users and creating an allow list of services they should be able to reach on the network.

Duo Network Gateway

The Duo Network Gateway allows users to access internal web applications without having to join a VPN. Users will be able to access the internal web applications after verifying their identity with a first factor and Duo MFA. For installation and configuration of the DNG see [Install Duo Network Gateway](#).

For this design guide, DNG was installed on an Ubuntu virtual machine and the primary authenticator used was [Duo SSO](#).

Control

Cisco Meraki SD-WAN Security Policy

Cisco Meraki appliances and access points can be configured with Layer 7 firewall rules to block traffic by application or destination hostname. The MX can also perform "Content Filtering," which blocks access to websites based on their content. However, this design guide has made the architectural decision to route all internet bound traffic through Umbrella, and all internal traffic will be sent back to the data center. To simplify the creation and management of security policies, all internet bound security will be performed by Umbrella, and it is assumed in this guide that the data center has the necessary security to protect its network and applications.

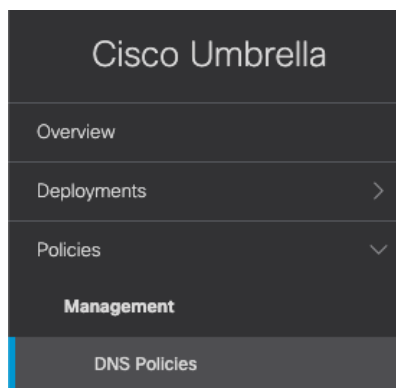
Note: This design guide assumes the use of Umbrella as the centralized enforcement point for the branch. Cisco Meraki appliances also have the capability to enforce security at the branch but its usage is out of scope for this design guide, For more information see [Meraki Content Filtering and Threat Protection](#).

Cisco Umbrella Security Policy

DNS Policies

Domain name system (DNS) resolution is typically the first step when connecting to a service on the Internet. Thus, enforcing security at the DNS and IP layers is the first line of defense against threats and is a great way to stop attacks before users connect to bad destinations.

Step 1. In the Umbrella Dashboard, navigate to **Policies > Management > DNS Policies**.



Step 2. Click **Add**. *Note: Your default policy in Umbrella (bottom of the list) is the catch-all for identities you haven't defined a specific policy for. While a new policy will be created that covers all branch and roaming users, ensure that this policy is defined and enforced for all connections that have not yet been defined.*



Step 3. Choose which type of access control or threats to block. For this design guide, since we have access to the full SIG suite of capabilities, we will only **Block Threats** in the DNS policy. Click **Next**.

How would you like to be protected?

Choose which type of access control or threats to block. Your selection will determine what features are available to the policy, what level of visibility is provided in your reports, and should match how Umbrella is deployed in your environment. For more information, click [here](#).

Select Your Protection:

Access Control
Restrict access with broad category based blocking and/or surgical block and allow destination lists.

- Content Category Blocking**
Block access to destinations based on content category.
- Apply Destination Lists**
Create or modify lists to explicitly block or allow destinations. Note: global block and global allow destination lists are applied by default.
- Application Control**
Block or allow access to applications individually or by group.

Block Threats
Secure your network and endpoints using a variety of antimalware engines and threat intelligence.

- Security Category Blocking**
Ensure domains are blocked when they host malware, command and control, phishing, and more.
- File Analysis**
Inspect files for malware using signatures, heuristics and file reputation (powered by Cisco Advanced Malware Protection).
- IP-Layer Enforcement**
Block threats that bypass DNS lookups by tunneling suspect IP connections. Note: this is only available for roaming computer identities.

[▶ Advanced Settings](#)

[CANCEL](#) [NEXT](#)

Step 4. Select the identity for **Roaming Computers**. This covers all identities that will be enabled through the AnyConnect Roaming Module. Branch identities will be added later through the Meraki Dashboard. Click **Next**.

What would you like to protect?

Select Identities

All Identities

<input type="checkbox"/>	AD Computers	4 >
<input type="checkbox"/>	AD Groups	15 >
<input type="checkbox"/>	AD Users	10 >
<input type="checkbox"/>	Chromebooks	
<input type="checkbox"/>	G Suite OUs	
<input type="checkbox"/>	G Suite Users	
<input type="checkbox"/>	Mobile Devices	
<input type="checkbox"/>	Network Devices	2 >
<input type="checkbox"/>	Networks	2 >

3 Selected [REMOVE ALL](#)

- Roaming Computers 3

[CANCEL](#) [PREVIOUS](#) [NEXT](#)

Step 5. On the **Security Settings** tab, leave as default and click **Next**.

Security Settings

Ensure identities using this policy are protected by selecting or creating a security setting. Click Edit Setting to make changes to any existing settings, or select Add New Setting from the dropdown menu.

Select Setting

Default Settings

Categories To Block [EDIT](#)

- Malware**
Websites and other servers that host malicious software, drive-by downloads/exploits, mobile threats and more.
- Newly Seen Domains**
Domains that have become active very recently. These are often used in new attacks.
- Command and Control Callbacks**
Prevent compromised devices from communicating with attackers' infrastructure.
- Phishing Attacks**
Fraudulent websites that aim to trick users into handing over personal or financial information.
- Dynamic DNS**
Block sites that are hosting dynamic DNS content.
- Potentially Harmful Domains**
Domains that exhibit suspicious behavior and may be part of an attack.
- DNS Tunneling VPN**
VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer.
- Cryptomining**
Cryptomining allows organizations to control cryptominer access to mining pools and web miners.

▶ [INTEGRATIONS](#)

[CANCEL](#) [PREVIOUS](#) [NEXT](#)

Step 6. **Disable File Analysis** (File inspection will occur in the web policies). Click **Next**.

File Analysis

Inspect files for malicious behaviors using a combination of static and dynamic analysis methods, in addition to file reputation and advanced heuristics.

File Inspection
Inspect files for malware using signatures, heuristics and file reputation (powered by Cisco Advanced Malware Protection).

[CANCEL](#) [PREVIOUS](#) [NEXT](#)

Step 7. This design guide will leave the **Block Page** as default. To modify, see [Customize Block and Warn Pages](#). Click **Next**.

Step 8. Give a meaningful name to the policy and review the configuration. *Note: **Ensure the Intelligent Proxy is disabled under Advanced Settings**. If there is no option to disable, edit the policy after it has been saved and the button will appear.* Click **Save**.

Policy Name

SASE Design Guide

4 Identities Affected
3 Roaming Computers, 1 Network Device
[Edit Identity](#)

2 Destination Lists Enforced
1 Block List
1 Allow List
[Edit](#)

Security Setting Applied: Default Settings
Command and Control Callbacks, Malware, Phishing Attacks, plus 5 more will be blocked
SecureX Integration is enabled.
[Edit](#) [Disable](#)

File Analysis Not Enabled
Requires Intelligent Proxy
File Inspection Not Enabled

No Content Settings Applied
[Enable](#)

Umbrella Default Block Page Applied
[Edit](#) [Preview Block Page](#)

Application Setting Applied: Default Settings
LinkedIn, Microsoft Office Online, Gmail, plus 1 more will be allowed.
4shared, Alibaba, Baidu, plus 777 more will be blocked.
[Edit](#) [Disable](#)

Advanced Settings

Enable Intelligent Proxy
Gain visibility into threats, content, or apps by proxying web connections for risky domains.

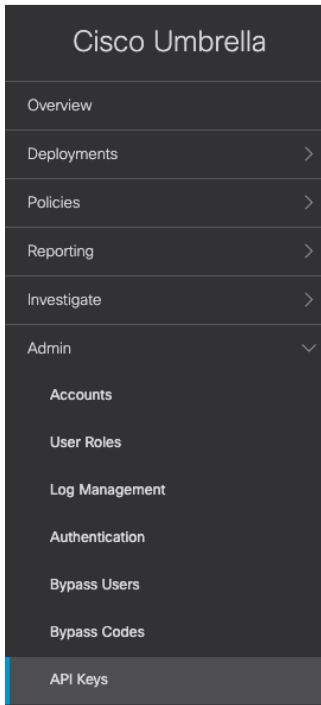
SSL Decryption
Enabling SSL decryption allows the intelligent proxy to inspect traffic over HTTPS and block custom URLs in destination lists. Turning on SSL decryption allows HTTPS URL blocking.

Enable IP-Layer Enforcement
Gain visibility into threats that bypass DNS lookups by tunneling suspect IP connections. Note: this is only available for Roaming Computer identities.

Integrate Cisco Umbrella & Cisco Meraki using API keys

After the DNS policy has been created, integrating Umbrella DNS with a Meraki Network is a simple process that requires only a few steps.

Step 1. In the Umbrella Dashboard, navigate to **Admin > API Keys**.



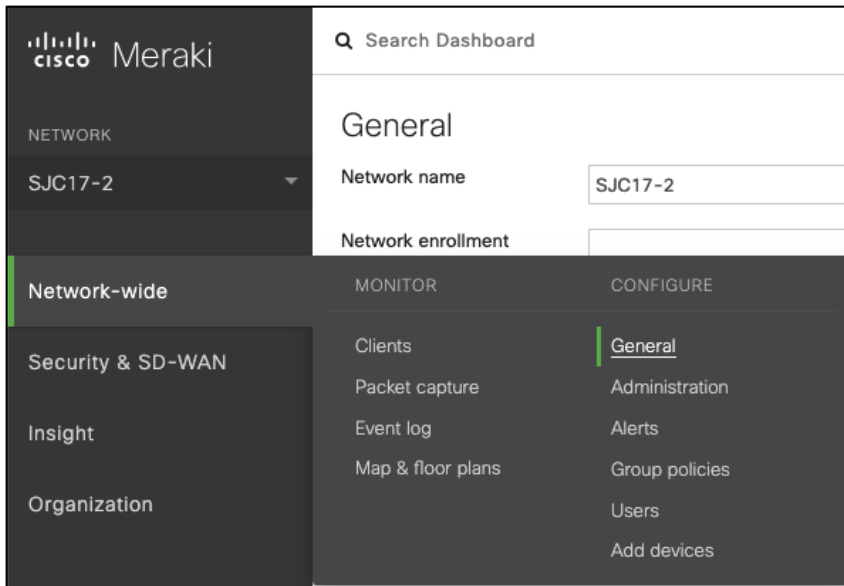
Step 2. If there is no existing key for **Umbrella Network Devices**, click **Create**.

Step 3. Select **Umbrella Network Devices** and click **Create**.

Step 4. Copy both the **Key** and **Secret**. *Note: make sure to store the secret somewhere secure as it will only ever be shown once.*

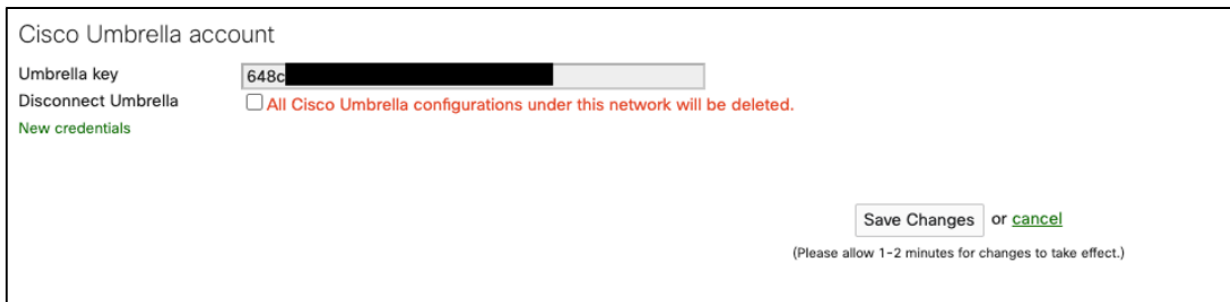


Step 5. In the Meraki Dashboard, navigate to **Network-wide > Configure > General**.



Step 6. At the bottom of the page, under **Cisco Umbrella Account**, click **New Credentials**.

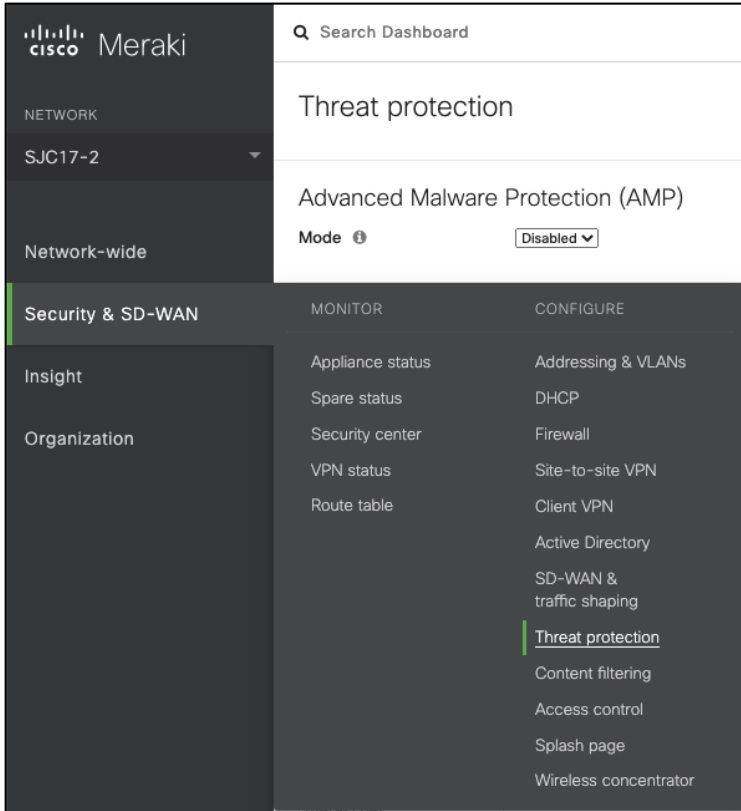
Step 7. Paste the **Umbrella API key** and **secret** in the appropriate fields and click **Save Changes**.



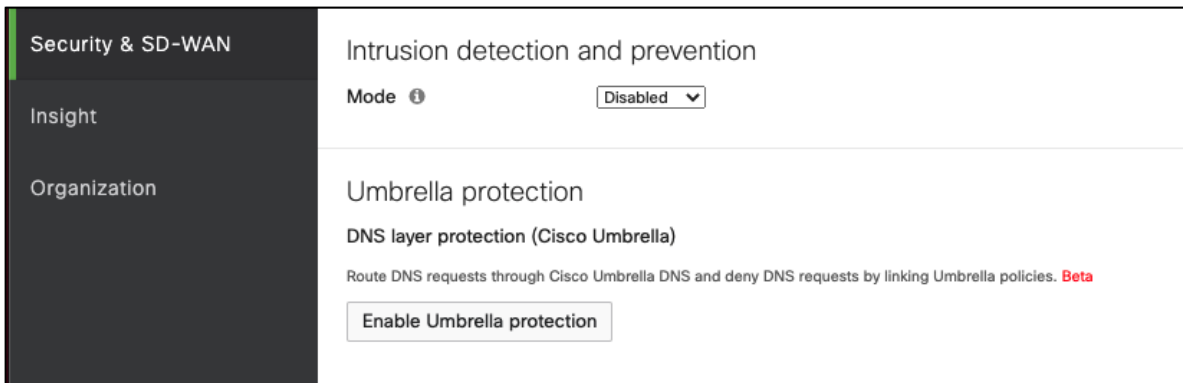
Add Cisco Umbrella DNS policy to Cisco Meraki network

At this point, DNS policies configured in Cisco Umbrella can now be applied to the Cisco Meraki network.

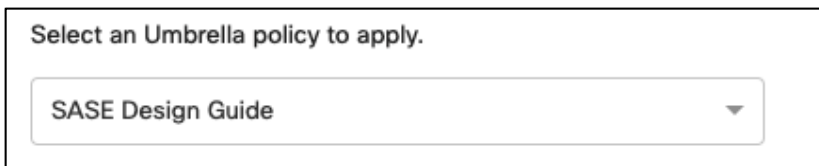
Step 1. In the Meraki Dashboard, navigate to **Security & SD-WAN > Threat Protection**.



Step 2. Under **Umbrella protection**, click **Enable Umbrella protection**.



Step 3. Under **Select an Umbrella policy to apply**, click on the newly created policy from the previous steps.



Step 4. Specify any domains that should not be forwarded to Umbrella.

Specify one or more domain names below (one per row) to be excluded from being routed to Cisco Umbrella.

Umbrella.

sasecampus.com

Save Changes or [cancel](#)

(Please allow 1-2 minutes for changes to take effect.)

Step 5. Click **Save Changes**.

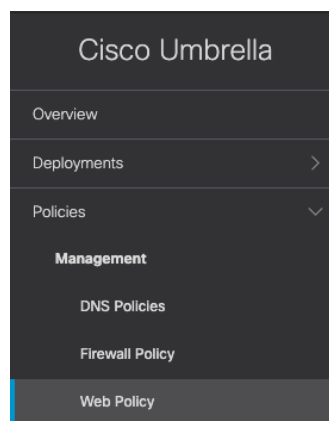
Web Policies

A cloud-based web proxy or SWG provides security functions such as malware detection, file sandboxing and dynamic threat intelligence, SSL decryption, app and content filtering, and DLP.

There are two parts to configuring the web policy:

- **Configuring a ruleset:** enable a ruleset by selecting identities and then configuring ruleset settings to determine protection options for that ruleset.
- **Add rules to a ruleset:** add rules to set actions (allow, block, and warn) against individual identities and the destination those identities attempt to access.

Step 1. In the Umbrella Dashboard, navigate to **Policies > Management > Web Policy**.



Step 2. Click **Add**.



Step 3. Expand the newly created rule set.

Step 4. Give a meaningful name to the ruleset by clicking the **Edit** button in the **Ruleset Name** row. Click **Save**.

▲ Ruleset Settings

Ruleset settings affect the rules within the ruleset and are not applied globally throughout your Web policy. Various settings listed must be configured through their respective components before being set here.

Ruleset Name Save

Step 5. Click the **Edit** button next to **Ruleset Identities**.

Step 6. Choose the **Identity** that this ruleset applies to. For this design guide, the identities chosen were the **Network Tunnels** associated with our branch and all **Roaming Computers**. Click **Save**.

Ruleset Identities

You must select ruleset identities for them to be added to this ruleset and have this ruleset enabled. Identities matching the ruleset can then be evaluated against the rules within the ruleset. This has the effect of a logical AND between the ruleset identity and the rule identity. Identities are first added to Umbrella through the Identities page. For more information, see Umbrella's [Help](#).

All Identities	
<input type="checkbox"/> AD Groups	15 >
<input type="checkbox"/> AD Users	10 >
<input checked="" type="checkbox"/> Tunnels	6 >
<input type="checkbox"/> Networks	3 >
<input checked="" type="checkbox"/> Roaming Computers	3 >

4 Selected REMOVE ALL

- Roaming Computers 3
- SASE Branch

CANCEL SAVE

Step 7. Next to **File Analysis**, click **Edit**.

Step 8. Enable both **File Inspection** and **Threat Grid Malware Analysis**.

File Analysis

Inspect files for malicious behavior using a combination of static and dynamic analysis methods, in addition to file reputation and advanced heuristics. For more information, see Umbrella's [Help](#).

File Inspection
Inspect files for malware using signatures, heuristics and file reputation. Powered by Cisco Advanced Malware Protection.

Threat Grid Malware Analysis
Analyze files for malicious behavior using advanced sandboxing with static and dynamic threat intelligence. Requires File Inspection.

Sandbox Region ⓘ

North America ▾

By checking this box, you acknowledge that once saved you cannot change your sandbox region.

[CANCEL](#) [SAVE](#)

Step 9. Next to **File Type Control**, click **Edit**.

Step 10. Choose the file types to block for this ruleset. For validation purposes, **Batch** files will be blocked. For more information, see [Manage File Type Control](#). Click **Save**.

File Type Control

Select file types to block for this ruleset. Umbrella checks a file based on its file extension and also uses a detection engine to evaluate the file and determine its type. For more information, see Umbrella's [Help](#).

🔍 Search File Types

All File Types / Executables

- apk
- bat
- bin
- cgi
- com
- dll
- exe
- hta
- jar
- is

1 Selected [REMOVE ALL](#)

bat	1
-----	---

[CANCEL](#) [SAVE](#)

Step 11. Next to **HTTPS Inspection**, click **Edit**.

Step 12. Click **Enable HTTPS Inspection**. *Note: A root certificate is required in any circumstances where Umbrella must proxy, and decrypt HTTPS traffic intended for a website. For certificate installation see **Appendix B**.*

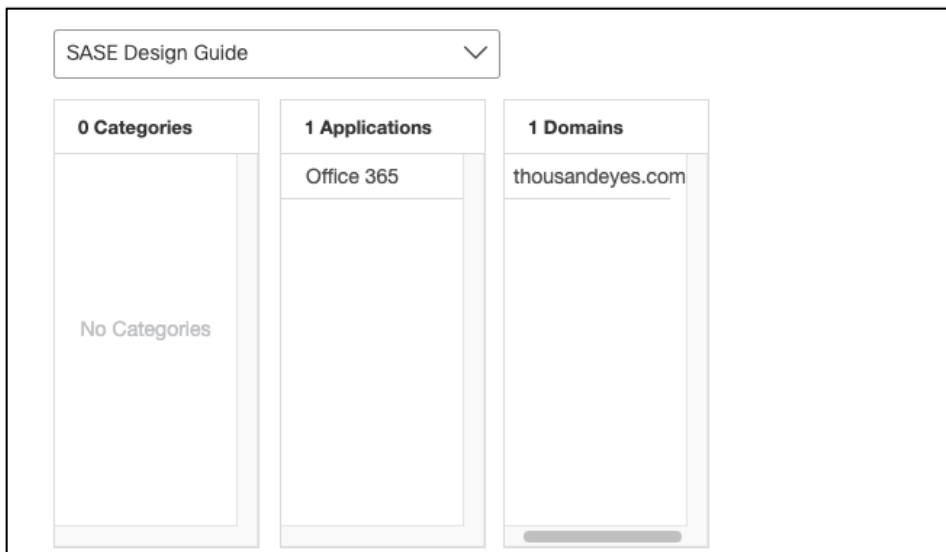
HTTPS Inspection

Select how Umbrella handles HTTPS traffic for this ruleset. For more information, see Umbrella's [Help](#).

Enable HTTPS Inspection

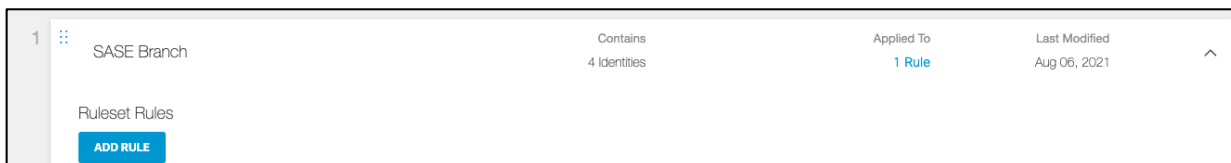
HTTPS traffic is intercepted and decrypted to provide security and ruleset enforcement at the URL layer, and visibility into the URL path. By default, HTTPS inspection attempts to decrypt all HTTPS traffic. To bypass HTTPS inspection, add a Selective Decryption List.

Step 13. Select the **Web Selective Decryption List**. *Note: Umbrella's Selective Decryption List component excludes selected content categories, applications, and domains from inspection when HTTPS Inspection is enabled for a ruleset. For more information on the excluded list for this design guide, see **Appendix C**.*



Step 14. Click **Save**.

Step 15. Scroll back to the top of the policy and click **Add Rule**.



Step 16. Give a meaningful **Rule Name**. For this rule we will block specified content categories.

Step 17. Under **Rule Action**, select **Block**.

Priority	Rule Name	Rule Action	Identities	Destinations
	Social Media Block	Block	No Selections Add Identity	No Selections Add Destination

Allow - Security Enforced
Allows selected ruleset identities access to destinations unless Umbrella detects a security issue.

Warn
Warns selected ruleset identities before allowing access to destinations.

Block
Blocks selected ruleset identities from accessing destinations. ✓

Isolate
Isolates selected ruleset identities' web requests in a virtual cloud-based browser.

Rule Settings

Ruleset settings affect the rules within the rule before being set here.

Ruleset Name

Ruleset Identities

Block Page

Tenant Controls

File Analysis

Step 18. Under **Identities**, click **Add Identity** and choose the option to **Inherit Ruleset Identities**. Click **Apply**.

IDENTITIES 1 Selected

- AD Groups 15 >
- AD Users 10 >
- Network Tunnels 6 >
- Networks 3 >
- Roaming Computers 3 >

Inherit Ruleset Identities
 [CANCEL](#)
[APPLY](#)

Step 19. Under **Destinations**, click **Add Destination** and choose an **Application Setting** to block. For validation testing, all **Social Networking** will be selected. Click **Apply**.

3 Social Media Block Block Ruleset Identities 114 Applications ... Any Day, Any Time

[Edit Identity](#) [Edit Destination](#) [Change Schedule](#) [CANCEL](#) [SAVE](#)

No additional configuration applied

Select Application Setting

social networking

1 Selected

Social Networking 114 >

[CANCEL](#) [APPLY](#)

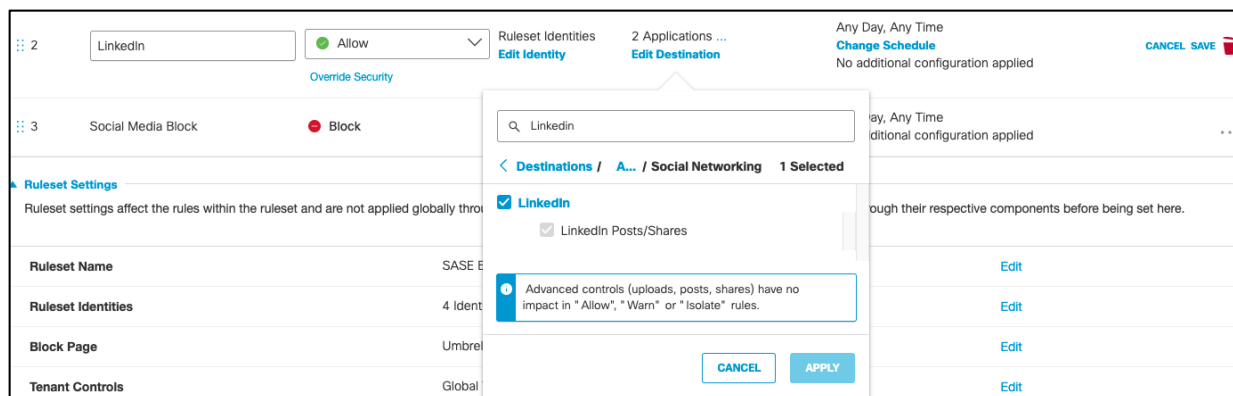
Ruleset settings affect the rules within the ruleset and are not applied globally through their respective components before being set here.

Ruleset Name	SASE E	Edit
Ruleset Identities	4 Ident	Edit
Block Page	Umbrel	Edit
Tenant Controls	Global	Edit
File Analysis	7 Settings	Edit

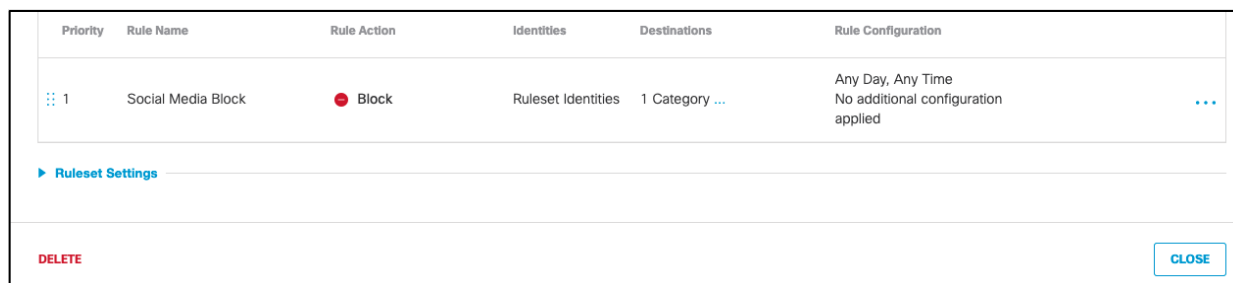
Step 20. **Rule Configurations** will not be used in this design guide. For more policy options, such as enforcing during a specified time of day, see [Add Rules to a Ruleset](#).

Step 21. Click **Save** on the rule.

Step 22. Web policies will be enforced on the first match. To allow specific social media sites, such as **LinkedIn**, create an **Allow** rule and place it *above* the **Block** rule. *Note: An alternate approach is to modify the Application Settings for a web policy. This would allow a user to remove LinkedIn from the Social Media category for a given policy. For more information, see [Manage Application Settings](#).*



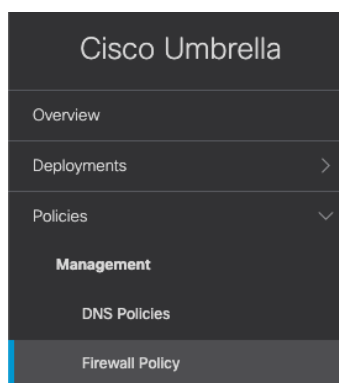
Step 23. At the bottom of the policy, click **Close** to save the policy.



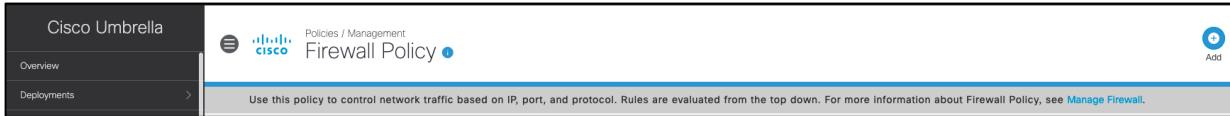
Cloud Firewall Policies

With Cisco Umbrella’s cloud-delivered firewall, all activity is logged, and unwanted traffic blocked using IP, port, and protocol rules. Rules are automatically applied to any tunnel connected to Umbrella. For this design guide, the firewall will be used to block any peer-to-peer (P2P) traffic such as BitTorrent. BitTorrent is a P2P protocol design to transfer files. Since these networks do not use HTTP(s), they would not fall under web traffic and therefore bypass web inspection.

Step 1. In the Umbrella Dashboard, navigate to **Policies > Management > Firewall Policy**.



Step 2. Click **Add**.



Step 3. Give a meaningful **Rule Name** and apply priority to the firewall rule. *Note: Rules are applied sequentially, with the Default Rule always in the last position.*

Rule Details
Provide a name, description, and priority order for the rule. Priority Order positions rules in the Firewall Policy in the order that rules are evaluated and then applied. Rules are applied sequentially, with the Default Rule always in the last position.

Rule Name: Priority Order:

Step 4. Under **Applications**, click **Specify Applications** from the drop-down menu.

Step 5. Click the **+** icon in the search bar and navigate down to **P2P**. Click to **Enable**.

Rule Criteria
Specify the protocols, IPs, network tunnels, and ports to be allowed or blocked.

Protocol:

Applications:

Source Tunnels:

Source IPs/CIDRs:

IPs/CIDRs (0):

Applications (2 Results Found):
 P2P 74 >
 statistical-p2p (P2P)

Step 6. Under **Rule Action**, click **Block Traffic** and ensure **Logging** is **Enabled**.

Rule Action
Choose **Block Traffic** or **Allow Traffic** to specify what happens to traffic matching these Firewall policy rules.

Block Traffic
 Allow Traffic

Logging Enabled
Logs for this firewall rule will be captured in Activity.

Firewall Rule Enabled
This rule is active.

Step 7. Click **Save**.

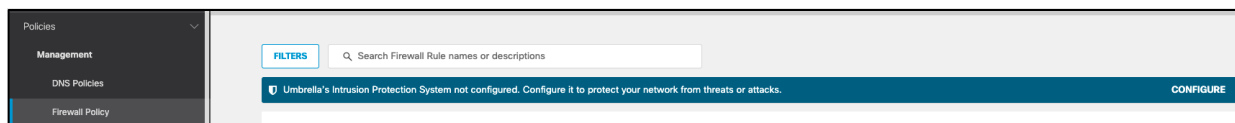
Intrusion Prevention System

IPS, based on SNORT 3 technology, uses signature-based detection to examine network traffic flows and take automated actions to catch and drop dangerous packets before they reach their target. An IPS capability is only as effective as the cyberattack dictionaries. Umbrella IPS uses extensive signatures

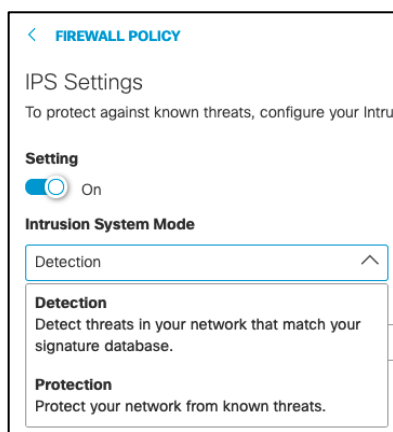
(40,000+ and growing) from Cisco Talos, the largest private security threat intelligence organization in the world.

Step 1. In the Umbrella Dashboard, navigate to **Policies > Management > Firewall Policy**.

Step 2. Next to **Umbrella's Intrusion Protection System**, click **Configure**.



Step 3. Click the **Intrusion System Mode** dropdown menu and choose either **Detection** or **Protection**. **Detection** mode will not block traffic, only alert on rules. **Protection**, if a rule is configured to do so, will block based on IPS detection. This design guide is configured with **Detection**.



Step 4. Click the **Apply to IPS Signature List** dropdown menu and choose the level of protection required:

- **Connectivity Over Security** places emphasis on network connectivity and throughput at the possible expense of security
- **Balanced Security and Connectivity** attempts to balance network connectivity and security to keep users secure while being less obtrusive toward normal traffic. *Note: This design guide is configured using **Balanced Security and Connectivity***
- **Security Over Connectivity** results in traffic to be inspected more deeply and more rules are evaluated
- **Maximum Detection** places all emphasis on security, such that network connectivity and throughput are compromised. Only select this setting when total protection is required

Step 5. Click **Save**.

