Trusted Internet Connections (TIC) 3.0

Design Guide

April, 2021

Contents

Overview

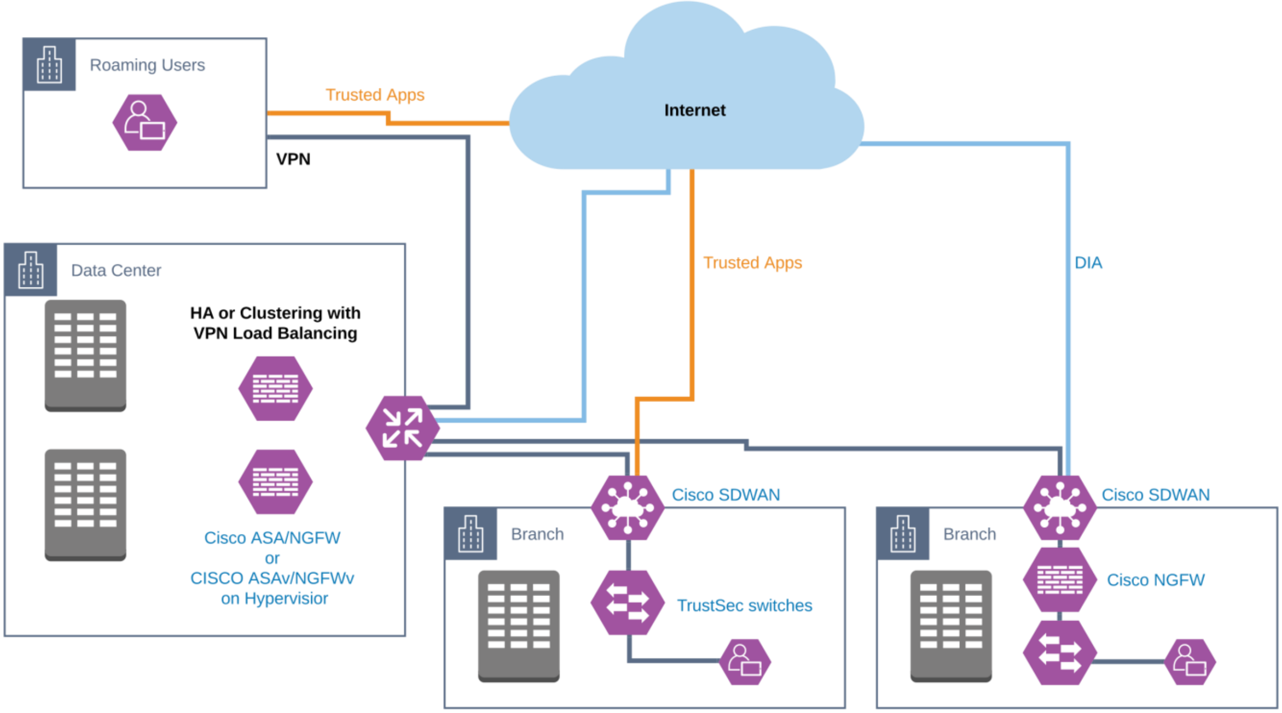


Figure 1.
TIC 3.0 architecture

Cisco's security approach for TIC 3.0 is not only designed to fulfill the requirements of distributed PEPs in the agency network but is also designed to fit with the relationships between TIC and other federal initiatives such as Continuous Diagnostics and Mitigations (CDM) and the National Institute of Standards and Technology (NIST) Zero trust Architecture. Zero Trust is a security model that shifts the access conversation from traditional perimeter-based security and instead focuses on secure access to applications based on user identity, the trustworthiness of their device and the security policies you set, as opposed to the network from where access originates. Zero Trust models assume that an attacker is present on the network and that an enterprise-owned network infrastructure is no different. Zero Trust Architecture (ZTA) focuses on three elements in the network, regardless of their location, securing the workforce, securing the workplace, and securing the workloads.

The guiding principles of ZTA resonate with the Universal capabilities outlined by TIC. For example:

- Developing, documenting, and maintaining a current inventory of all systems, networks, and components so that only authorized devices are given access.
- Least privilege for each entity on the network.
- Verifying the identity of users. Devices, or other entities through rigorous means such as MFA before granting access.
- Constantly monitoring the network for vulnerabilities and staying up to date with the latest and greatest Threat Intelligence.

TIC 3.0 offers agencies the freedom to implement a more flexible TIC model. It is common for agencies to utilize cloud services and accommodate remote workers' need access to all agency resources. These changes also impact the attack surface of the Federal Government. Instead of a singular location for policy enforcement, TIC 3.0 allows for distributing enforcement to different locations along the path if the deployed protections maintain a commensurate level of protection based on the agency's risk tolerance. This document is an extension to the TIC 3.0 Architecture Guide and will detail deployment steps for securing remote users and branch offices as per the guidance shown in that document.

Design Guide

Software Version used in this guide

Location	Product	Version
Data Center	vManage	20.3.1
Data Center	vSmart	20.3.1
Data Center	vBond	20.3.1
Data Center	Firepower Management Center (FMC)	6.6
Data Center	Splunk Enterprise	8.1.0
Data Center	CESA	3.7.1
Data Center	Cisco NVM Flow collector	3.7.1
Data Center	Cisco AnyConnect profile editor(s)	4.8
Branch	ISR4461	IOS-XE 17.2
Branch	FTD 1010	6.6
Cloud	Duo	
Cloud	AMP & ThreatGrid	
Cloud	Cloudlock	
Endpoint	AnyConnect Secure Mobility Client	4.9

Branch

In this deployment a private SD-WAN environment consisting of vManage, vBond, vSmart and a single ISR-4461 were used following the procedure in the Cisco SD-WAN End-to-End Deployment Guide.

Direct Cloud Access (DCA)

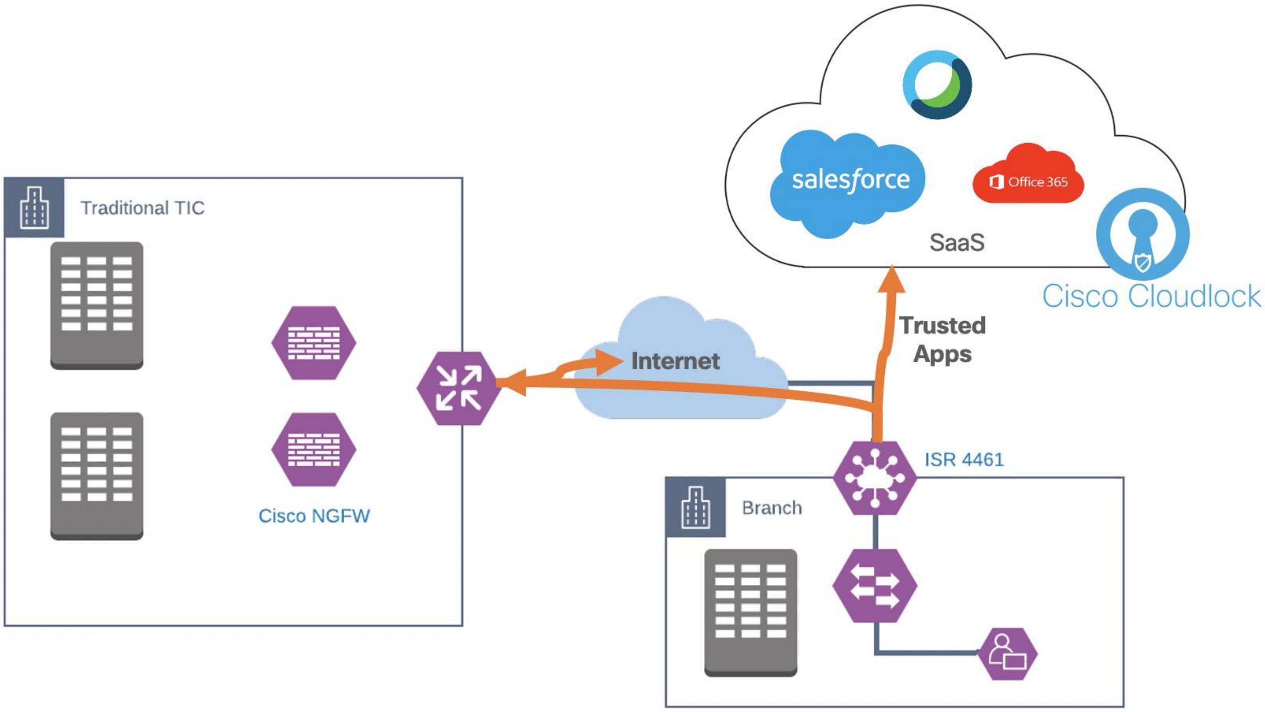


Figure 2.
Enabling DCA in Cisco SD-WAN

This guide offers two options for Branch security. The first option is to enable DCA with the native firewall of a Cisco IOS XE SD-WAN device sitting at the edge of the branch. The firewall capabilities in the Cisco IOS XE SD-WAN can apply enforcement up to and including layer 7 (applications) and is managed using the same vManage dashboard that was used to create the SD-WAN overlay. For more details on this deployment see Cisco SD-WAN: Enabling Direct Internet Access.

Pre-requisites

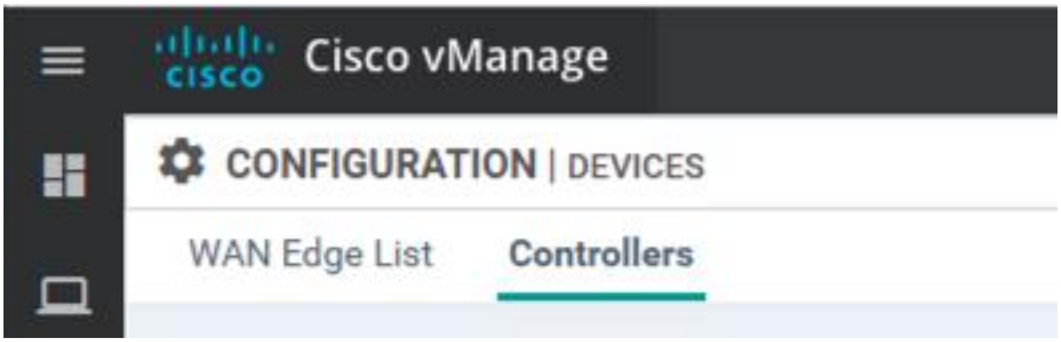
- The SD-WAN controllers are set up and deployed (vManage, vBond, vSmart)
- A router has been configured using device templates in order to establish a functional and secure overlay fabric to pass data traffic across the organizations distributed sites. An SD-WAN Deployment guide can be found here.
- Upload a Security Virtual Image to vManage. For an installation guide see Security Virtual Image.

Application Routing

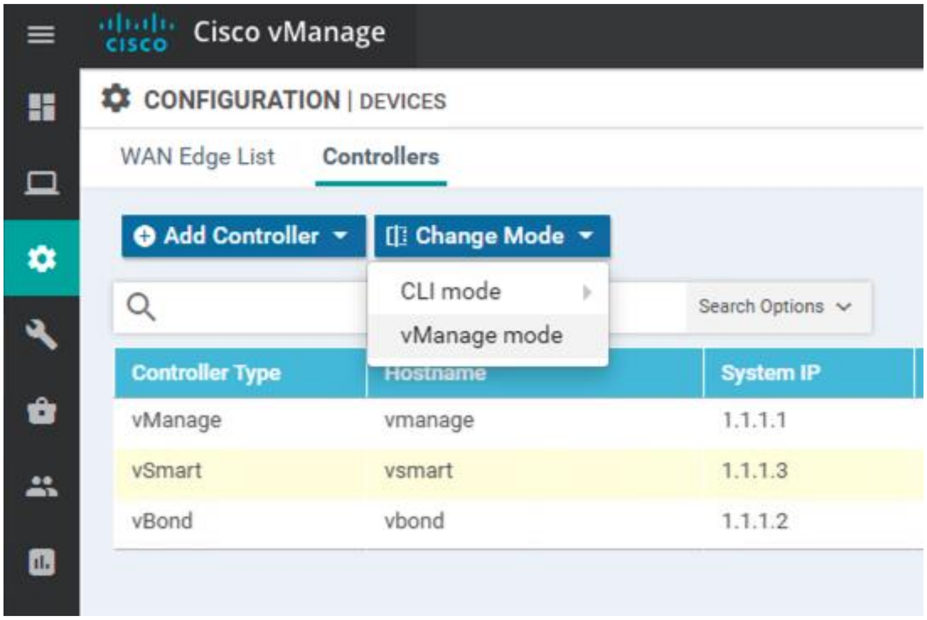
Application routing in the Cisco SD-WAN platform can be achieved using a couple of different methods. For simplicity, and since this guide mainly focuses on security, applications will be configured to always take the direct path. The alternate method is to configure Application-Aware routes which choose the optimum path based on the Service Level Agreement (SLA) of each route. For more information see Cisco SD-WAN: Application-Aware Routing Deployment Guide.

Procedure 1. Verify the SD-WAN vSmart controller is in vManage mode.

Step 1. In vManage, navigate to **Configuration > Devices** and select **Controllers**. If controller is in vManage mode, continue to the next procedure, otherwise continue to follow the steps.

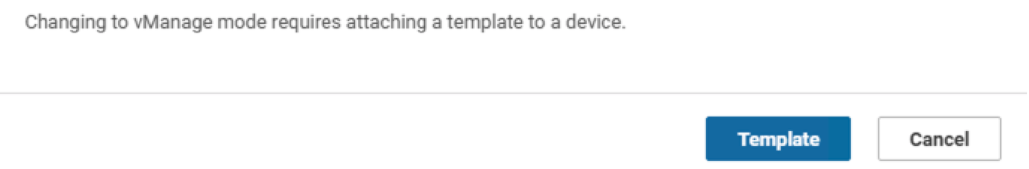


Step 2. If the vSmart is in CLI mode, a device template must be configured and attached to vSmart. Highlight vSmart and click on **Change Mode > vManage mode**.

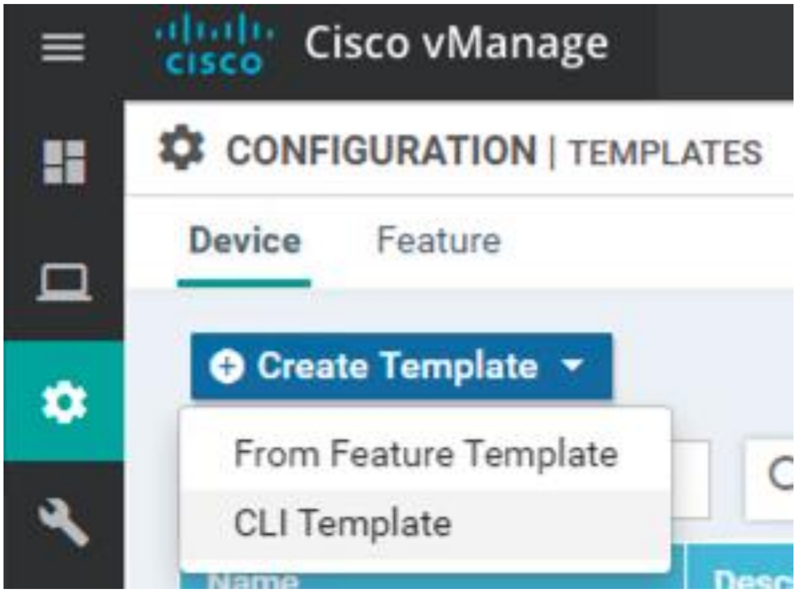


Controller Type	Hostname	System IP
vManage	vmanage	1.1.1.1
vSmart	vsmart	1.1.1.3
vBond	vbond	1.1.1.2

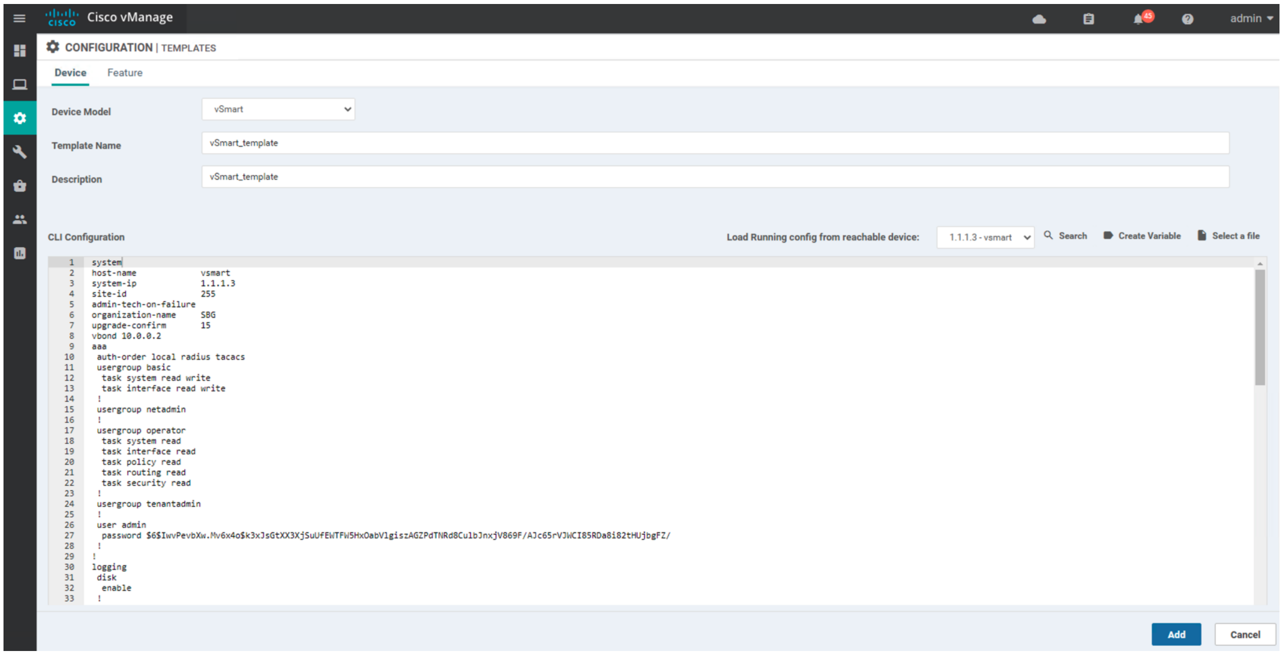
Step 3. Click Template.


Changing to vManage mode requires attaching a template to a device.

Step 4. Click **Create Template > CLI Template**.



Step 5. In the **Device Model** dropdown, choose **vSmart**. Add a meaningful name to the Template Name and Description. In the **Load Running config from reachable device dropdown**, choose the vSmart device. This loads the current CLI configuration from the device.