The screenshot shows the 'FIREWALL POLICY' configuration page for 'IPS Settings'. The page title is '< FIREWALL POLICY'. Below the title, it says 'IPS Settings' and provides a brief instruction: 'To protect against known threats, configure your Intrusion Prevention System. Choose an Intrusion System mode and then apply an IPS Signature list to it.'

The configuration options are as follows:

- Setting:** A toggle switch is turned 'On'.
- Intrusion System Mode:** A dropdown menu is set to 'Detection'.
- Apply to IPS Signature List:** A dropdown menu is set to 'Balanced Security and Connectivity'.

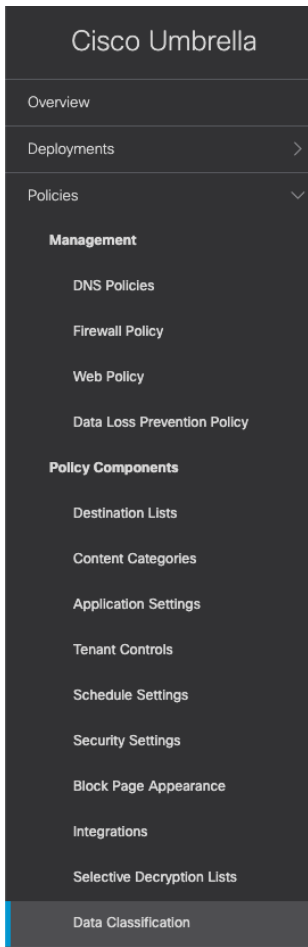
At the bottom right of the configuration area, there are two buttons: 'CANCEL' and 'SAVE'.

Data Loss Prevention

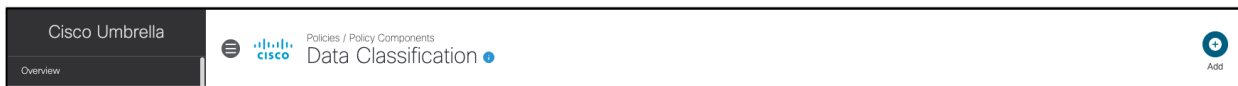
The DLP policy monitors content classified as personally identifiable or sensitive information. When necessary, content is blocked from an upload or a post. Rules are added to the policy to define what traffic to monitor (identities and destinations), the data classifications that require monitoring, and whether content should be blocked or only monitored. For example, an office may want to monitor its network for file uploads that include credit card numbers, because the uploads are a breach of company privacy and security policies. A rule designed to monitor the network and uploads to domains can block these files.

Note: HTTPS Inspection must be enabled (see Appendix B for details on the Umbrella root certificate) on the web policy ruleset where this DLP policy applies. DLP cannot be applied to encrypted traffic. For destinations that have been excluded from the decryption list, such as Office 365, it is recommended to use an API based solution such as Cisco Cloudlock or use the DLP policies included in Office 365.

Step 1. In the Umbrella Dashboard, navigate to **Policies > Policy Components > Data Classification**.



Step 2. Click **Add**.



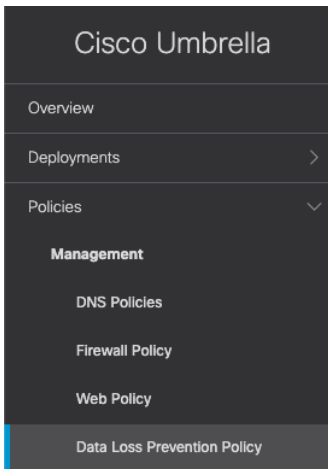
Step 3. Give a meaningful **Data Classification Name**.

Step 4. Select **Built-in-Data Identifiers** and choose the identifiers. For this design guide, **Credit Card Number - Strict** is selected. For a full list of identifiers, along with their description, see [Built-In Data Identifiers](#). Additionally, to create custom identifiers such as classified project code names, see [Create a Custom Dictionary](#).

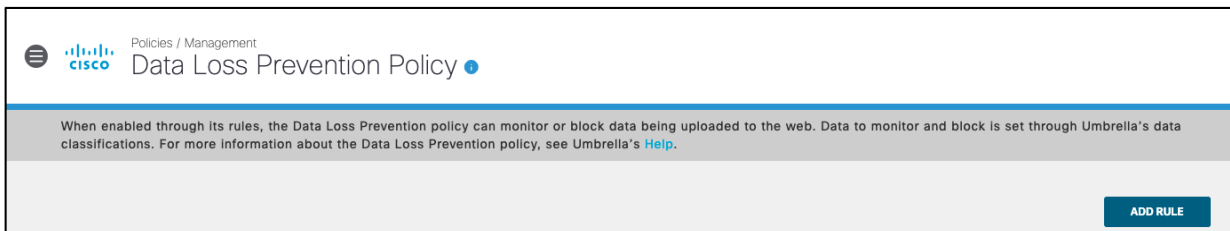
SASE Design Guide	Data Identifier 1	Last Updated Jul 12, 2021	^
Data Classification Name	Description (Optional)		
<input type="text" value="SASE Design Guide"/>	<input type="text"/>		
Selected Data Identifiers			
<input checked="" type="checkbox"/> Credit Card Number - Strict			>
▶ Built-in Data Identifiers			
▶ Custom Data Identifiers			
DELETE		CANCEL	SAVE

Step 5. Click **Save**.

Step 6. Navigate to **Policies > Management > Data Loss Prevention Policy**.

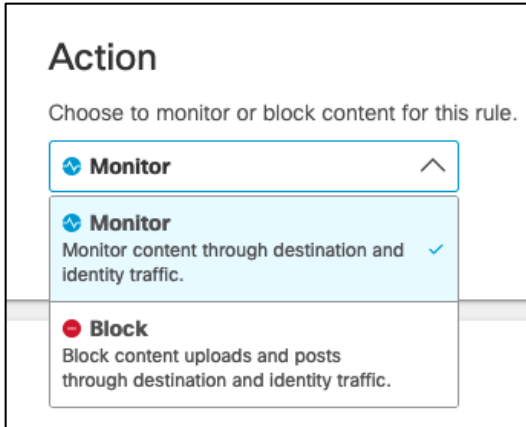


Step 7. Click **Add Rule**.

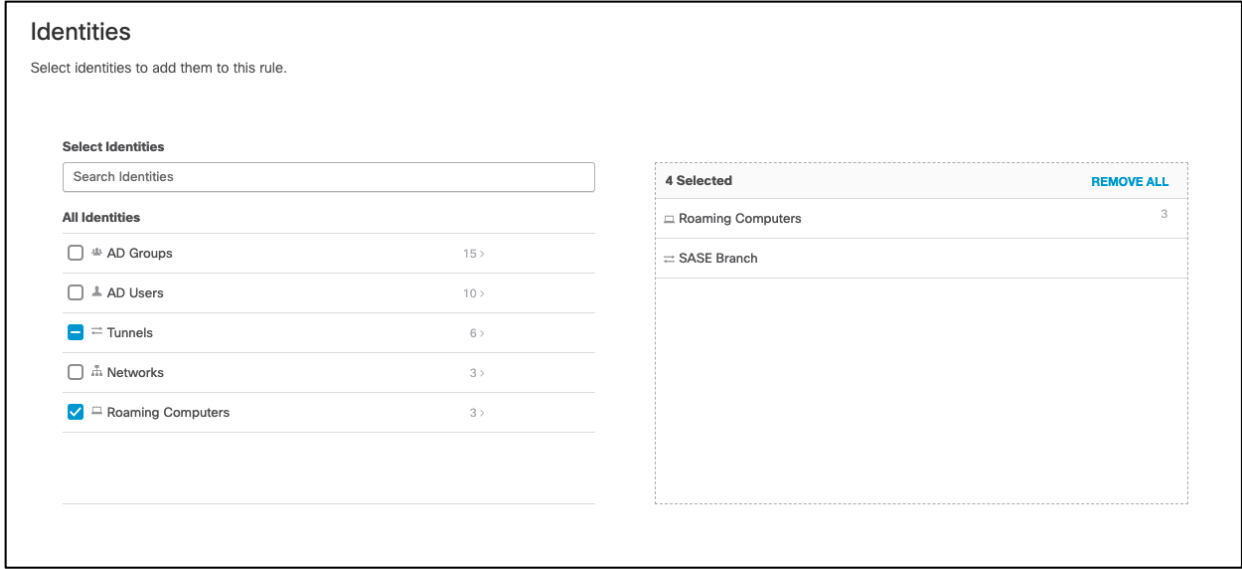


Step 8. Give a meaningful **Rule Name**.

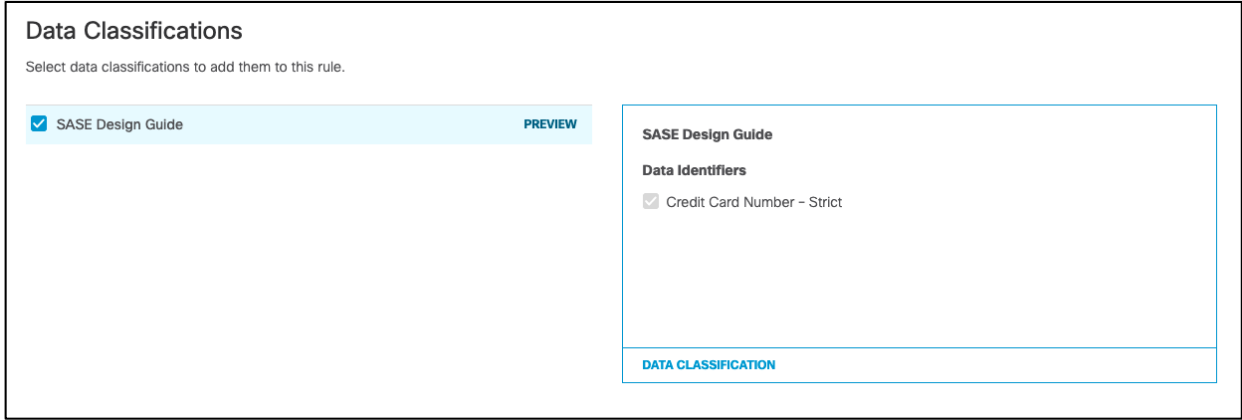
Step 9. Choose an **Action**. This guide will **Monitor** traffic that matches the DLP policy.



Step 10. Under **Identities**, select identities that will be monitored. This design guide will monitor all **Roaming Computers** and the **network tunnel** from our Branch.



Step 11. Under **Data Classifications**, select the data classification that was created in the previous steps.



Step 12. Under **Destinations**, select **All Destinations**. *Note: If blocking traffic, not all destinations are supported. The level of support for each application can be found at [Supported Applications](#).*

Destinations

Manage destination lists and verified applications for this rule.

- All Destinations**
Scans all destination lists and verified applications.
- Select Destinations**
Scans all selected destination lists and verified applications.

Step 13. Click **Save**.

Remote Browser Isolation (RBI)

RBI protects identities from potential malware and other threats by redirecting browsing to a cloud-based host. Destinations supported by an RBI add-on can be isolated when added to a rule in a Web policy's ruleset. When you add a rule and choose **Action > Isolate**, the selected destination in the rule will create a remote browser when users attempt to access those destinations. Instead of blocking identities from the destination endpoints, a cloud-based browser hosts the browsing session for that destination.

Step 1. In the Umbrella Dashboard, navigate to **Policies > Management > Web Policy**. We will modify the policy created in a previous section.

Step 2. Click the policy in which RBI will apply.

	Contains	Applied To	Last Modified
1 SASE Branch	4 Identities	-	Aug 07, 2021

Step 3. Click **Add Rule**.

Step 4. Give a meaningful **Rule Name**.

Step 5. Under **Rule Action**, select **Isolate**.

Priority	Rule Name	Rule Action	Identities	Destinations
	RBI	Isolate	No Selections Add Identity	No Selections Add Destination
1	Social Media Block			

Allow - Security Enforced
Allows selected ruleset identities access to destinations unless Umbrella detects a security issue.

Warn
Warns selected ruleset identities before allowing access to destinations.

Block
Blocks selected ruleset identities from accessing destinations.

Isolate
Isolates selected ruleset identities' web requests in a virtual cloud-based browser. ✓

Ruleset Settings

Ruleset settings affect the rules within the rule before being set here.

Ruleset Name

Ruleset Identities

Block Page

Step 6. Under **Identities**, click **Add Identity** and choose the option to **Inherit Ruleset Identities**.

Priority	Rule Name	Rule Action	Identities	
	RBI	Isolate	Ruleset Identities Add Identity	
1	Social Media Block	Block	Ruleset Identities	

IDENTITIES 1 Selected

AD Groups 15 >

AD Users 10 >

Network Tunnels 6 >

Networks 3 >

Roaming Computers 3 >

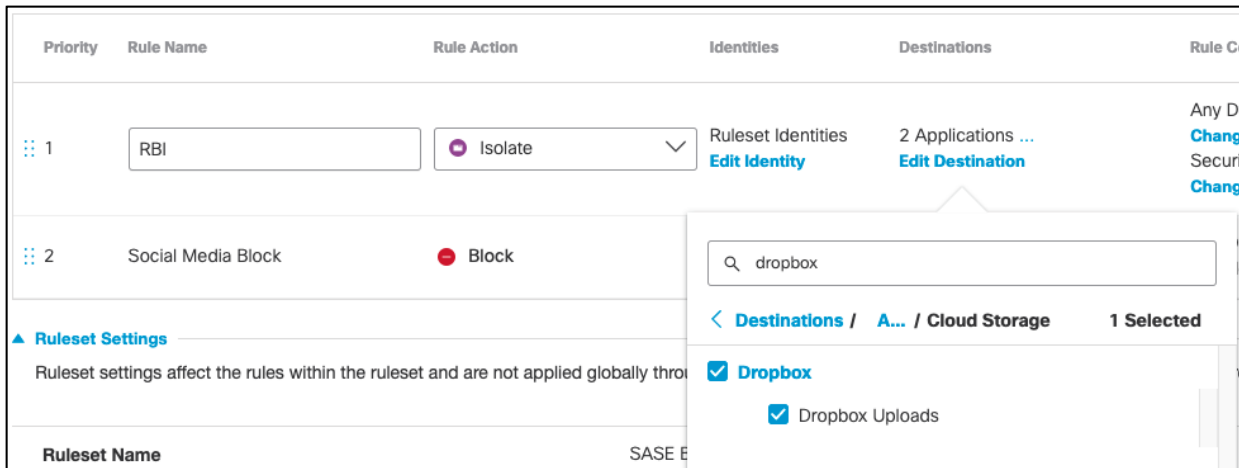
Inherit Ruleset Identities ●

[CANCEL](#) [APPLY](#)

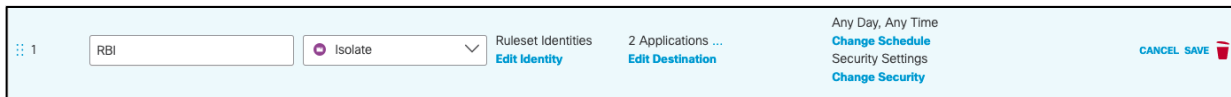
Ruleset Settings

Ruleset settings affect the rules within the ruleset and are not applied globally throughout y before being set here.

Step 7. Under **Destinations**, click **Add Destination**. For this validation, RBI will be used to access **Dropbox** so that if any malware is accidentally downloaded when browsing a cloud storage website, it does not get downloaded onto the client's machine. Click **Apply**.



Step 8. Click **Save** on the rule.

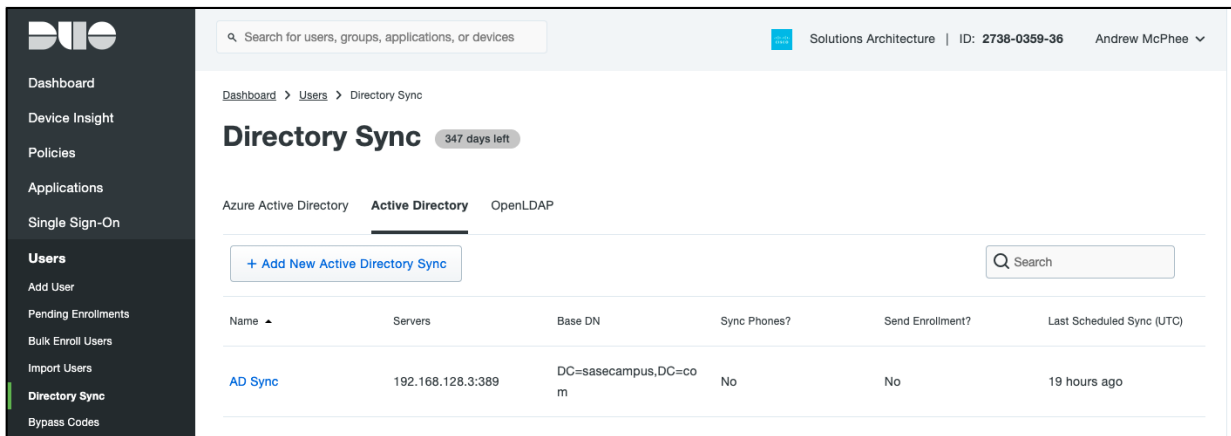


Step 9. Click **Close** on the policy.

Cisco Duo Network Gateway (DNG) Application protection

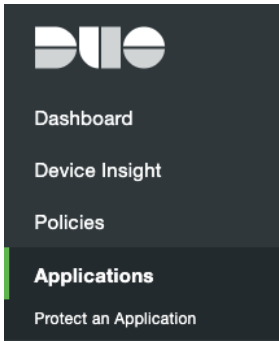
Since many large organizations already rely on an on-premises Active Directory (AD) server, OpenLDAP Directory, or a cloud-hosted Azure AD directory to manage their users, Duo offers tools to import users and groups from those identity stores into Duo, with the option of automatically sending an enrollment email to every user imported without an attached phone who has a valid email address.

To automatically enroll users from AD into Duo, see [Synchronizing Users from Active Directory](#). For this design guide, a group called SASECampus was created, and an option was chosen to only synchronize users who belong within that group.

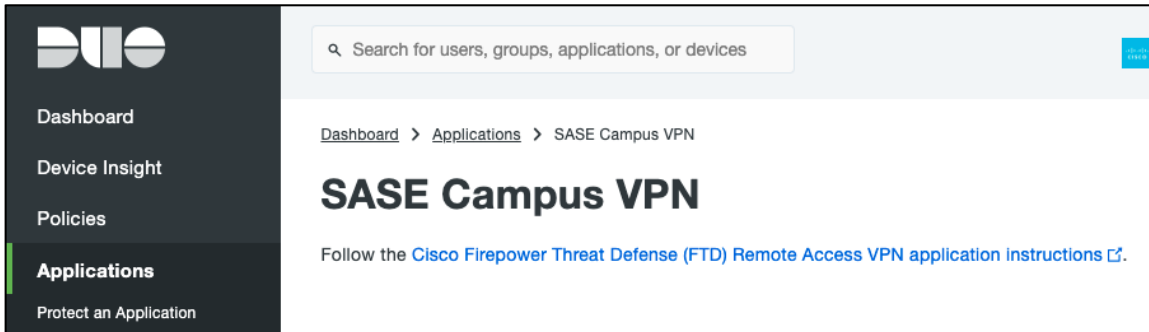


Now that a group of users has been classified, applications in Duo can be restricted to only allow members of the group to access.

Step 1. In the Duo Dashboard, navigate to **Applications**.

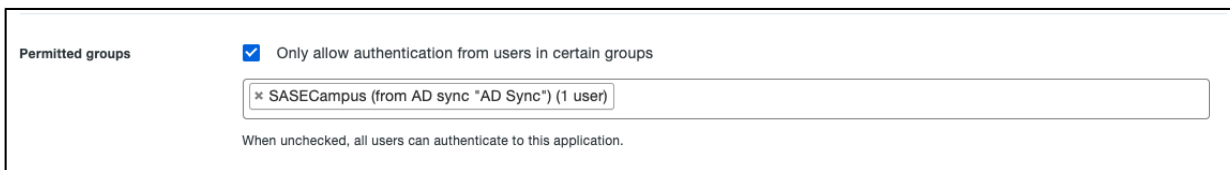


Step 2. Select the application used to enforce 2FA on the VPN.



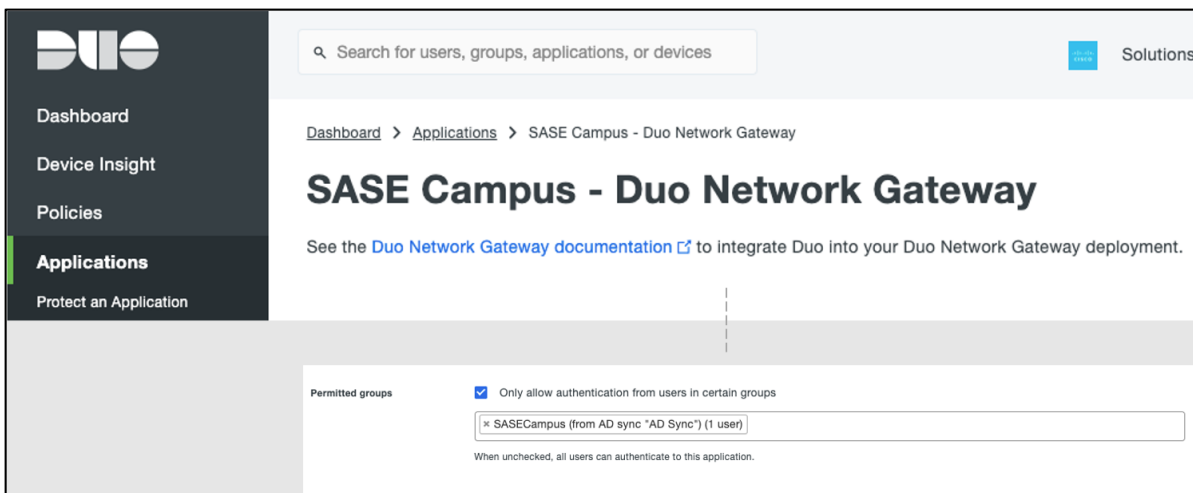
Step 3. Scroll down to the bottom of the page and beside **Permitted Groups**, click the checkbox for **Only allow authentication from users in certain groups**.

Step 4. In the search bar, choose the group(s) that should have access to the VPN. All other users will be denied.



Step 5. Click **Save**.

Step 6. Repeat the process for the application protections for DNG.

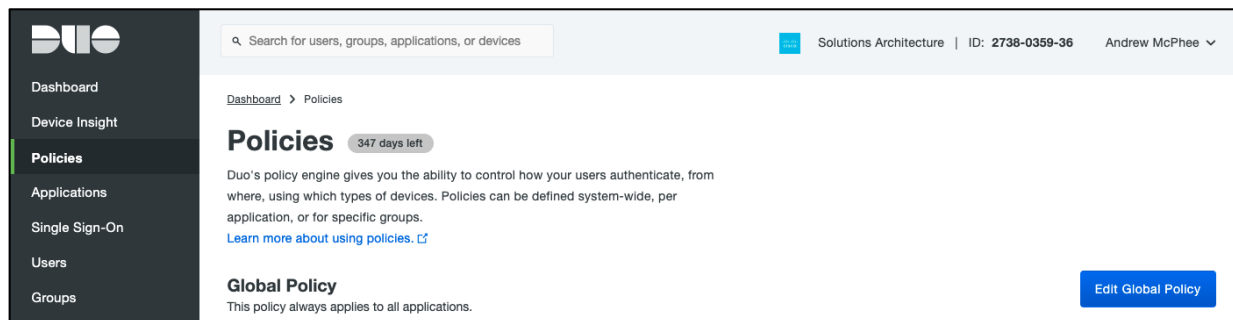


The Global Policy in Duo applies to all applications. If certain applications require policy and controls that differ from the Global policy, you can create a Custom Policy and assign it to those applications (for example, VPN

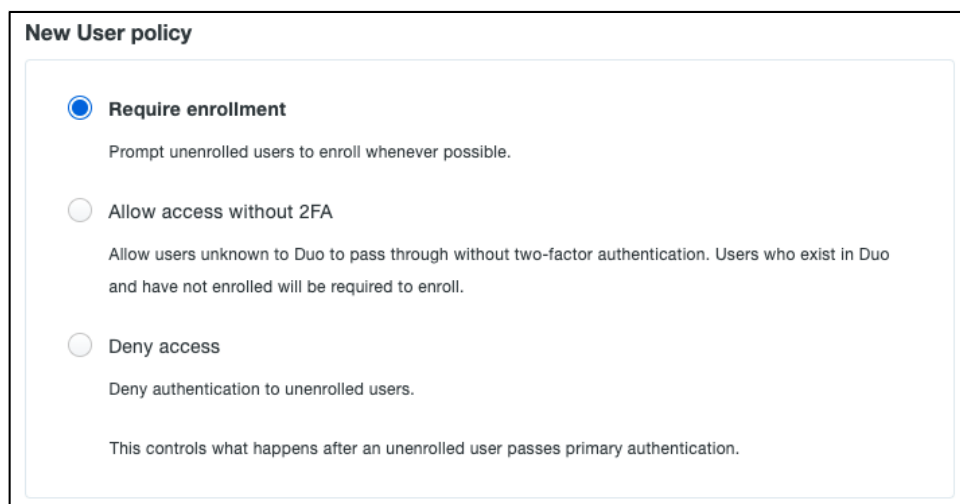
policy may allow access from non-trusted devices, but DNG may require Cisco Secure Endpoint). For this design guide, since we are already restricting policy access at a user level, the Global Policy will be configured and applied to all applications protected by Duo (i.e., remote access VPN and the Duo Network Gateway).

Step 1. In the Duo Dashboard, navigate to **Policies**.

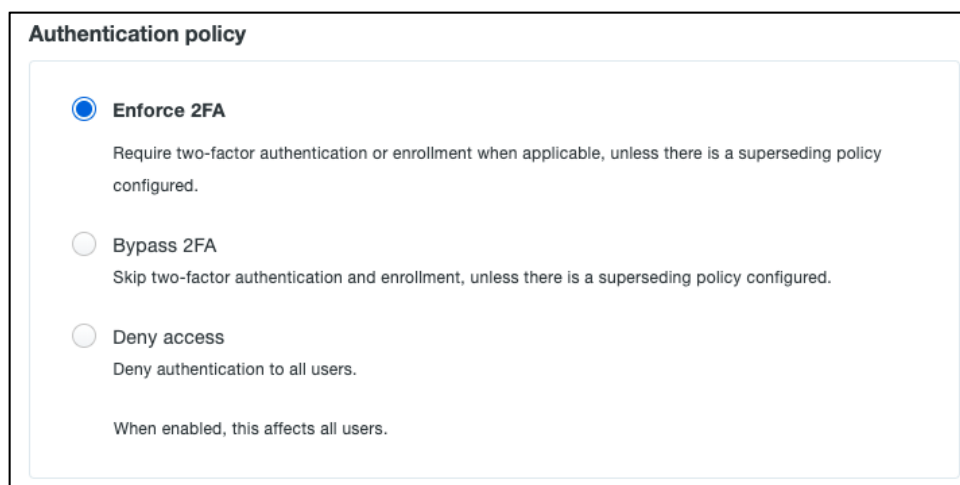
Step 2. Click **Edit Global Policy**.



Step 3. Under **New User policy**, click **Require enrollment** (default).



Step 4. Under **Authentication policy**, click **Enforce 2FA** (default).



Step 5. Under **User location**, enter all countries that you expect to receive authentication from and choose **No action** from the dropdown list. For all other countries choose **Deny access**. *Note: Access attempts from Internal Ips and unknown countries will default to "No action".*

User location

Duo will do a country lookup on the host IP address and can apply actions based on the country.

Note: Access attempts from internal IPs (some applications don't report the user's IP) and unknown countries will default to "No action."

Step 6. Under **Trusted Endpoints**, click **Require endpoints to be trusted** and **Allow AMP for Endpoints to block compromised endpoints**. This allows Duo to block devices that have been deemed to be compromised by Cisco Secure Endpoint. *Note: To create the integration between Duo and Cisco Secure Endpoint, see [Trusted Endpoints – Cisco AMP for Endpoints](#).*

Trusted Endpoints

A Trusted Endpoint is an endpoint that exists in a management system such as your EAM or MDM. It can be matched to your management system using Duo certificates or information provided by Duo Mobile.

Allow all endpoints
 Endpoints will be checked for trustworthiness to aid reporting, but un-trusted endpoints will be allowed.

Require endpoints to be trusted
 Only Trusted Endpoints will be able to access browser-based applications.

Allow AMP for Endpoints to block compromised endpoints
 Endpoints that AMP deems to be compromised will be blocked from accessing browser-based applications.

Note: This option only applies to trusted endpoints.

Step 7. Under **Device Health application**, choose if you want your application to require the Duo Device Health application. This allows us to restrict user access for device metrics such as if the device firewall is off or if a password has not been set on the device. For this design guide, we will click **Don't require users to have the app**. For more information, see [Enabling the Device Health Application Policy](#).

Device Health application

This section only affects applications protected by Duo's Device Health application.
[Learn More](#)

macOS

Don't require users to have the app ⓘ

Require users to have the app ⓘ

Step 8. Under **Remembered devices**, click **Do not remember devices** (default). Remembered devices allow users to skip subsequent 2FA requests.

Remembered devices

Remembered devices allow users to skip subsequent 2FA requests. Remembered devices can only be enabled on browser-based applications.

Do not remember devices

Users may choose to remember their device for

Per each application

For all protected web applications

Step 9. Under **Operating systems**, leave all settings as default. This section allows us to do version control, such as forcing users to update their operating system to a specified version or by completely blocking an operating system from the network.

Step 10. Scroll down to **Authentication methods** and choose which methods to use for authentication. For this design guide, only **Duo Push** and **SMS passcodes** will be enabled.

Authentication methods

Only allow users to authenticate with:

Duo Push

Duo Mobile passcodes

Phone callback

SMS passcodes

Security Keys (U2F)

WebAuthn

Security Keys (WebAuthn)

Touch ID

Hardware tokens

Step 11. The remaining policies refer to enforcement of specific smartphone features. Smartphone access is out of scope for this design guide. For more information on configuring these policies, see [Policy & Control](#).

Step 12. Click **Save Policy**.

Cisco Secure Endpoint

Cisco Secure Endpoint contains a comprehensive database of every file that has ever been seen and maintains a corresponding good or bad disposition. As a result, known malware is quickly and easily quarantined at the point of entry without any processor-intensive scanning. For this design guide, custom policies will not be created, and Secure Endpoint alerts will be triggered using the EICAR file.

NOTE: EICAR is safe to pass around, because it is not a virus, and does not include any fragments of viral code. It is a file that has been created for Anti-virus products to react to for test purposes. Cisco Umbrella also blocks access to this file.

For a more comprehensive analysis of both Secure Endpoint and Secure Malware Analytics, see [Cisco Breach Defense Design Guide](#).

SaaS App protection

Cisco Duo Single Sign-On is a cloud hosted SAML identity provider that adds two-factor authentication to popular cloud services like Salesforce and Microsoft 365 using SAML 2.0 federation. This design guide will use Microsoft 365 for testing and validation.

Cisco Duo authenticates your users using existing on-premises AD credentials and prompting for two-factor authentication before permitting access to Microsoft 365. The solution requires deployment of the Duo Authentication Proxy on your internal network to verify primary logon credentials against AD. End users will sign in and perform 2FA at Duo's cloud-hosted SSO service, and do not contact the on-premises authentication proxy servers directly.

For step-by-step deployment, see [Duo SSO for Microsoft 365](#).

Converge

Cisco ThousandEyes

Cisco ThousandEyes' global vantage points are Linux-based software agents that allow users to run a variety of layered monitoring tests, in order to gain insight into network and application performance and user experience.

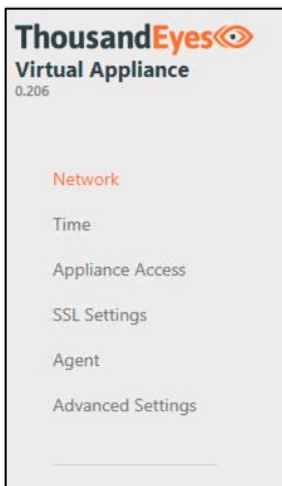
Cloud and Enterprise Agents are hosts containing Cisco ThousandEyes software capable of running instant or scheduled tests and device discoveries. The main (and almost only) difference between Cloud and Enterprise Agents is who deploys and manages them. Cloud Agents are deployed by Cisco ThousandEyes, on many locations across the globe, instantly available for your new tests. Enterprise Agents, on the other hand, are deployed by you, our customer, in locations of interest (branch offices for example). For this design guide, an Enterprise Agent will be installed in the branch network.

For step-by-step installation of the ThousandEyes enterprise agent, see [installing the enterprise agent](#). For this design guide, an enterprise agent was installed using a virtual appliance (OVA) in the branch network.

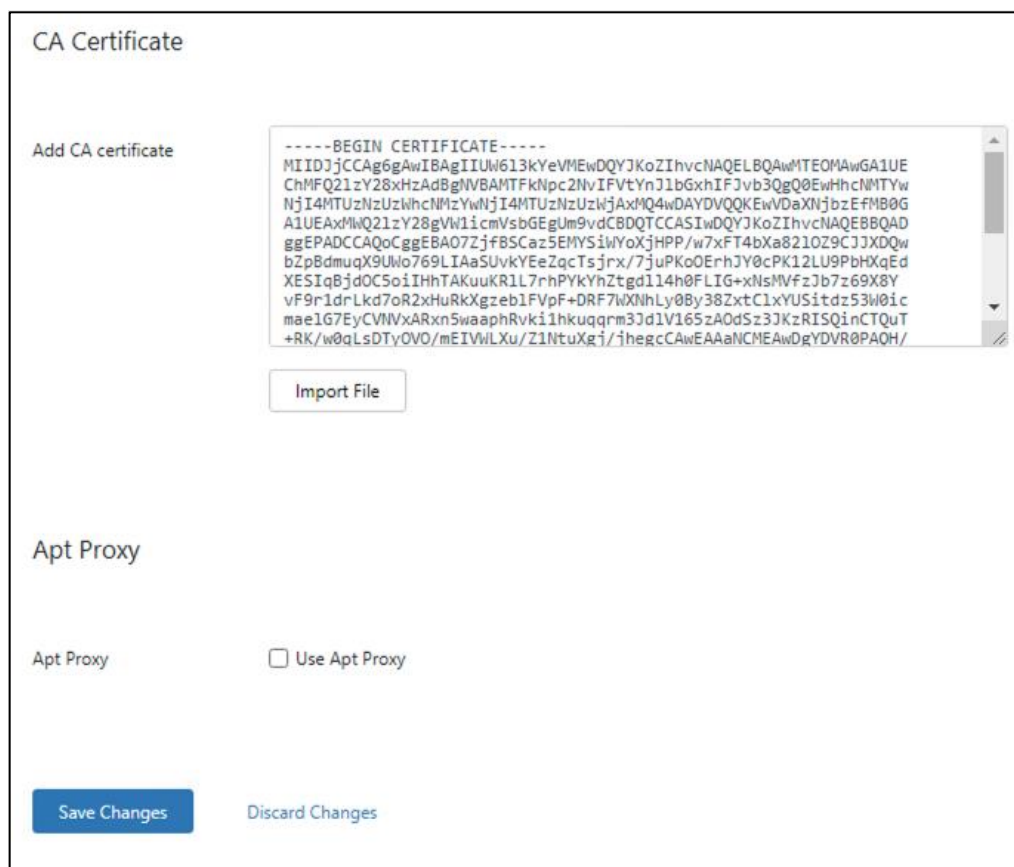
Note: Communication between the enterprise agent and the cloud will flow through Umbrella which has been configured to proxy all web traffic. As a result, the Umbrella Root CA certificate will need to be installed on the Enterprise Agent. Additionally, the domain for ThousandEyes should be added to the selective decryption list so communication between agents and dashboard are not proxied.

Add Cisco Umbrella Root CA to Cisco ThousandEyes Enterprise Agent

- Step 1.** In the Umbrella Dashboard, navigate to **Deployments > Configuration > Root Certificate**.
- Step 2.** Download the **Cisco Root Certificate Authority**.
- Step 3.** In the ThousandEyes Virtual Appliance web interface, navigate to **Network**.



Step 4. Under **CA Certificate**, click **Import File** and add the Umbrella certificate.



Step 5. Click **Save Changes**.

Add Cisco ThousandEyes to the Selective Decryption List in Cisco Umbrella

Step 1. In the Umbrella Dashboard, navigate to **Policies > Policy Components > Selective Decryption Lists**.

Step 2. Click the dropdown button next to the list that is attached to the web policy.

Step 3. In the **Domains** tab, click **Add**.

Step 4. Type *thousandeyes.com* and click **Add**.

Step 5. Save the policy.

Endpoint Agents are your Windows or macOS workstations that have ThousandEyes Endpoint Agent software installed. These agents, whenever they are present in one of the defined networks, collect network and application layer performance data as your users are accessing websites or applications on configured domains. In addition to that, Endpoint Agents provide basic support for running scheduled tests. Pulse version of Endpoint Agents are also available dedicated to running scheduled tests, these can be installed on customer hosts.

For a step-by-step installation of the ThousandEyes endpoint agent, see [installing the endpoint agent](#). For this design guide, an endpoint agent was manually installed by directly downloading the agent on to the device. To install on multiple devices, a group policy can be created in Active Directory.

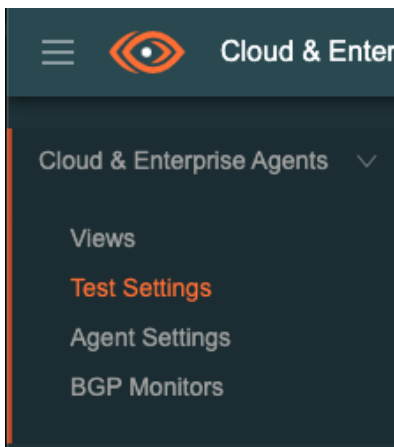
Cisco ThousandEyes Tests

ThousandEyes tests are classified into categories based on layers of operation:

- **Routing Layer** tests provide methods for collecting internet routing-related information.
- **Network Layer** tests measures network performance and path between agent and a target device.
- **DNS Layer** tests provide record validation and service performance metrics.
- **Web Layer** tests touch on various web technologies starting from the most basic measurement of availability of web server all the way up to performing precision transactions on a target.
- **Voice Layer** tests look at whether a connection can be established, as well as testing the exchange of packets after the connection is made.

This design guide will focus attention on DNS and Web layer testing.

Step 1. In the ThousandEyes Dashboard, navigate to **Cloud & Enterprise Agents > Test Settings**.



Step 2. Click **Add New Test**.

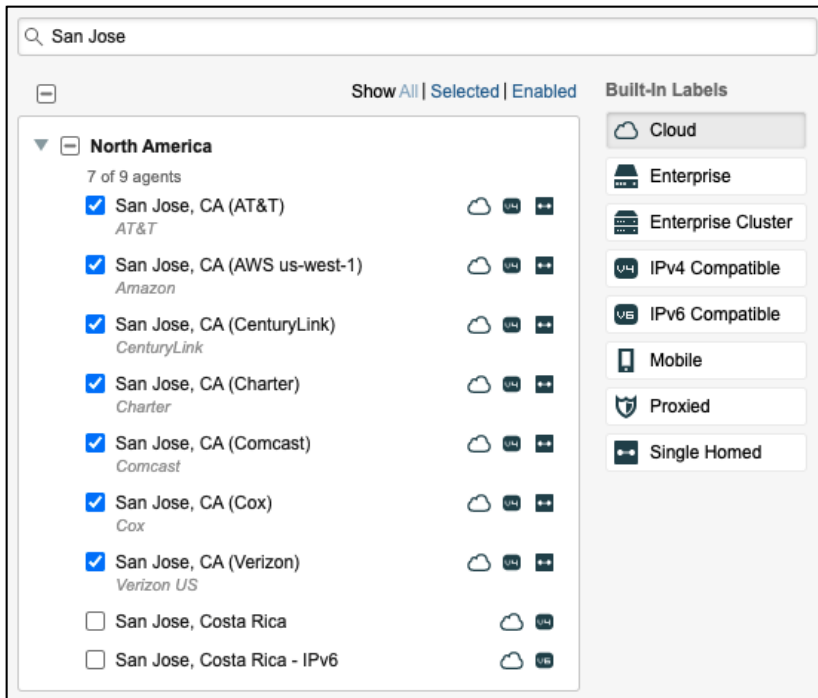
Step 3. Using the default **Web > HTTP Server** test, add the **URL** for **Salesforce**.

The screenshot shows the 'Add New Test' configuration interface. At the top, there's a 'New Test' section with tabs for 'Layer' (Routing, Network, DNS, Web, Voice) and 'Test Type' (HTTP Server, Page Load, Transaction, FTP Server). The 'Test Name' field contains 'Salesforce' and the 'Test Description' field contains 'Optional'. Below this is the 'Basic Configuration' section, which includes a 'URL' field with 'https://salesforce.com' and an 'Interval' dropdown menu set to '2 minutes'.

Step 4. In the **Agents** drop-down menu, click the **Enterprise** label and select the virtual appliance installed in the branch network.

The screenshot shows the 'Agents' selection dropdown menu. The 'Enterprise' label is selected, and the 'thousandeyes-va-335286' agent is chosen. The 'Agents' dropdown at the bottom shows '1 of 1 selected'. The interface also includes a search bar, a 'Show All | Selected | Enabled' filter, and a 'Built-In Labels' section with options like 'Cloud', 'Enterprise', 'Enterprise Cluster', 'IPv4 Compatible', 'IPv6 Compatible', 'Mobile', 'Proxied', and 'Single Homed'.

Step 5. Additionally, add some **Cloud Agent** connections for latency comparisons with the branch.



Step 6. In the **Advanced Settings** tab, click the checkbox next to **Verify Content**.



Step 7. In the textbox, enter the value **www.salesforce.com**. *Note: This extra validation is added when sending tests through the Umbrella web proxy. When content is blocked, Umbrella returns a blocked content page which results in a 200 status code which would normally indicate to the client that the connectivity has succeeded. We want the ThousandEyes test to fail on policy block, therefore we must check that the content is valid.*

Step 8. Click **Create New Test**.

Step 9. Repeat for each test. For this design guide, the following additional tests were created

- <https://office.com>
- <https://facebook.com>
- <https://linkedin.com>
- <http://app.cvdtest.net:3000> (private application in the data center)

Step 10. To create a DNS test, navigate to **Cloud & Enterprise Agents > Test Settings** and click **Add New Test**.

Step 11. Click the **DNS Layer** and choose **DNS Server** as the **Test Type**.

Add New Test

New Test

Layer: Routing Network **DNS** Web Voice

Test Type: **DNS Server** DNS Trace DNSSEC

Test Name: Internal DNS Test

Test Description: Optional

Step 12. Under **Basic Configuration**, choose a **Domain** that is commonly accessed by the organization.

Basic Configuration Advanced Settings

Domain: cisco.com IN A

Interval: 2 minutes

Step 13. In the **Agents** drop-down menu, choose the virtual appliance located in the branch network.

Step 14. Enter the **DNS Server** IP address for the private network.

Agents: 1 of 1 selected

DNS Servers: 192.168.128.3 Lookup Servers

Alerts: Enable
3 of 4 alert rules selected Edit Alert Rules

Cancel Run Once Create New Test

Step 15. Click **Create New Test**.

Step 16. Click **Add New Test**, but this time choose the **Cloud Agent(s)** for your region and enter the **DNS Server** addresses for Umbrella. This allows us to check the availability of Umbrella outside the local network in the case that the DNS is failing internally.

New Test

Layer: Routing Network DNS Web Voice

Test Type: DNS Server DNS Trace DNSSEC

Test Name:

Test Description:

Basic Configuration

Advanced Settings

Domain: IN A

Interval: 2 minutes

Agents: 7 of 416 selected

DNS Servers: 208.67.222.222 * 208.67.220.220 * * 🔍 Lookup Servers

Alerts: Enable 3 of 4 alert rules selected [Edit Alert Rules](#)

Cancel
Run Once
Create New Test

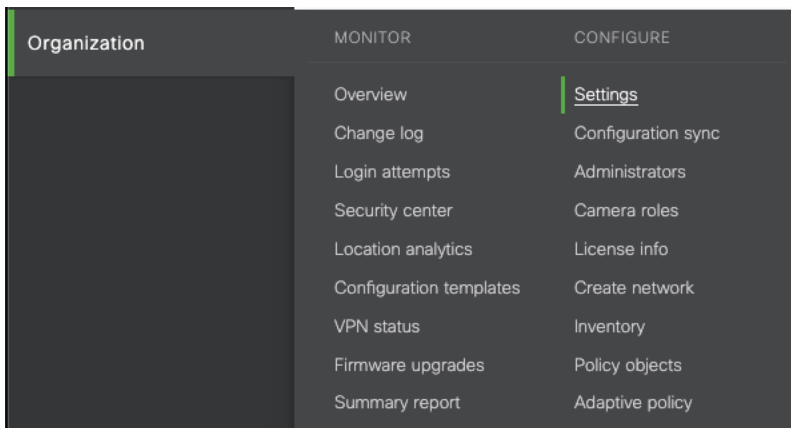
Note: All tests can be repeated for the endpoint agents located in the network.

Cisco SecureX

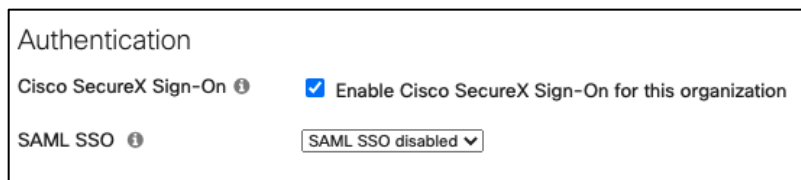
This deployment guide will primarily focus on the unified visibility and SSO capabilities of Cisco SecureX, by demonstrating the integrations it has with other products in the Cisco security portfolio. Other capabilities of SecureX, such as threat response and the dashboard ribbon can be explored further in the [Cisco Breach Defense Design guide](#).

Enabling SSO In Cisco Meraki

Step 1. In the Meraki Dashboard, navigate to **Organization > Settings**.



Step 2. Under Authentication, click **Enable Cisco SecureX Sign-On for this organization**.



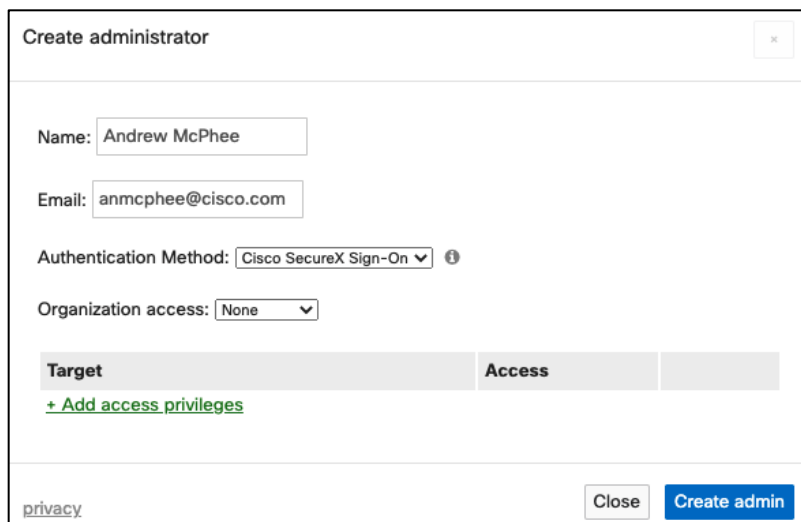
Authentication

Cisco SecureX Sign-On Enable Cisco SecureX Sign-On for this organization

SAML SSO

Step 3. Make sure to **Save Changes**.

Once enabled, every time a new Dashboard user is created under **Organization > Administrators**, you will see an option to choose if that user would use SecureX Sign-On to login.



Create administrator

Name:

Email:

Authentication Method:

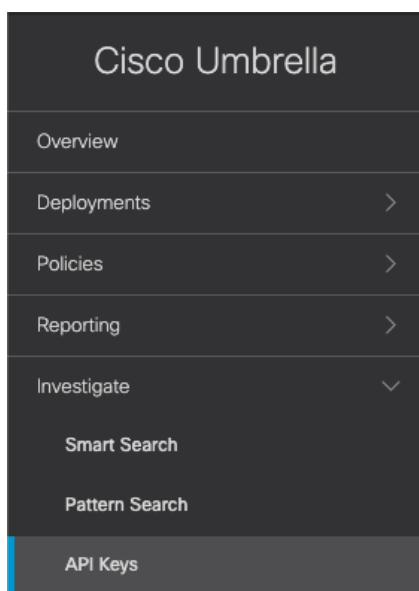
Organization access:

Target	Access
+ Add access privileges	

[privacy](#)

Cisco Umbrella

Step 1. In the Umbrella Dashboard, navigate to **Investigate > API Keys**.



Step 2. Click **Create New Token**.

Investigate
API Keys

The Umbrella Investigate API is organized around the principles of REST. Our API lets you gather results from Investigate with anything that can send an HTTP request, including cURL and modern internet browsers. For more information on Investigate REST API, view [Investigate API](#).

API Access Tokens CREATE NEW TOKEN

Step 3. Enter a meaningful **Title** and click **Create**.

API Access Tokens CREATE NEW TOKEN

To create a new API access token enter a title

Title

CREATE CANCEL

Step 4. Take note of the **Investigate API Token**.

SASE Design Guide

ACCESS TOKEN: 968 [REDACTED]

DATE CREATED: August 8th 2021, 9:28:30 pm

CREATED BY: anmcphee@cisco.com

Step 5. In the Umbrella Dashboard, navigate to **Admin > API Keys**.

Cisco Umbrella

- Overview
- Deployments >
- Policies >
- Reporting >
- Investigate >
- Admin ▾
 - Accounts
 - User Roles
 - Log Management
 - Authentication
 - Bypass Users
 - Bypass Codes
 - API Keys

Step 6. If an **Umbrella Reporting API Key** does not already exist, click **Create**. *Note: Only one instance of the API Key can exist for each function.*



Step 7. Under **What should this API do?**, click the **Umbrella Reporting** radio button and click **Create**.

What should this API do?
Choose the API that you would like to use.

- Umbrella Network Devices**
Integrate Umbrella-enabled hardware with your organization's networks. This also enables you to create, update, list, and delete identities in Umbrella.
You can only generate one token. Refresh your current token to get a new token.
- Legacy Network Devices**
A Network Devices token enables hardware network devices such as Cisco Wireless Lan Controllers and Cisco Integrated Services Routers 4000 series to integrate with Umbrella.
You can only generate one token. Refresh your current token to get a new token.
- Umbrella Reporting**
Enables API access to query for Security Events and traffic to specific Destinations
- Umbrella Management**
Manage organizations, networks, roaming clients and more using the Umbrella Management API
You can only generate one token. Refresh your current token to get a new token.

CANCEL **CREATE**

Step 8. Take note of both the **Reporting API Key** and **API Secret**. *Note: The secret will only be shown once. Make sure to store it in a secure location for future use.*

Umbrella Reporting Key: b4965af9f80f4ab7a792d6c197f3beb8 Created: Aug 8, 2021

The API key and secret here are used to perform API requests against your Umbrella organization.

Your Key: b4965a [REDACTED]

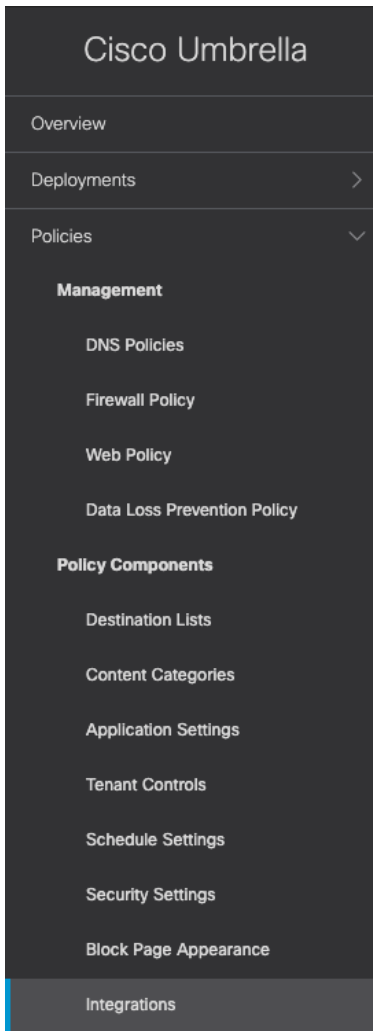
Your Secret: cd424 [REDACTED]

To keep it secure, we only display your key's secret once. For future reference, copy this secret and keep it in a safe place. Tick this box to acknowledge this.

Check out the [documentation](#) for step by step instructions.

DELETE **REFRESH** **CLOSE**

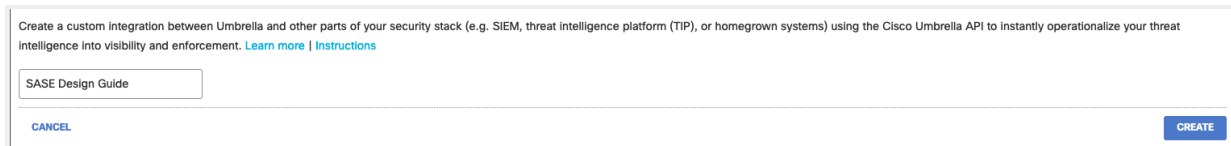
Step 9. In the Umbrella Dashboard, navigate to **Policies > Policy Components > Integrations**.



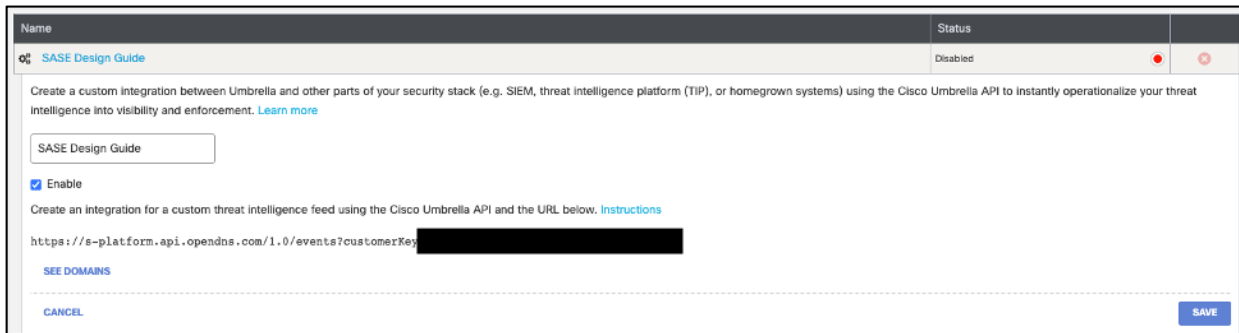
Step 10. Click **Add**.



Step 11. Give a meaningful **Integration Name** and click **Create**.

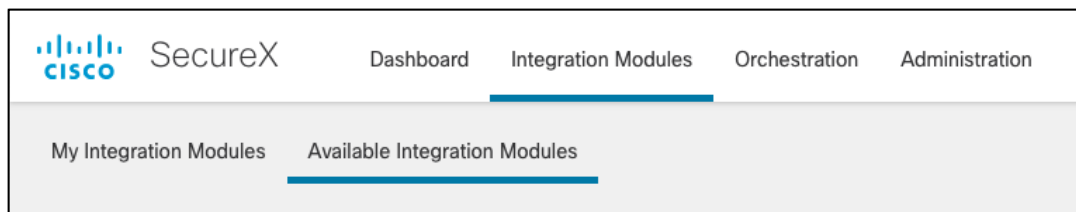


Step 12. Click the newly created integration, check the **Enable** box and click **Save**.

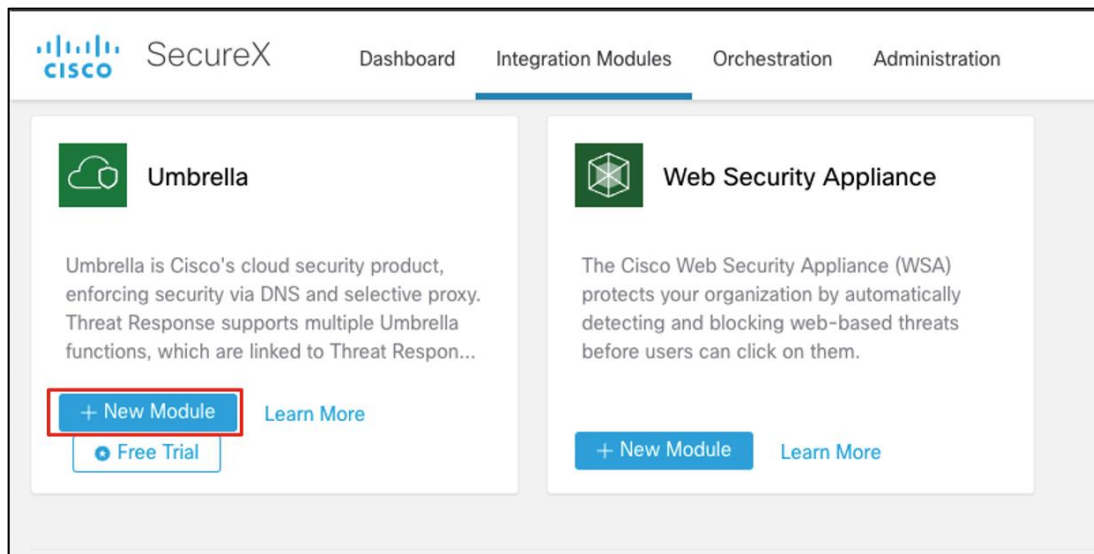


Step 13. Click the integration to display the **Custom Umbrella Integration URL**.

Step 14. In the SecureX Dashboard, navigate to **Integration Modules > Available Integration Modules**.



Step 15. Under **Cisco Products**, search for **Umbrella** and click **+ New Module**.



Step 16. Enter a meaningful **Integration Module Name**.

Step 17. Using the values generated in the previous steps, enter the required fields in the **Investigate, Enforcement** and **Reporting** forms.

Integration Module Name

Umbrella

Investigate

API Token

.....

Enforcement

Custom Umbrella Integration URL

.....

Reporting

API Key

b4965 [REDACTED]

API Secret

.....

Request Timeframe (days)

300

Organization ID

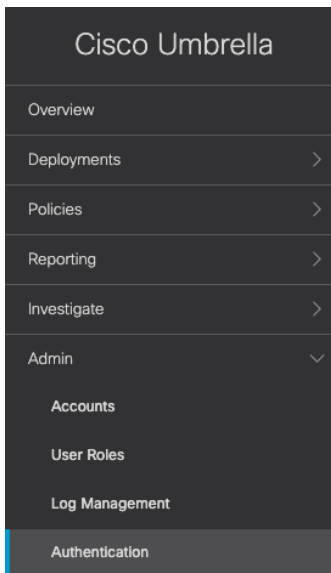
2 [REDACTED]

Delete Cancel Save

Step 18. Click **Save**.

To enable SSO with SecureX in Umbrella, make sure the SecureX account is the same across all environments. If the user is not in the Umbrella organization, please add it under **Admin > Accounts**. Once completed, follow these deployment steps to enable SSO:

Step 1. In the Umbrella Dashboard, navigate to **Admin > Authentication**.



Step 2. Under **SAML Dashboard User Configuration**, click **Configure**.

SAML Dashboard User Configuration

Cisco Umbrella supports Security Assertion Markup Language or SAML for logins to the Umbrella dashboard. This allows you to provide single sign-on (SSO) access to Umbrella using enterprise identity providers such as Okta, OneLogin, Azure and Ping Identity. SAML SSO is available to all Cisco Umbrella dashboard users. For more detailed information, [read here](#).

Status ● Enabled
Provider Cisco SecureX sign-on

DISABLE CONFIGURE

Step 3. Select **Cisco SecureX sign-on** and click **Next**.

SAML Dashboard User Configuration

Step 1 of 3

Select Umbrella SAML Provider

Select the SAML provider you'd like to authenticate users to Umbrella.

- Cisco SecureX sign-on
- PingID
- Okta
- OneLogin
- Azure
- Other

CANCEL NEXT

Step 4. Click **Test Configuration** to verify the setup and click **Next**.

SAML Dashboard User Configuration

Step 2 of 3

Verify Cisco SecureX sign-on

Using Cisco SecureX sign-on as your SAML provider for Umbrella requires all accounts in this organization to already have existing Cisco SecureX sign-on accounts, and for those accounts to have the Cisco Umbrella app assigned. You can create Cisco SecureX sign-on accounts and assign the Cisco Umbrella app at <https://sign-on.security.cisco.com>.

Please verify your Cisco SecureX sign-on account by clicking the "Test Configuration" button below.

TEST CONFIGURATION

● Your SAML settings have been properly configured!

CANCEL PREVIOUS NEXT

Step 5. Agree to the conditions and click **Save and Notify Users**.

SAML Dashboard User Configuration

Step 3 of 3

Save and Notify

After clicking 'Save', all users in your organization will be required to use the single sign-on service rather than a password. Umbrella will send an email to every administrative user in the dashboard, stating their password has been removed from their account.

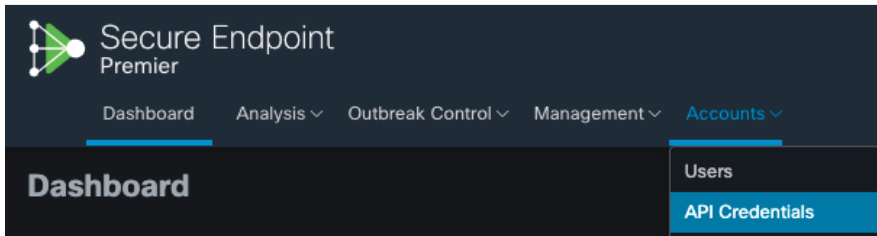
- If you disable the single sign-on service in the future, all users in your dashboard will be emailed a link to reset their passwords and their old passwords are not restored.
- Block page bypass users will no longer work once SAML is enabled. Instead, you must use codes for bypassing block pages. For more information, [read here](#).

Two step verification with Umbrella is not available when SAML is enabled. Instead, use the two factor options available with your SSO provider.

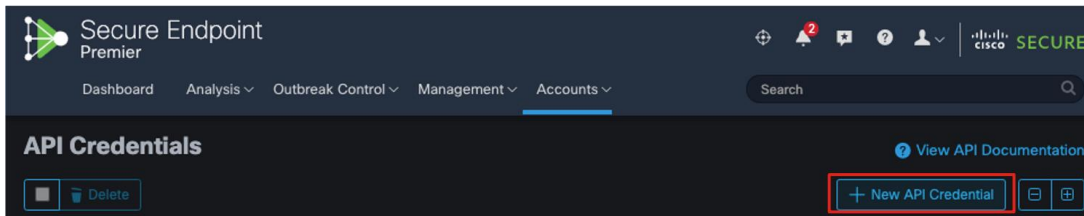
PREVIOUS SAVE AND NOTIFY USERS

Cisco Secure Endpoint

Step 1. In the Cisco Secure Endpoint Dashboard, navigate to **Accounts > API Credentials**.



Step 2. Click **New API Credential**.



Step 3. Enter a meaningful **Application name** and choose the desired **Scope**. *Note: This design guide will only require the Read-only scope, however, the Read & Write scope has been chosen for readers who will also be using the Breach Defense guide and would like to take response actions with Secure Endpoint.* Click **Create**.

Step 4. From the **API Key Details** page, copy both the **3rd Party API Client ID** and the **API Key**. *Note: Do not close the tab without retrieving these values. The API key is not retrievable once the tab is closed.*

The API credentials have been generated. Keep the new API credentials in a password manager or encrypted file.



< API Key Details

3rd Party API Client ID

7da

API Key

034d

API credentials (API Client ID & API Key) will allow other programs to retrieve and modify your Secure Endpoint data. It is functionally equivalent to a username and password, and should be treated as such.

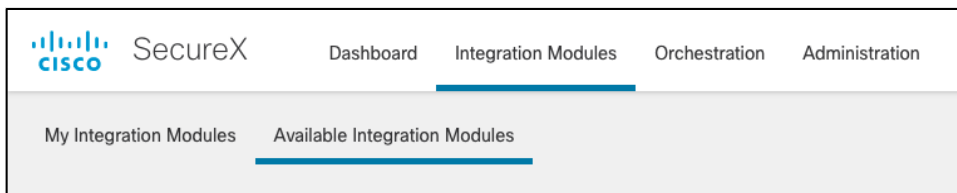
Delete the API credentials for an application if you suspect they have been compromised and create new ones.

Deleting API credentials will lock out any clients using the old ones so make sure to update them to the new credentials.

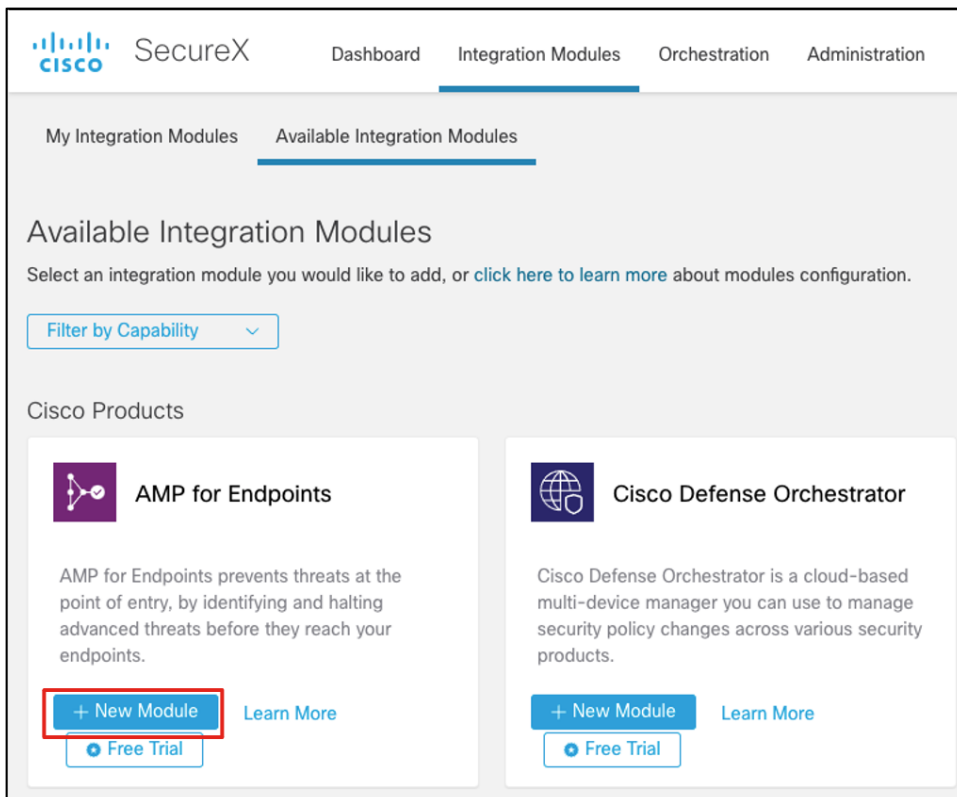
Your API credentials are not stored in plain text and can only be displayed once. If you lose the credentials you will have to generate new ones.

[View API Documentation](#)

Step 5. In the SecureX Dashboard, navigate to **Integration Modules > Available Integration Modules**.



Step 6. Under **Cisco Products**, search for **AMP for Endpoints** (former name to Secure Endpoint) and click **+ New Module**.



Step 7. Add the **3rd Party API Client ID** and the **API Key** from the previous steps.

Edit AMP for Endpoints Module

✓ This integration module has no issues.

Integration Module Name
AMP for Endpoints

URL*
https://api.amp.cisco.com

3rd Party API Client ID*
c8c8f24fd77e59201f9

API Key*
.....

Act in the name of Active User

When selected, Cisco Threat Response will act in the name of the currently logged in user. For this to work, the 3rd Party API Client ID and the API Key must be administrator credentials. More information is available in our [module documentation](#)

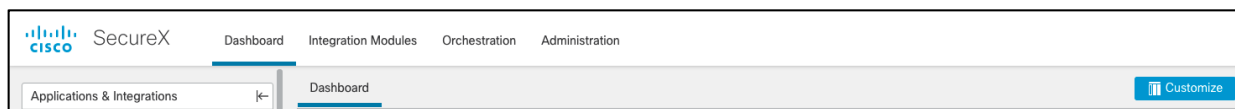
Delete Cancel Save

Step 8. Click **Save**.