Device Model: vSmart

Template Name: vSmart_template

Description: vSmart_template

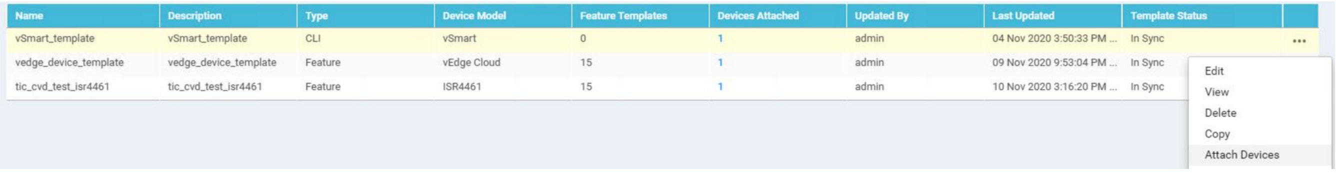
CLI Configuration

Load Running config from reachable device: 1.1.1.3 - vsmart

```
system
host-name             vsmart
system-ip             1.1.1.3
site-id               255
admin-tech-on-failure
organization-name     SBG
upgrade-confirm       15
vbond 10.0.0.2
aaa
 auth-order local radius tacacs
 usergroup basic
  task system read write
  task interface read write
 !
 usergroup netadmin
 !
 usergroup operator
  task system read
  task interface read
  task policy read
  task routing read
  task security read
 !
 usergroup tenantadmin
 !
 user admin
  password $6$IwvPevbXw.Mv6x4o$k3xJsGtXX3XjSuUfEWTFW5HxOabVlgiszAGZPdTNRd8CulbJnxjV869F/AJc65rVJWCI85RDa8i82tHUjbgFZ/
 !
!
logging
 disk
  enable
 !
```

Step 6. Click **Add**.

Step 7. On the newly created vSmart device template, click the **ellipses** and choose **Attach Devices**.

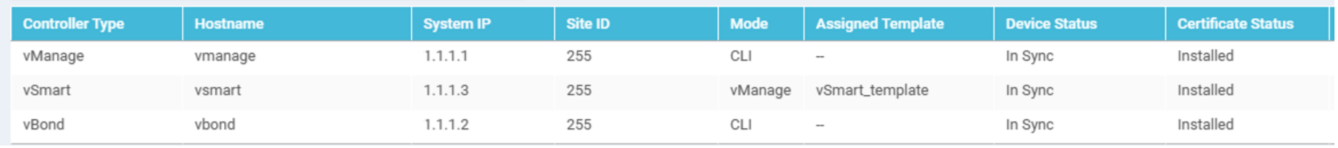


Name	Description	Type	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template Status	
vSmart_template	vSmart_template	CLI	vSmart	0	1	admin	04 Nov 2020 3:50:33 PM ...	In Sync	...
vedge_device_template	vedge_device_template	Feature	vEdge Cloud	15	1	admin	09 Nov 2020 9:53:04 PM ...	In Sync	
tic_cvd_test_isr4461	tic_cvd_test_isr4461	Feature	ISR4461	15	1	admin	10 Nov 2020 3:16:20 PM ...	In Sync	

Step 8. Choose the vSmart device and click **Attach**.

Step 9. Click on the vSmart device on the left-hand panel, double check the configuration and click **Configure Devices**.

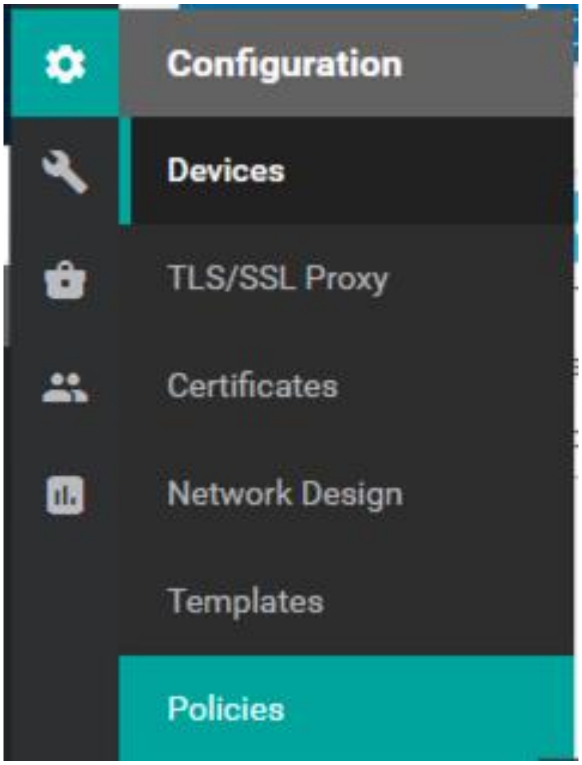
Step 10. Once complete, navigate back to **Configuration > Devices** and select **Controllers.** The device will now be in vManage mode.



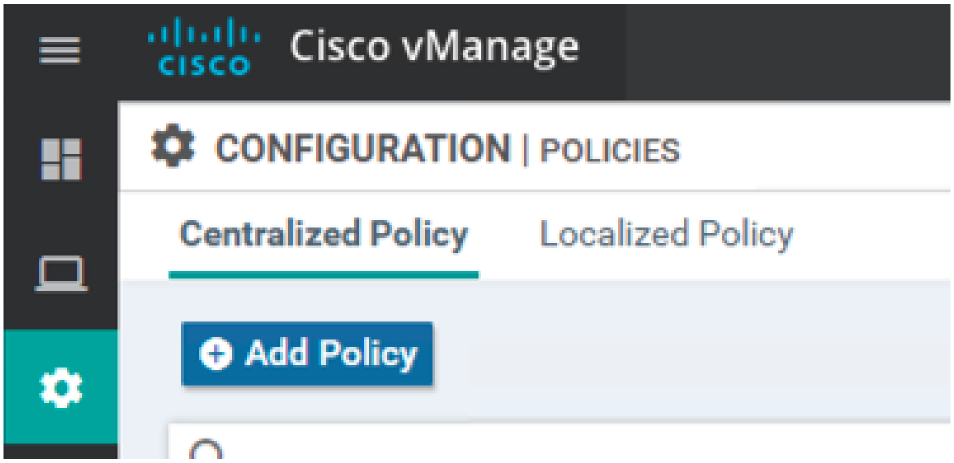
Controller Type	Hostname	System IP	Site ID	Mode	Assigned Template	Device Status	Certificate Status
vManage	vmanage	1.1.1.1	255	CLI	--	In Sync	Installed
vSmart	vsmart	1.1.1.3	255	vManage	vSmart_template	In Sync	Installed
vBond	vbond	1.1.1.2	255	CLI	--	In Sync	Installed

Procedure 2. Configuring the Routing policy

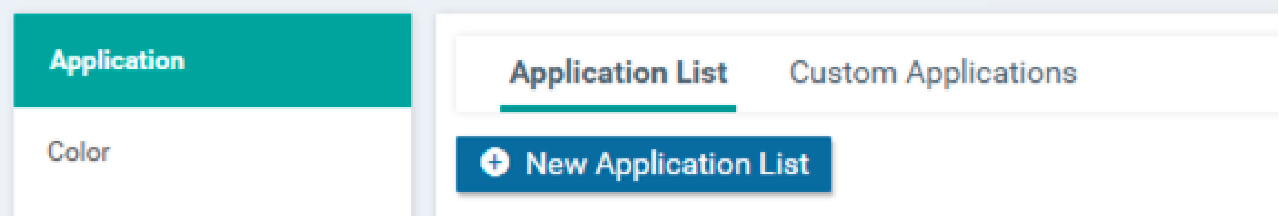
Step 1. In vManage, navigate to **Configuration > Policies.**



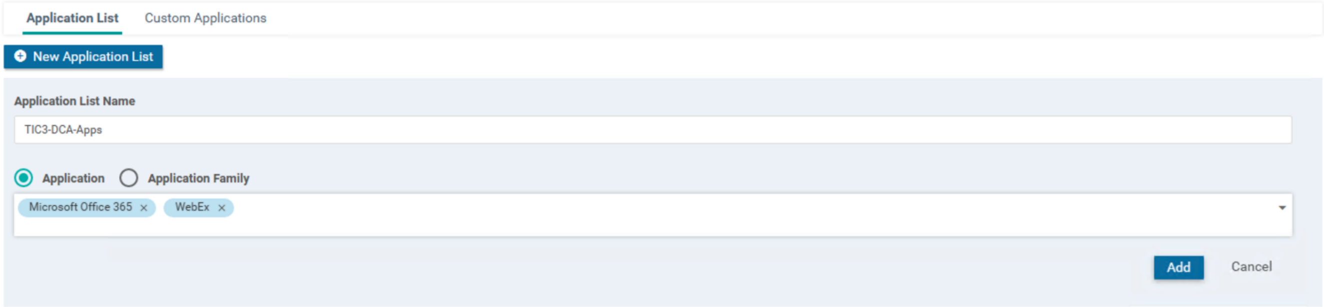
Step 2. Under **Centralized Policy**, click + **Add Policy.**



Step 3. The first task is to create an application list that your agency would like to break from the tunnel. This example will show Office365 and WebEx. In the **Application** tab, click **+ New Application List**.



Step 4. Give a meaningful **name** to the policy and with the **Application** radio button selected, search and click **Microsoft Office 365** and **WebEx**. Click **Add**.



Application List Name

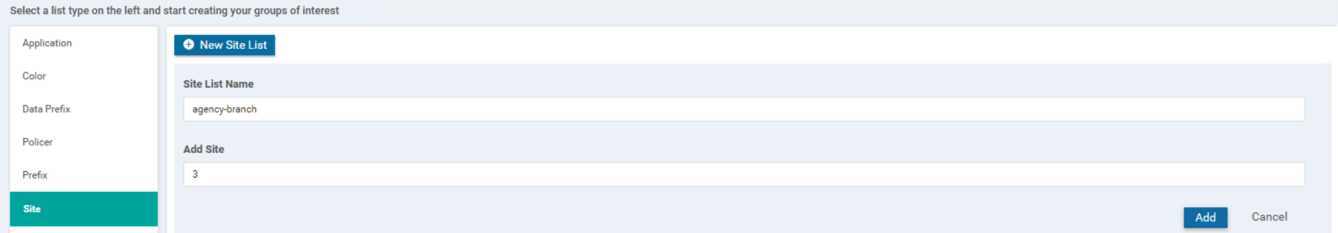
TIC3-DCA-Apps

● Application ○ Application Family

Microsoft Office 365 × WebEx ×

Step 5. In the **Site** tab, click **+ New Site List**.

Step 6. This is where we define which sites this policy will apply to. Add a meaningful **name** to the site list and add all **site id's** that this DCA policy will apply to. This example used only a single branch so only a single site was added. When all sites have been added, click **Add**.


Select a list type on the left and start creating your groups of interest

Site List Name

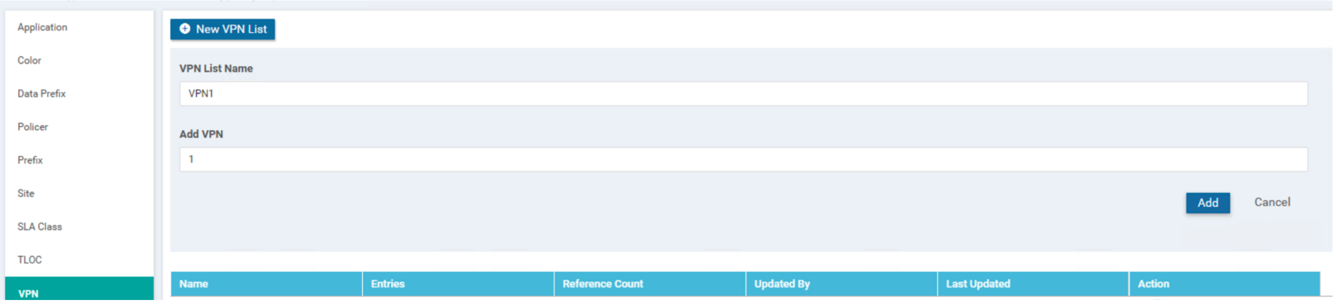
agency-branch

Add Site

3

Step 7. In the **VPN** tab, click **+ New VPN List**.

Step 8. Give a meaningful **name** to the VPN list and all **VPNs** that this rule applies to. Click **Add**.



VPN List Name

VPN1

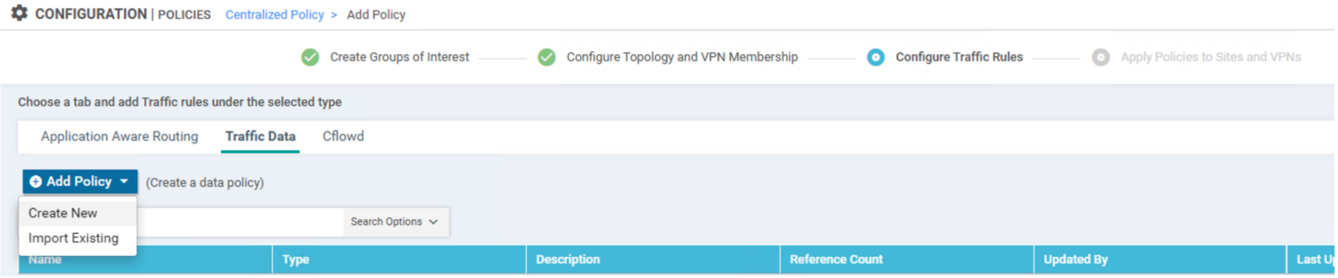
Add VPN

1

Name	Entries	Reference Count	Updated By	Last Updated	Action

Step 9. Click **Next** until you get to the **Configure Traffic Rules** tab.

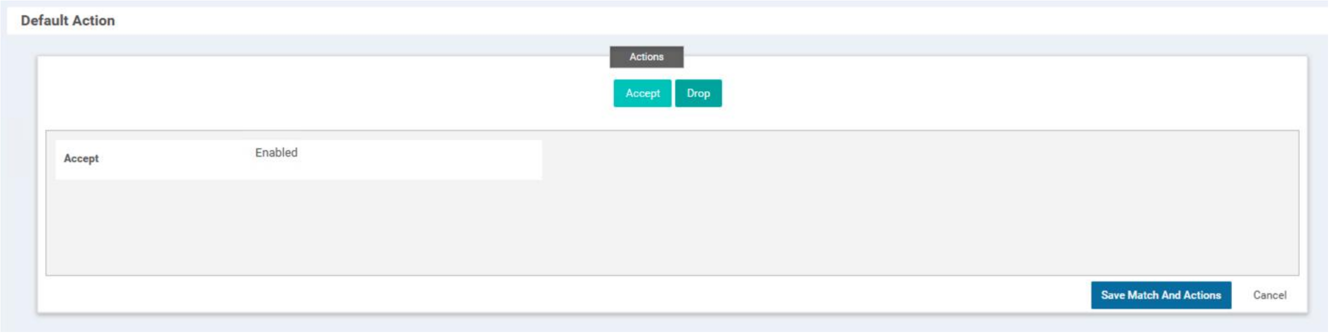
Step 10. In the **Traffic Data** tab, click **+ Add Policy > Create New**.



Choose a tab and add Traffic rules under the selected type

Step 11. Add a **Name** and **Description**.

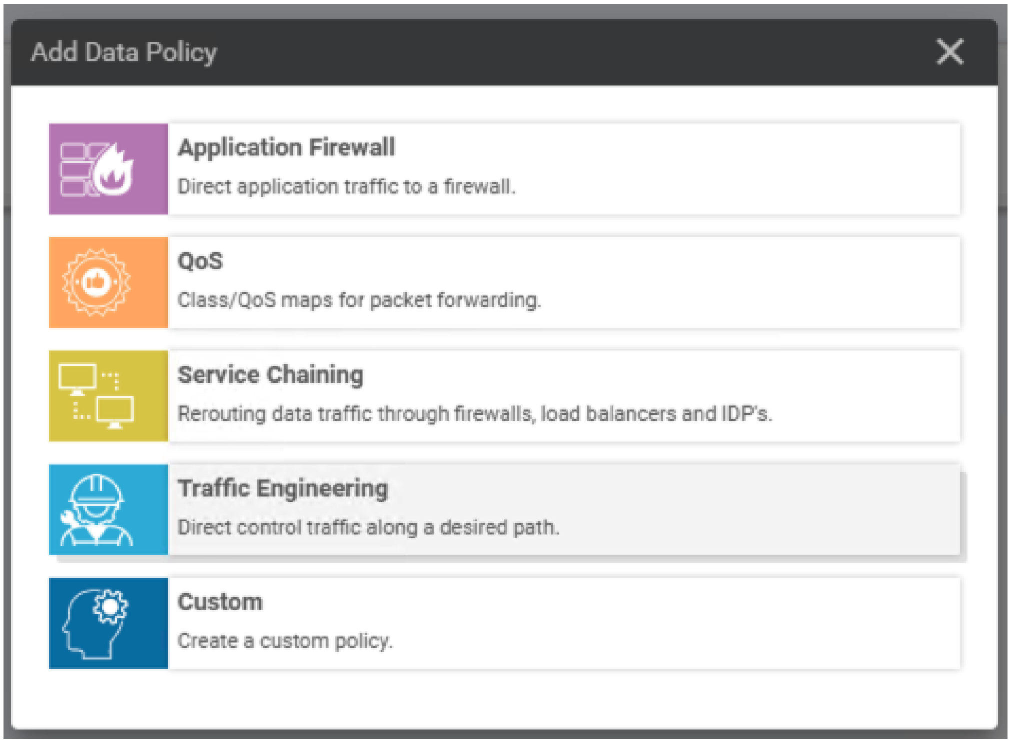
Step 12. By default, all traffic is dropped. To change this, click the **pencil icon** and click **Accept**. Click **Save Match and Actions.** In this example, default routes were learned through BGP and therefore accepting all traffic in this policy will send traffic to these default routes. An alternate approach to BGP would be to configure the default routes in this policy and to re-order the application routes accordingly.



Accept	Enabled

Step 13. Click **+ Sequence Type**.

Step 14. Choose **Traffic Engineering**.



Add Data Policy

Application Firewall
Direct application traffic to a firewall.

QoS
Class/QoS maps for packet forwarding.