*Note: SecureX SSO was enabled by default for the organization used in validating this design. If SSO is not enabled under **Accounts > Organization Settings** in the Secure Endpoint Dashboard, see [Enabling Cisco SecureX Sign-On for Secure Endpoint](#).*

SecureX Dashboard

Step 1. In the SecureX Dashboard, click **Customize**.



Step 2. Give a meaningful **Dashboard Name**.

Customize Dashboards

My Dashboards

- ☰ SASE Design Guide
- Shared Dashboards
- No Dashboards

Dashboard Name*

Dashboard name is required

Share this dashboard with my organization Share

Available Tiles

- > AMP for Endpoints (1 selected)
Remove All
- > Cisco Tetration - Application-First Workload Pro...
Add All
- > Firepower (0 selected)
Add All
- > Private Intelligence (0 selected)
Add All
- > Stealthwatch Cloud (0 selected)
Add All
- > Umbrella (1 selected)
Remove All

+ Create Dashboard
Delete
Refresh Tiles
Cancel
Save

Step 3. Under Available Tiles, expand both **AMP for Endpoints** and **Umbrella**.

Step 4. Choose the tiles that you would like to add to the SecureX Dashboard and click **Save**.

SASE Design Guide Customize Timeframe* ▾

AMP for Endpoints
Summary Last 24 Hours ▾ ⋮ ↻

0

Computers With Quarantines [↗](#)

0

Computers Compromised [↗](#)

0

Vulnerable Executions [↗](#)

Umbrella
Request Summary Last 24 Hours ▾ ⋮ ↻

26,464

Total Requests [↗](#)

760

Total Blocked [↗](#)

© 2021 Cisco and/or its affiliates. All rights reserved.

Page 80 of 131

Validation Tests

Remote Worker to Public Application (SaaS)

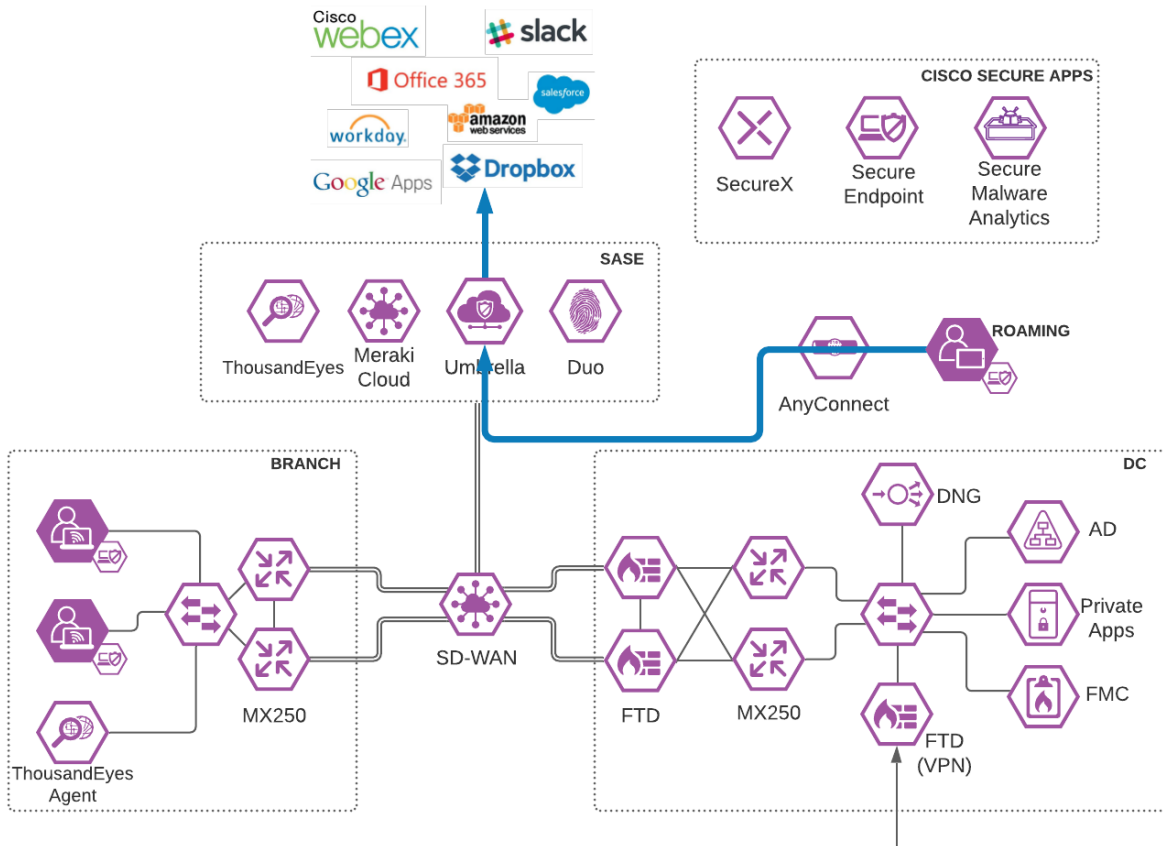
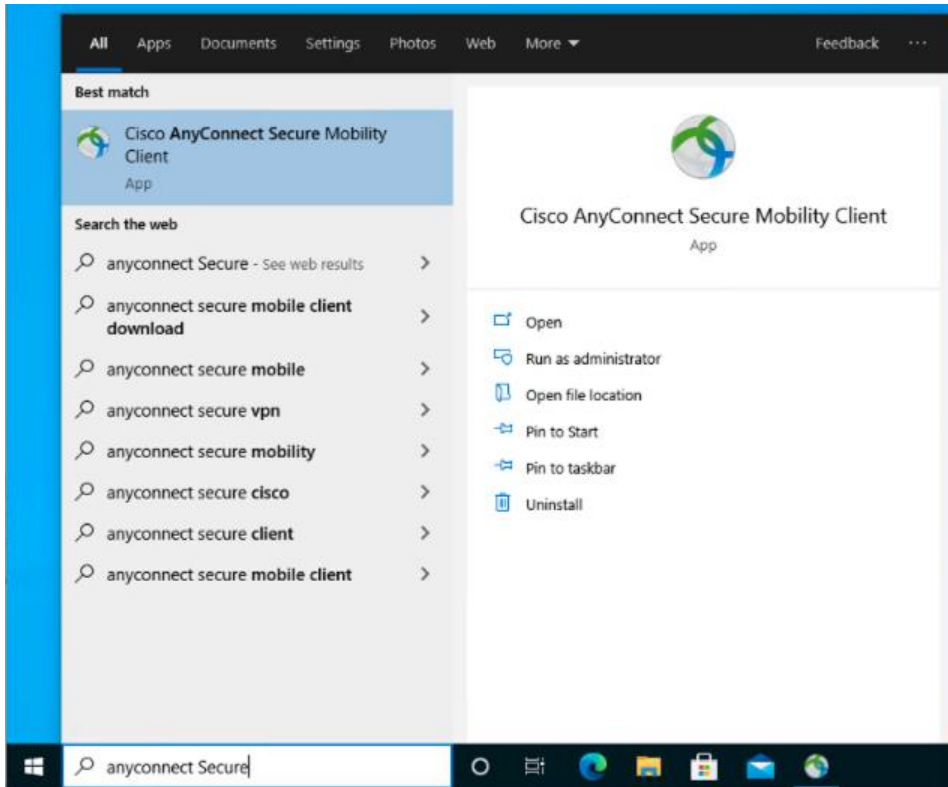


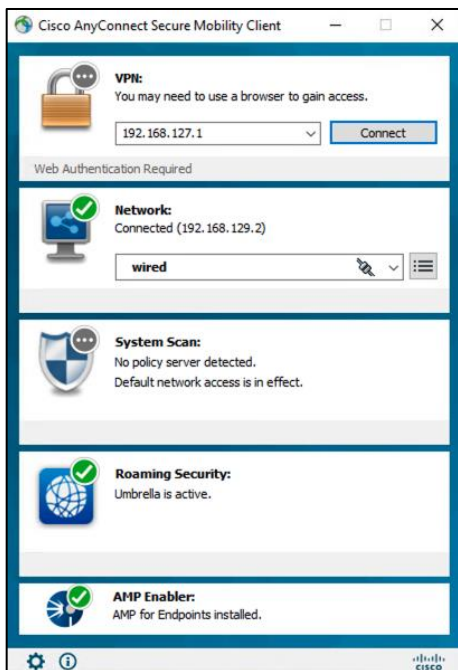
Figure 22.
Roaming User to SaaS application through Umbrella

Validation Test #1 - Umbrella Roaming Client successfully installed with AnyConnect

Step 1. On a roaming device from the AnyConnect installation steps, open AnyConnect Secure Mobility Client.

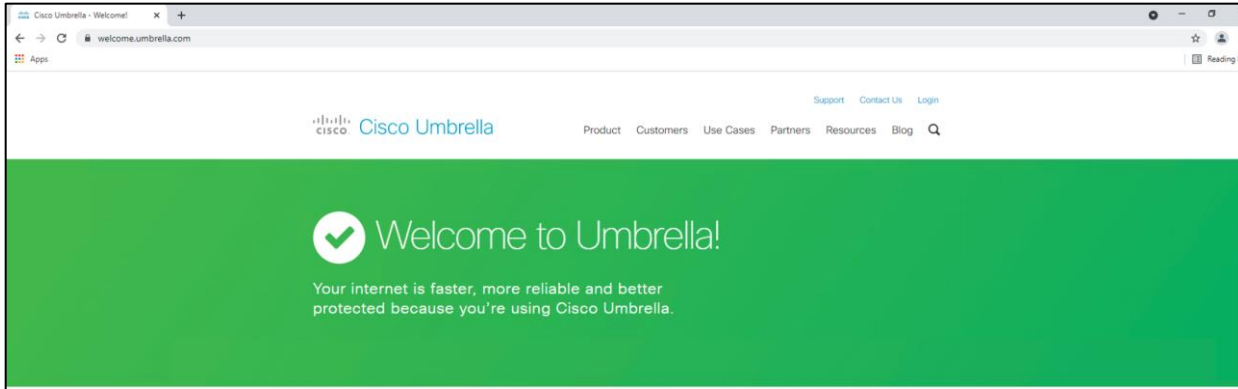


Step 2. When on a network other than the office network, verify that Umbrella Roaming is active.



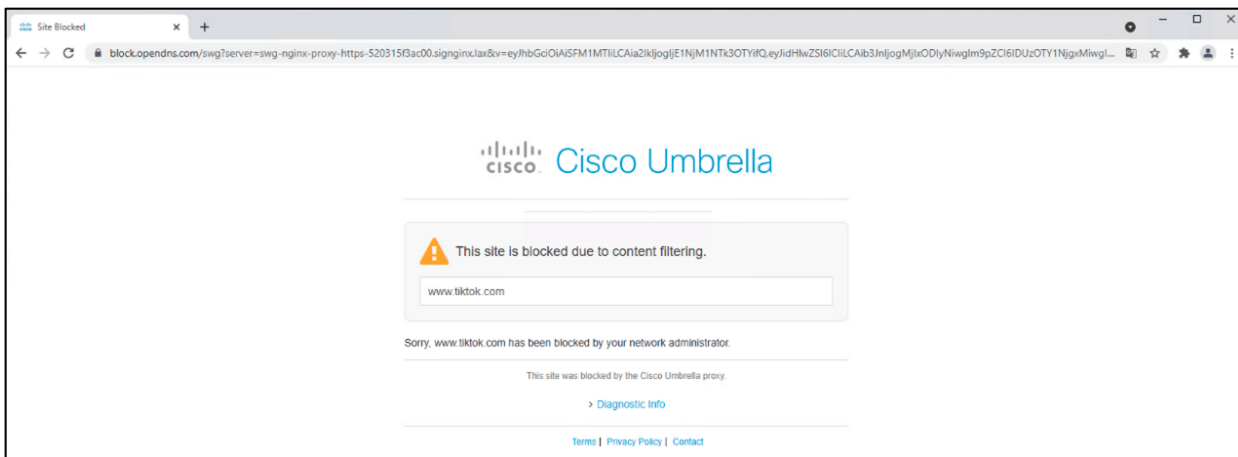
Step 3. Also verify that Cisco Secure Endpoint (AMP Enabler) has been installed as part of AnyConnect.

Step 4. In any browser, navigate to <https://welcome.umbrella.com> to verify that you are using Umbrella DNS.

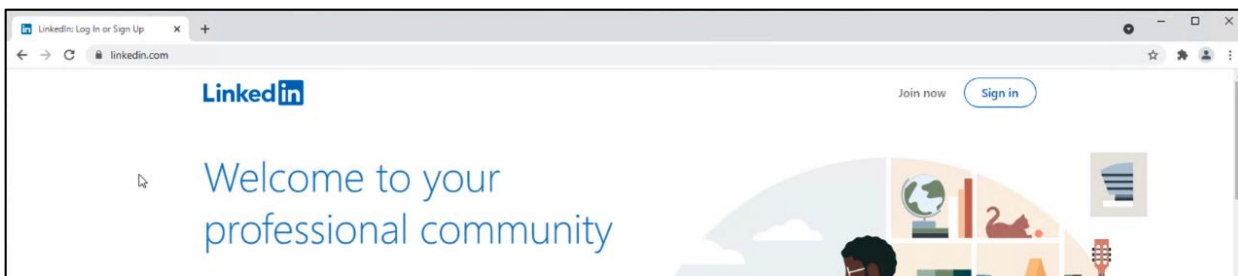


Validation Test #2 - Umbrella Content Filtering is being applied

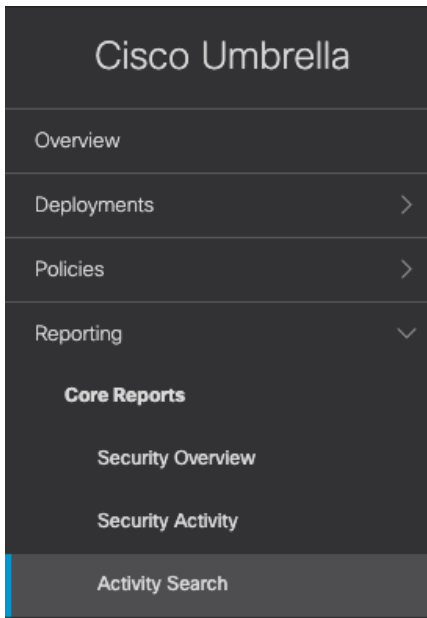
Step 1. In any browser, navigate to <https://facebook.com>. The Umbrella block page should be returned.



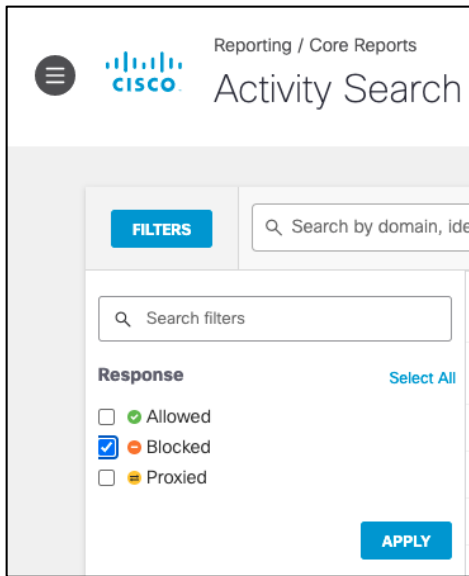
Step 2. In any browser, navigate to <https://linkedin.com>. Access to the site should be granted.



Step 3. In the Umbrella Dashboard, navigate to **Reporting > Core Reports > Activity Search**.



Step 4. In the **Filters** tab, check the **Blocked** box under **Response** and click **Apply**.

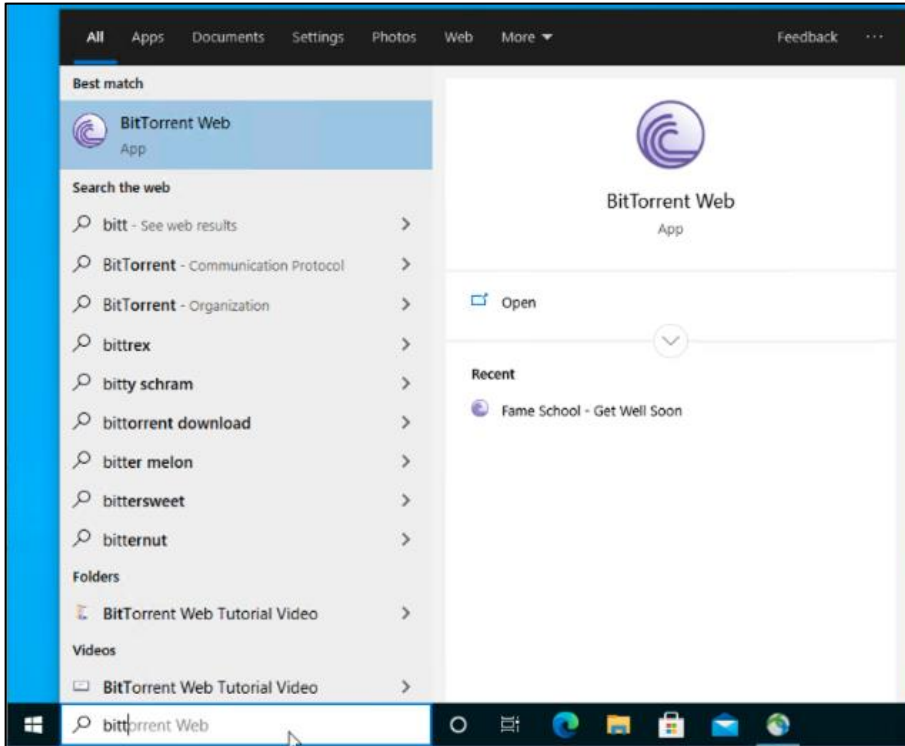


Step 5. Verify the entry for **Facebook** has been logged.

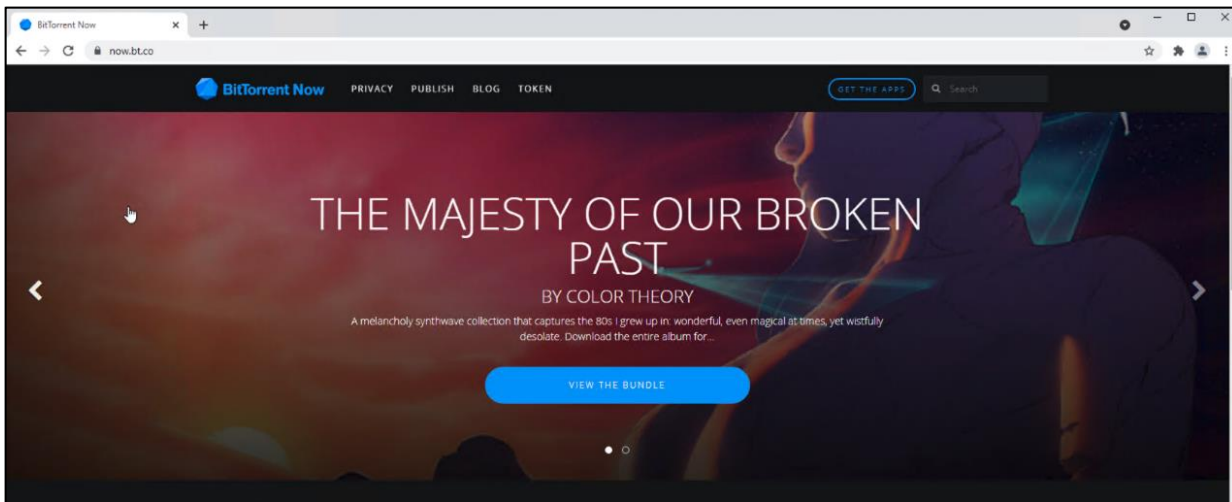
Internal IP	External IP	Action	Categories	Application	Application Category	Application Protocol	Date & Time
192.168.129.2		Blocked	Application Block, Social Networking	Facebook	Social Networking		Aug 13, 2021 at 1:01 AM
192.168.129.2		Blocked	Application Block, Social Networking	Facebook	Social Networking		Aug 13, 2021 at 1:01 AM

Validation Test #3 - Umbrella Firewall policies are being triggered

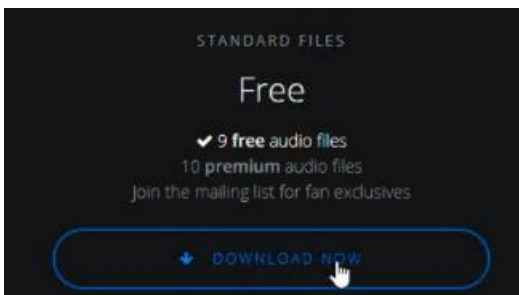
Step 1. Download and install the [BitTorrent application](#) onto the client machine.



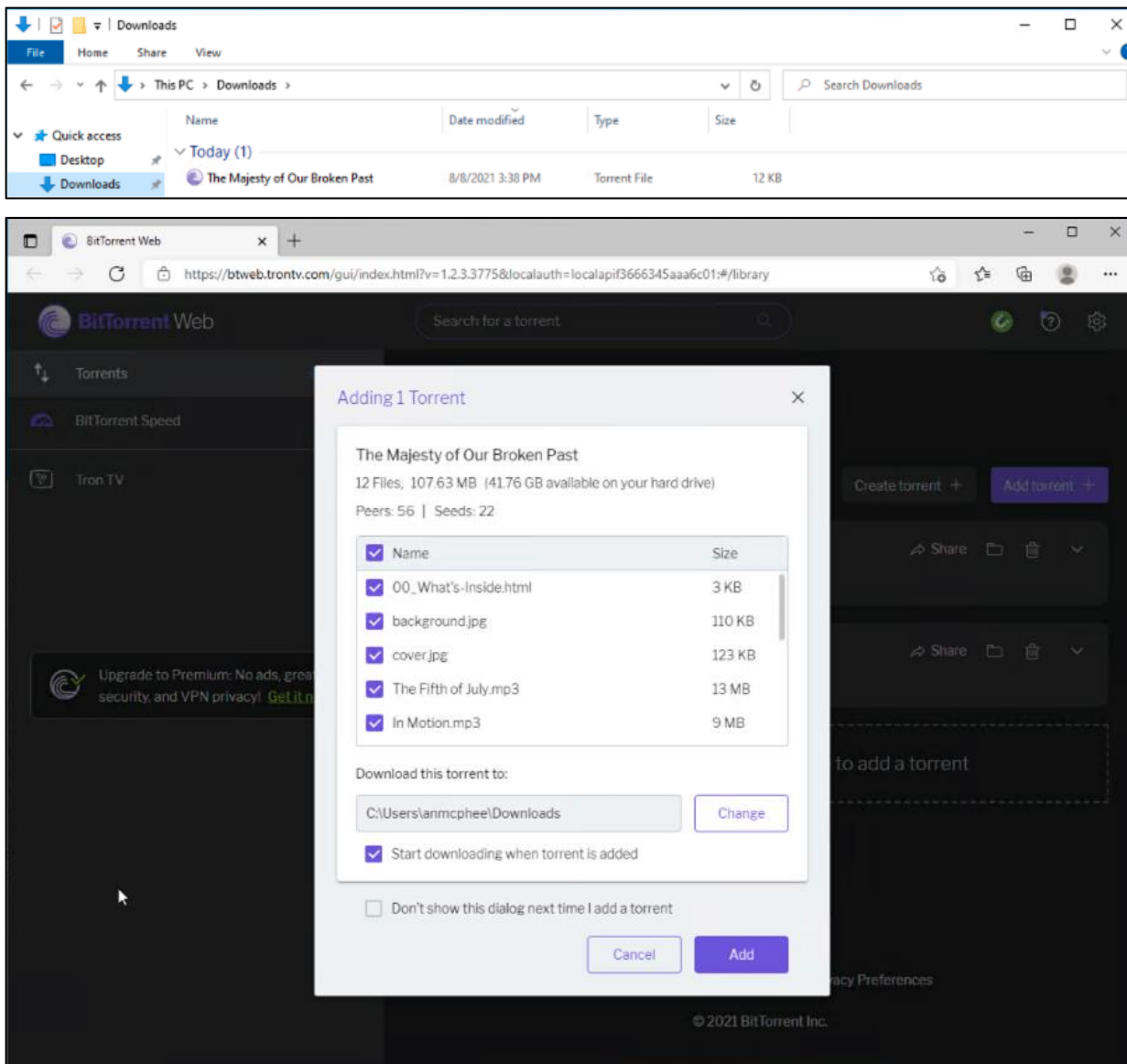
Step 2. In any browser, navigate to <https://now.bt.co>.



Step 3. Download any file from the site.



Step 4. Open the file on the client machine. This will attempt to download the file from a P2P network.



Note: There is a chance that some files will make it into the network. In this case, Cisco Secure Endpoint will analyze any malicious files and block accordingly. Nevertheless, it was validated that no data was seeded to other clients, meaning 100% of outbound activity was blocked by Umbrella policy.

- Step 5.** In the Umbrella Dashboard, navigate to **Reporting > Core Reports > Activity Search**.
- Step 6.** In the **Filters** tab, check the **Blocked** box under **Response** and click **Apply**.
- Step 7.** Verify the **P2P** activity has been logged.

Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:08 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:08 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:08 PM	...
Blocked	Uncategorized	Bittorrent	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...

Validation Test #4 - Umbrella DLP Policies have been triggered


Step 1. In any browser, navigate to any cloud storage site. This design guide will use Box.



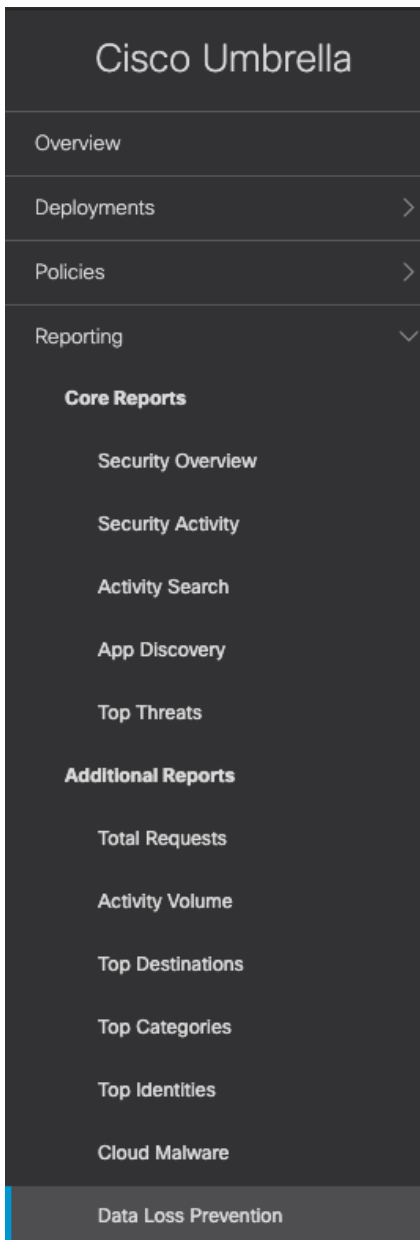
Step 2. Upload a file containing random US credit card numbers. Example below.

6011 1834 5527 3209
Discover
6011 2150 2716 5024
Discover
4328 1373 5449 1554
Visa
5430 3563 9033 0772
MasterCard
6011 0430 8746 4644
Discover
6011 6766 2381 3665
Discover

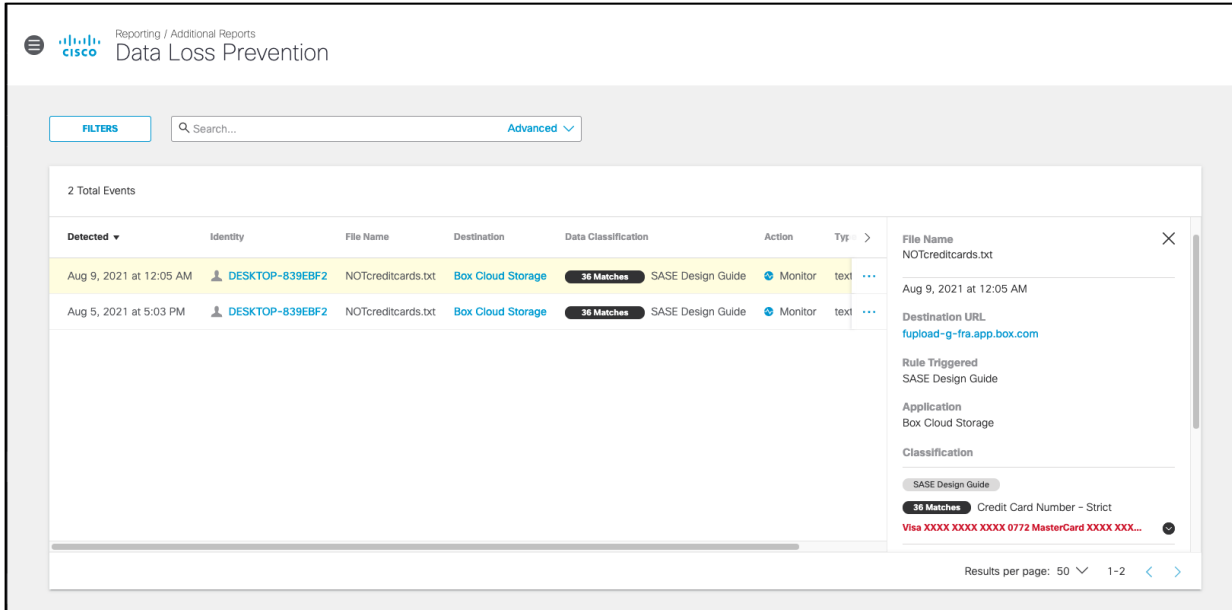
All Files > SASE Design Guide

Name	Updated	Size	
 NOTcreditcards.txt	Today by Andrew Mcphee	182 B	

Step 3. In the Umbrella Dashboard, navigate to **Reporting > Additional Reports > Data Loss Prevention**.

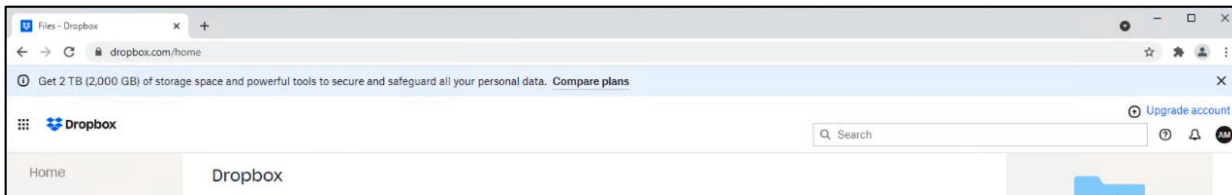


Step 4. An event will be created for the file that was uploaded.



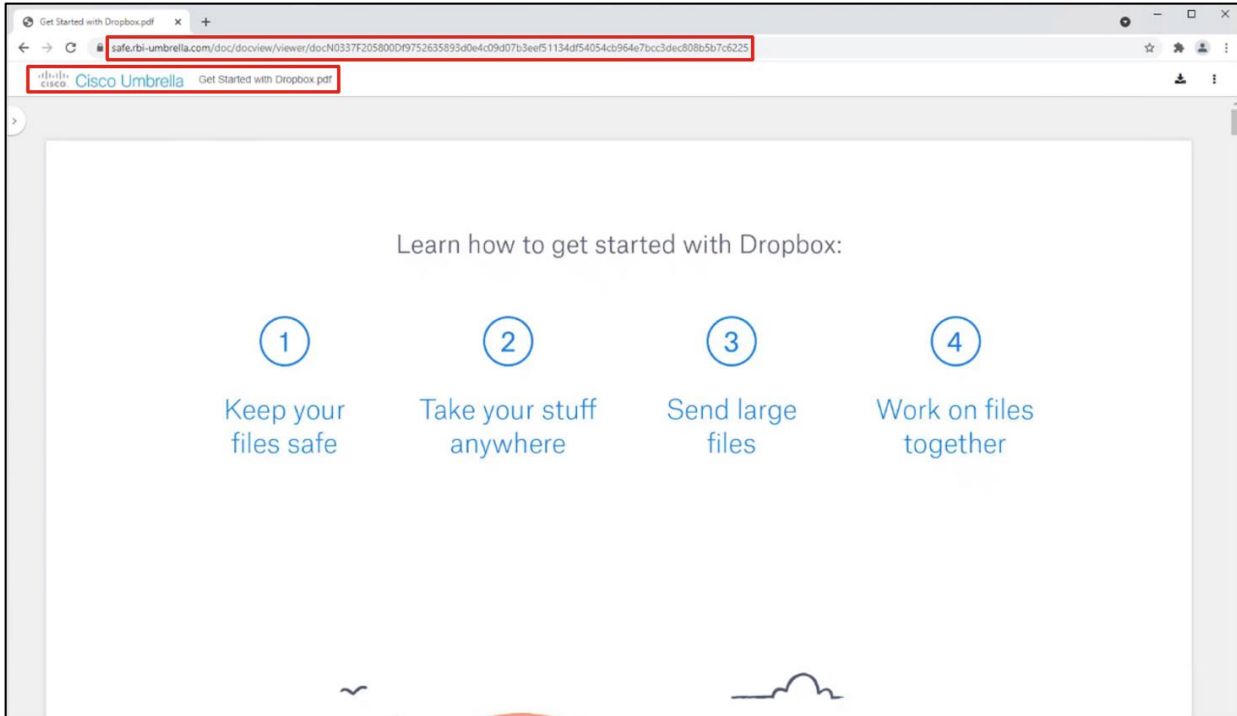
Validation Test #5 - Umbrella Remote Browser Isolation

Step 1. In any browser, navigate to <https://dropbox.com> (the site chosen for our DLP policy).



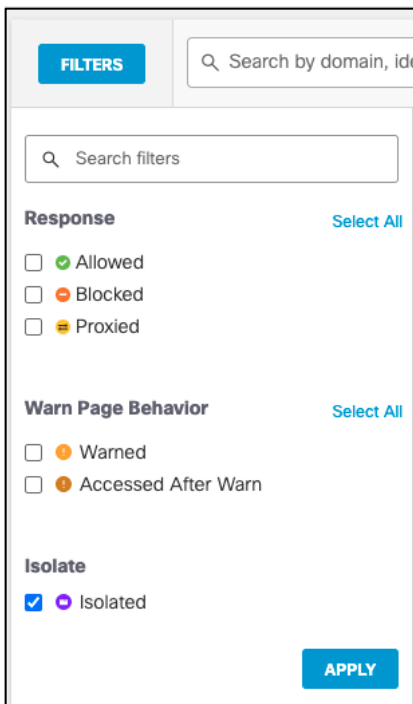
Step 2. Download any file.

Step 3. The file will download and open in a remote browser, which can be confirmed by looking at the URL of the opened file.



Step 4. In the Umbrella Dashboard, navigate to **Reporting > Core Reports > Activity Search**.

Step 5. In the **Filters** tab, check the **Isolated** box under **Isolate** and click **Apply**.



Step 6. Verify that the session to Dropbox has been logged.

Internal IP	External IP	Action	Categories	Application	Application Category	Application Protocol	Date & Time
192.168.127.2	12.151.35.209	Allowed (Isolated)					Aug 9, 2021 at 12:09 AM ...
192.168.127.2	12.151.35.209	Allowed (Isolated)	File Storage	Dropbox	Cloud Storage		Aug 9, 2021 at 12:09 AM ...
192.168.127.2	12.151.35.209	Allowed (Isolated)	File Storage	Dropbox	Cloud Storage		Aug 9, 2021 at 12:09 AM ...
192.168.127.2	12.151.35.209	Allowed (Isolated)	File Storage	Dropbox	Cloud Storage		Aug 9, 2021 at 12:09 AM ...
192.168.127.2	12.151.35.209	Allowed (Isolated)	File Storage	Dropbox	Cloud Storage		Aug 9, 2021 at 12:07 AM ...
192.168.127.2	12.151.35.209	Allowed (Isolated)	File Storage	Dropbox	Cloud Storage		Aug 8, 2021 at 9:06 PM ...

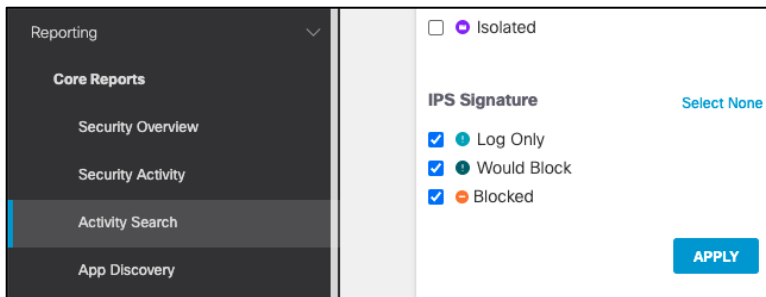
Validation Test #6 - Intrusion Prevention System

Step 1. Open a command prompt and type the following:

```
curl http://3.25.228.160/test.emf
```

Step 2. In the Cisco Umbrella dashboard, navigate to **Reporting > Core Reports > Activity Search**.

Step 3. Under **IPS Signature** filters, click **Select All** and then **Apply**.

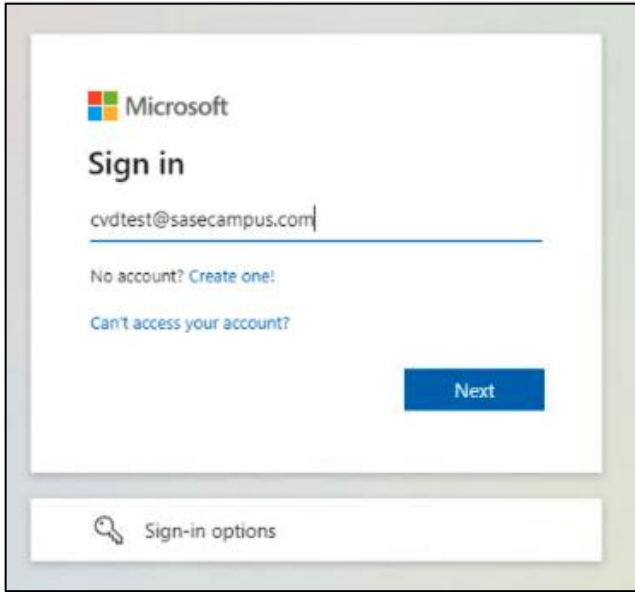


Step 4. The activity log should show an IPS log that triggered based on a Microsoft emf file download request.

Request	Identity	Policy or Ruleset Identity	Destination	Internal IP	External IP	Action	Categories	Application
IPS	SASE Branch		146.112.255.50:80			Allowed (Log Only)		...

Validation Test #7 - Duo SSO for SaaS Applications

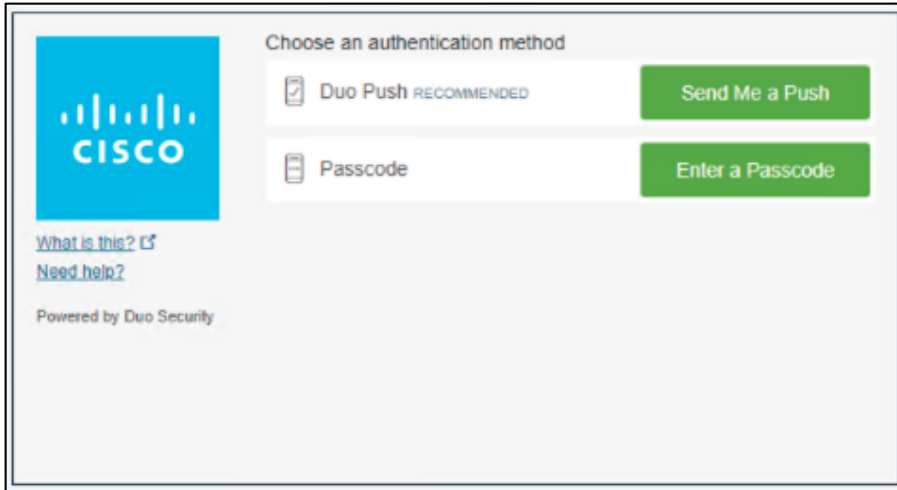
Step 1. In any browser, navigate to <https://login.microsoftonline.com> and sign into your Microsoft 365 domain.



Step 2. Verify that the sign-on process is routed to Cisco Duo SSO.



Step 3. Verify your identity with Cisco Duo MFA.



Step 4. In the Duo Dashboard, navigate to **Reports > Authentication Log** and verify an SSO event was logged.

Timestamp (UTC)	Result	User	Application	Access Device	Second Factor
12:16:49 AM AUG 9, 2021	✓ Granted User approved	cvdtest	Microsoft 365 - Single Sign-On	> Windows 10 As reported by the browser	> Duo Push San Jose, CA, United States

Remote Worker to Private Application (VPNless)

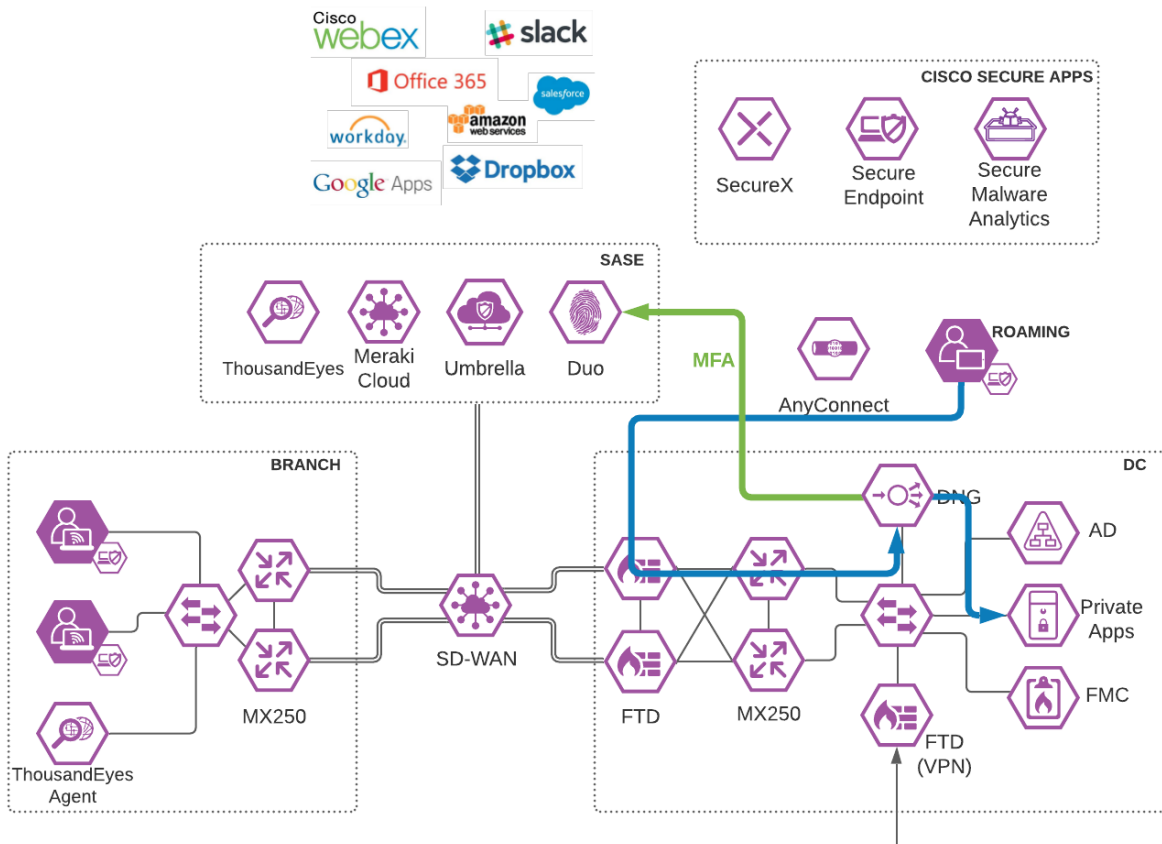
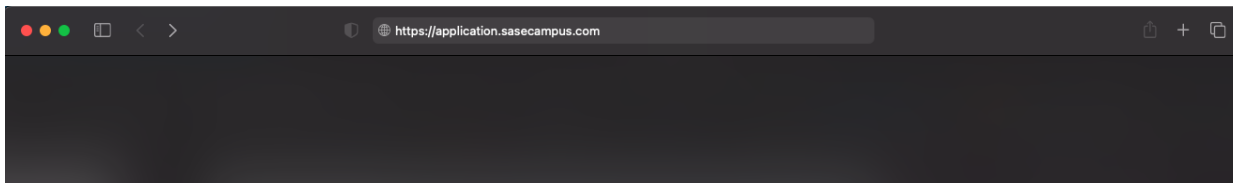


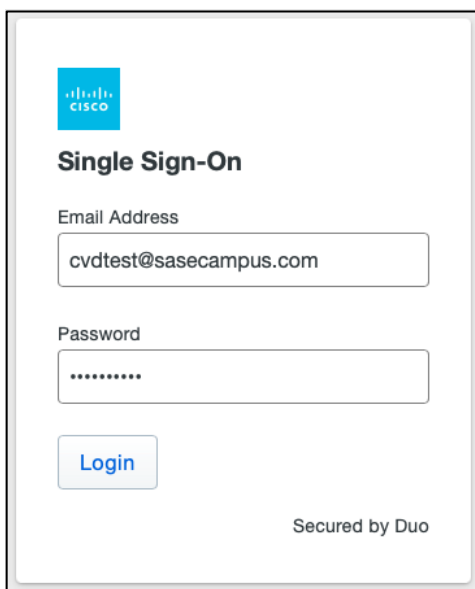
Figure 23.
Roaming User to Private Application through Duo Network Gateway

Validation Test #1 - Verify Private Application can be reached from Public Internet

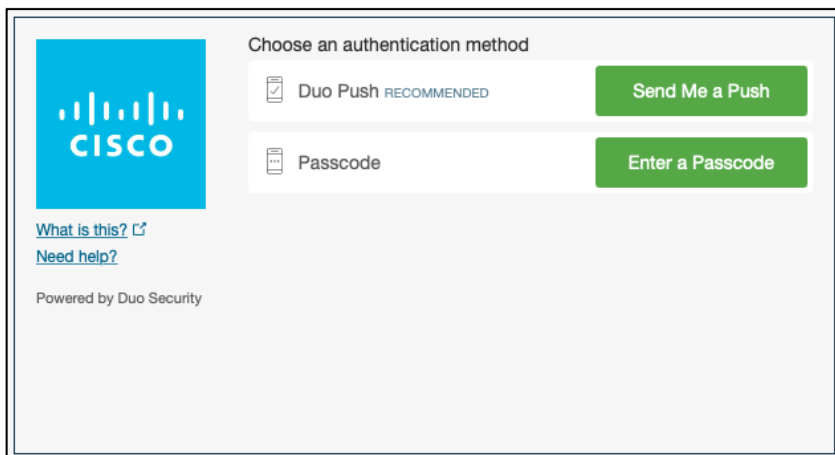
Step 1. Using any browser on a client **off network**, navigate to the URL that was assigned to your application in the DNG installation.



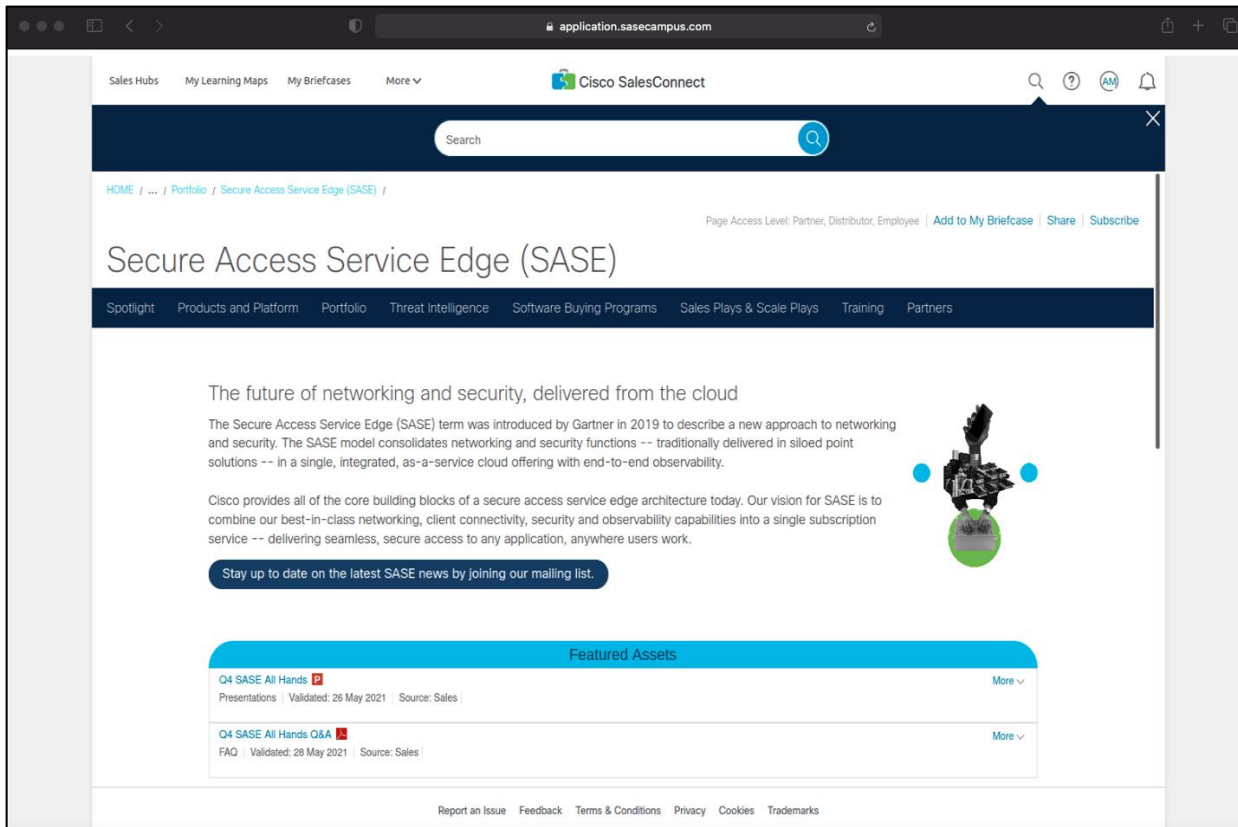
Step 2. Sign into Cisco Duo SSO.



Step 3. Verify your identity with Cisco Duo MFA.



Step 4. The HTTPS should be proxied to the private application.



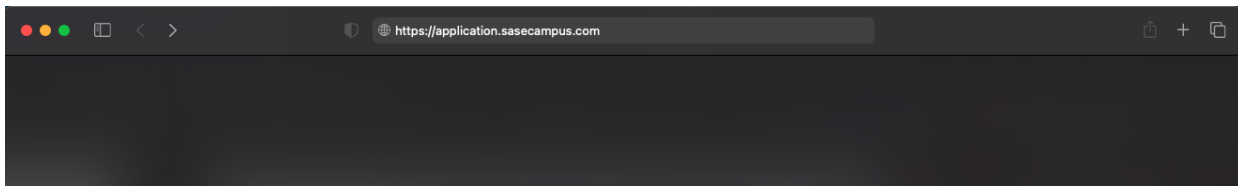
Step 5. In the Duo Dashboard, navigate to **Reports > Authentication Log**.

Step 6. Verify that the user connection has been logged.


Timestamp (UTC)	Result	User	Application	Access Device	Second Factor
4:27:28 AM AUG 9, 2021	✔ Granted User approved	cvdtest	SASE Campus - Duo Network Gateway	Mac OS X 11.4 (20F71) As reported by Device Health	Duo Push San Jose, CA, United States

Validation Test #2 - Verify Application is restricted by User

Step 1. Using any browser on a client off network, navigate to the URL that was assigned to your application in the DNG installation.



Step 2. Sign into Cisco Duo SSO using an account that was not added to the Duo Group Policy.


Single Sign-On

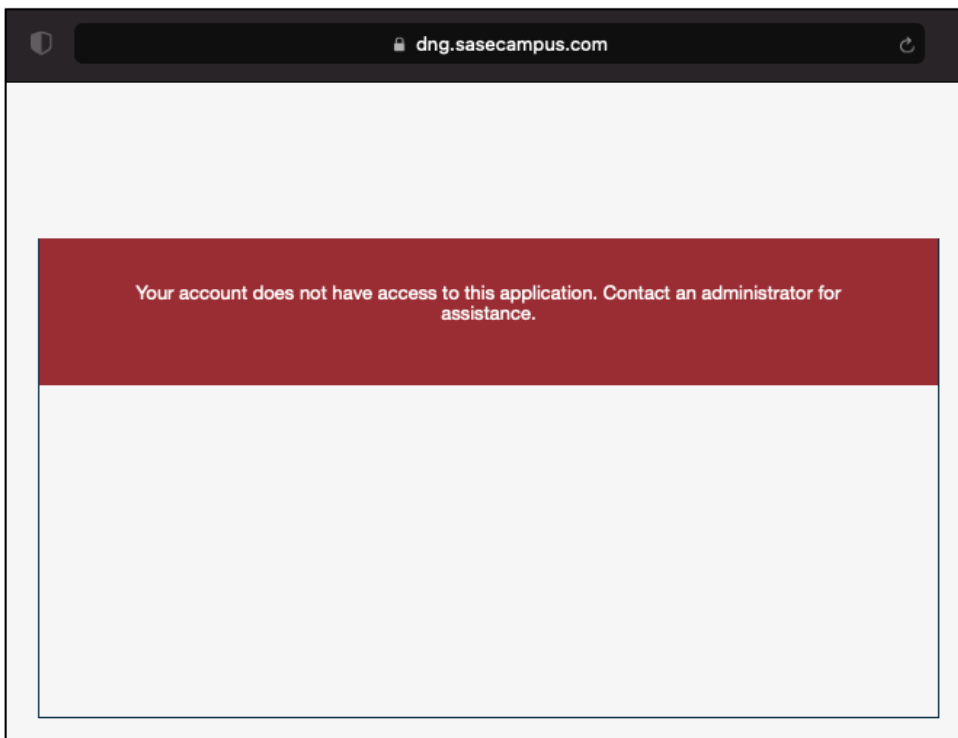
Email Address

Password

[Login](#)

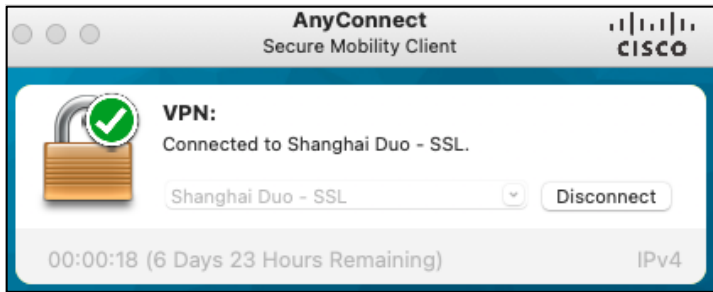
Secured by Duo

Step 3. Duo will return a page to show that access has been denied.



Validation Test #3 - Verify Application is restricted by User location

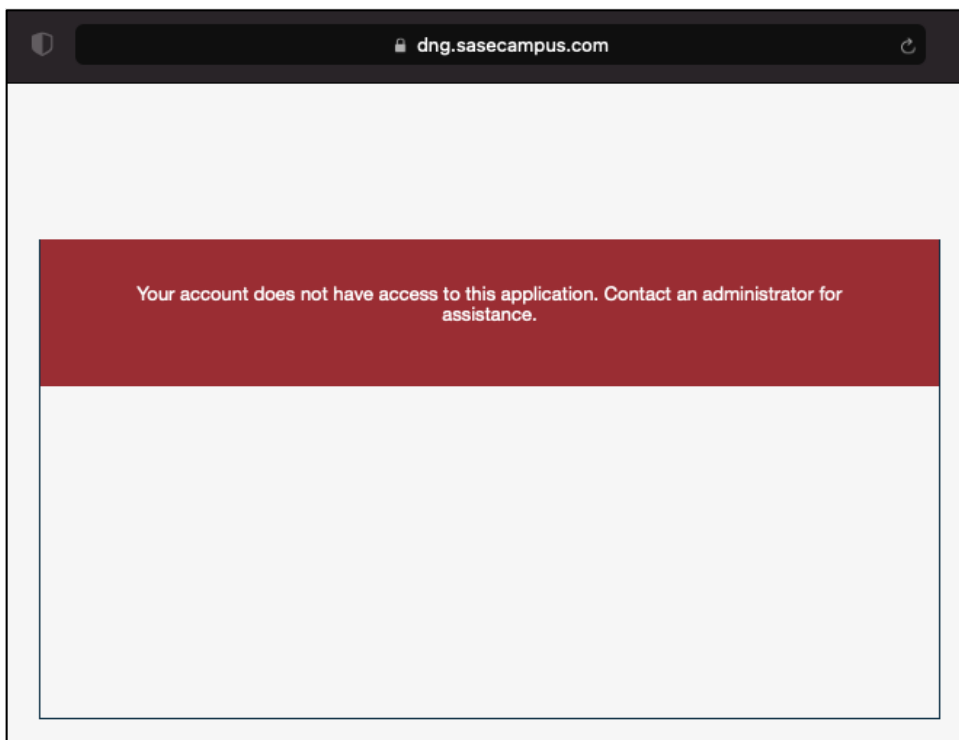
Step 1. On the client machine, use a VPN to connect to a location outside of the allowed locations. For this design guide, only devices in the United States are allowed access.



Step 2. Using any browser, navigate to the URL that was assigned to your application in the DNG installation.

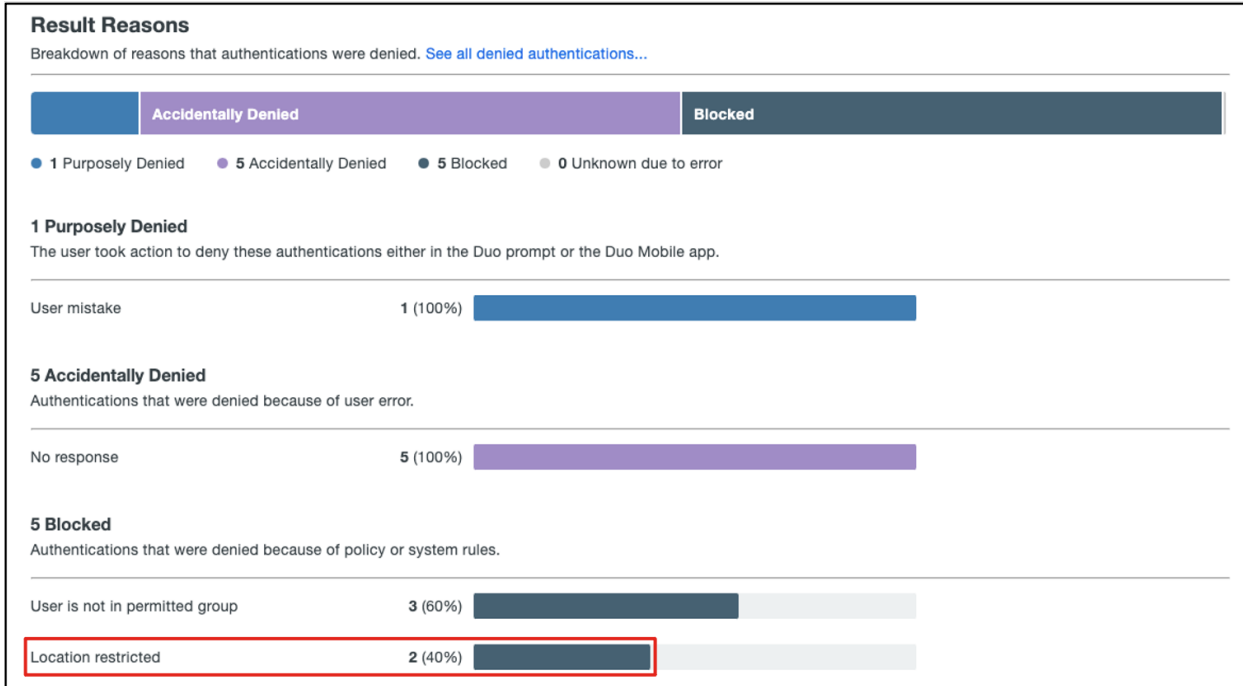
Step 3. Sign into Duo SSO.

Step 4. Duo will return Login request denied.



Step 5. In the Duo Dashboard, navigate to **Reports > Denied Authentications**.

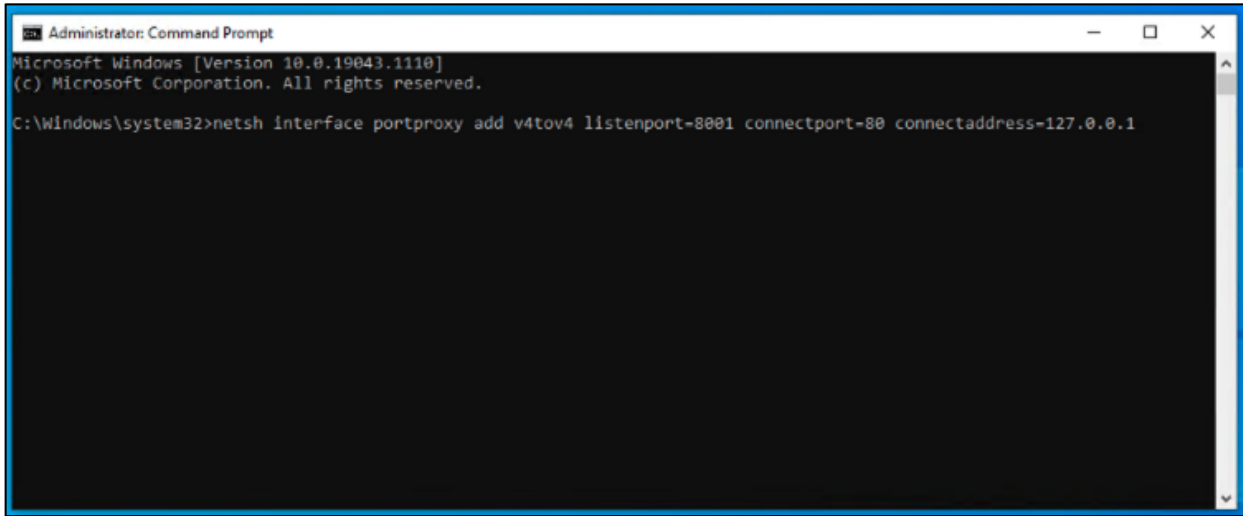
Step 6. Scroll down to **Result Reasons** and a **Location restricted** reason will be present.



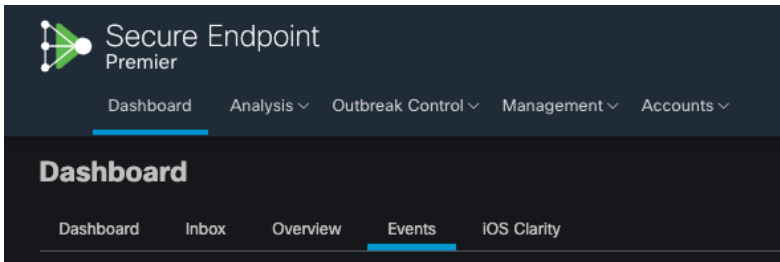
Validation Test #4 - Verify Application is restricted by Device Health

Step 1. On a [trusted device](#), trigger a Cisco Secure Endpoint alarm. Example below.

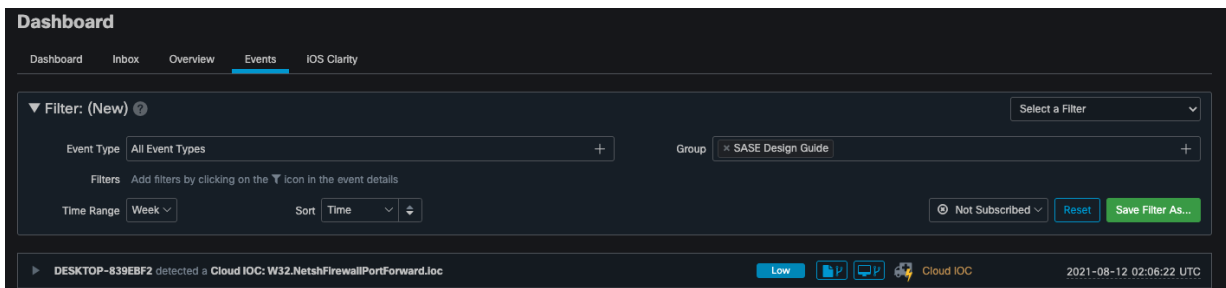
```
netsh interface portproxy add v4tov4 listenport=8001 connectport=80 connectaddress=127.0.0.1
```



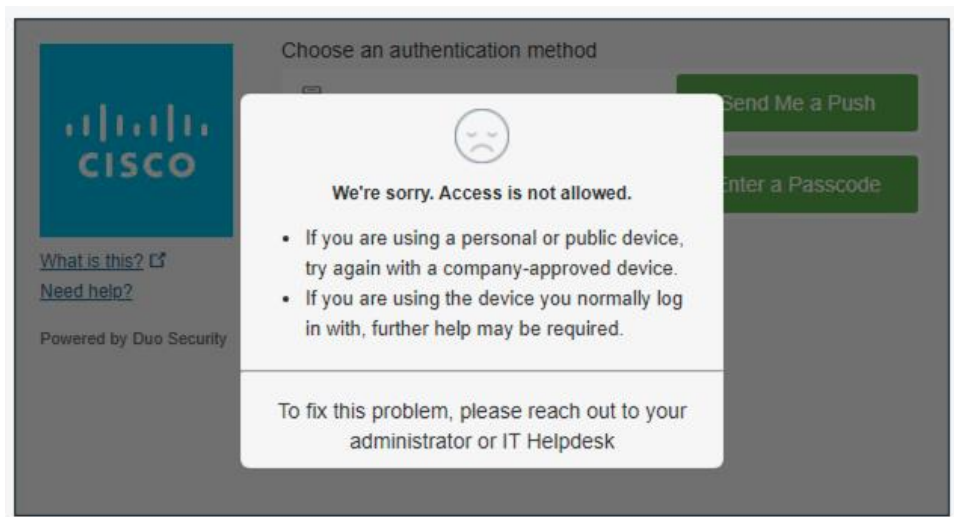
Step 2. In Cisco Secure Endpoint Dashboard, navigate to **Events**.



Step 3. Verify that an Indicator of Compromise (IoC) has occurred on the machine.