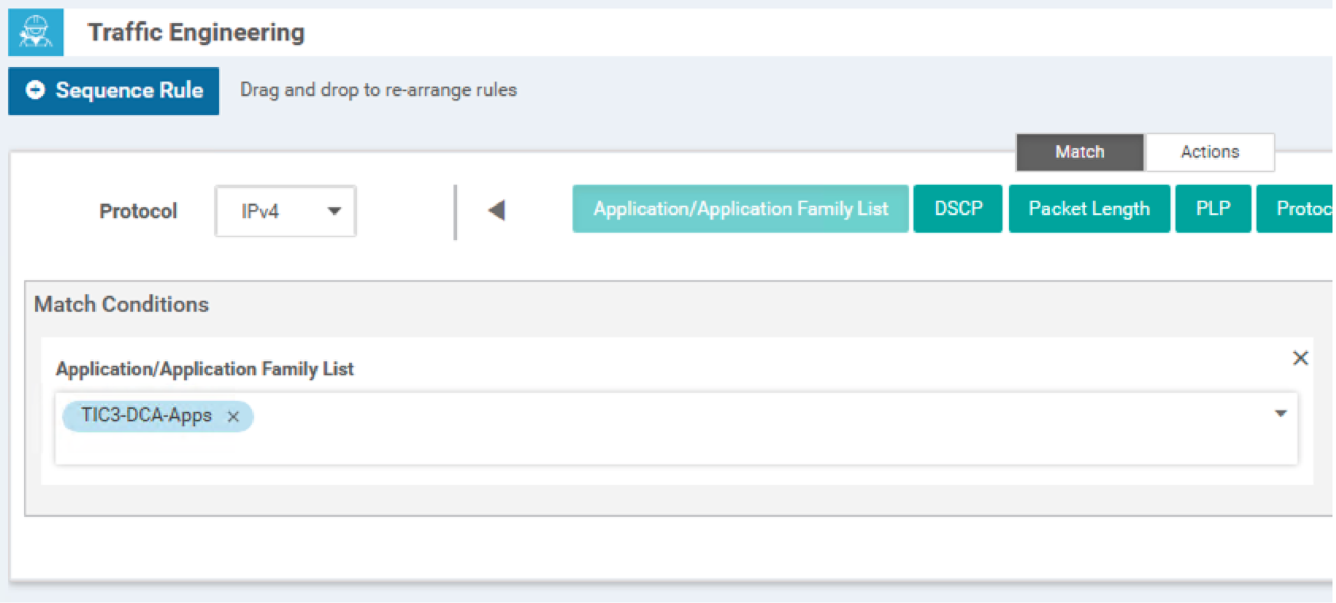
Service Chaining
Rerouting data traffic through firewalls, load balancers and IDP's.

Traffic Engineering
Direct control traffic along a desired path.

Custom
Create a custom policy.

Step 15. Click **+ Sequence Rule**.

Step 16. In the **Match** tab, click **Application/Application Family List** and choose the application list previously created.



Traffic Engineering

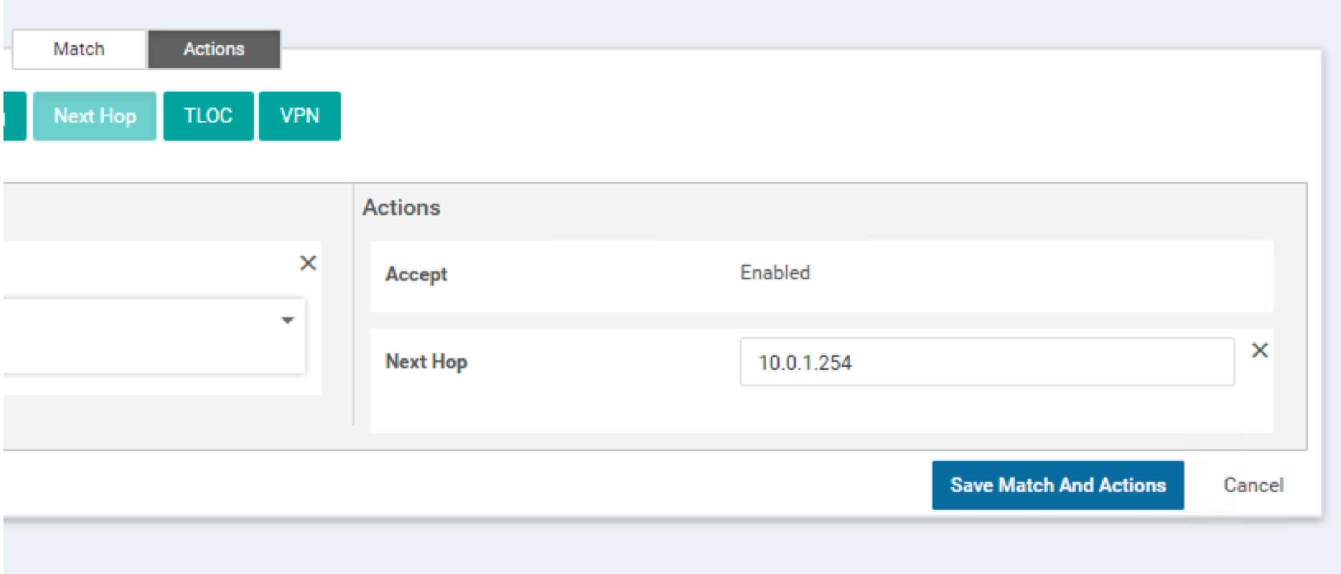
Sequence Rule
Drag and drop to re-arrange rules
Match
Actions
Application/Application Family List
DSCP
Packet Length
PLP
Protoc

Protocol: IPv4

Match Conditions

Application/Application Family List: TIC3-DCA-Apps

Step 17. For this example, a static route was used to directly connect to the cloud. For more routing options, such as using a TLOC, see [Cisco SD-WAN Design Guide](). In the **Actions** tab, click **Next Hop** and provide the next hop route for direct cloud connectivity. Click **Save Match and Actions**.



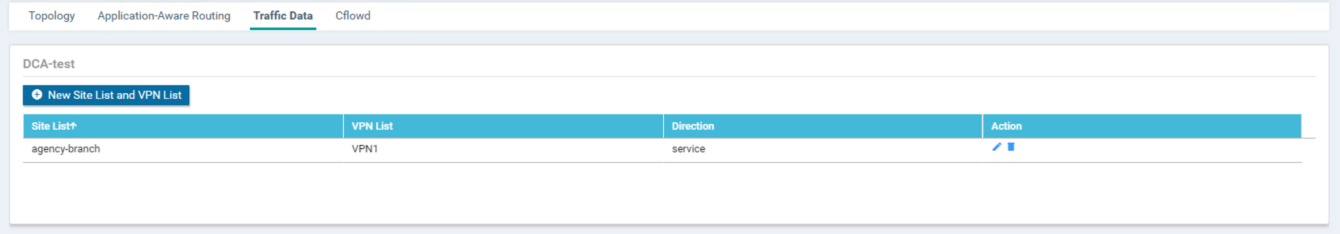
Accept	Enabled
Next Hop	10.0.1.254

Step 18. Click **Save Data Policy**.

Step 19. Click **Next**.

Step 20. Provide a **Policy Name** and **Policy Description**.

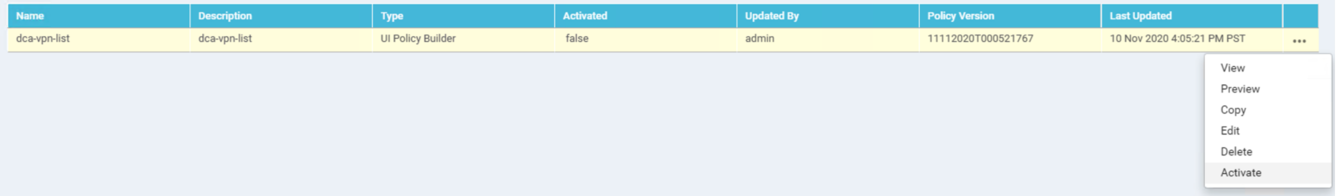
Step 21. In the **Traffic Data** tab, click **+ New Site List** and VPN List and add the previously created **Site List** and **VPN List**.



Site List↑	VPN List	Direction	Action
agency-branch	VPN1	service	

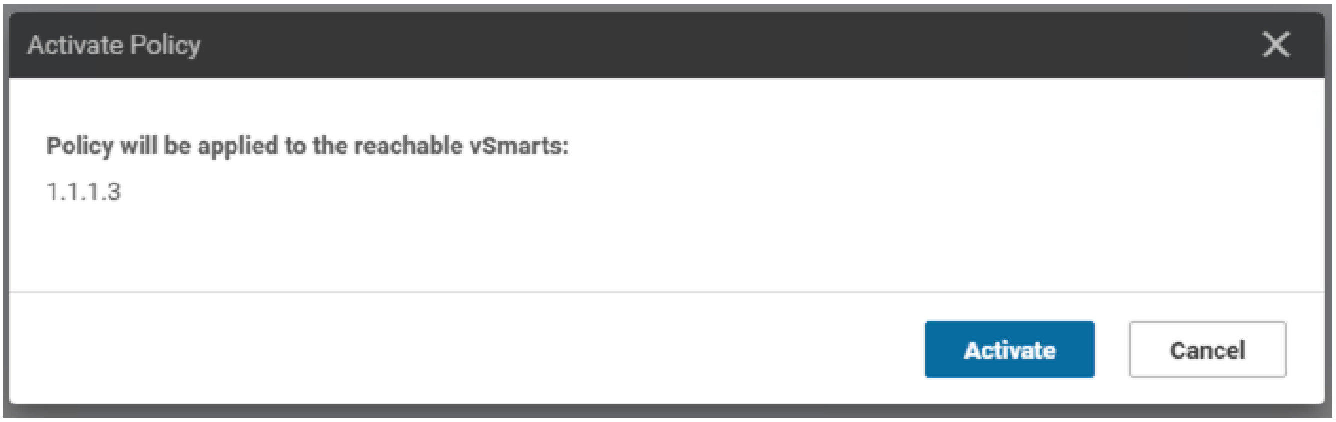
Step 22. Click **Save Policy**.

Step 23. This action should take you to the **Configuration > Policies** screen. Click the **ellipses** in the newly defined policy and click **Activate.**



Name	Description	Type	Activated	Updated By	Policy Version	Last Updated	
dca-vpn-list	dca-vpn-list	UI Policy Builder	false	admin	11112020T000521767	10 Nov 2020 4:05:21 PM PST	•••

Step 24. A popup will appear. Click **Activate**.



Activate Policy

Policy will be applied to the reachable vSmarts:

1.1.1.3

SD-WAN Security policies

The purpose of this guide is to show the user the security options available in the device(s), not necessarily the recommended deployment policies as this will be highly dependent on the environment. Each procedure shown here will provide an example configuration that maps to a TIC security requirement. It is the responsibility of the user to decide how these policies are implemented in their network.

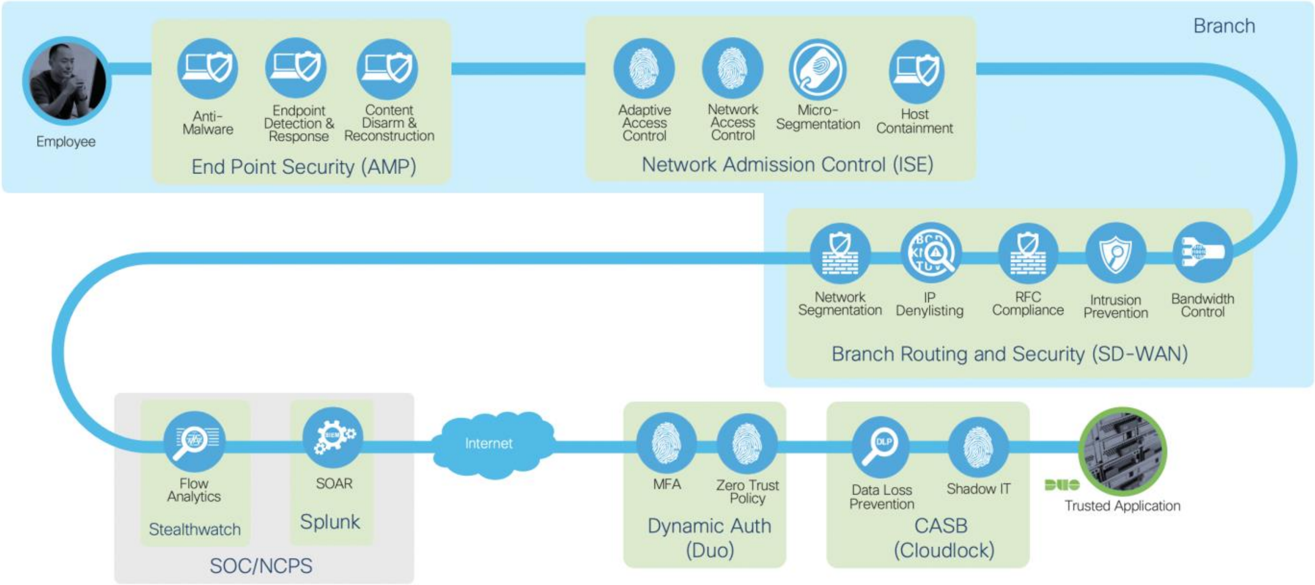
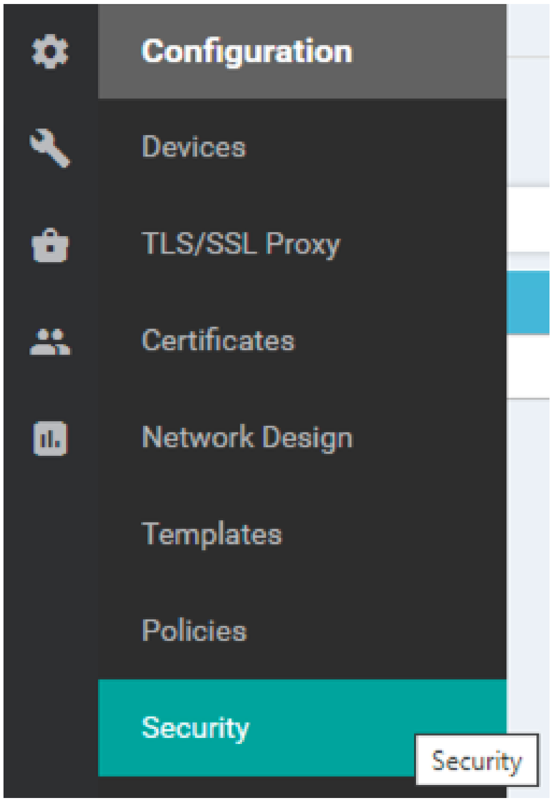


Figure 3.
Secure access to trusted applications with required capabilities

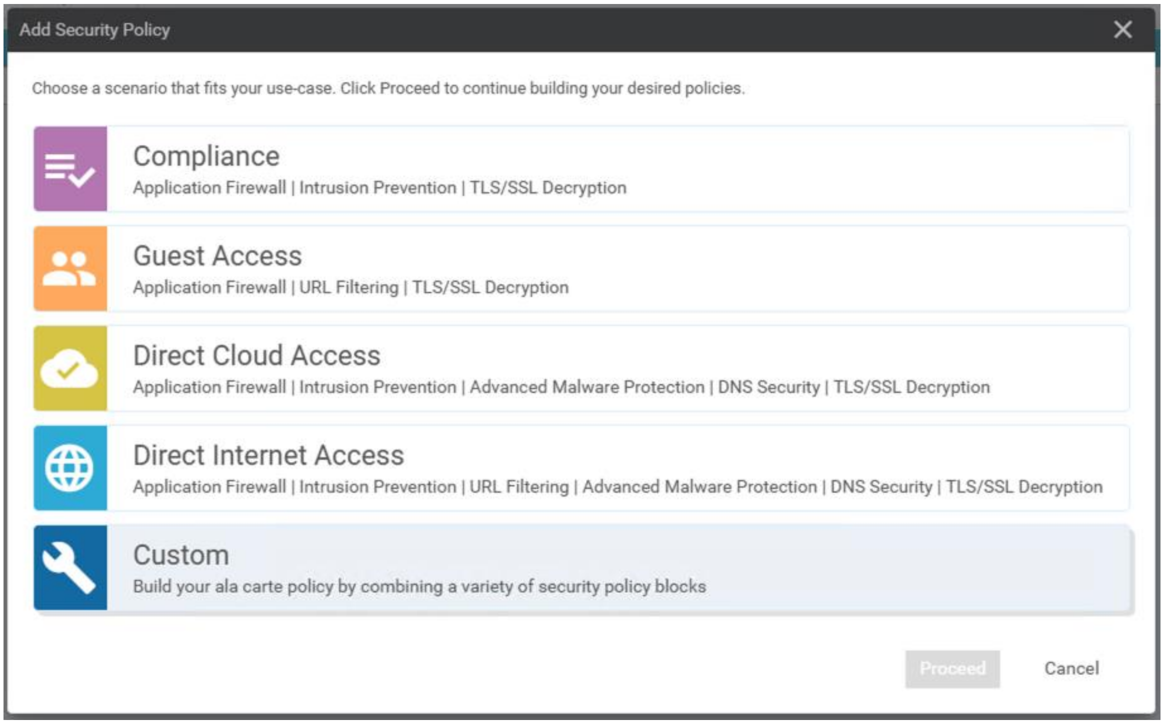
In the TIC 3.0 Architecture Guide a reduced set of security capabilities were outlined for DCA traffic. As all untrusted web traffic is being backhauled to the Traditional TIC, and only trusted traffic is split from the tunnel, a smaller subset of security capabilities are necessary. Nevertheless, the SD-WAN security stack does have more features that won't be configured here such as **Break and Inspect** and **URL filtering**. Later in this guide, additional security measures will be implemented in the Branch using a Cisco Secure Firewall device. For a full Direct Internet Access guide using Cisco SD-WAN and a Secure Internet Gateway, see Cisco SD-WAN Secure Direct Internet Access.

Step 1. In vManage, navigate to **Configuration > Security**.



Step 2. Click **+ Add Security Policy**.

Step 3. vManage provides multiple pre-set policy combinations, depending on the level of security you require at the branch. In this guide we will choose **Custom**. Not all features in Custom will be needed for the recommended deployment, however, links will be provided for more information on each to allow customization options in your agency.



Add Security Policy

Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.

Compliance
Application Firewall | Intrusion Prevention | TLS/SSL Decryption

Guest Access
Application Firewall | URL Filtering | TLS/SSL Decryption

Direct Cloud Access
Application Firewall | Intrusion Prevention | Advanced Malware Protection | DNS Security | TLS/SSL Decryption

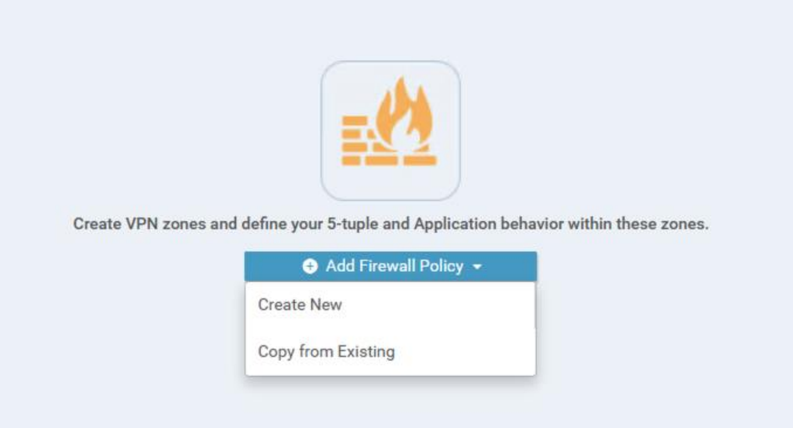
Direct Internet Access
Application Firewall | Intrusion Prevention | URL Filtering | Advanced Malware Protection | DNS Security | TLS/SSL Decryption

Custom
Build your ala carte policy by combining a variety of security policy blocks

Firewall

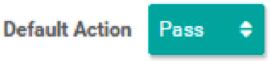
The Firewall policy configuration can be used to meet the requirements for **IP Blacklisting, Content Filtering, Domain Category Filtering** and **Network Segmentation.** For a full SD-WAN firewall policy guide see Enterprise Firewall with Application Awareness.