Step 4. Using any browser on the trusted endpoint, navigate to the URL that was assigned to your application in the DNG installation. Duo prompt should return **“We’re sorry. Access is not allowed.”**



Remote Worker to Private Application (VPN)

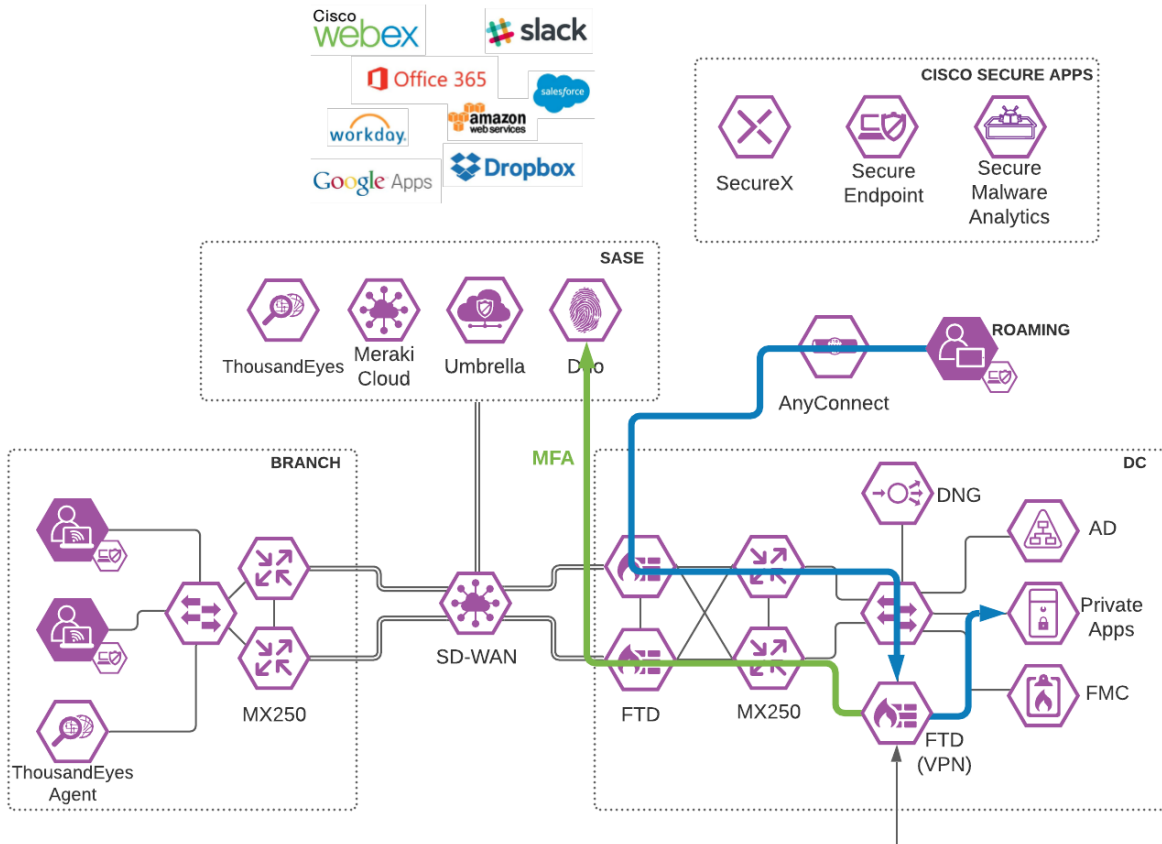
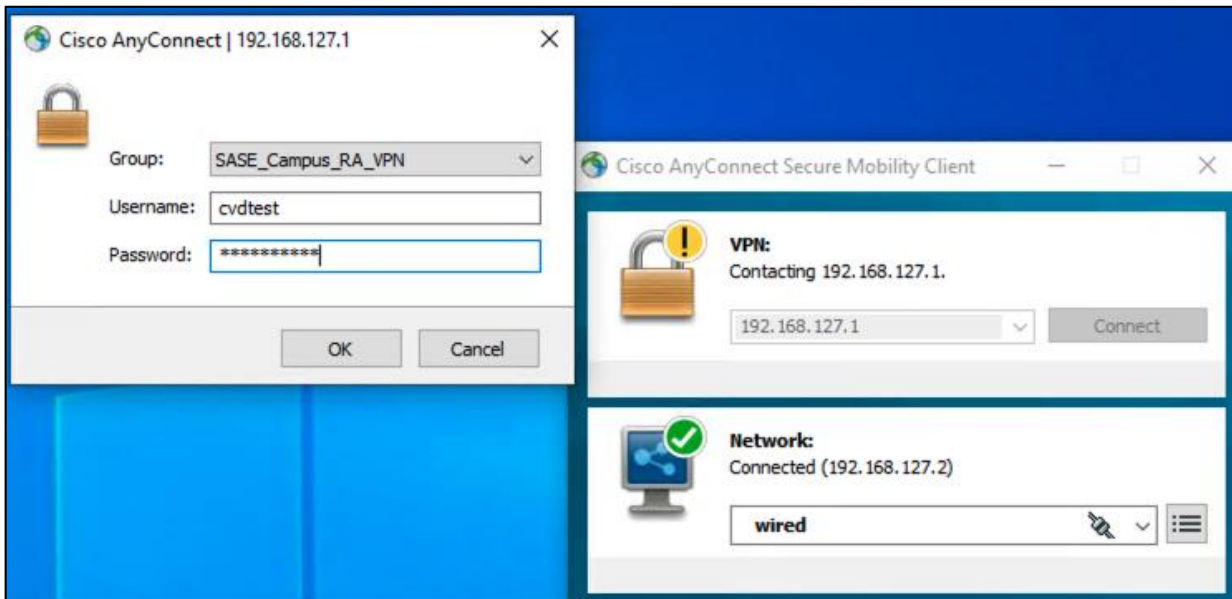


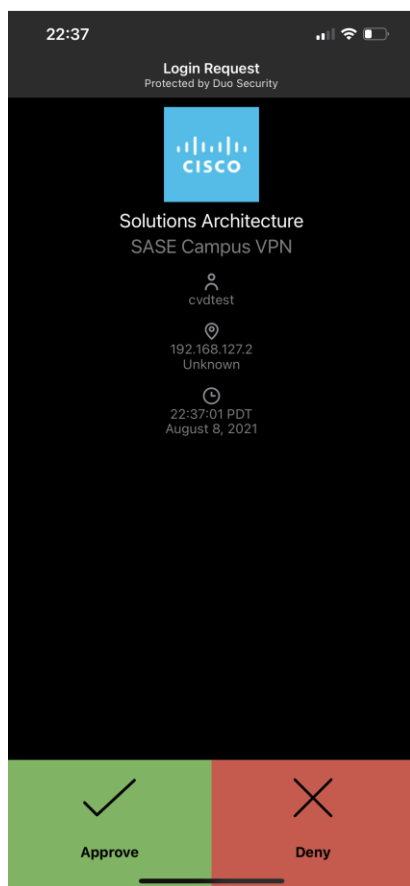
Figure 24.
Roaming User to Private Application through VPN

Validation Test #1 - Verify User can connect to VPN

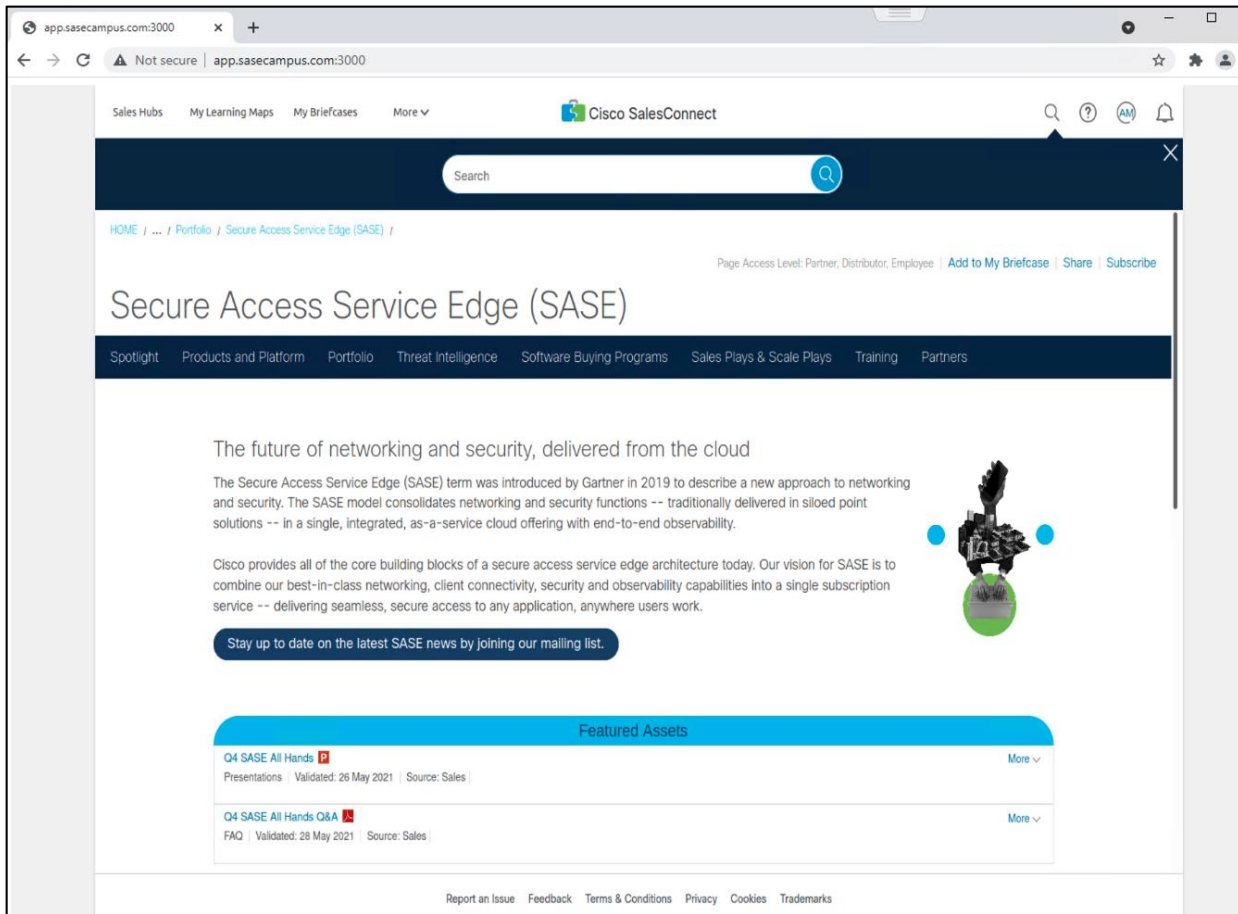
Step 1. Using AnyConnect, connect to the IP/FQDN of the VPN firewall in the data center.



Step 2. Verify your identity with Cisco Duo MFA.



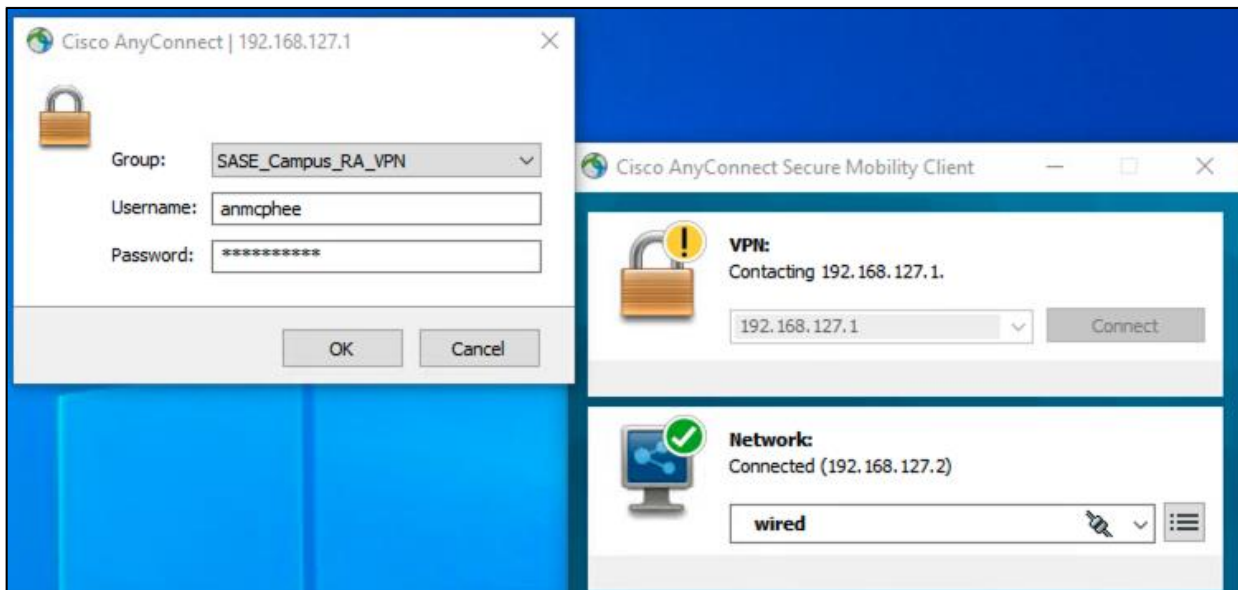
Step 3. Once connected to VPN, navigate to an application on the internal network.



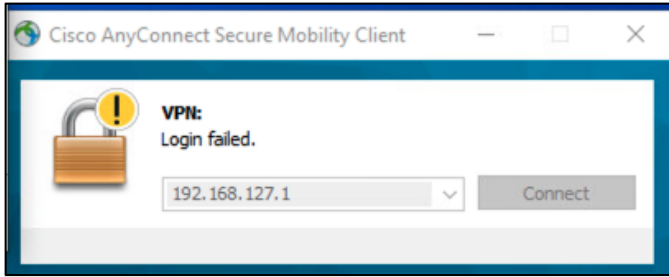
Validation Test #2 - Verify VPN access is restricted by Duo Policy

Step 1. Using AnyConnect, connect to the IP/FQDN of the VPN firewall in the data center.

Step 2. Use log-on credentials for a user who is not part of the VPN user group, as per policies created in the deployment steps.



Step 3. AnyConnect should return a failed login attempt.



Step 4. In the Duo Dashboard, navigate to **Reports > Authentication Log**.

Step 5. The **Denied** attempt should be logged for the user.

Reports						
Authentication Log						
Timestamp (UTC)	Result	User	Application	Access Device	Second Factor	
5:40:21 AM AUG 9, 2021	Denied User is not in permitted group	anmcphee	SASE Campus VPN	Location Unknown 192.168.127.2	Unknown	

Note: All other Duo policy tests work for the private application as they have in the public application validation tests.

Branch DIA

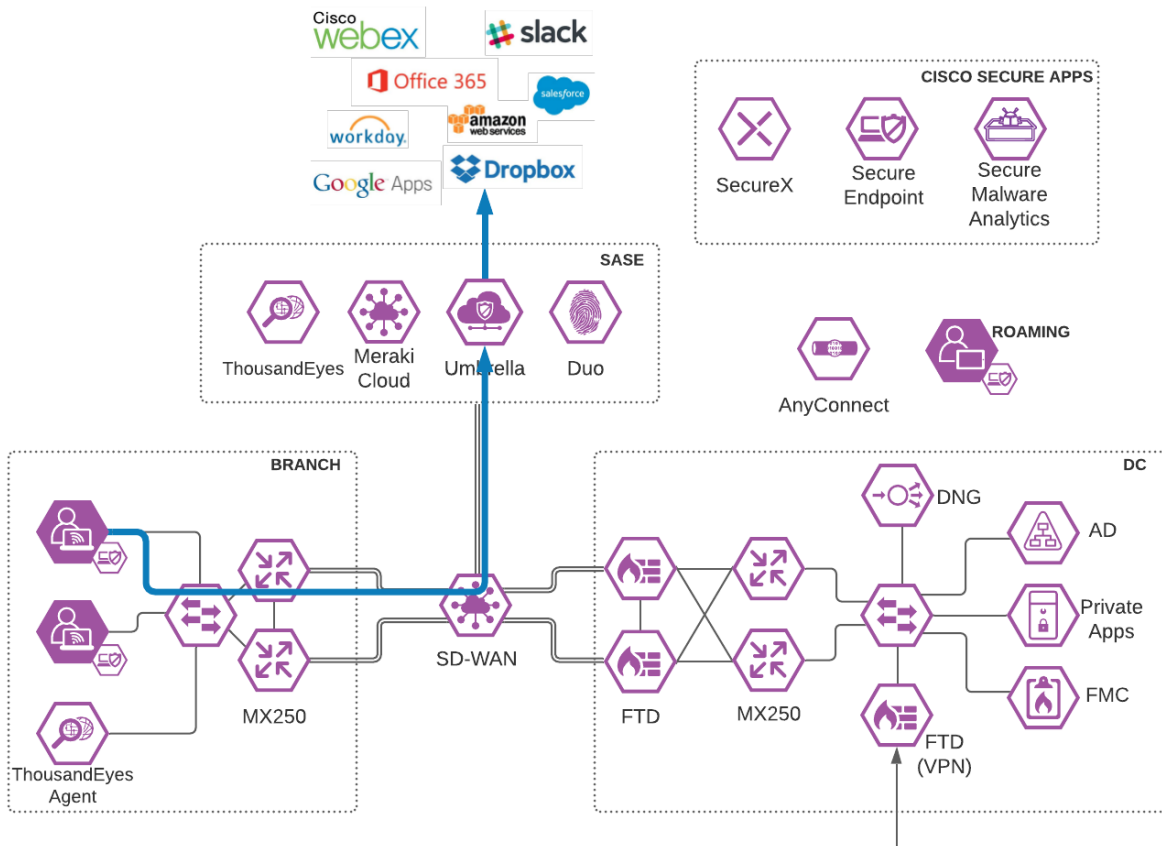
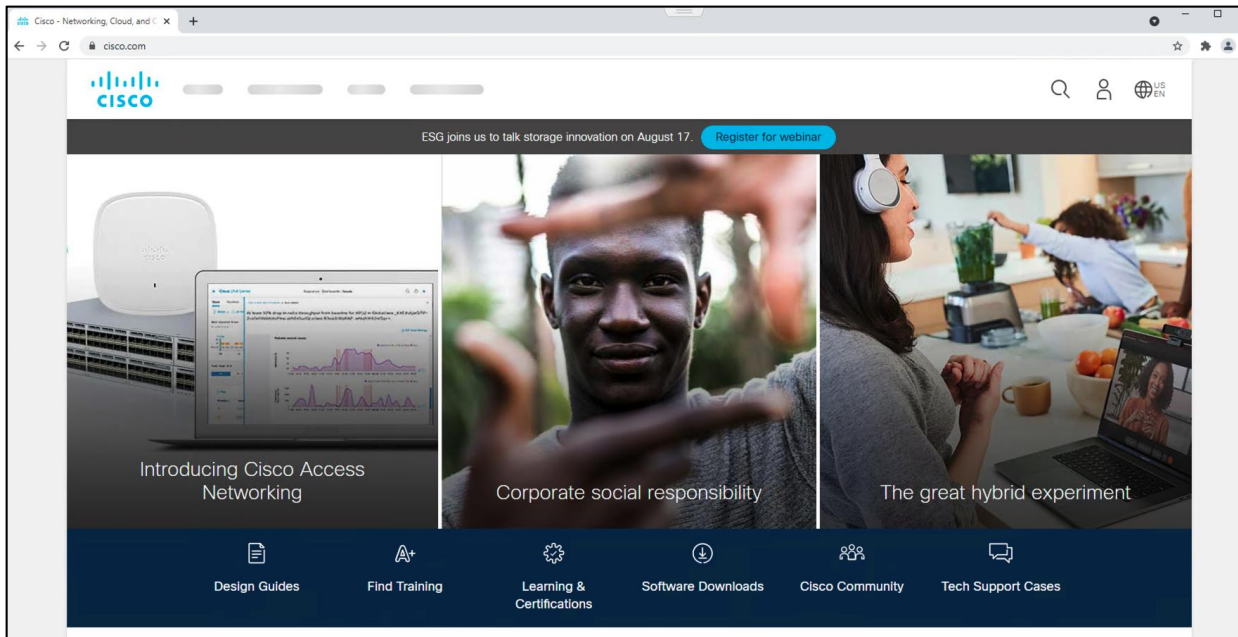


Figure 25.
Branch User to SaaS Application through Umbrella

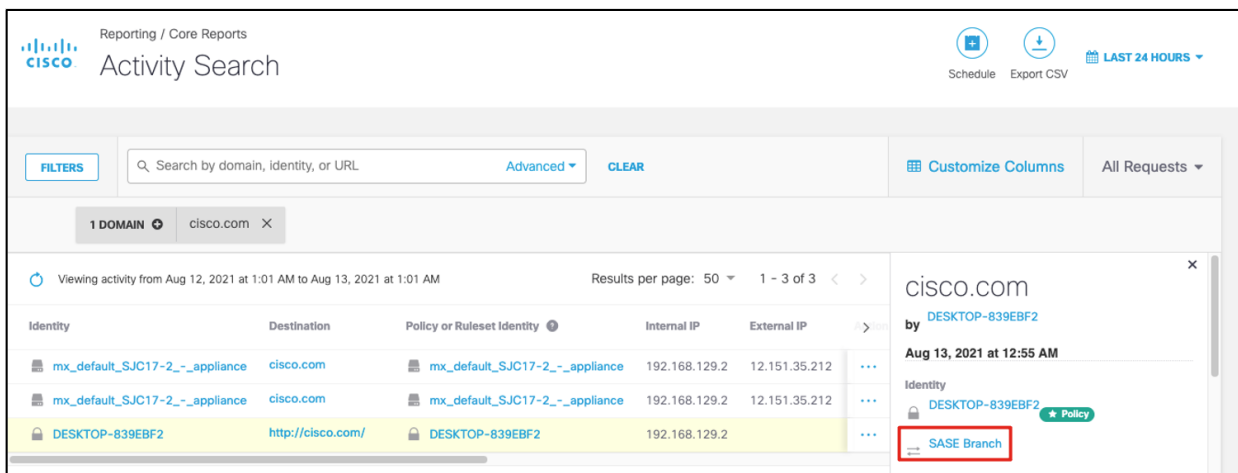
Validation Test #1 - Verify Internet traffic flows through Umbrella

Step 1. On a device in the branch network, navigate to any website.



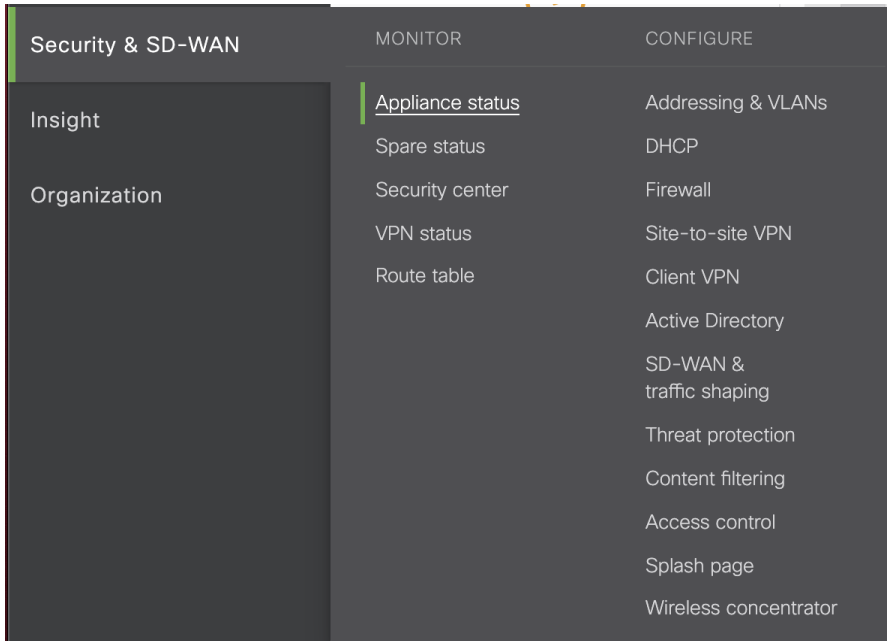
Step 2. In Umbrella, navigate to **Reporting > Core Reports > Activity Search**.

Step 3. Verify there is an activity record to the chosen site with the identity of the network tunnel present.

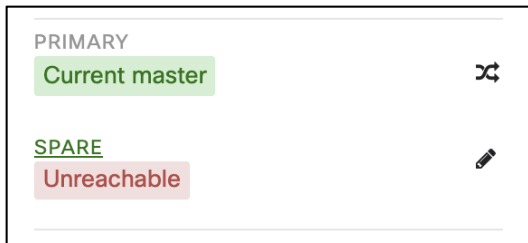


Step 4. Since the Meraki devices are in a HA pair, disconnect the WAN connection of the primary device in the branch.

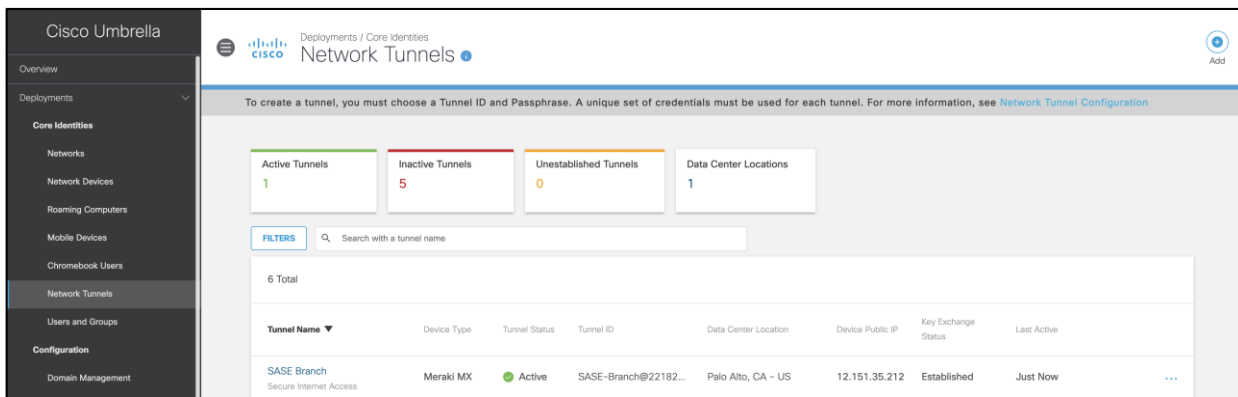
Step 5. In the Meraki Dashboard, navigate to **Security & SD-WAN > Appliance status**.



Step 6. One of the devices should be shown as **Unreachable**.

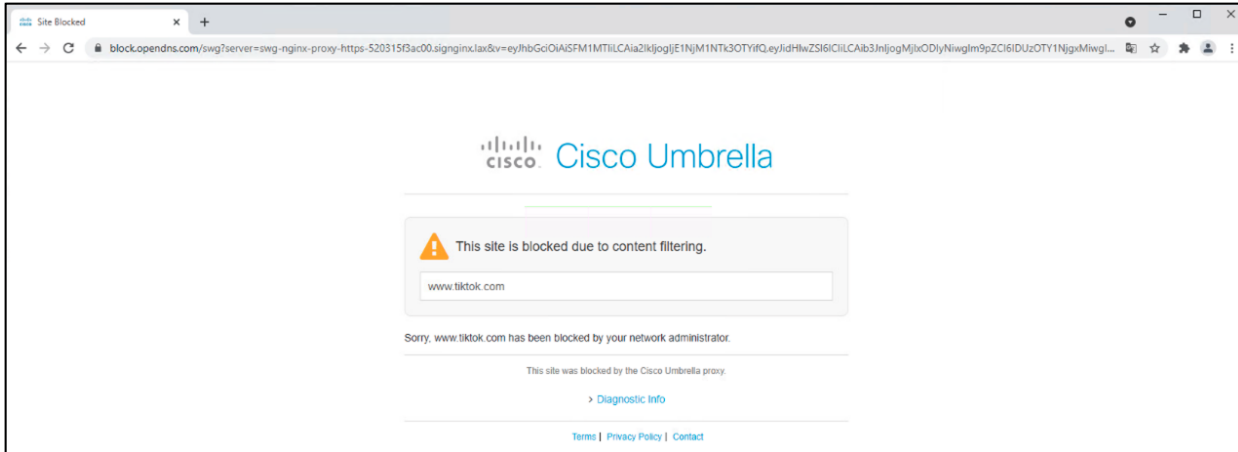


Step 7. In the Umbrella Dashboard, navigate to **Deployments > Core Identities > Network Tunnels** to ensure that the tunnel from the Meraki network is still **Active**.

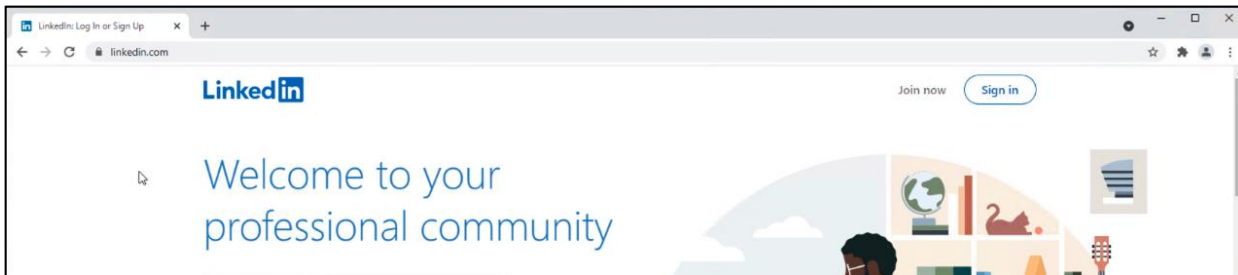


Validation Test #2 - Umbrella Content Filtering is being applied

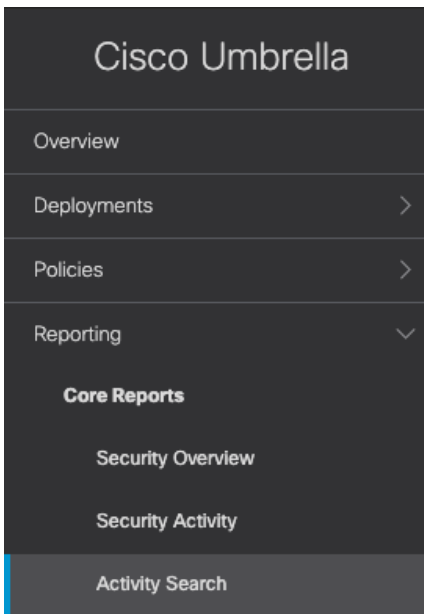
Step 1. In any browser, navigate to <https://facebook.com>. The Umbrella block page should be returned.



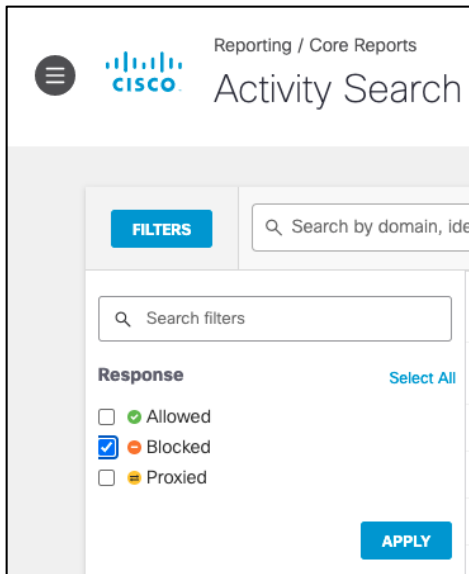
Step 2. In any browser, navigate to <https://linkedin.com>. Access to the site should be granted.



Step 3. In the Umbrella Dashboard, navigate to **Reporting > Core Reports > Activity Search**.



Step 4. In the **Filters** tab, check the **Blocked** box under **Response** and click **Apply**.

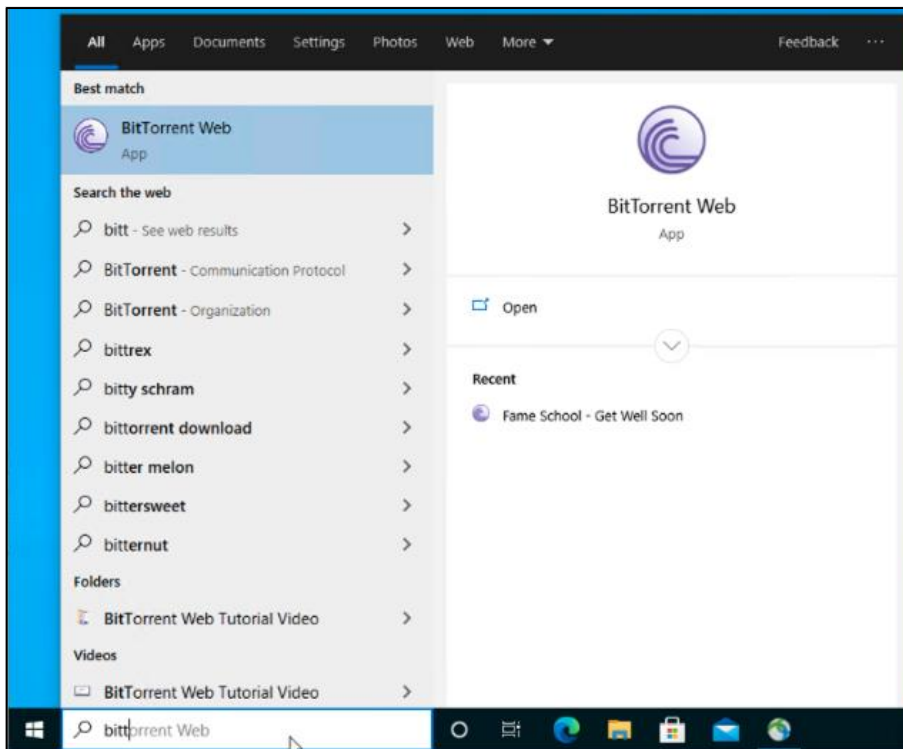


Step 5. Verify the entry for **Facebook** has been logged.

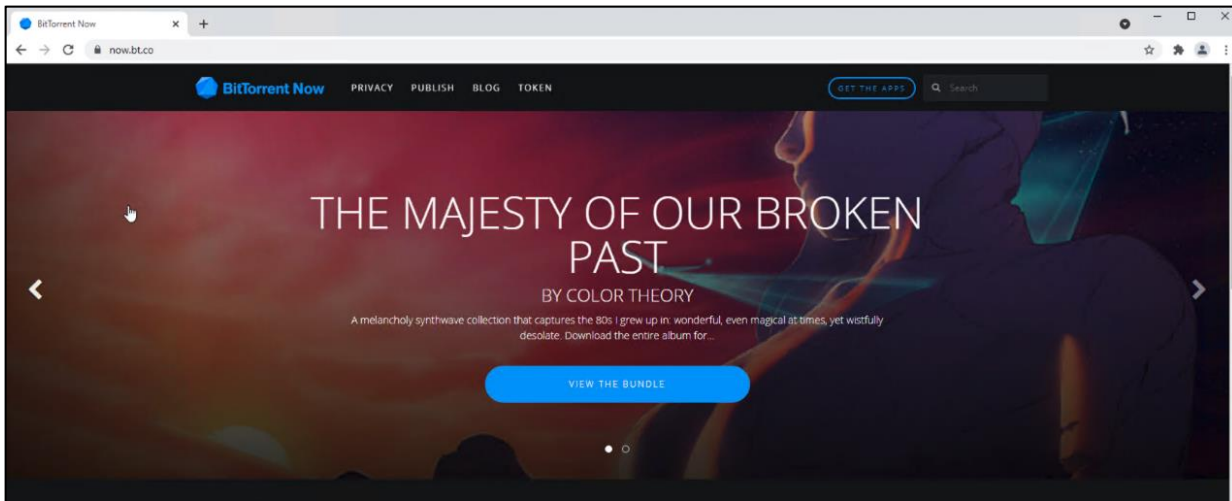
Internal IP	External IP	Action	Categories	Application	Application Category	Application Protocol	Date & Time
192.168.129.2		Blocked	Application Block, Social Networking	Facebook	Social Networking		Aug 13, 2021 at 1:01 AM
192.168.129.2		Blocked	Application Block, Social Networking	Facebook	Social Networking		Aug 13, 2021 at 1:01 AM

Validation Test #3 - Umbrella Firewall policies are being triggered

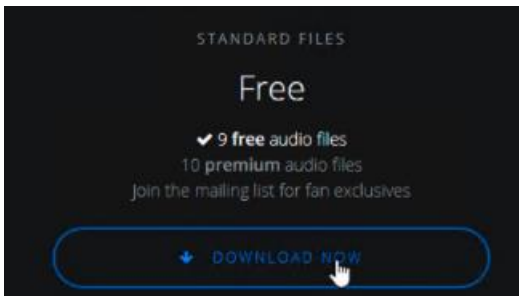
Step 1. Download and install the [BitTorrent application](#) onto the client machine.