Step 1. Click **+ Add Firewall Policy > Create New**.

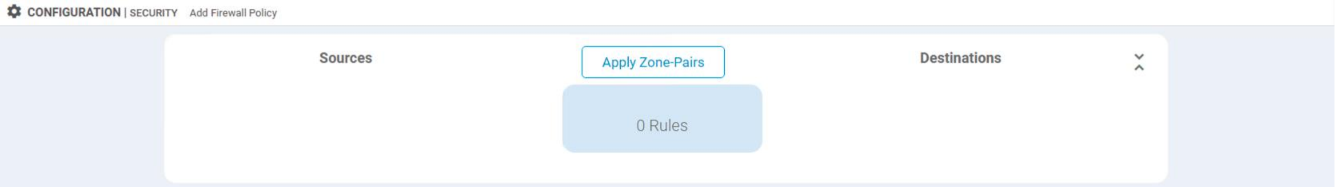

Create VPN zones and define your 5-tuple and Application behavior within these zones.

Step 2. Add a **Name** and **Description**.

Step 3. Change **Default Action** to **Pass**.


Default Action: Pass

Step 4. **Network Segmentation.** At the top of the page, click **Apply Zone-Pairs**. This feature allows you to define firewall policies for incoming and outgoing traffic between a self-zone of an edge router and another zone. When a self-zone is configured with another zone, the traffic in this zone pair is filtered as per the applied firewall policy.

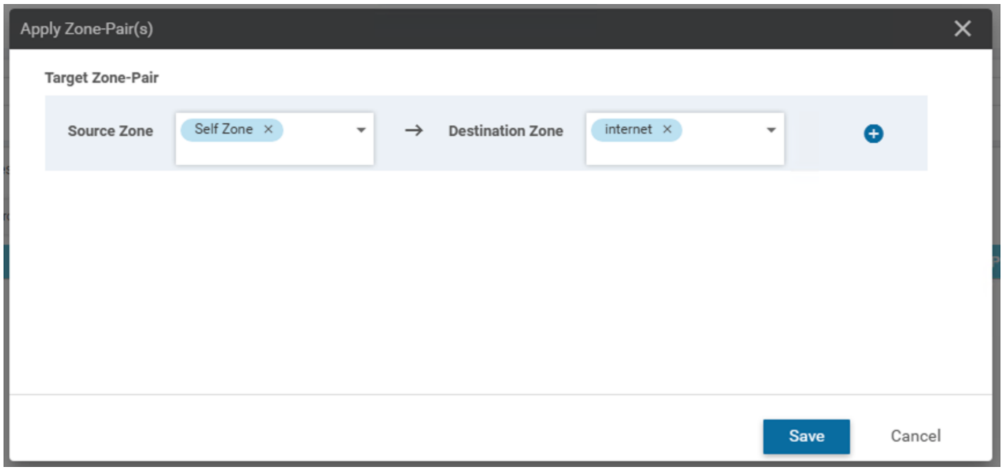


Step 5. In the **Source Zone** field, choose the zone that is the source of the data packets.

Step 6. In the **Destination Zone** field, choose the zone that is the destination of the data packets.

Step 7. Optional: Click the **+** icon to create a zone pair.

Step 8. Click **Save**.



Apply Zone-Pair(s)

Target Zone-Pair

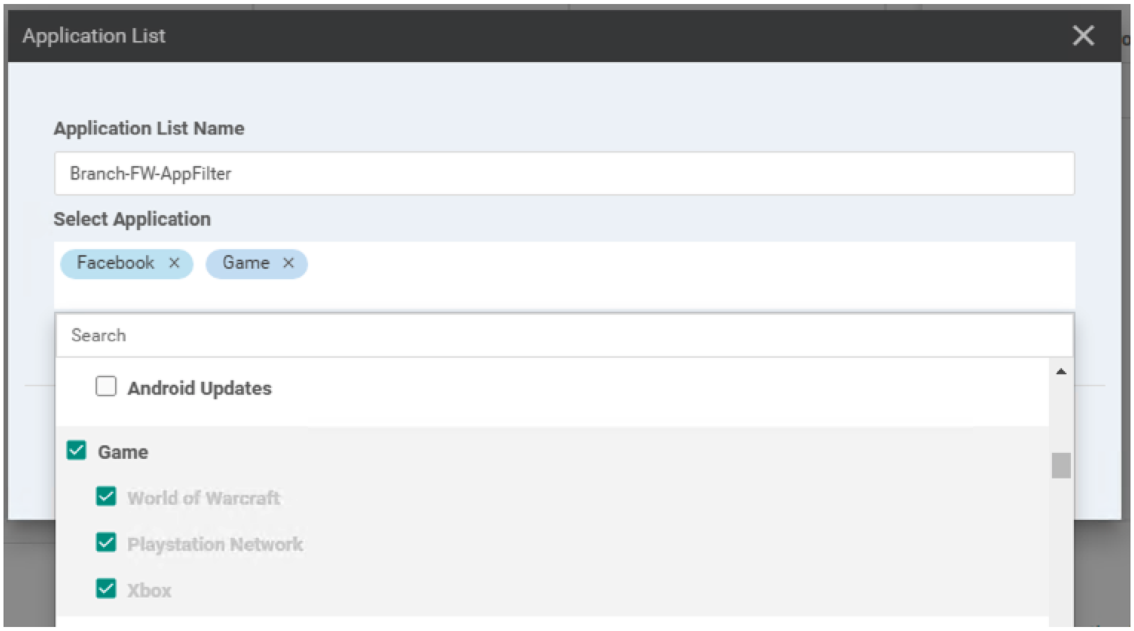
Source Zone: Self Zone → Destination Zone: internet

Step 9. Click **+ Add Rule.**

Step 10. Choose if this policy will **Pass**, **Drop** or **Inspect** the traffic in the **Action** drop down menu.

Step 11. **IP Denylisting**. In the **Source Data Prefix** column, add the IP range that this rule applies. In the **Destination Data Prefix** column, add the IP range that this rule applies. Blocking traffic from a source network is used to stop devices from sending traffic through the firewall. Applying Denylists at the Destination network ensures hosts don't reach devices or servers at a specified IP address.

Step 12. **Content Filtering, Domain Category Filter**. In the **Application List to Drop** column, add the Applications that should be dropped when this rule is triggered. To add a new application list, click **+ Application List to Drop** and then click **+ New Application List.** The chosen applications can be individual, such as Facebook, or based on category, such as gaming.



Application List

Application List Name: Branch-FW-AppFilter

Select Application: Facebook, Game

□ Android Updates

☑ Game

☑ World of Warcraft

☑ Playstation Network

☑ Xbox

Step 13. Click **Save**.

Step 14. Click **Save Firewall Policy**.

Step 15. At the bottom of the page, click **Next.**

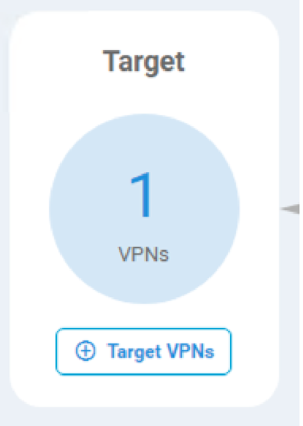
Intrusion Prevention

The Intrusion Prevention policy configuration can be used to meet the requirements for **Intrusion Prevention** and **Malicious Content Filtering.** For a full SD-WAN Intrusion Prevention policy guide see Intrusion Prevention System.

Note: Please upload compatible Security App Hosting Image File to the software repository in order to support IPS functions. You can upload the image file in vManage from **Maintenance > Software Repository > Virtual Images.**

Step 1. Click **+ Add Intrusion Prevention Policy > Create New**.

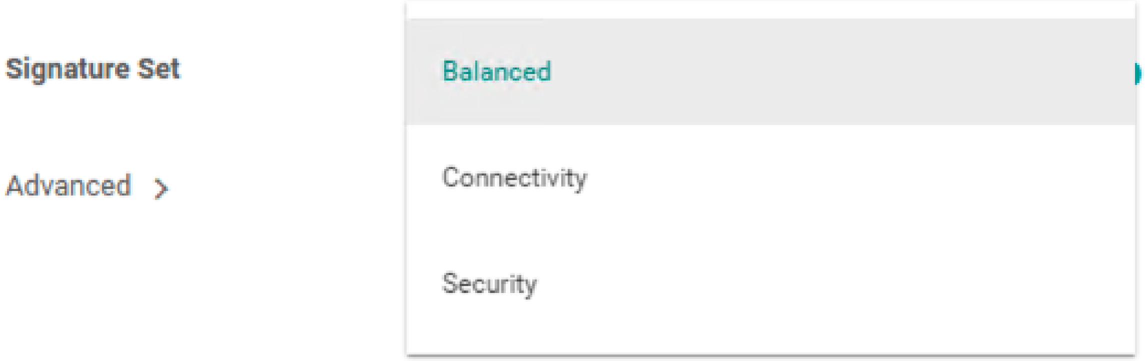
Step 2. Click **+ Target VPNs**. Add VPNs that this policy applies to and **Save**.



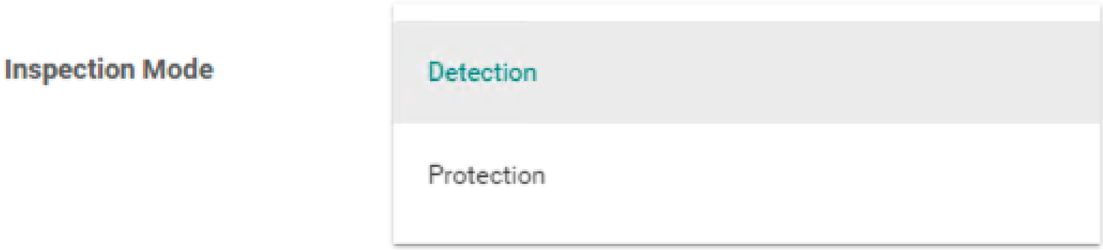
Step 3. Add a **Policy Name**.

Step 4. When choosing a **Signature Set** there are three options:

- **Connectivity** – Enables signatures with a CVSS score of 10 and CVE published within last 2 years.
- **Balanced** – Enables signatures with a CVSS score >= 9 and CVE published within last 2 years. Includes rule categories Malware CNC, Exploit Kits, SQL Injection and Denylist.
- **Security** – Enables signatures with a CVSS score >= 8 and CVE published within last 3 years. Included rules categories Malware CNC, Exploit Kits, SQL Injection, Denylist and App Detect Rules.



Step 5. In the **Inspection Mode** dropdown choose either **Detection** (alert only) or **Protection** (alert and block) depending on agency needs.



Step 6. Click **Save Intrusion Prevention Policy**.

Step 7. Click **Next**.

URL Filtering

The URL filtering policy configuration can be used to meet the requirement for **Domain Category and Reputation Filtering**. In this example deployment, all web traffic, with the exception of Office365 and WebEx, are backhauled to a Traditional TIC where URL filtering policies will be applied and centrally managed. To apply URL Filtering policies at the branch, see URL Filtering.

Advanced Malware Protection (AMP)

The AMP policy can be used to meet the requirements for **Anti-Malware, Content Disarm, Detonation Chamber, Content Filtering** and **Malicious Content Filtering**. AMP is composed of three processes:

- **File Reputation** - The process of using a 256-bit Secure Hash Algorithm (SHA256) signature to compare the file against the AMP cloud server and access its threat intelligence information. The response can be Clean, Unknown, or Malicious. If the response is Unknown, and if File Analysis is configured, the file is automatically submitted for further analysis.
- **File Analysis** - The process of submitting an Unknown file to the Threat Grid (TG) cloud for detonation in a sandbox environment. During detonation, the sandbox captures artifacts and observes behaviors of the file, then gives the file an overall score. Based on the observations and score, Threat Grid may change the threat response to Clean or Malicious. Threat Grid's findings are reported back to the AMP cloud, so that all AMP customers will be protected against newly discovered malware.
- **Retrospective** - By maintaining information about files even after they are downloaded, we can report on files that were determined to be malicious after they were downloaded. The disposition of the files could change based on the new threat intelligence gained by the AMP cloud. This re-classification will generate automatic retrospective notifications.

For details on adding AMP and TG to an SD-WAN security policy see Advanced Malware Protection.

DNS Security

The DNS Security policy can be used to meet the requirements for **DNS Sinkholing, DNNSEC** and **NCPS E3A DNS Protections**. Configuring the DNS policy configures the router to act as a DNS forwarder on the network edge, transparently intercepts DNS traffic, and forwards the DNS queries to a specified location. For a full SD-WAN DNS Security policy guide see Cisco Umbrella Integration.

TLS/SSL Decryption

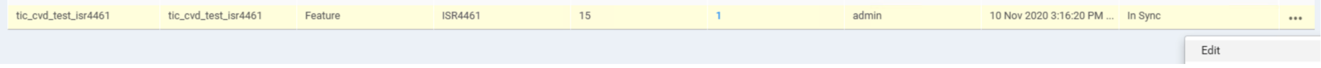
The TLS/SSL Decryption policy can be used to meet the requirements for **Break and Inspect** and **Certificate Denylisting**. Decrypting and re-encrypting traffic is a resource intensive capability and has been deemed out of scope for this particular use case. According to Microsoft "Most enterprise networks enforce network security for Internet traffic using technologies like proxies, SSL inspection, packet inspection, and data loss prevention systems. These technologies provide important risk mitigation for generic Internet requests but can dramatically reduce performance, scalability, and the quality of end user experience when applied to Microsoft 365 endpoints". In the DCA use case, we only break trusted applications off from the tunnel, and therefore mitigate the need to do TLS decryption on this traffic. Extra protections can be added in the cloud such as a CASB for visibility into the application itself, and TLS decryption can be reserved for unknown or untrusted web traffic. If your agency has a requirement to do SSL decryption at the branch, a full SD-WAN TLS/SSL Decryption guide can be found at SSL/TLS Proxy.

Adding the policy to the network

Step 1. In the **Policy Summary** tab, add a **Security Policy Name** and **Description**. Click **Save Policy**.

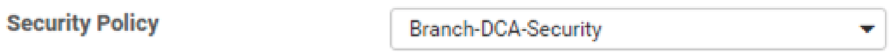
Step 2. In vManage, navigate to **Configuration > Templates**.

Step 3. Click the **ellipses** on the device template that this policy applies to and click **Edit**.



tic_cvd_test_isr4461	tic_cvd_test_isr4461	Feature	ISR4461	15	1	admin	10 Nov 2020 3:16:20 PM ...	In Sync	•••

Step 4. In the **Additional Templates** section, click on the **Security Policy** dropdown list and choose the newly created policy.



Security Policy: Branch-DCA-Security

Step 5. Click **Update** and push the policy to the device(s).

Cisco TrustSec

Cisco TrustSec is an end-to-end network infrastructure that provides a scalable architecture for the enforcement of role-based access control, identity-aware networking, and data confidentiality to secure the network and its resources. Cisco TrustSec uses Security Group Tags (SGT) to represent user and device groups. The switches, routers, and firewalls inspect these tags and enforce SGT-based traffic policies.

Cisco TrustSec is defined in three phases: classification, propagation, and enforcement. After traffic is classified, the SGT is propagated from where Classification took place, to where enforcement action is invoked. This process is called propagation. One of the SGT propagation methods that Cisco TrustSec offers is inline tagging.

With inline tagging, a special Ethernet frame is used to propagate these SGTs between network hops where the policies can be enforced based on the SGT policy. Cisco IOS XE SD-WAN devices support propagation of SGT.

For full details on how to configure SGT enforcement across the WAN network see Cisco TrustSec Integration.

Additional DCA Security Controls

The above configuration primarily focused on configuring the security policies located on networking infrastructure. In figure 3, where security capabilities were mapped to Cisco products, additional security products were shown in order to provide end to end protection in the agency's architecture. These security controls, namely AMP for endpoints and Cloudlock, will be discussed in the Remote User section.

Direct Internet Access (DIA)

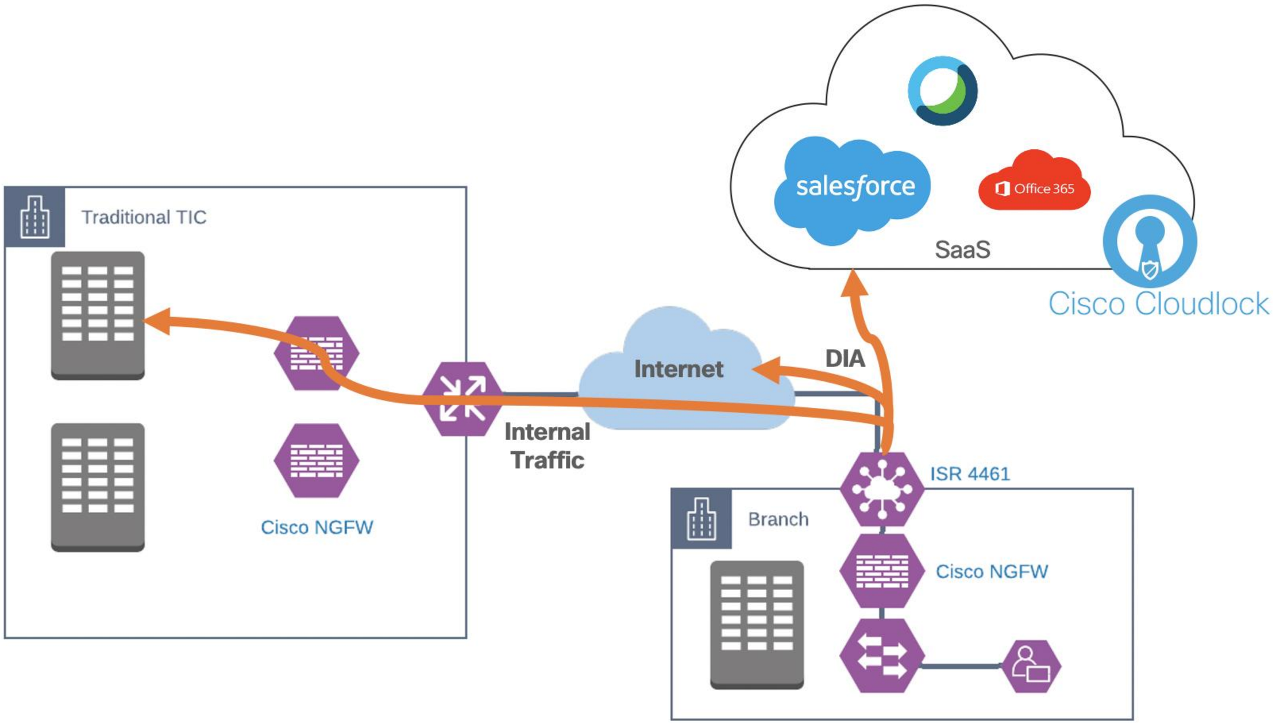


Figure 4.
Cisco SD-WAN Direct Internet Access with Cisco NGFW

The second option involves using a Cisco FTD device in combination with an SD-WAN router. The advantage of this deployment is the use of FMC to manage firewall policies across the full organization, regardless of location. The same rules that were created for the datacenter, can be extended to the branches, using the same management platform.

Pre-requisites

- The SD-WAN controllers are set up and deployed (vManage, vBond, vSmart)
- An FMC has been deployed to manage the firewall
- The FTD device has gone through its initial configuration and has a functioning route to the FMC. The quick-start guide for the FTD 1010 can be found here
- Necessary licenses have been obtained for the device (more details can be found in the '**Install FTD device'** section below)
- A router has been configured using device templates in order to establish a functional and secure overlay fabric to pass data traffic across the organizations distributed sites. An SD-WAN deployment guide can be found here.

Install FTD device

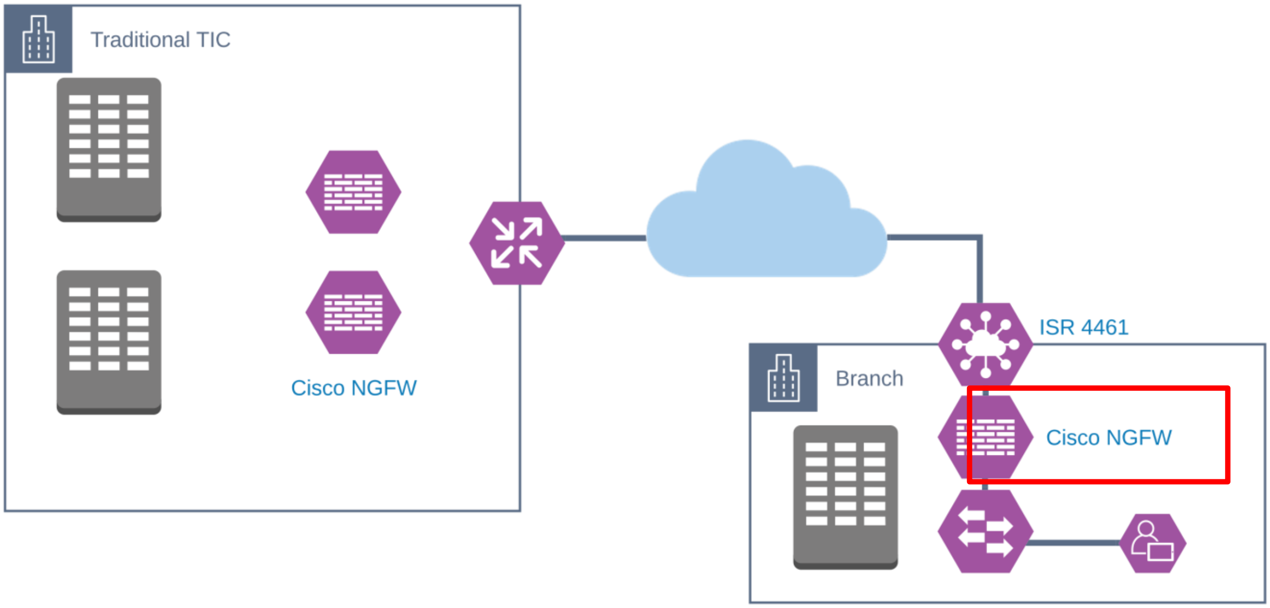


Figure 5.
Cisco FTD 1010 in transparent mode

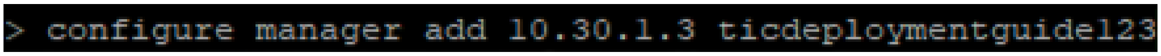
The Cisco Firepower 1010 security appliance is an NGFW desktop product in the Cisco Secure Firewall family of devices. Hardware installation guidance can be found here. The Cisco Firepower 1010, which the rest of this guidance will refer to as the FTD (Firepower Threat Defense) device, is the lowest performing in the Secure Firewall family. For detailed performance specs, such as throughput when all features are enabled, see the datasheet. If more performance is needed, there are larger appliances in the range.

Procedure 1. Add device to FMC

Step 1. Access the command line interface of the FMC. The easiest method is through the console port.

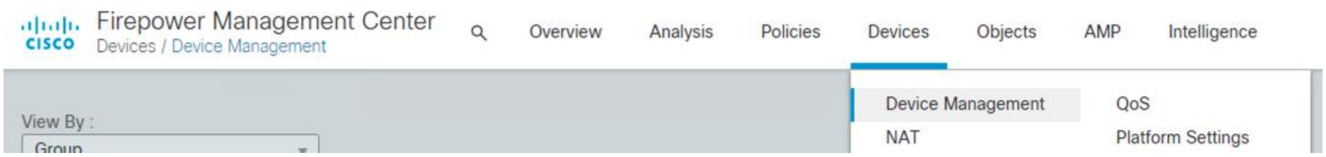
Step 2. Identify the FMC that will manage this FTD using the command

```
configure manager add {hostname | IPv4_address | IPv6 address | DONTRESOLVE} reg_key
[nat_id]
```



```
> configure manager add 10.30.1.3 ticdeploymentguide123
```

Step 3. In FMC, navigate to **Devices > Device Management**.

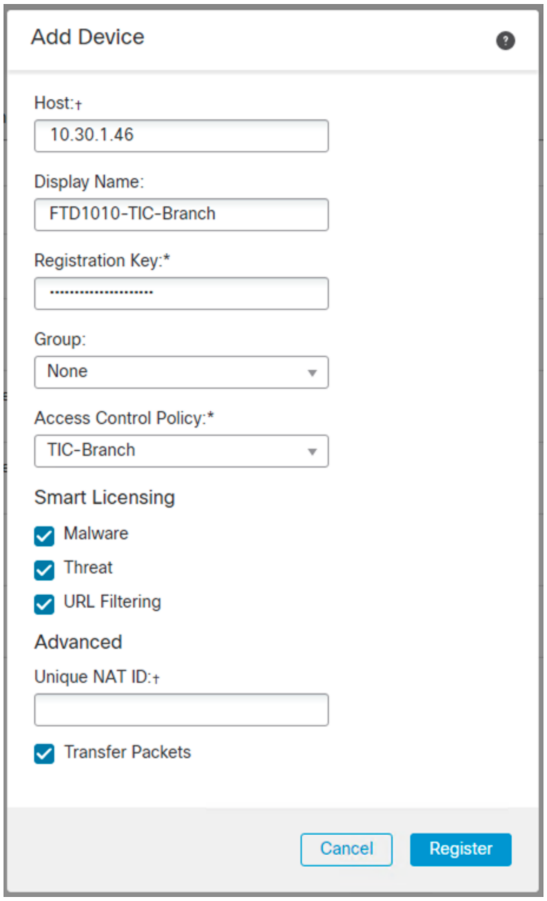


Step 4. In the **Add** drop-down list, choose **Device**.

Step 5. Enter the following parameters.

- **Host** – IP address or hostname of the FTD device.
- **Display Name** – the name FMC will use for display purposes.
- **Registration Key** – the key that was specified in step 2 above.

- **Group** – assign to device group if required.
- **Access Control Policy** – choose an initial policy. Unless you already have a customized policy, you know you need to use, choose Create new policy, and choose Block All traffic. This will be modified later to suit the use case.
- **Smart Licensing** – enable the features you need to deploy. This guide will use features that require all three licensing options.
  - **Threat** – enables intrusion prevention capabilities
  - **URL** – enables category-based URL filtering
  - **Malware** – enables AMP malware inspection
- **Transfer packets** – allows the device to transfer packets to the FMC. When events like IPS are triggered, this option allows the device to send packet data to FMC for inspection.



Add Device

Host:† 10.30.1.46

Display Name: FTD1010-TIC-Branch

Registration Key:* ••••••••••••••••••••

Group: None

Access Control Policy:* TIC-Branch

Smart Licensing

☑ Malware

☑ Threat

☑ URL Filtering

Advanced

Unique NAT ID:†

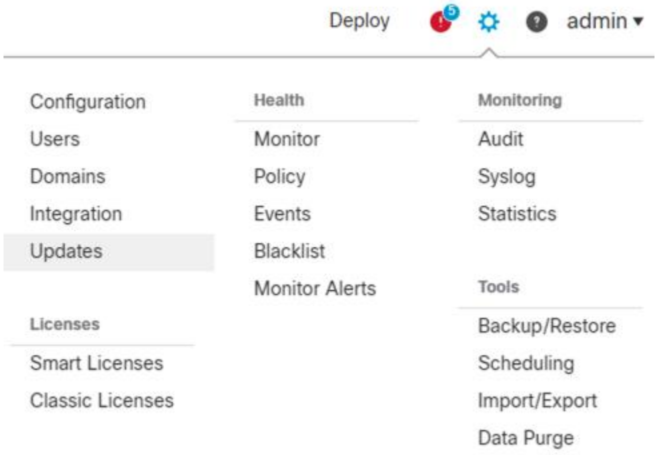
☑ Transfer Packets

Procedure 2. Upgrade the FTD device

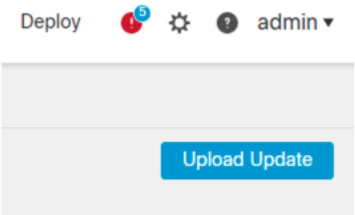
This guide is using Firepower Threat Defense software version 6.6.0. If your device is lower than that it is recommended to upgrade before continuing on to the next steps.

Step 1. Download the latest software upgrade image from software.cisco.com.

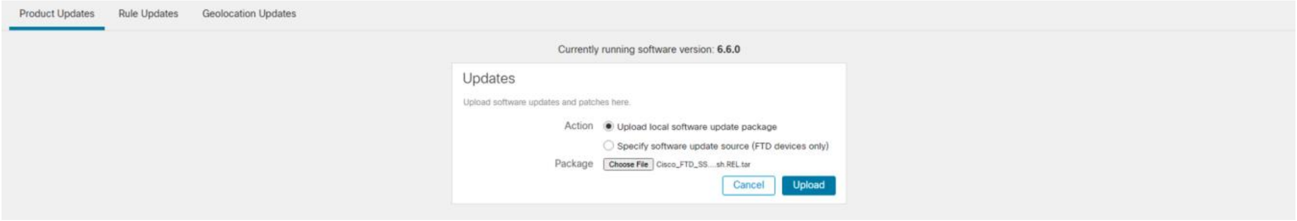
Step 2. In FMC navigate to **System Settings > Updates**.



Step 3. Click Upload Update.



Step 4. Click **Choose File** and upload the file that was downloaded in step 1. Click **Upload**.



Currently running software version: **6.6.0**

Updates

Upload software updates and patches here.

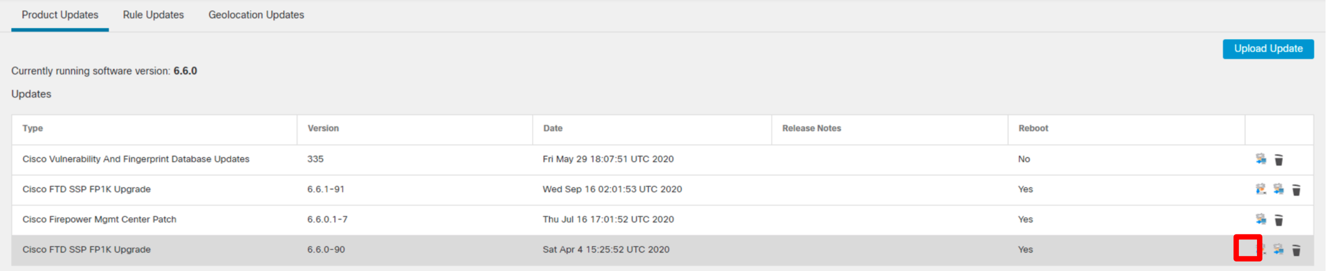
Action ● Upload local software update package

○ Specify software update source (FTD devices only)

Package Choose File Cisco_FTD_SS....sh.REL.tar

Cancel Upload

Step 5. In the updates page (**System Settings > Updates**), click **Push or Stage update** on the upgrade package that was uploaded in the previous step. **Note: By pushing the update to the device, the amount of downtime is being reduced. As the package is being transferred to the device, the device remains operational. In a new build, this isn't as critical, but it is a good practice to follow when updating Firepower devices.**

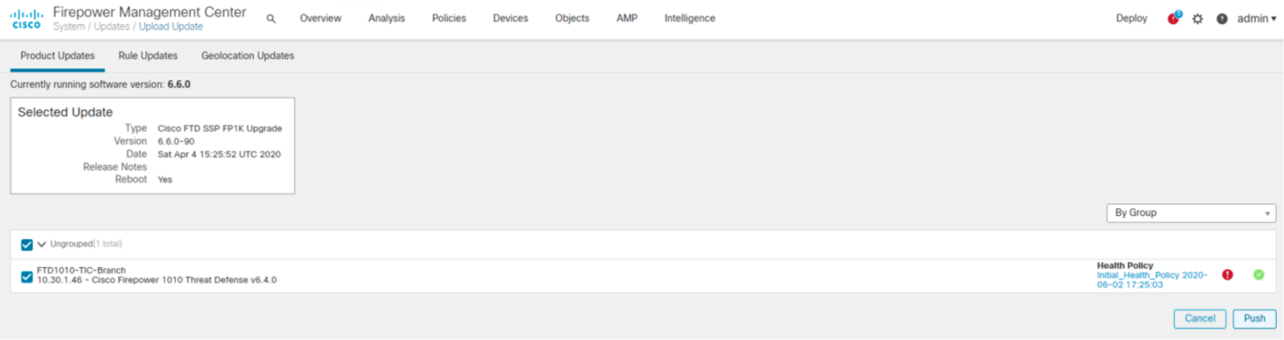


Currently running software version: **6.6.0**

Updates

Type	Version	Date	Release Notes	Reboot
Cisco Vulnerability And Fingerprint Database Updates	335	Fri May 29 18:07:51 UTC 2020		No
Cisco FTD SSP FP1K Upgrade	6.6.1-91	Wed Sep 16 02:01:53 UTC 2020		Yes
Cisco Firepower Mgmt Center Patch	6.6.0.1-7	Thu Jul 16 17:01:52 UTC 2020		Yes
Cisco FTD SSP FP1K Upgrade	6.6.0-90	Sat Apr 4 15:25:52 UTC 2020		Yes

Step 6. Choose the FTD device(s) you wish to update and click **Push**.



Currently running software version: **6.6.0**

Selected Update

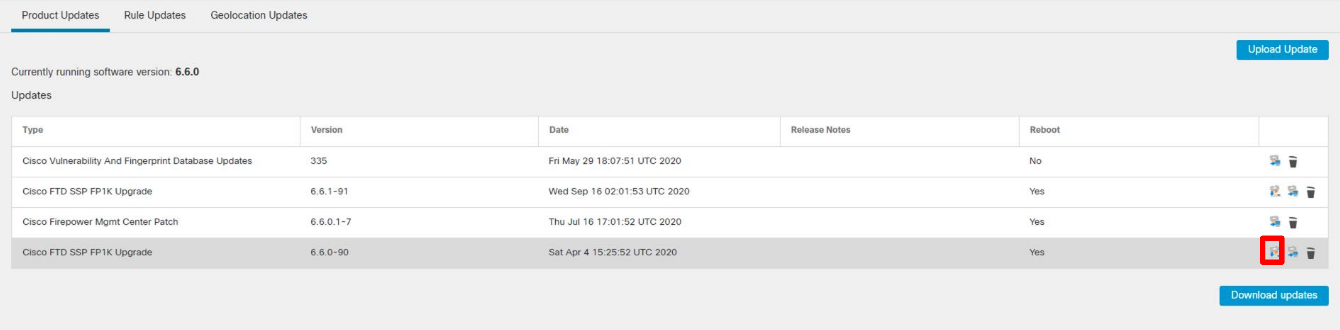
Type	Cisco FTD SSP FP1K Upgrade
Version	6.6.0-90
Date	Sat Apr 4 15:25:52 UTC 2020
Release Notes	
Reboot	Yes

☑ Ungrouped(1 total)

☑ FTD1010-TIC-Branch
10.30.1.46 - Cisco Firepower 1010 Threat Defense v6.4.0

Health Policy
Initial_Health_Policy 2020-06-02 17:25:03

Step 7. After the update has been successfully pushed, return back to the updates page and click install on the upgrade package that was pushed in the previous step.



Currently running software version: **6.6.0**

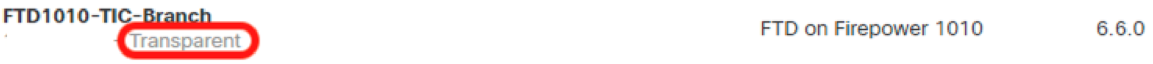
Updates

Type	Version	Date	Release Notes	Reboot
Cisco Vulnerability And Fingerprint Database Updates	335	Fri May 29 18:07:51 UTC 2020		No
Cisco FTD SSP FP1K Upgrade	6.6.1-91	Wed Sep 16 02:01:53 UTC 2020		Yes
Cisco Firepower Mgmt Center Patch	6.6.0.1-7	Thu Jul 16 17:01:52 UTC 2020		Yes
Cisco FTD SSP FP1K Upgrade	6.6.0-90	Sat Apr 4 15:25:52 UTC 2020		Yes

Step 8. Choose the FTD device(s) you wish to update and click **Install**.

Procedure 3. Create Transparent route

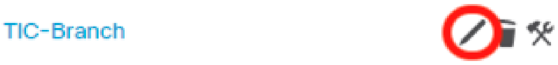
Step 1. In FMC, navigate to **Devices > Device Management**. Check the FTD device is in transparent mode.