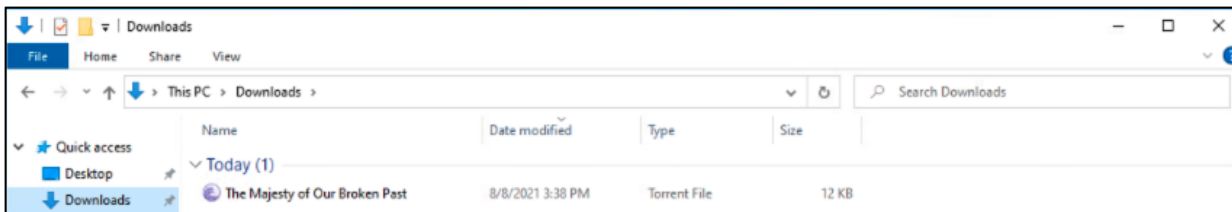
Step 2. In any browser, navigate to <https://now.bt.co>.

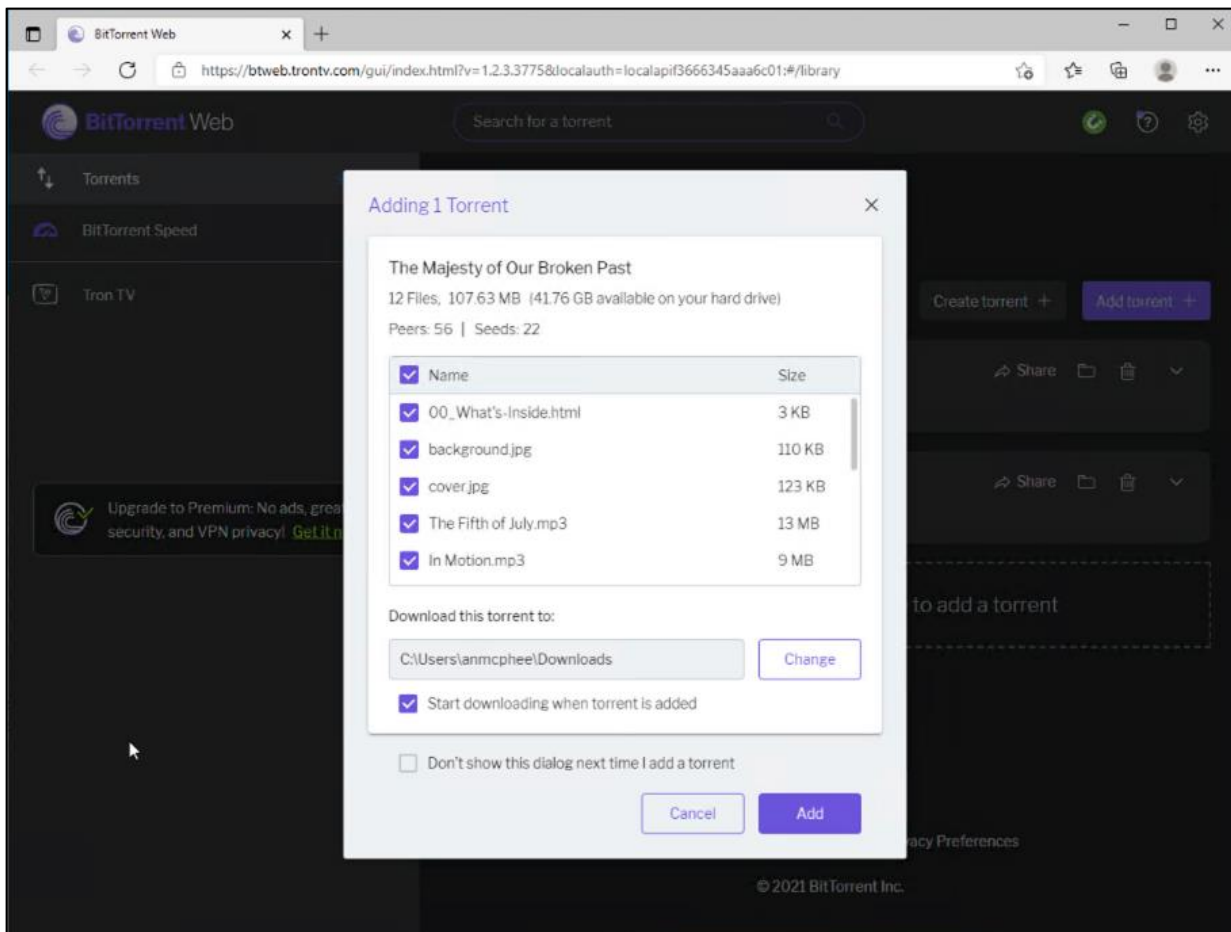


Step 3. Download any file from the site.



Step 4. Open the file on the client machine. This will attempt to download the file from a P2P network.





Note: There is a chance that some files will make it into the network. In this case, Cisco Secure Endpoint will analyze any malicious files and block accordingly. Nevertheless, it was validated that no data was seeded to other clients, meaning 100% of outbound activity was blocked by Umbrella policy.

- Step 5.** In the Umbrella Dashboard, navigate to **Reporting > Core Reports > Activity Search**.
- Step 6.** In the **Filters** tab, check the **Blocked** box under **Response** and click **Apply**.
- Step 7.** Verify the **P2P** activity has been logged.

Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:08 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:08 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:08 PM	...
Blocked	Uncategorized	Bittorrent	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...
Blocked	Uncategorized	Bittorrent Networking	P2P	Aug 8, 2021 at 10:07 PM	...

Validation Test #4 - Umbrella DLP Policies have been triggered


Step 1. In any browser, navigate to any cloud storage site. This design guide will use Box.



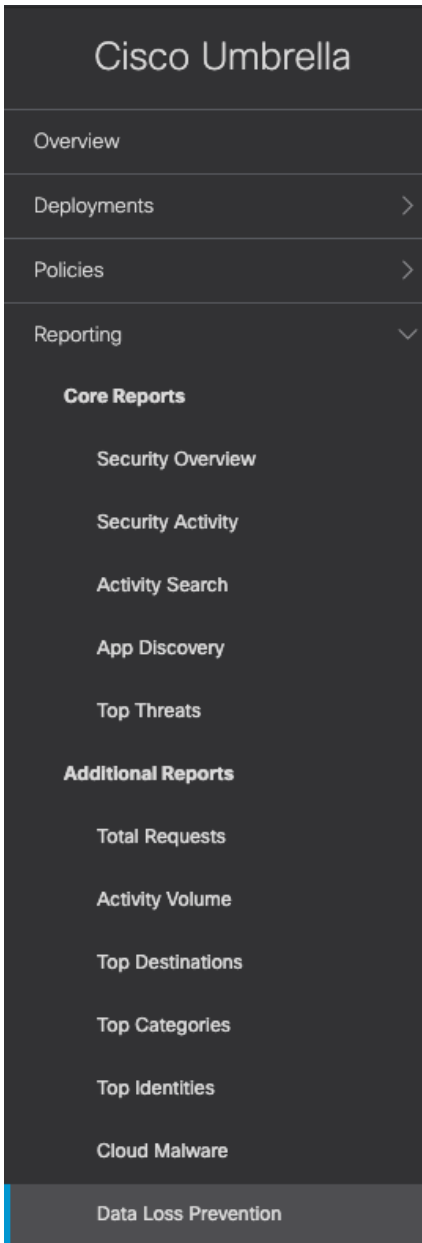
Step 2. Upload a file containing random US credit card numbers. Example below.

6011 1834 5527 3209
Discover
6011 2150 2716 5024
Discover
4328 1373 5449 1554
Visa
5430 3563 9033 0772
MasterCard
6011 0430 8746 4644
Discover
6011 6766 2381 3665
Discover

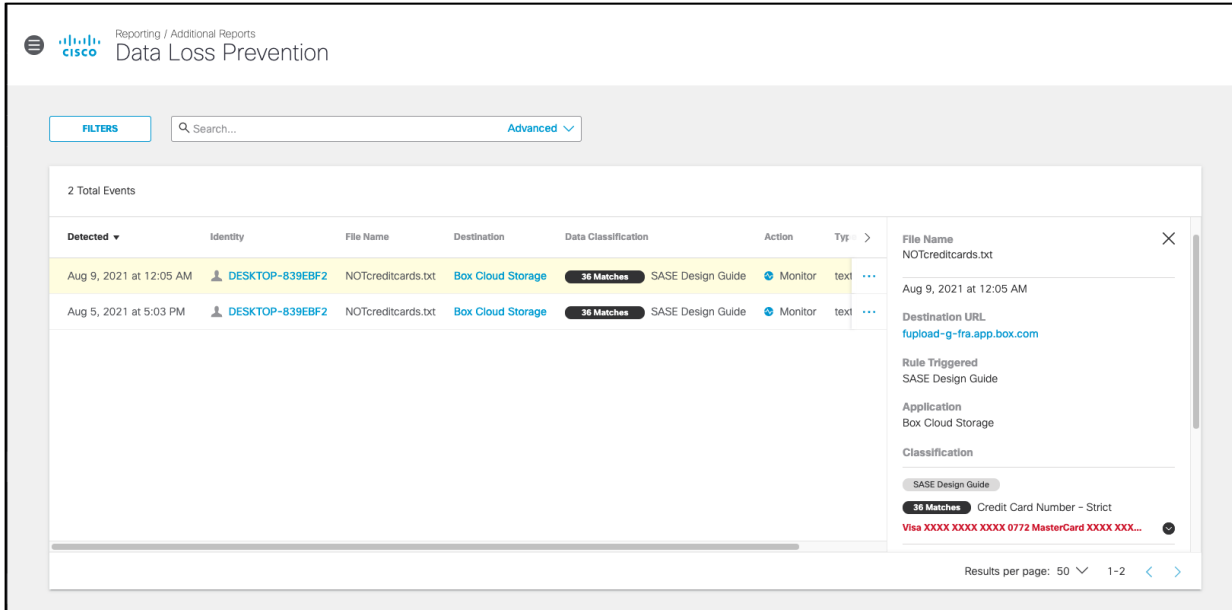
All Files > SASE Design Guide

Name	Updated	Size	
 NOTcreditcards.txt	Today by Andrew Mcphee	182 B	

Step 3. In the Umbrella Dashboard, navigate to **Reporting > Additional Reports > Data Loss Prevention**.

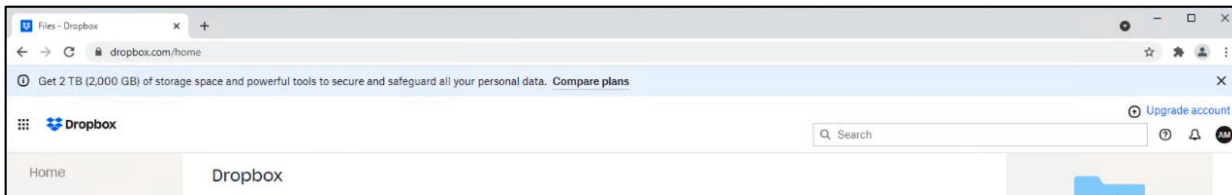


Step 4. An event will be created for the file that was uploaded.



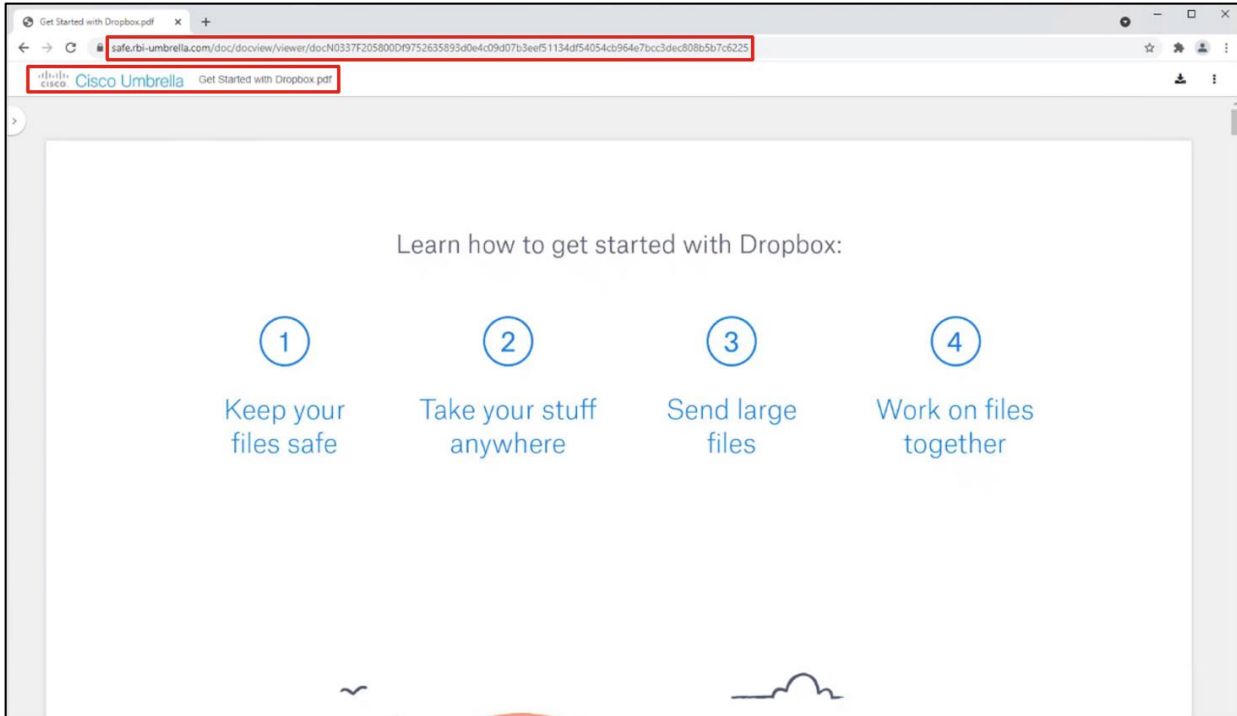
Validation Test #5 - Umbrella Remote Browser Isolation

Step 1. In any browser, navigate to <https://dropbox.com> (the site chosen for our DLP policy).



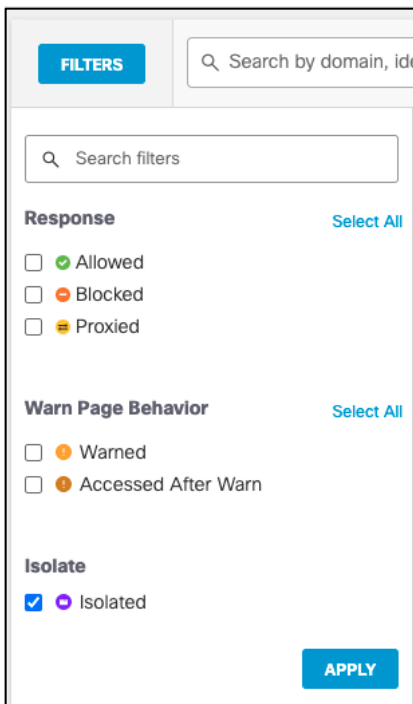
Step 2. Download any file.

Step 3. The file will download and open in a remote browser, which can be confirmed by looking at the URL of the opened file.



Step 4. In the Umbrella Dashboard, navigate to **Reporting > Core Reports > Activity Search**.

Step 5. In the **Filters** tab, check the **Isolated** box under **Isolate** and click **Apply**.



Step 6. Verify that the session to Dropbox has been logged.

Internal IP	External IP	Action	Categories	Application	Application Category	Application Protocol	Date & Time
192.168.127.2	12.151.35.209	Allowed (Isolated)					Aug 9, 2021 at 12:09 AM ...
192.168.127.2	12.151.35.209	Allowed (Isolated)	File Storage	Dropbox	Cloud Storage		Aug 9, 2021 at 12:09 AM ...
192.168.127.2	12.151.35.209	Allowed (Isolated)	File Storage	Dropbox	Cloud Storage		Aug 9, 2021 at 12:09 AM ...
192.168.127.2	12.151.35.209	Allowed (Isolated)	File Storage	Dropbox	Cloud Storage		Aug 9, 2021 at 12:09 AM ...
192.168.127.2	12.151.35.209	Allowed (Isolated)	File Storage	Dropbox	Cloud Storage		Aug 9, 2021 at 12:07 AM ...
192.168.127.2	12.151.35.209	Allowed (Isolated)	File Storage	Dropbox	Cloud Storage		Aug 8, 2021 at 9:06 PM ...

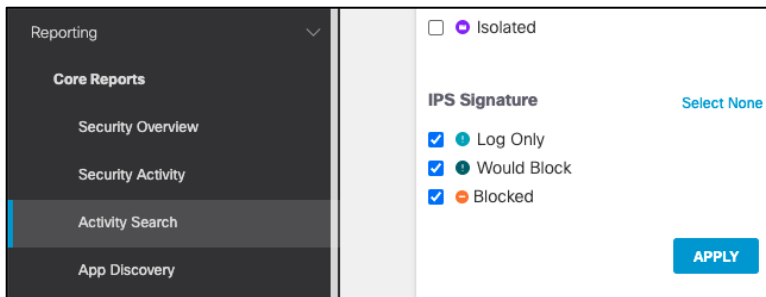
Validation Test #6 - Intrusion Prevention System

Step 1. Open a command prompt and type the following:

```
curl http://3.25.228.160/test.emf
```

Step 2. In the Cisco Umbrella dashboard, navigate to **Reporting > Core Reports > Activity Search**.

Step 3. Under **IPS Signature** filters, click **Select All** and then **Apply**.

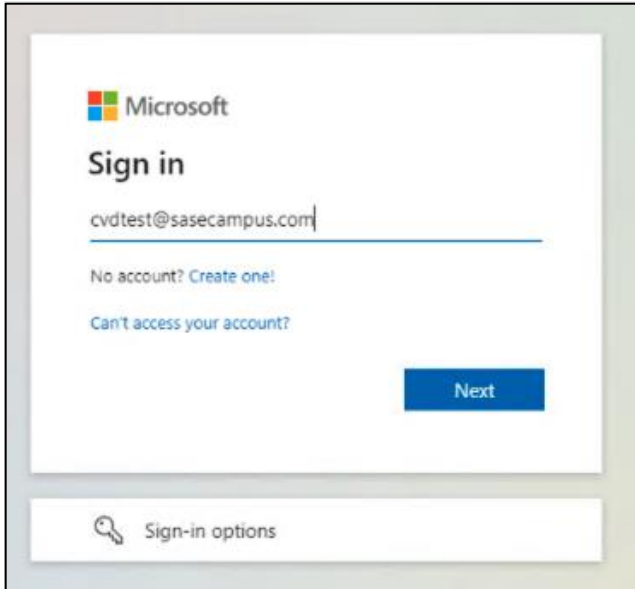


Step 4. The activity log should show an IPS log that triggered based on a Microsoft emf file download request.

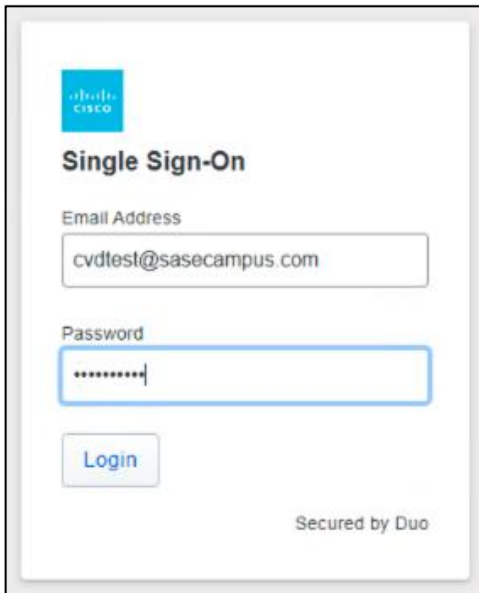
Request	Identity	Policy or Ruleset Identity	Destination	Internal IP	External IP	Action	Categories	Application
IPS	SASE Branch		146.112.255.50:80			Allowed (Log Only)		...

Validation Test #7 - Duo SSO for SaaS Applications

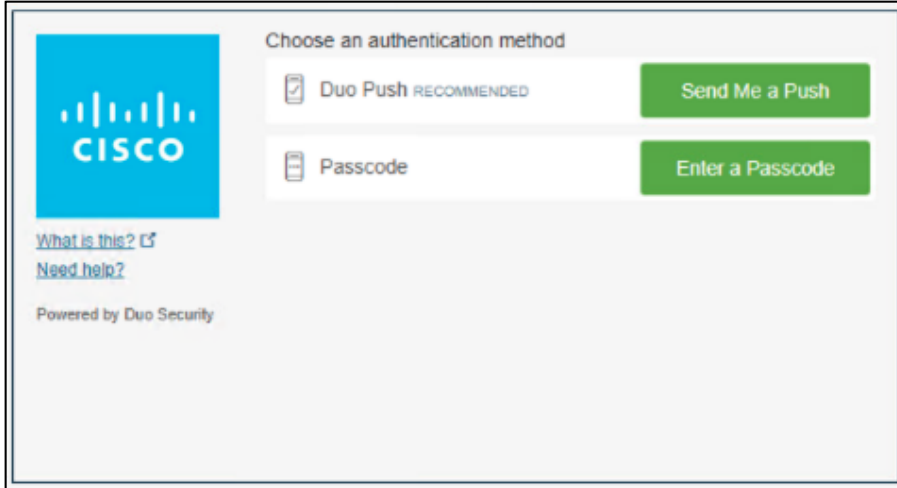
Step 1. In any browser, navigate to <https://login.microsoftonline.com> and sign into your Microsoft 365 domain.



Step 2. Verify that the sign-on process is routed to Cisco Duo SSO.



Step 3. Verify your identity with Cisco Duo MFA.

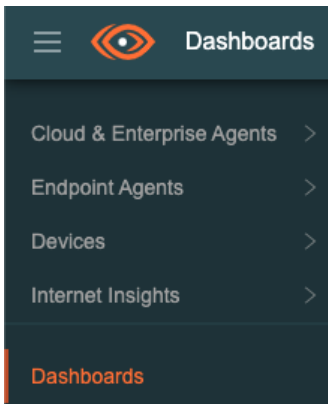


Step 4. In the Duo Dashboard, navigate to **Reports > Authentication Log** and verify an SSO event was logged.

Timestamp (UTC)	Result	User	Application	Access Device	Second Factor
12:16:49 AM AUG 9, 2021	✓ Granted User approved	cvdtest	Microsoft 365 - Single Sign-On	Windows 10 As reported by the browser	Duo Push San Jose, CA, United States

Validation Test #8 - ThousandEyes Observability matches desired outcomes

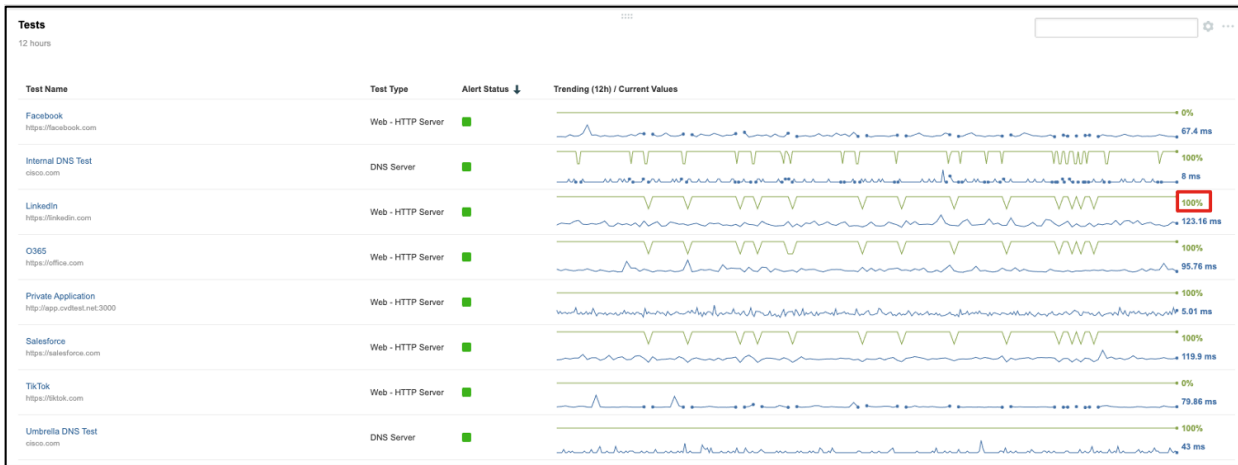
Step 1. In the ThousandEyes dashboard, navigate to **Dashboards**.



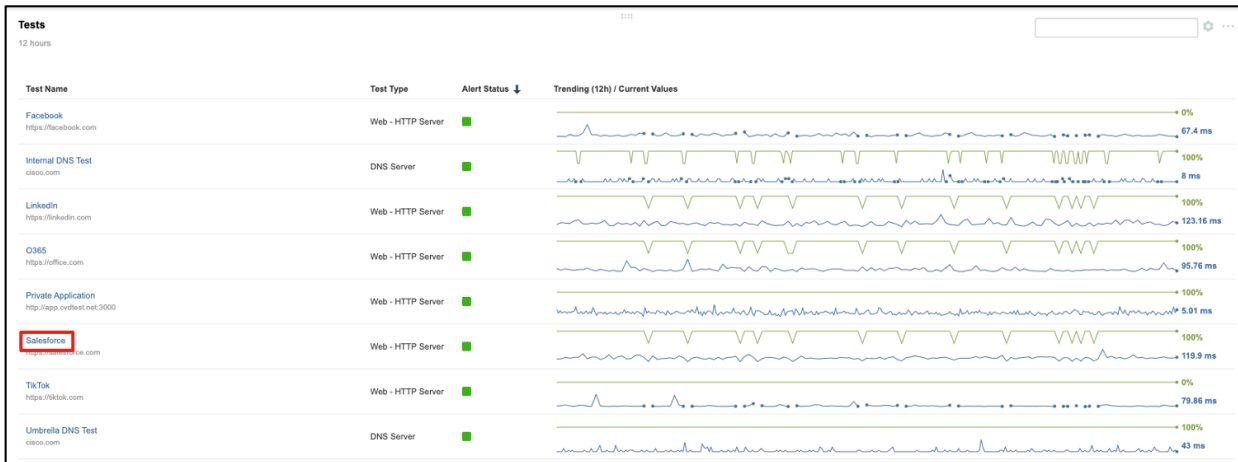
Step 2. Under **Tests**, verify that the blocked websites (**Facebook** and **TikTok**) are running at **0% availability**.



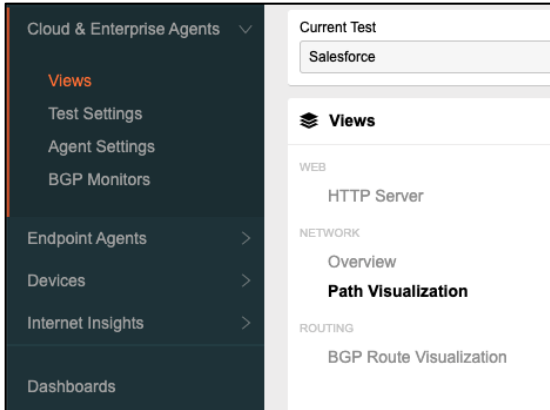
Step 3. Under **Tests**, verify that **LinkedIn** is running closer to **100% availability**.



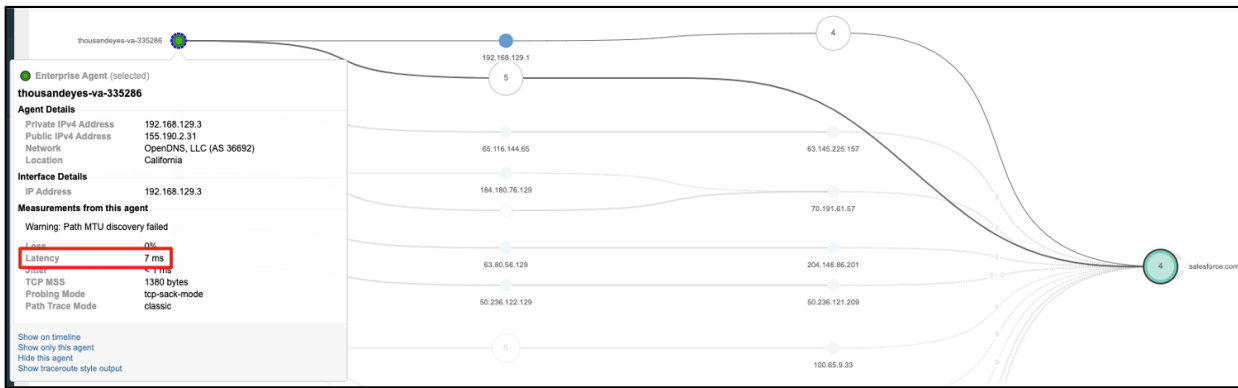
Step 4. Under **Tests**, click **Salesforce**.



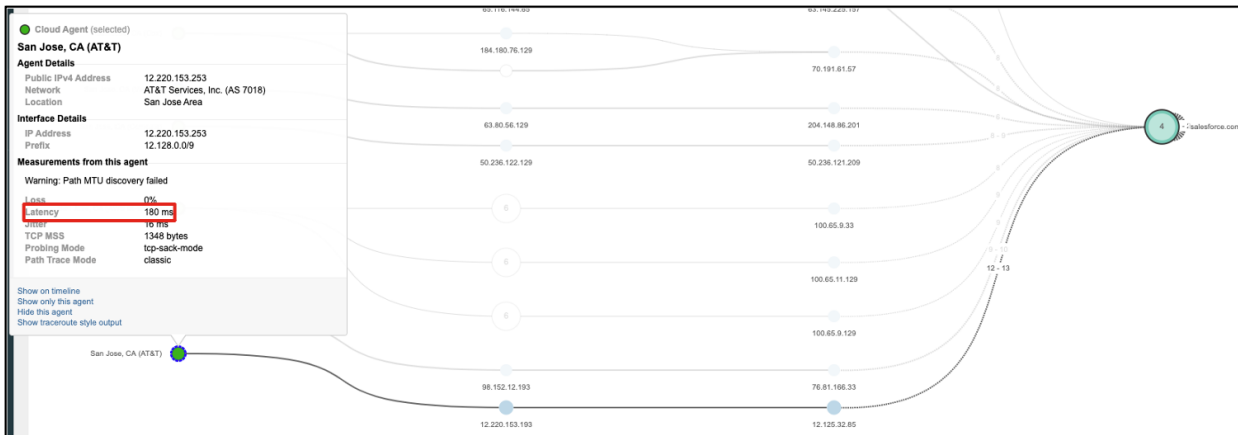
Step 5. Under **Views > Network** click on **Path Visualization**.



Step 6. To check the **latency** through Umbrella, highlight the virtual appliance node. In this case, latency is 7ms.



Step 7. Hover over a cloud agent node and check the **latency**. A Cloud agent in the AT&T network has a 180ms latency to Salesforce.