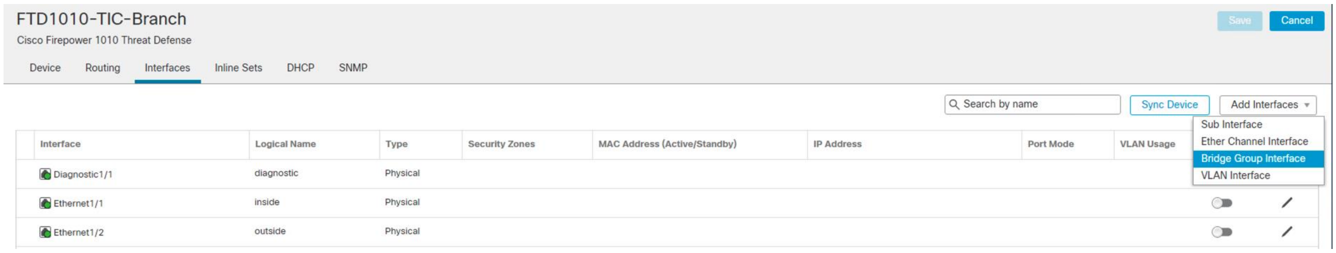
FTD1010-TIC-Branch
Transparent

FTD on Firepower 1010 6.6.0

Step 2. Click the **pencil icon** to edit the device.



Step 3. While on the **Interfaces** tab, click **Add Interfaces > Bridge Group Interface.**

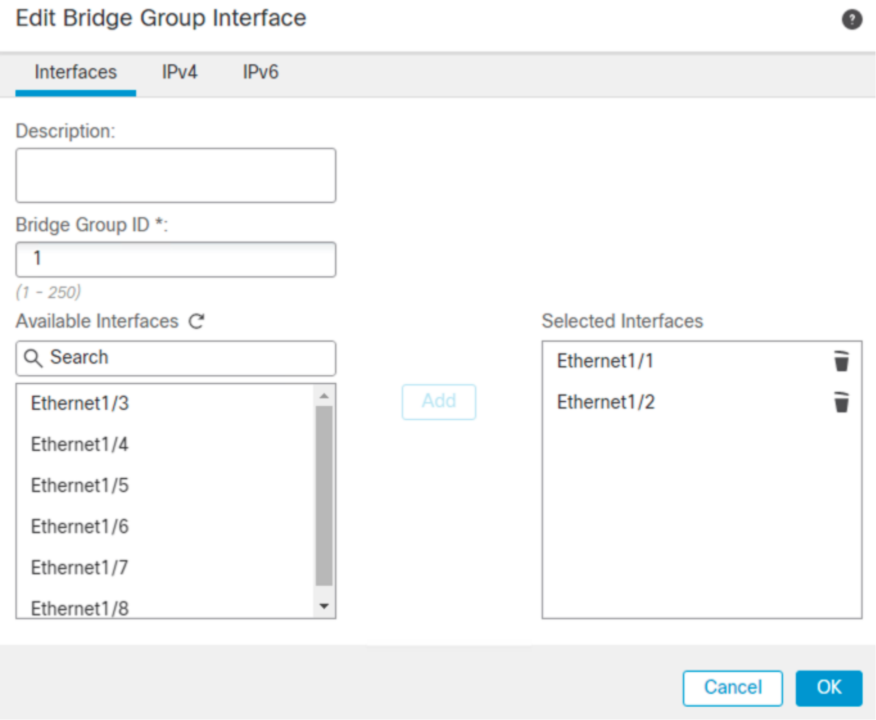


FTD1010-TIC-Branch

Cisco Firepower 1010 Threat Defense

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Port Mode	VLAN Usage
Diagnostic1/1	diagnostic	Physical					
Ethernet1/1	inside	Physical					
Ethernet1/2	outside	Physical					

Step 4. On the **Interfaces** tab choose the two interfaces on the interface that will act as the bump in the wire from the router. When running in transparent mode, the firewall needs to know which ports are paired together. Assign a unique **Bridge group ID**.



Edit Bridge Group Interface

Description:

Bridge Group ID *: 1

(1 - 250)

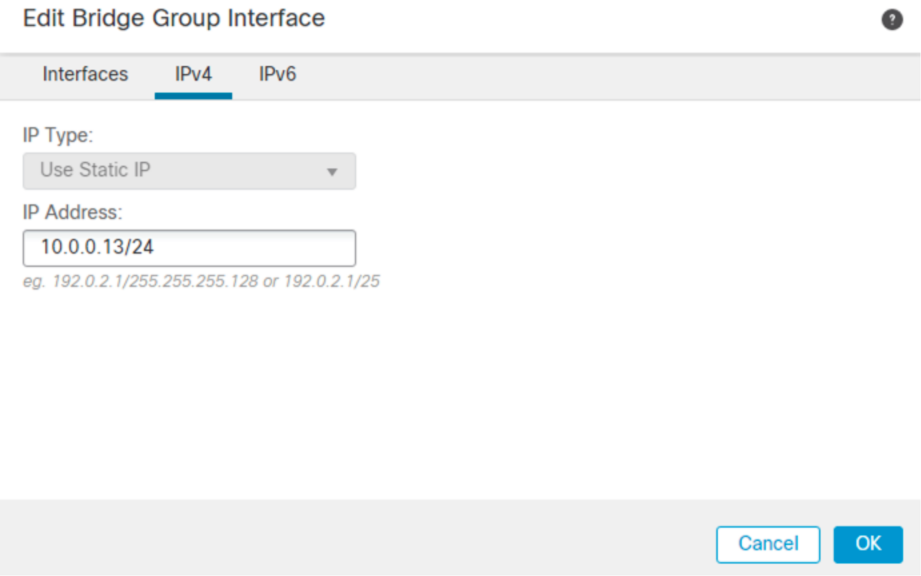
Available Interfaces

Selected Interfaces

Ethernet1/1

Ethernet1/2

Step 5. On the **IPv4** tab, assign an IP address to the BridgeGroup.



Edit Bridge Group Interface

IP Type: Use Static IP

IP Address: 10.0.0.13/24

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Step 6. Click **OK**.

Enabling TIC Security Capabilities

The purpose of this guide is to show the user the configuration options available on the firewall, not necessarily the recommended deployment policies as this will be highly dependent on the environment. Each procedure shown here will provide an example configuration that maps to a TIC security requirement. It is the responsibility of the user to decide how these policies are implemented in their network.

Creating SSL Policies

The SSL policy configuration can be used to meet the requirements for **Break & Inspect** and **Certificate Denylisting**. For a full SSL policy guide see SSL Policies.

If the system detects a TLS/SSL handshake over a TCP connection, it determines whether it can decrypt the detected traffic. If it cannot, it applies a configured action:

- Block the encrypted traffic
- Block the encrypted traffic and reset the TCP connection
- Not decrypt the encrypted traffic

If the system can decrypt the traffic, it blocks the traffic without further inspection, evaluates undecrypted traffic with access control, or decrypts it using one of the following methods:

- Decrypt with a known private key. When an external host initiates a TLS/SSL handshake with a server on your network, the system matches the exchanged server certificate with a server certificate previously uploaded to the system. It then uses the uploaded private key to decrypt the traffic.
- Decrypt by resigning the server certificate. When a host on your network initiates a TLS/SSL handshake with an external server, the system resigns the exchanged server certificate with a previously uploaded certificate authority (CA) certificate. It then uses the uploaded private key to decrypt the traffic.

Note: Set up decrypt rules only if your managed device handles encrypted traffic. Decryption rules require processing overhead that can impact performance.

Creating DNS Policies

The DNS policy configuration can be used to meet the requirements for **DNS Sinkholing** and **NCPS E3A DNS Protections**. For a full DNS policy guide see DNS Policies.

DNS-based Security Intelligence allows you to block traffic based on the domain name requested by a client, using a Security Intelligence Block list. Cisco provides domain name intelligence you can use to filter your traffic; you can also configure custom lists and feeds of domain names tailored to your deployment.

Traffic on a DNS policy Block list is immediately blocked and therefore is not subject to any further inspection—not for intrusions, exploits, malware, and so on, but also not for network discovery. You can use a Security Intelligence Do Not Block list to override a Block list and force access control rule evaluation, and, recommended in passive deployments, you can use a “monitor-only” setting for Security Intelligence filtering. This allows the system to analyze connections that would have been blocked by a Block list, but also logs the match to the Block list and generates an end-of-connection Security Intelligence event.

Creating File Policies

The File policy configuration can be used to meet the requirements for **Anti-Malware, Content Disarm, Detonation Chamber, Content Filtering** and **Malicious Content Filtering**. For a full File policy guide see File Policies and Malware Protection.

To detect and block malware, use file policies. You can also use file policies to detect and control traffic by file type. Connections to public or private clouds are required in order to protect your network from malware.

AMP Clouds

The AMP cloud is a Cisco-hosted server that uses big data analytics and continuous analysis to provide intelligence that the system uses to detect and block malware on your network.

The AMP cloud provides dispositions for possible malware detected in network traffic by managed devices, as well as data updates for local malware analysis and file pre-classification.

If your organization has deployed AMP for Endpoints and configured Firepower to import its data, the system imports this data from the AMP cloud, including scan records, malware detections, quarantines, and indications of compromise (IOC).

Cisco offers the following options for obtaining data from the Cisco cloud about known malware threats:

- **AMP public cloud** - Your Firepower Management Center communicates directly with the public Cisco cloud.
- **AMP private cloud** - An AMP private cloud is deployed on your network and acts as a compressed, on-premises AMP cloud, as well as an anonymized proxy to connect to the public AMP cloud. For details, see Cisco AMP Private Cloud. **NOTE: If you integrate with AMP for Endpoints, the AMP private cloud has some limitations. See AMP for Endpoints and AMP Private Cloud.**

Dynamic Analysis Cloud

- **Cisco Threat Grid cloud** - Public cloud that processes eligible files that you send for dynamic analysis and provides threat scores and dynamic analysis reports.
- **On-premises Cisco Threat Grid appliance** - If your organization's security policy does not allow the Firepower System to send files outside of your network, you can deploy an on-premises appliance. This appliance does not contact the public Cisco Threat Grid cloud. For more information, see Dynamic Analysis On-Premises Appliance (Cisco Threat Grid).

Creating the Intrusion Policies

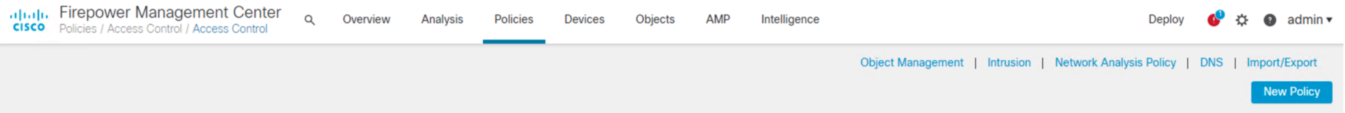
The Intrusion policy configuration can be used to meet the requirements for **Active Content Mitigation, Malicious Content Filtering,** and **Intrusion Protection Systems (IPS)**. For a full Intrusion prevention policy guide see Intrusion Policies.

Intrusion policies are defined sets of intrusion detection and prevention configurations that inspect traffic for security violations and, in inline deployments, can block or alter malicious traffic. Intrusion policies are invoked by your access control policy and are the system’s last line of defense before traffic is allowed to its destination.

Create the Access Policy

The access policy configuration is where all of the above functionality comes together for enforcement. In addition to above access policies can be used to meet the requirements for **Content Filtering, DNS-over-HTTPS Filtering, RFC Compliance Enforcement, Domain Category and Reputation Filtering, Access Control, IP Denylisting, Network Segmentation, Microsegmentation, NCPS E3A DNS Protections, Adaptive Access Control** and **Protections for Data in Transit**. For more details on Access Control Policies see Access Control.

Step 1. In FMC, navigate to **Policies > Access Control**. Click **New Policy**.

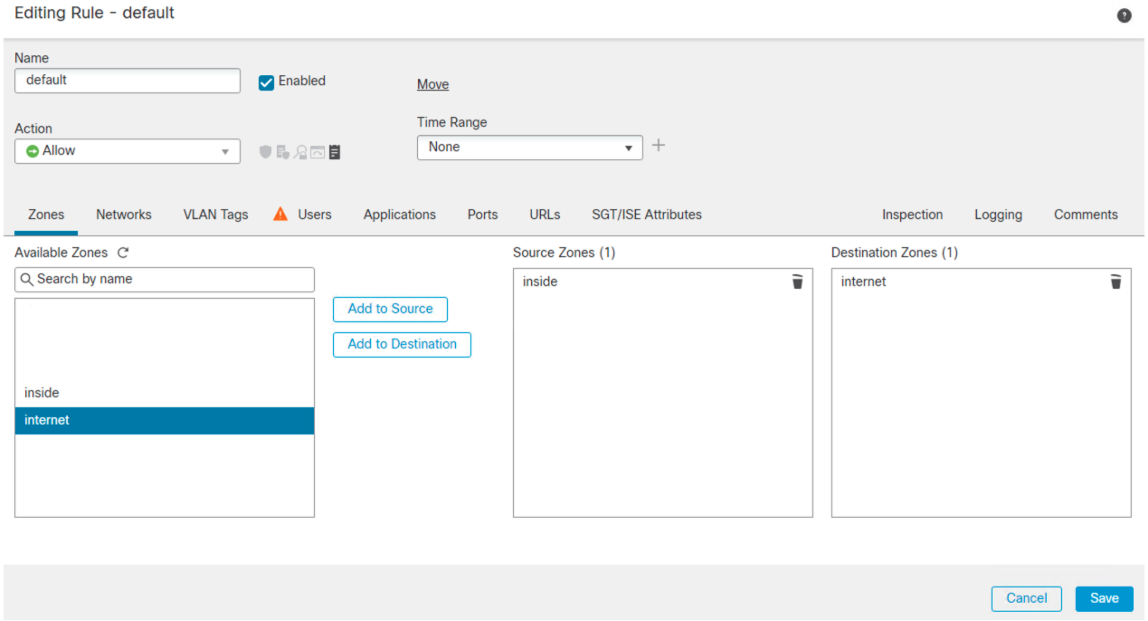

Firepower Management Center
Policies / Access Control / Access Control
Overview
Analysis
Policies
Devices
Objects
AMP
Intelligence
Deploy
admin
Object Management | Intrusion | Network Analysis Policy | DNS | Import/Export
New Policy

Step 2. File in the required fields:

- Give a meaningful **Name**.
- Select a **Base Policy**. For this example, **None** is chosen, however, if rules have already been created for another location, and they need to be modified slightly for a new location, it is recommended you choose that policy and build from that.
- Choose a **Default Action**. This lab will **Block all traffic** by default and allow only what is needed.
- Add the relevant device(s) that this policy applies.

Step 3. Click **Add Rule**.

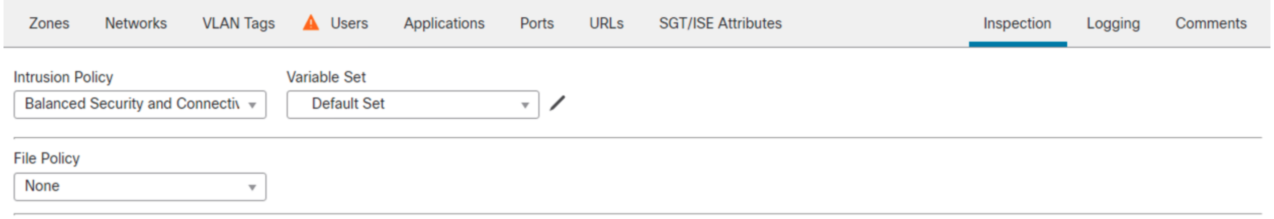
Step 4. The level of security applied at this point is up to the user. In this lab example, we will build a base rule that allows most traffic from inside to outside and block all traffic from outside to inside. In the **Zones** tab, choose the **inside** interface as **Source** and **WAN** interface as **Destination**.


Editing Rule - default

Name: default
☑ Enabled
Action: Allow
Time Range: None

Source Zones (1): inside
Destination Zones (1): internet

Step 5. In the **Inspection** tab, choose the **Balanced Security and Connectivity** from the **Intrusion Policy** dropdown menu. This enables a predefined set of Intrusion rules to keep users safe from known threats. For more information on each of the base options see [Intrusion Base Policy](#).

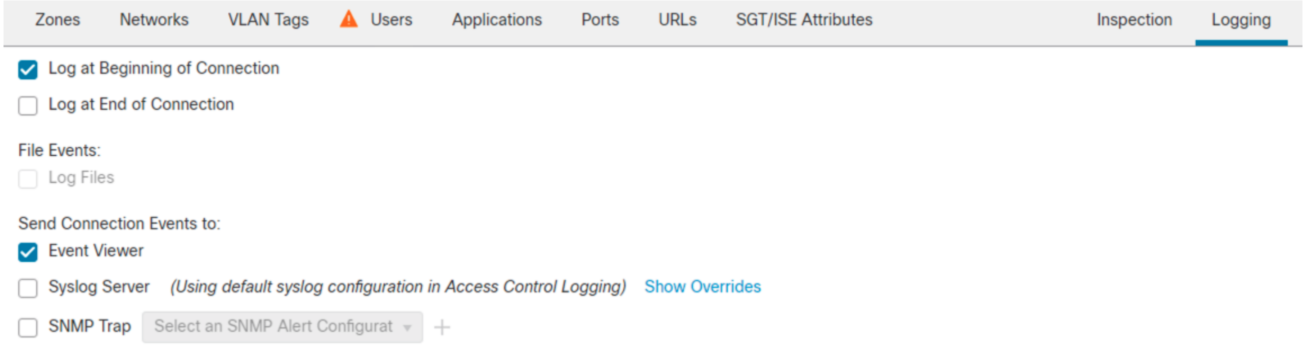


Intrusion Policy: Balanced Security and Connectiv ▾

Variable Set: Default Set ▾

File Policy: None ▾

Step 6. In the **Logging** tab, choose **Log at Beginning of Connection**.



☑ Log at Beginning of Connection

□ Log at End of Connection

File Events:

□ Log Files

Send Connection Events to:

☑ Event Viewer

□ Syslog Server *(Using default syslog configuration in Access Control Logging)* Show Overrides

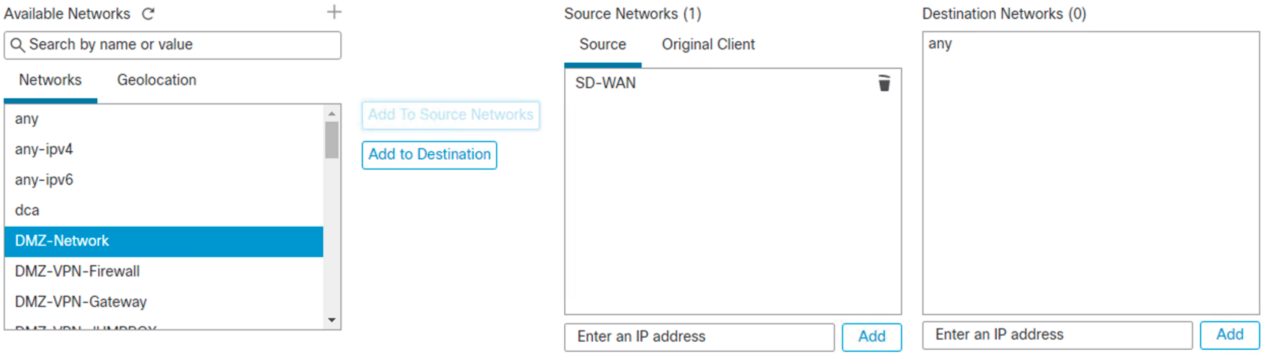
□ SNMP Trap Select an SNMP Alert Configurat ▾ +

Step 7. Click **Add**.

Step 8. For every new rule created, make sure to **Insert** rule **above** the base rule created in the previous step. The firewall will enforce traffic on the first matched rule and therefore there must be no conflicting rules.

Step 9. **Network Segmentation**. In the **Zones** tab, FMC will list all of the **Available Zones** in the network. These zones are the names assigned to interfaces on the devices. To segment the network bases on zones, add relevant zones to the source and destination and choose **Allow** or **Block** in the **Action** tab, depending on what you are trying to achieve.

Step 10. **IP Denylisting**. In the **Networks** tab, network objects can be defined to group IP address' for use in access rules. Blocking traffic from a source network is used to stop devices from sending traffic through the firewall. Applying Denylists at the Destination network ensures hosts don't reach devices or servers at a specified IP address.

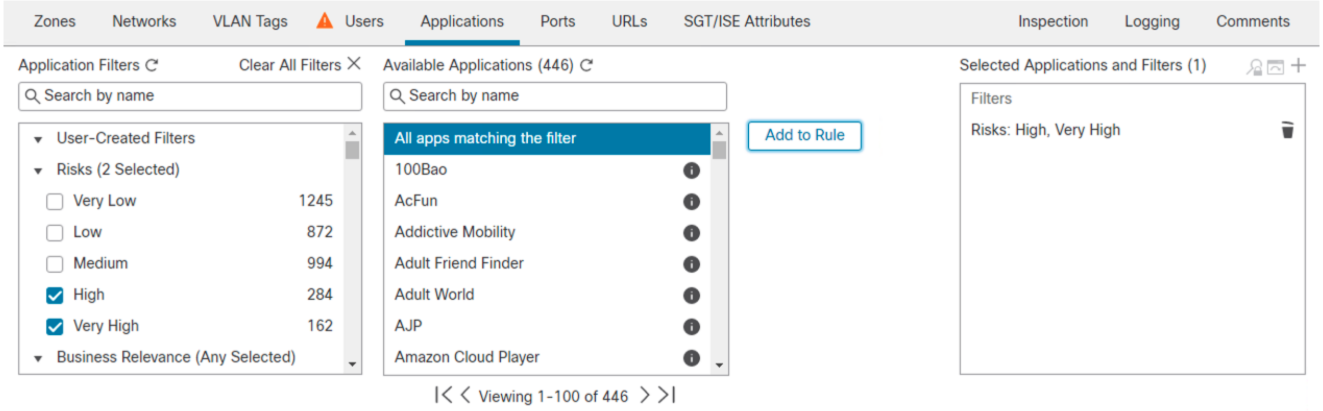


Source Networks (1): SD-WAN

Destination Networks (0): any

Step 11. **Access Control**. Although Access Control is a broad topic, we will focus on identity-based access control. In the **Users** tab, policies can be created for a specific group of users, rather than network objects. FMC gets User information from Microsoft Active Directory. For more information see [Identity Services Engine Passive Identity Connector (ISE-PIC)](#).

Step 12. **Content Filtering.** In the **Applications** tab, application detectors can be selected based on category or alternatively, individual applications can be chosen. Requirements will differ between agencies. One agency may choose to block all content related to Facebook. This can be achieved by blocking all traffic assigned to the Facebook application category. Another branch may want to allow Facebook, but to block Facebook Games. This can be achieved by selecting the individual application detector for Facebook Games, while leaving the others alone such as Facebook Comment or Messenger. In the **Inspection** tab, a **File Policy** can be selected to limit file content through the firewall. The File Policy does not have to include malware, it could be a rule that blocks all files of a particular type, such as .exe.



Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Application Filters C Clear All Filters ✕

Search by name

- User-Created Filters
- Risks (2 Selected)

□ Very Low	1245
□ Low	872
□ Medium	994
☑ High	284
☑ Very High	162

- Business Relevance (Any Selected)

Available Applications (446) C

Search by name

All apps matching the filter
100Bao
AcFun
Addictive Mobility
Adult Friend Finder
Adult World
AJP
Amazon Cloud Player

Viewing 1-100 of 446

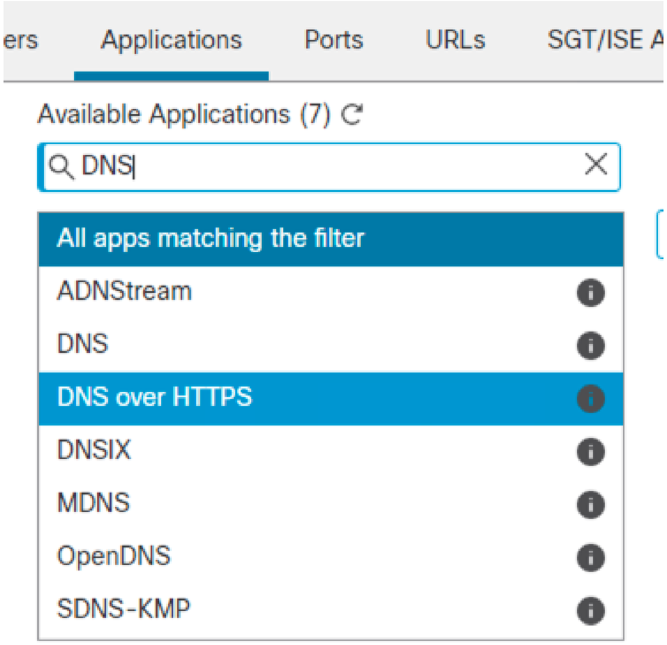
Add to Rule

Selected Applications and Filters (1)

Filters

Risks: High, Very High

Step 13. **DNS-over-HTTPS Filtering.** In the **Applications** tab, there is an application detector for **DNS over HTTPS**. Add this to the list of blocked applications to ensure DNS traffic is not encrypted.



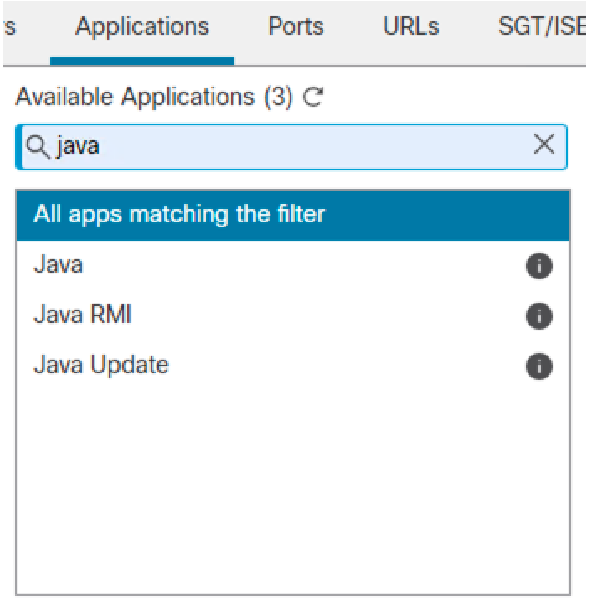
ers Applications Ports URLs SGT/ISE A

Available Applications (7) C

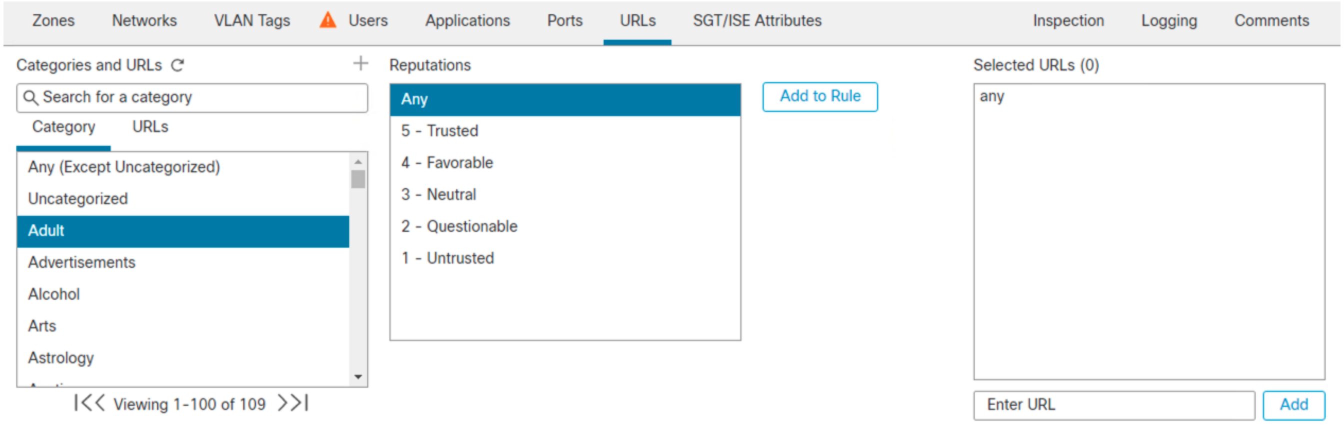
DNS

All apps matching the filter
ADNStream
DNS
DNS over HTTPS
DNSIX
MDNS
OpenDNS
SDNS-KMP

Step 14. **Active Content Mitigation.** In the **Applications** tab, there is an application detector for **Java.** Add this to the list of blocked applications to block any Java activity from passing the firewall. Alternatively, monitor the traffic and respond to any unusual activity.



Step 15. **Domain Category and Reputation Filtering.** In the **URLs** tab, domains can be blocked based on category and/or by reputation. For example, your agency may block all **Adult** traffic with **Any** reputation, however, may only block **Shopping** with **Questionable** or **Untrusted** reputation.



Step 16. **Intrusion Protection System**. In the **Inspection** tab, choose the Intrusion Policy rules that apply to the organization. For details on setting custom Intrusion rules, see the section above on Intrusion Policies.

Step 17. When all access policies have been added and ordered appropriately, make sure to **Save** and **Deploy**.

Remote User

This guide will take you through a sample configuration, specific to the devices used in this lab. More information on alternate deployments may be found here;

- Remote Access VPNs for Firepower Threat Defense
- Remote Access VPNs for ASA
- Secure Remote Worker Design Guide for AWS
- Secure Remote Worker Design Guide for Azure

FTD Remote Access VPN

Pre-requisites

- FMC is deployed and is managing the FTD device
- A RADIUS server group object exists for primary authentication. For purposes of this design guide, ISE will be used as the identity store
- Download the latest AnyConnect image files from Cisco Software Download Center
- All devices are appropriately licensed. For more information, see VPN Licensing
- Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

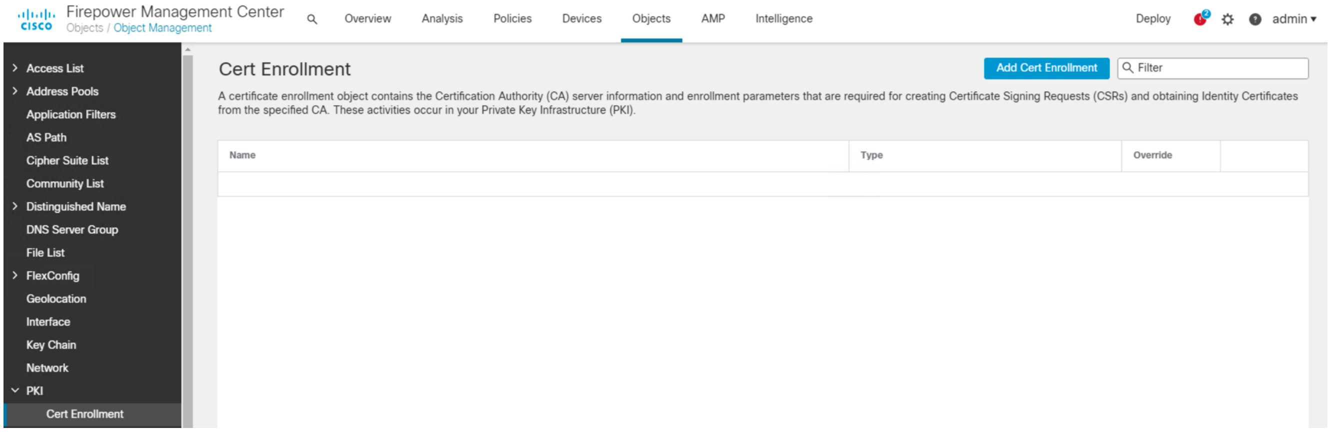
For a comprehensive guide to configure Remote Access VPN on Cisco Secure Firewall devices see Remote Access VPNs for Firepower Threat Defense.

Add Identity Certificate to FTD Device

The example configuration installed a certificate using Self-Signed Enrollment. For other alternatives, such as using a Trusted Certificate Authority (CA) see Firepower Threat Defense Certificate-Based Authentication.

Step 1. In FMC, navigate to **Object > Object Management > PKI > Cert Enrollment.**

Step 2. Click **Add Cert Enrollment.**

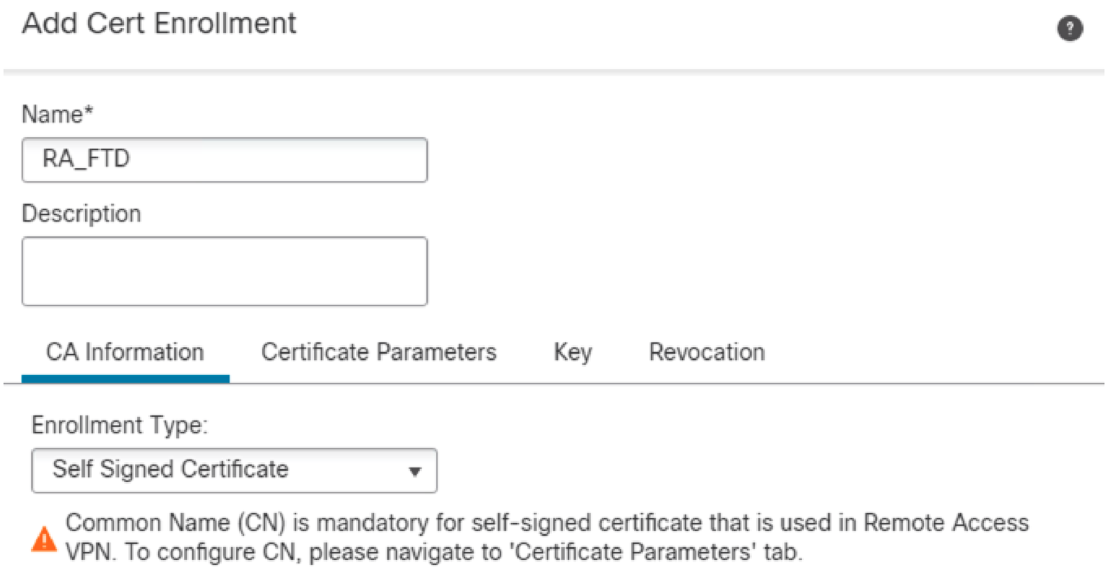


Cert Enrollment

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI).

Name	Type	Override

Step 3. Add a meaningful **Name** and optional **Description.** In the **CA Information** tab choose **Self Signed Certificate** in the **Enrollment Type** dropdown menu.



Add Cert Enrollment

Name*

RA_FTD

Description

Enrollment Type:

Self Signed Certificate

⚠ Common Name (CN) is mandatory for self-signed certificate that is used in Remote Access VPN. To configure CN, please navigate to 'Certificate Parameters' tab.

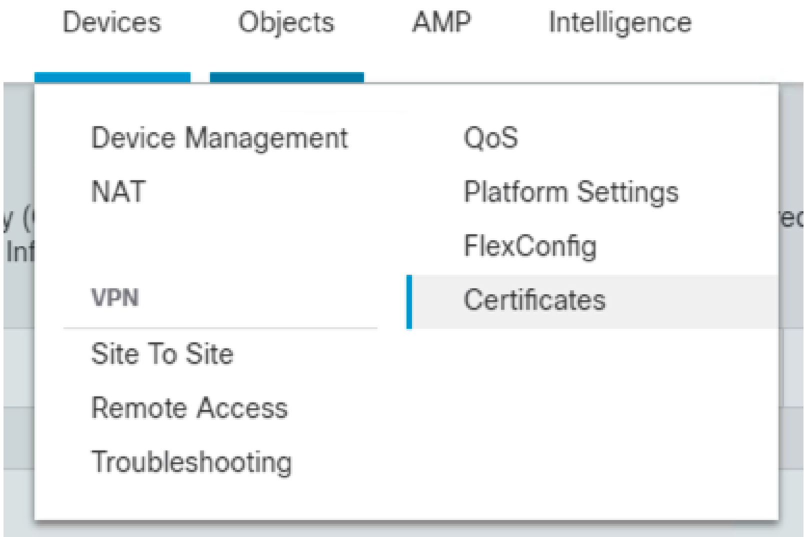
Step 4. In the **Certificate Parameters** tab, specify the certificate contents. **NOTE: Common Name (CN) is mandatory for self-signed certificates in remote access VPN.**

Step 5. Optional: Open the **Key** tab and specify the Key information. For more information click the hyperlink at start of this section.

Step 6. Optional: Click the Revocation tab and specify the revocation options. For more information click the hyperlink at start of this section.

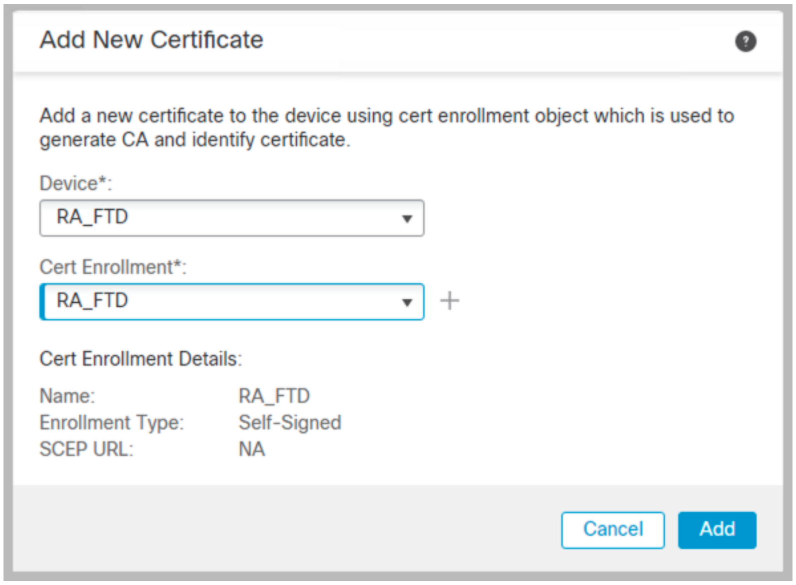
Step 7. Click **Save**.