Branch to Data Center

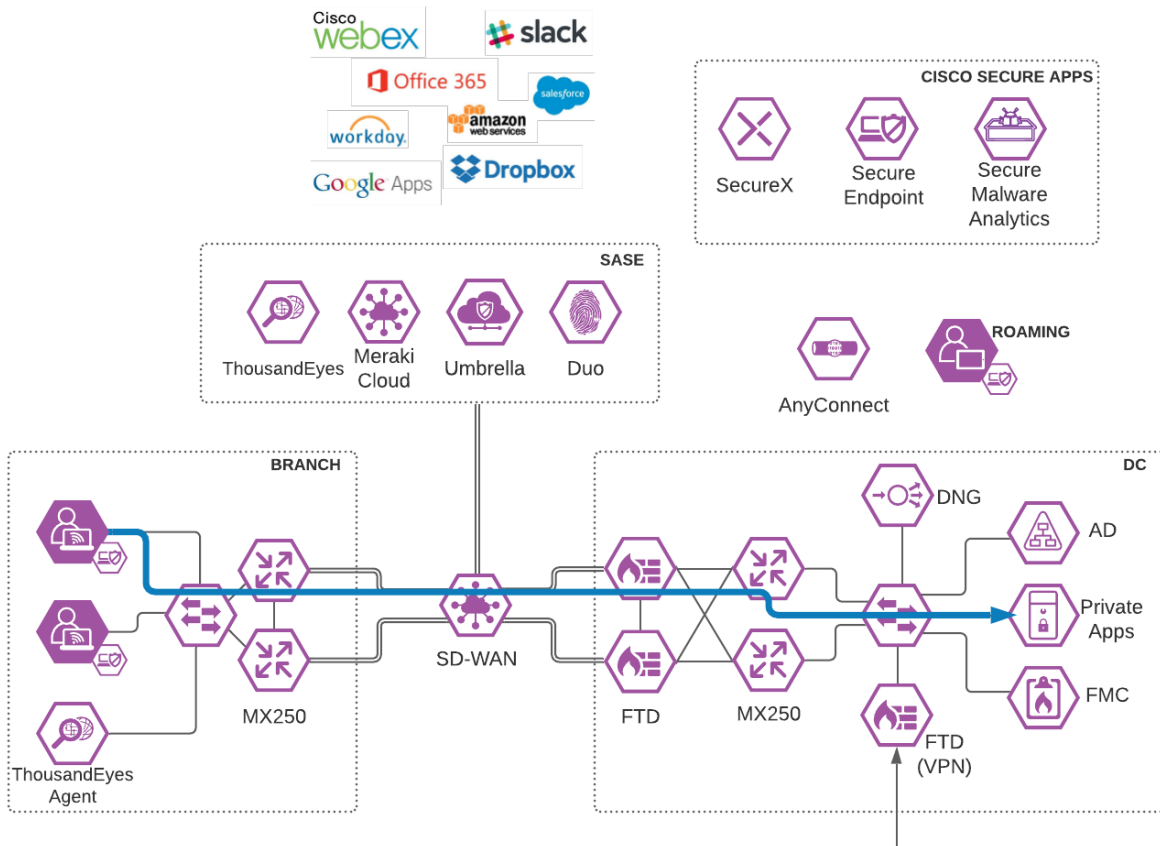
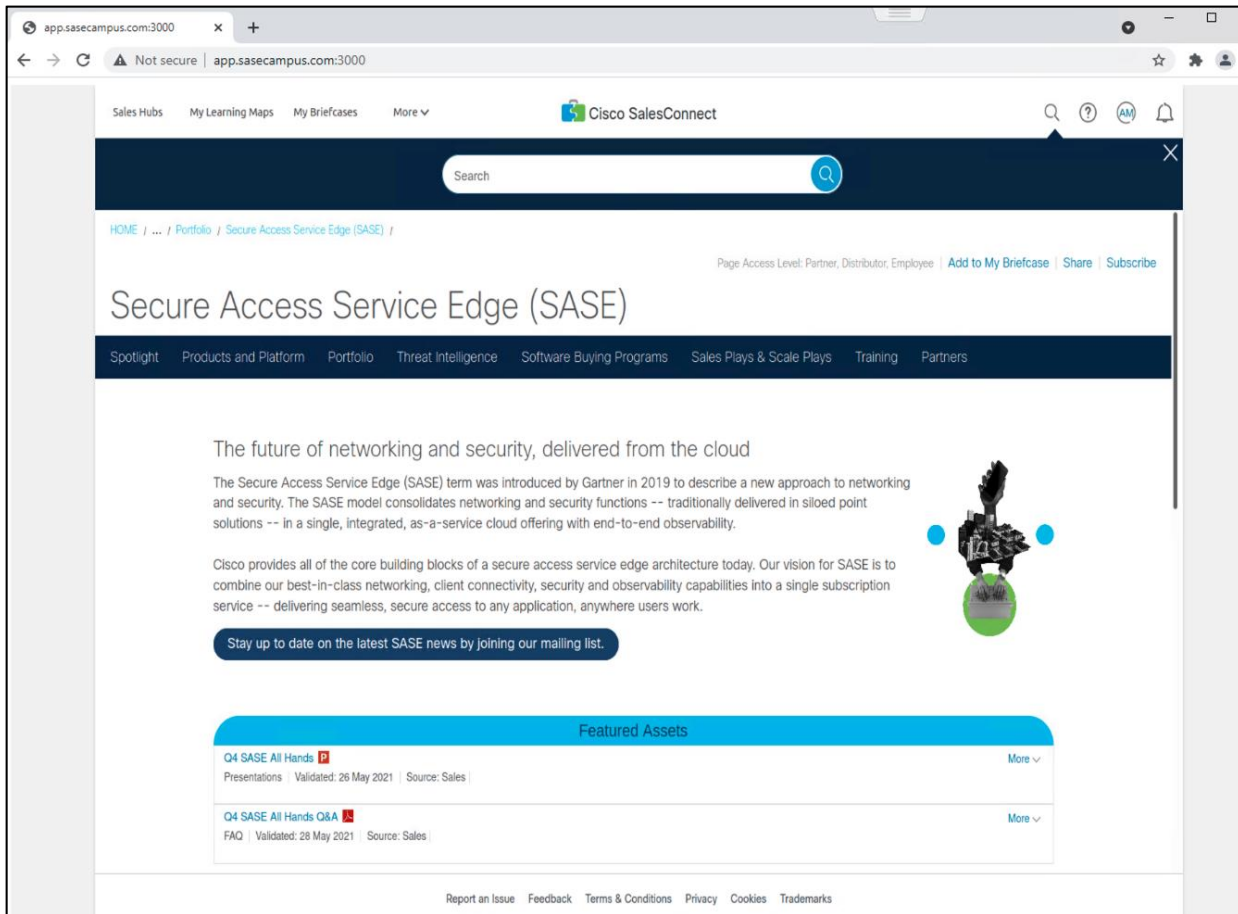


Figure 26.
Branch User to Private Application in Data Center

Validation Test #1 - Private domain access does not flow through Umbrella

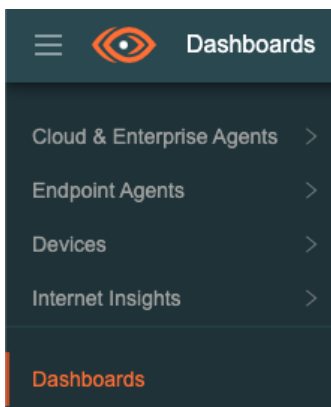
Step 1. Using any browser while on a client in the branch network, navigate to a private application located in the Data Center. Internal traffic should be routed in the Meraki network, and not through Umbrella, where the internal domain would not be resolvable.



Note: This Design Guide is limited in scope, and therefore does not include security that would exist within the Data Center. An assumption has been made that the appropriate protections will be in place within the Data Center to protect private application access from users in the branch network.

Validation Test #2 - ThousandEyes Observability matches desired outcomes

Step 2. In the ThousandEyes dashboard, navigate to **Dashboards**.



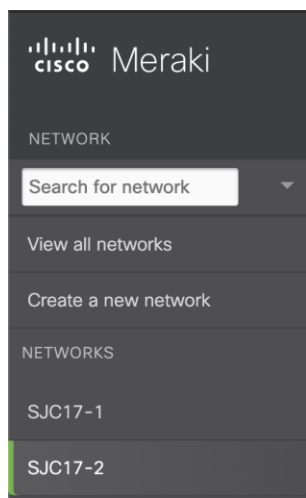
Step 3. Under **Tests**, verify that the private application(s) is running near **100% availability**.



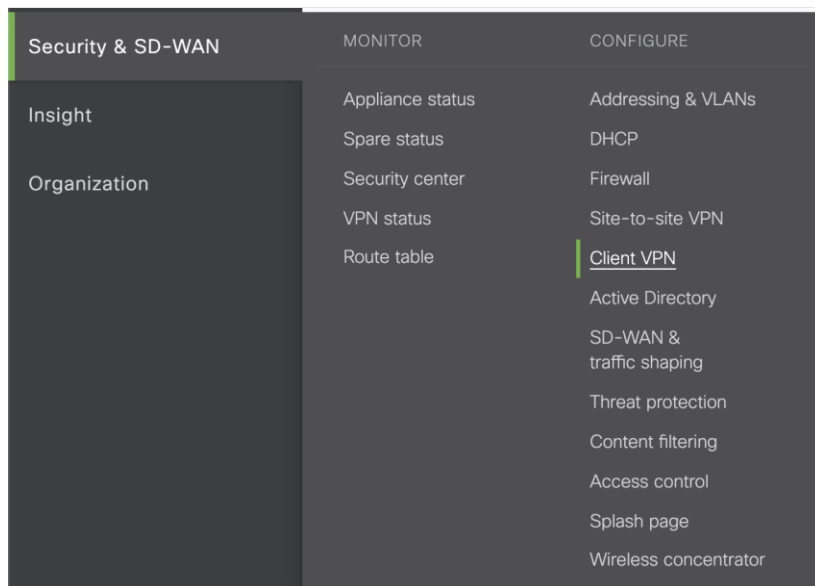
Appendix

Appendix A - Meraki Remote Access VPN

Step 1. In the Meraki Dashboard, navigate to the network in which VPN should be applied.

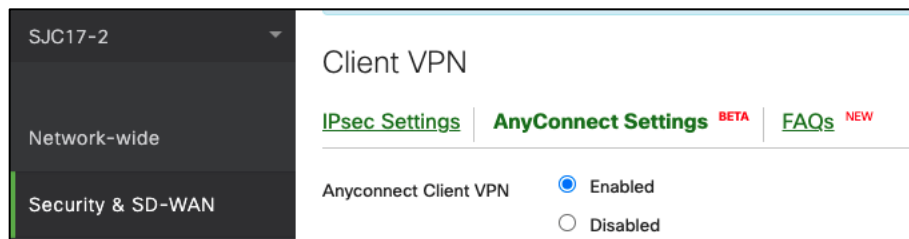


Step 2. Navigate to **Security & SD-WAN > Configure > Client VPN**.



Step 1. Under **Client VPN**, click **AnyConnect Settings**.

Step 2. Next to **Anyconnect Client VPN**, click **Enabled**.



Step 3. In the **Authentication Type** tab, choose **RADIUS** (this will allow us to connect to Duo for MFA).

Step 4. Next to **RADIUS servers**, click **Add a RADIUS server**.

Step 5. Fill in the Duo Authentication Proxy details. See the remote access VPN setup in this design guide for details on how that was done.

Authentication Type	RADIUS		
RADIUS servers	Host	Port	Secret
	192.168.128.4	1812
Add a RADIUS server			

Step 6. In the **RADIUS timeout** box, increase the time to **30 seconds**.

RADIUS timeout ⓘ	30	seconds
------------------	----	---------

Step 7. In the **AnyConnect VPN Subnet** field, choose a subnet that will be assigned upon connectivity.

AnyConnect VPN subnet	192.168.131.0/24
-----------------------	------------------

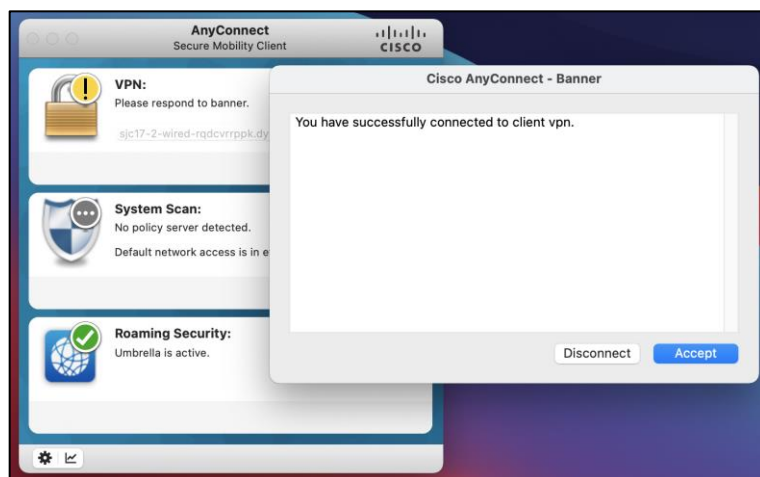
Step 8. In the **DNS nameservers** dropdown menu, choose **Specify nameservers**. Enter the DNS server for your network.

DNS nameservers ⓘ	Specify nameservers... ▼
Custom nameservers	192.168.128.3

Step 9. Click **Save Changes**.

Step 10. In AnyConnect, connect to the **Hostname** that is displayed under **Client Connection Details**.

Step 11. Verify that client connectivity has been reached with Duo MFA protections. For more details on the AnyConnect client and Duo protections, refer back to the body of this document.

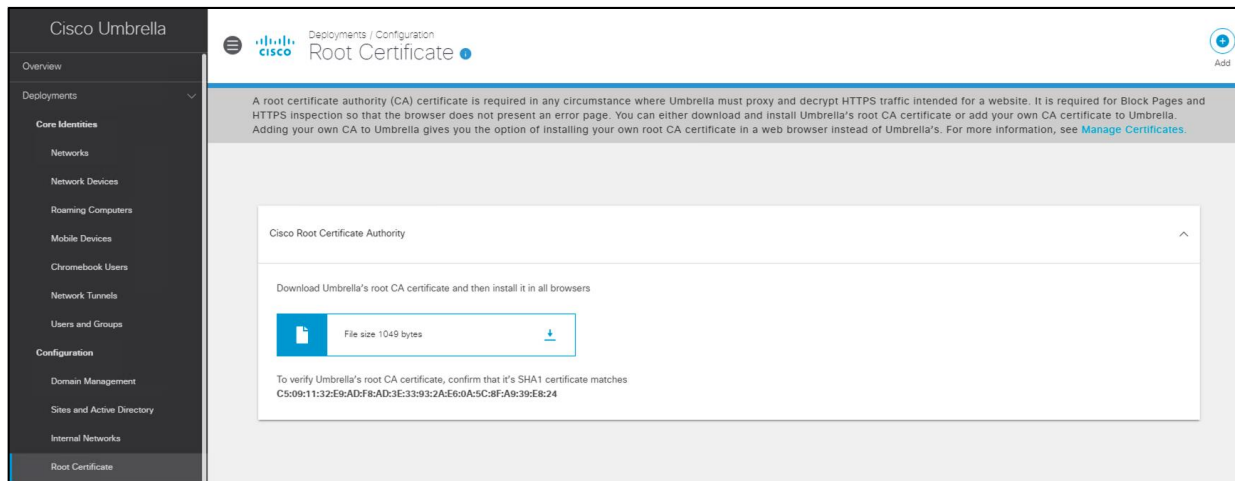


Appendix B - Install the Cisco Umbrella Root Certificate

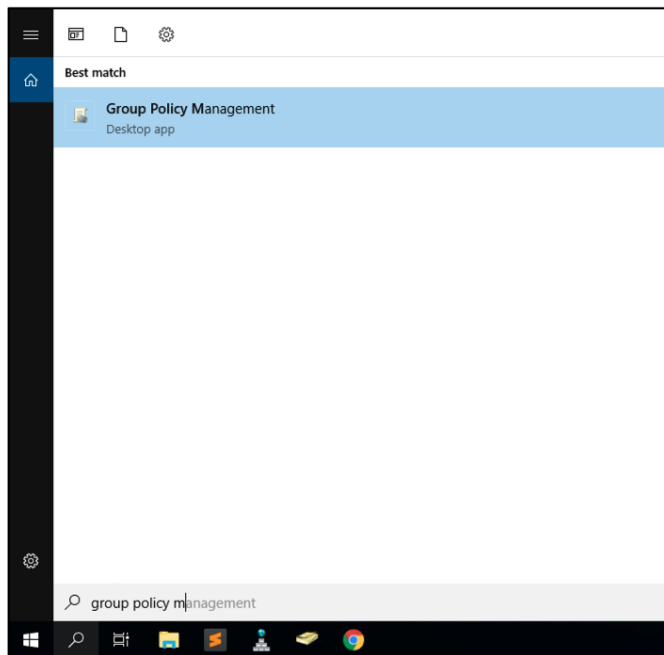
Umbrella's Block Page and Block Page Bypass features present an SSL certificate to browsers that make connections to HTTPS sites. This SSL certificate matches the requested site but will be signed by the Cisco Umbrella certificate authority (CA). If the CA is not trusted by your browser, an error page may be displayed. Typical errors include "The security certificate presented by this website was not issued by a trusted certificate authority" (Internet Explorer), "The site's security certificate is not trusted!" (Google Chrome) or "This Connection is Untrusted" (Mozilla Firefox). Although the error page is expected, the message displayed can be

confusing and you may wish to prevent it from appearing. The example below shows how to install the root certificate to an Active Directory Network. For more examples see [Install Cisco Umbrella Root Certificate](#).

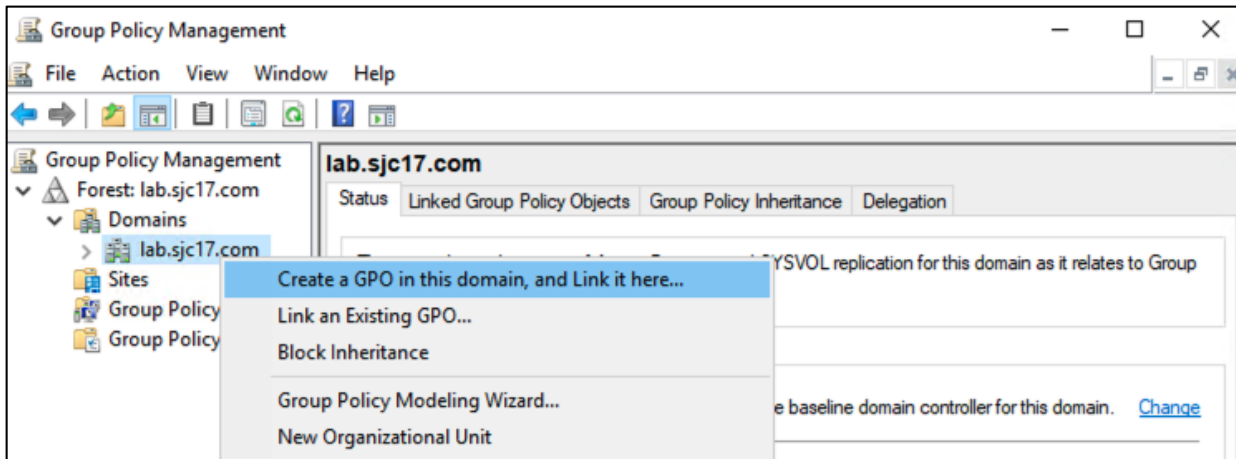
Step 12. In the **Umbrella Dashboard**, navigate to **Deployments > Configuration > Root Certificate** and download the **Cisco Root Certificate Authority**.



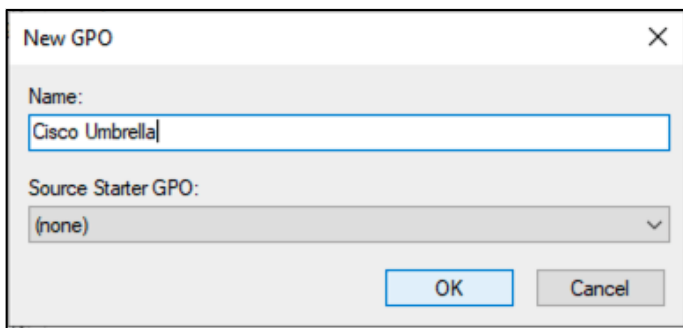
Step 13. In the Active Directory server for your network, open **Group Policy Management**.



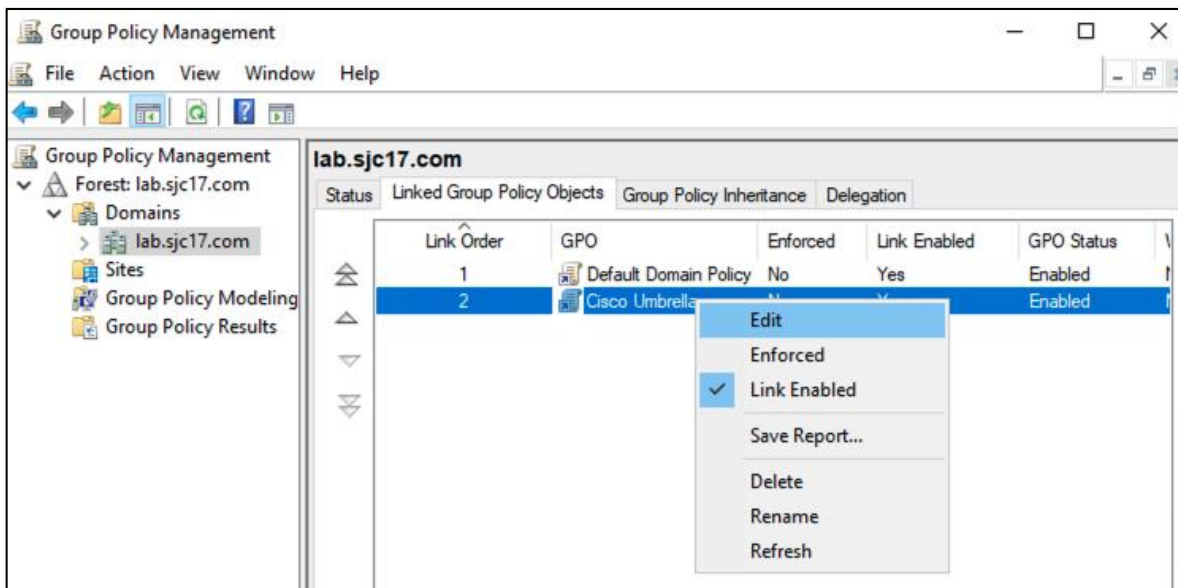
Step 14. Right-click your domain root **Organizational Unit (OU)**, which is displayed as your domain name, and select **Create a GPO in this domain, and Link it here** from the context menu.



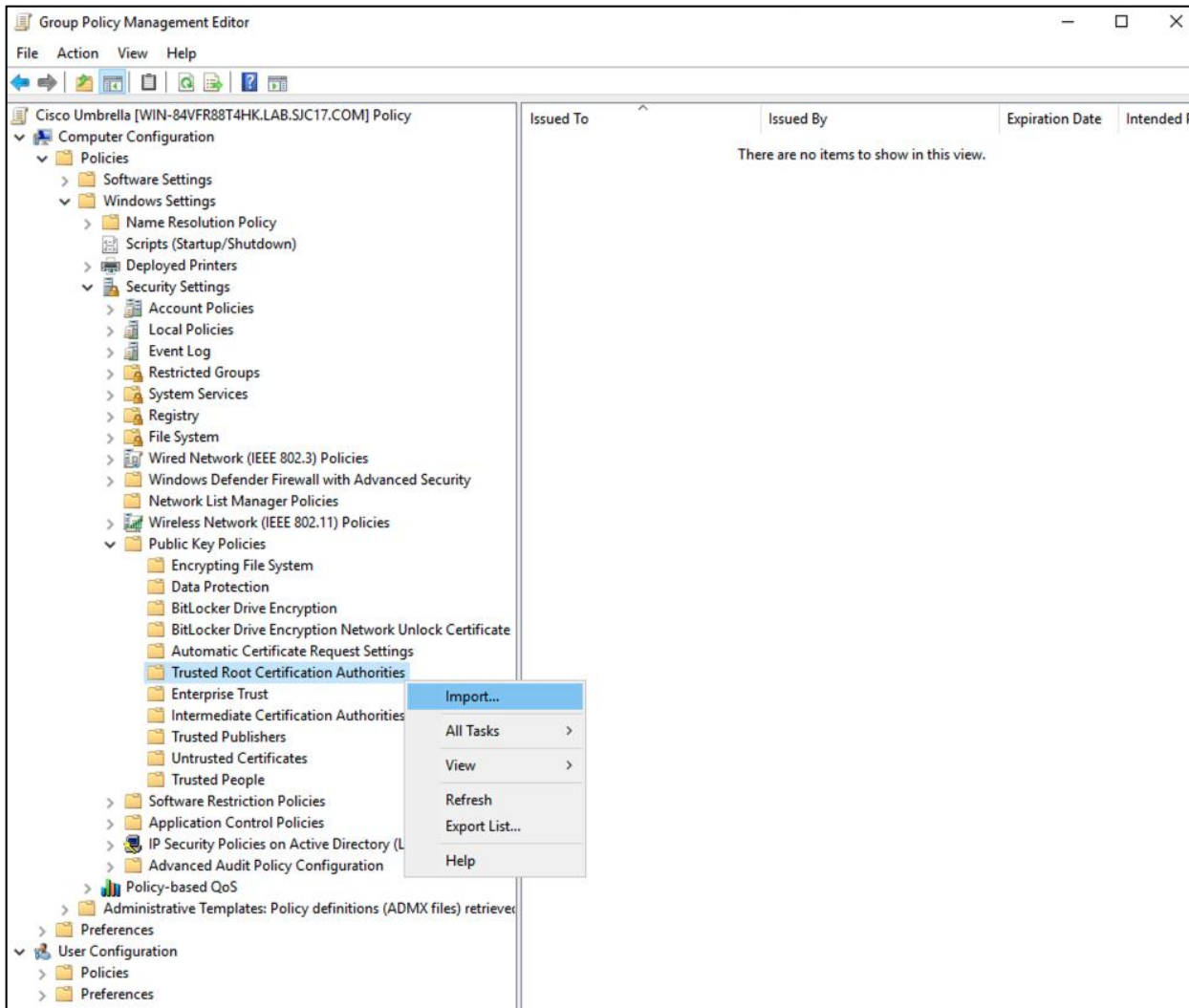
Step 15. In the **Name** field of the **New GPO** dialog box, enter a meaningful name for the policy object.



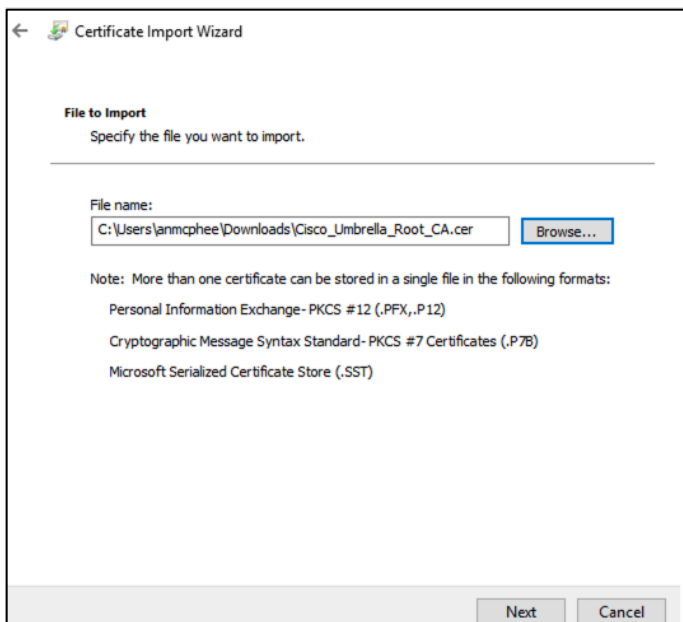
Step 16. Right-click on the new **Group Policy Object** that was created in the previous step and click **Edit**.



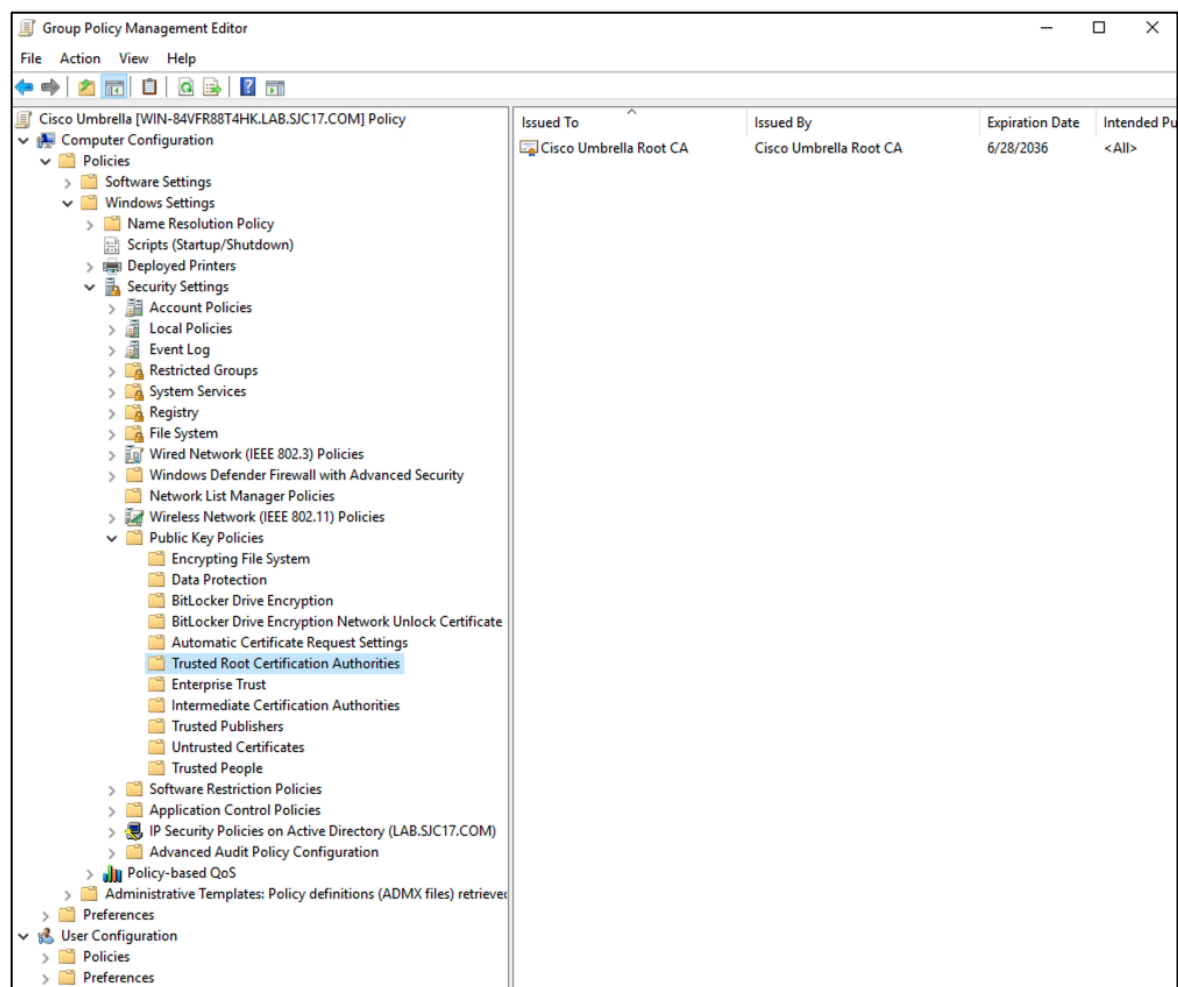
Step 17. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies** and right-click **Trusted Root Certification Authorities**. Click **Import**.



Step 18. In the **Certificate Import Wizard** click **Browse** and add the certificate downloaded from Umbrella in step 1. Click **Next**.



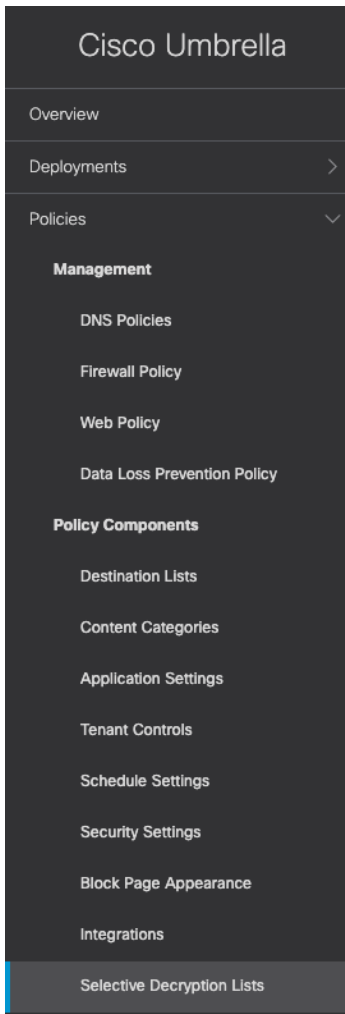
Step 19. Accept all default options until the final windows and click **Finish**.



Appendix C - Umbrella Web Selective Decryption List

For this design guide, Office 365 will be excluded from decryption through Umbrella. There are several known compatibility issues with Office 365 and web proxies, and exempting Office 365 traffic authentication and decryption can help with some of these issues.

Step 1. In the Umbrella Dashboard, navigate to **Policies > Policy Components > Selective Decryption Lists**.



Step 2. Click **Add**.



Step 3. Give a meaningful **List Name** to the decryption list.

Step 4. Beside **Applications Selected**, click **Add**.

List Name

SASE Design Guide

0 Categories Selected **ADD**

0 Applications Selected **ADD**

0 Domains **ADD**

No Categories Selected

No Applications Selected

No Domains

DELETE **CANCEL** **SAVE**

Step 5. Search for **Office 365** and click the checkbox to enable. Click **Close**.

List Name

SASE Design Guide

0 Categories Selected **ADD**

1 Applications Selected **ADD**

Office 365

APPLICATIONS **REMOVE ALL**

Office 365

Office 365

CLOSE

No Categories Selected

Step 6. Click **Save**.

To add more content that should bypass decryption, continue to add to this list using either a content category, application, or domain.

Appendix D - Acronyms Defined

AMP - Advanced Malware Protection

ASA - Adaptive Security Appliance

ASDM - Adaptive Security Device Manager

CA - Certificate Authority

CASB - Cloud Access Security Broker

CDFW - Cloud Delivered Firewall

DIA - Direct Internet Access

DLP - Data Loss Prevention

DNG – Duo Network Gateway

DNS – Domain Name System

FMC – Firepower Management Center

FTD – Firepower Threat Defense

IoC – Indicator of Compromise

IPS – Intrusion Prevention System

MFA – Multi-factor Authentication

MPLS – Multiprotocol Label Switching

OU – Organizational Unit

P2P – Peer-to-Peer

PHI – Personal Health Information

PII – Personally Identifiable Information

RBI – Remote Browser Isolation

SaaS – Software as a Service

SASE – Secure Access Service Edge

SD-WAN – Software Defined Wide Area Network

SSL – Secure Sockets Layer

SSO – Single Sign-On

SWG – Secure Web Gateway

VPN – Virtual Private Network

Appendix E – References

- **Cisco Breach Defense Design Guide:**
<https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/breach-defense-design-guide.html>
- **Cisco SAFE:**
https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_safe.html
- **Cisco SASE:**
<https://www.cisco.com/site/us/en/solutions/secure-access-service-edge-sase/index.html>
- **Cisco SD-WAN powered by Meraki:**
<https://meraki.cisco.com/sdwhat/en>
- **Cisco Secure Access by Duo:**
<https://duo.com/>
- **Cisco ThousandEyes User Documentation:**
<https://docs.thousandeyes.com/>

-
- **Cisco Umbrella:**
<https://umbrella.cisco.com/>
 - **Cisco Umbrella User Documentation:**
<https://docs.umbrella.com/>
 - **SASE for Dummies:**
<https://umbrella.cisco.com/info/secure-access-service-edge-sase-for-dummies-ebook>

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)