Step 8. In FMC, navigate to **Devices > Certificates**.



Step 9. Click **Add**.

Step 10. Choose the Firepower device that shall be used for remote access in the **Device** dropdown. Choose the associated certificate in the **Cert Enrollment** dropdown.



Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*: RA_FTD

Cert Enrollment*: RA_FTD

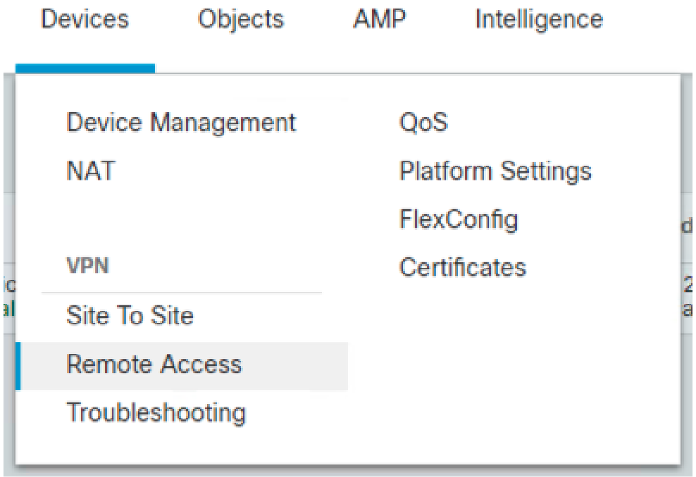
Cert Enrollment Details:

Name: RA_FTD
Enrollment Type: Self-Signed
SCEP URL: NA

Step 11. Click **Add**.

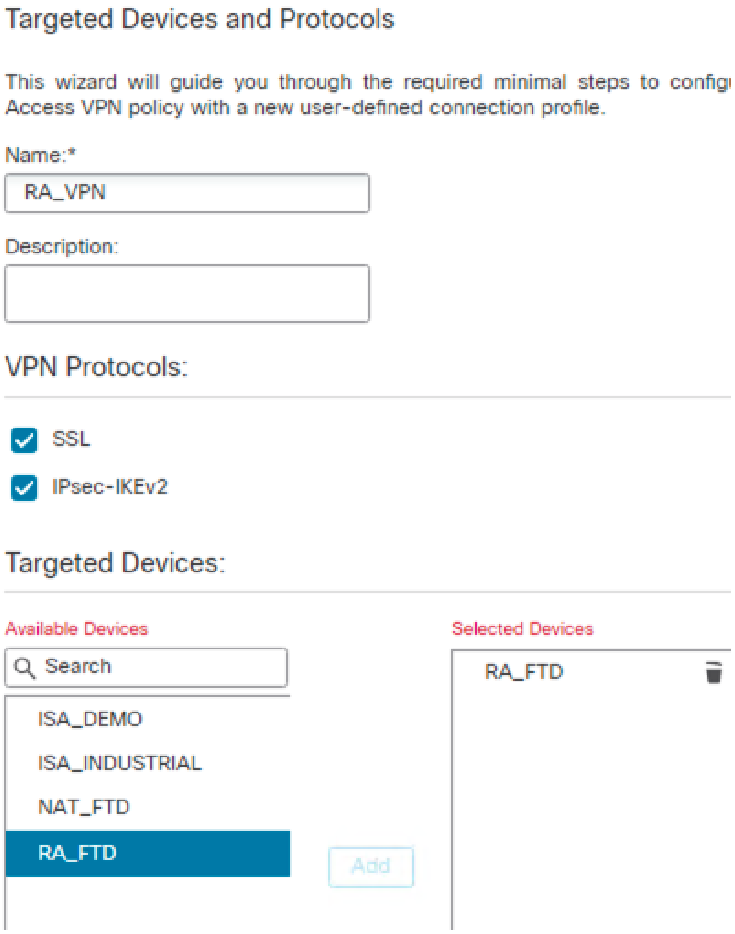
Using the Remote Access VPN Policy Wizard in FMC

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



Step 2. To create a new policy, click **Add.**

Step 3. Give a meaningful name to the configuration and **select the device(s)** that will be used for remote access. Click **next.**



Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configu
Access VPN policy with a new user-defined connection profile.

Name:* RA_VPN

Description:

VPN Protocols:

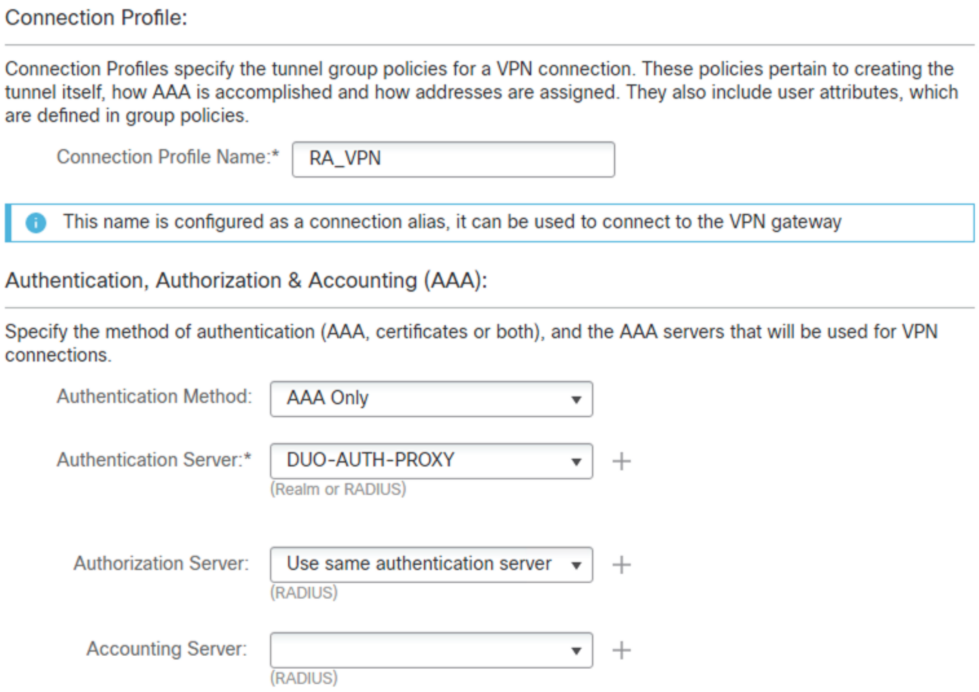
☑ SSL

☑ IPsec-IKEv2

Targeted Devices:

Step 4. Choose the **Authentication Method**. This setup uses **AAA only** as it will also be protected by Duo MFA in later steps. If running a deployment where MFA does not exist (not recommended), using certificates is another way for protecting the system from exposed user credentials.

Step 5. Choose the **Authentication Server**. This guide uses the Duo Authentication Proxy as the authentication server. See the next section on Duo for configuration options.



Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:* RA_VPN

This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

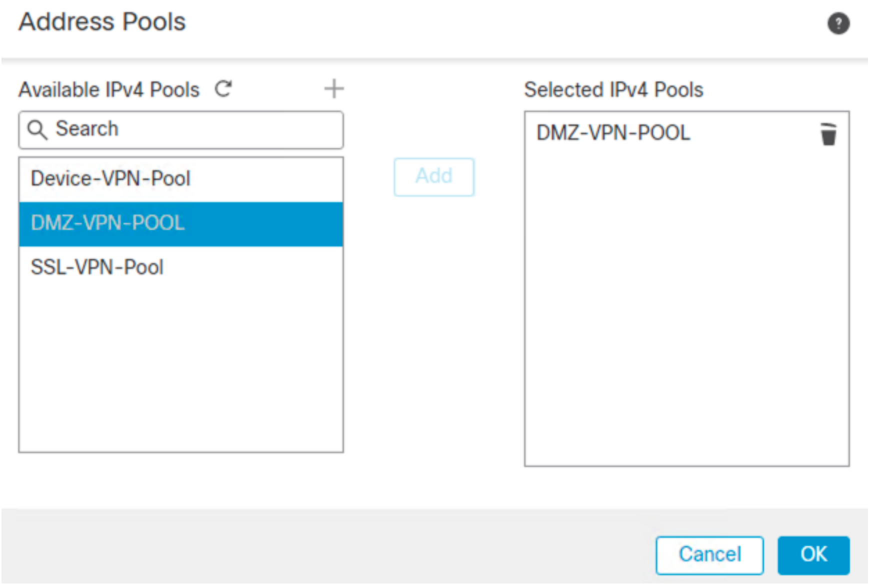
Authentication Method: AAA Only

Authentication Server:* DUO-AUTH-PROXY (Realm or RADIUS)

Authorization Server: Use same authentication server (RADIUS)

Accounting Server: (RADIUS)

Step 6. Assign the IP address pool for VPN users. Click the **pencil icon** beside IPv4 address pools. **Add** all of the address pools that will be assigned to a VPN user on the network. If the address pool has not already been created, click **+** and specify the range of addresses that will be assigned to VPN users. Make sure to give a meaningful name to this address pool. Repeat for IPv6 if desired.



Address Pools

Available IPv4 Pools

Device-VPN-Pool

DMZ-VPN-POOL

SSL-VPN-Pool

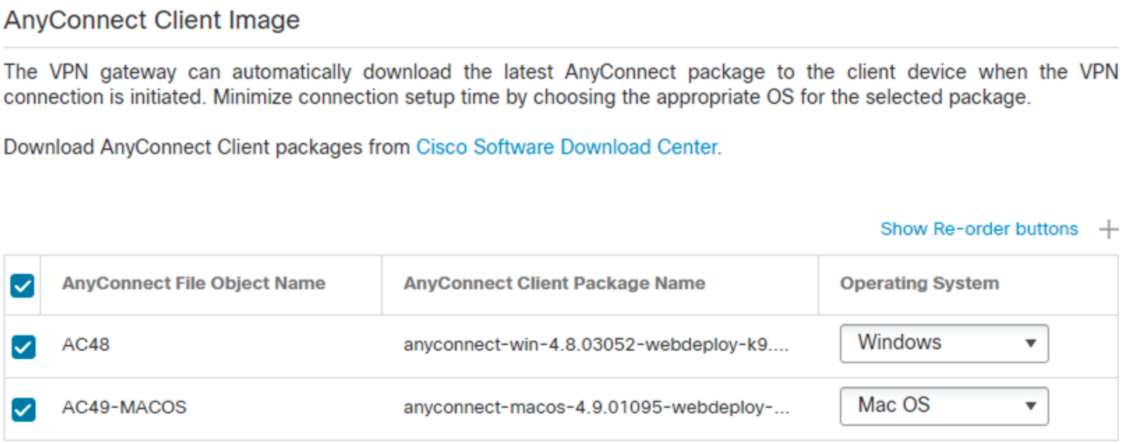
Selected IPv4 Pools

DMZ-VPN-POOL

Step 7. Assign a Group Policy. At this stage, we will create a new default policy that will be modified in later steps of this document. Click **+** beside the dropdown menu. Assign a meaningful name and click **Save**.

Step 8. Click **next** at bottom of the screen.

Step 9. Upload the latest AnyConnect image both each OS that will connect to the network using the **+** button. The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated.



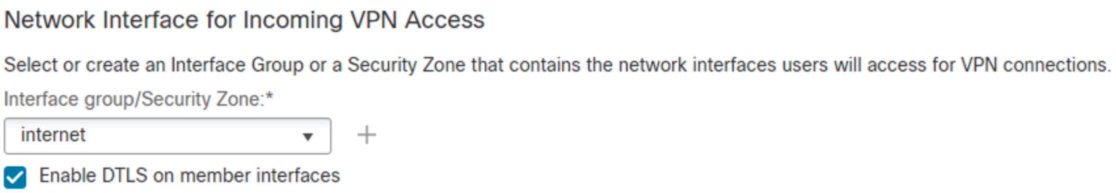
AnyConnect Client Image

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.

☑	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
☑	AC48	anyconnect-win-4.8.03052-webdeploy-k9....	Windows ▾
☑	AC49-MACOS	anyconnect-macos-4.9.01095-webdeploy-...	Mac OS ▾

Step 10. Tell the policy wizard which interface on the FTD is the outside interface, or in other words, the interface users will use to connect over VPN.



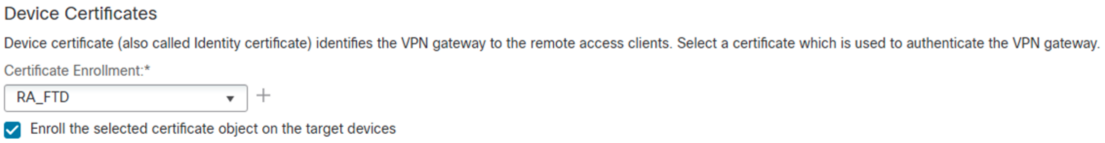
Network Interface for Incoming VPN Access

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:* internet ▾ +

☑ Enable DTLS on member interfaces

Step 11. Add the device certificate created in a previous step.



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.

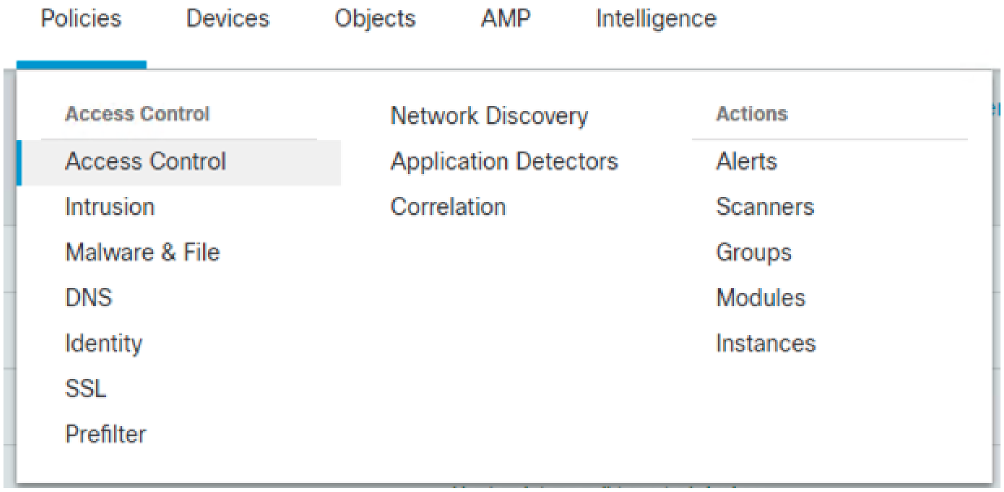
Certificate Enrollment:* RA_FTD ▾ +

☑ Enroll the selected certificate object on the target devices

Step 12. Review the configuration before clicking **Finish**. **Note: the subsequent configuration steps will be detailed in the next part of this document, however, FMC does detail the additional configuration requirements before the remote VPN will work.**

Create Access Policy

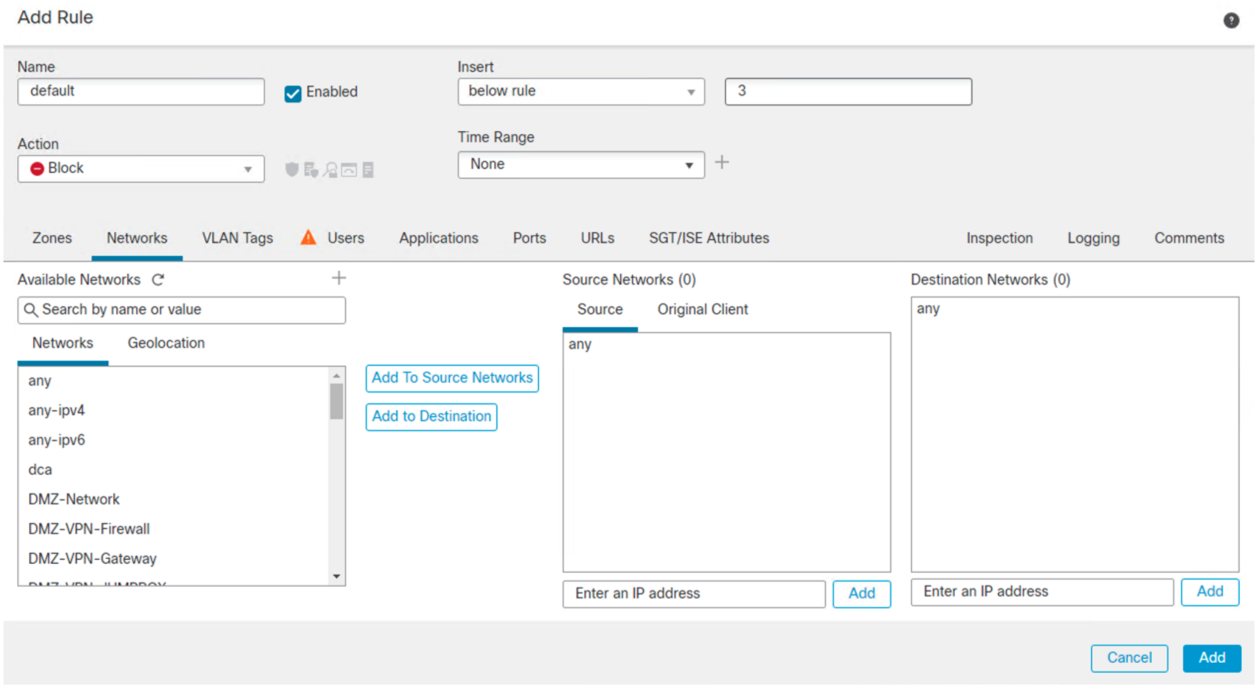
Step 1. Navigate to **Policies > Access Control > Access Control**.



Step 2. Edit the policy attached to the FTD assigned for remote access VPN by clicking the **pencil icon**.

Step 3. At this stage the policies you assign will be dependent on the security controls that are to be put in place. For specific functionality that can be applied to the firewall, navigate to the DIA section of the Branch use case. Since this is a zero-trust deployment model, and we want to follow the principle of least privilege, we will deny all users by default and then add allow policies on top of that. Click **+ Add Rule** to create a rule specific to VPN users.

Step 4. Give a meaningful name to the policy. Change the **Action** to **Block**.



Add Rule

Name: default

☑ Enabled

Insert: below rule ▾ 3

Action: ● Block ▾

Time Range: None ▾ +

Zones | Networks | VLAN Tags | ⚠ Users | Applications | Ports | URLs | SGT/ISE Attributes | Inspection | Logging | Comments

Available Networks C +

Search by name or value

Networks | Geolocation

- any
- any-ipv4
- any-ipv6
- dca
- DMZ-Network
- DMZ-VPN-Firewall
- DMZ-VPN-Gateway

Source Networks (0)

Source | Original Client

any

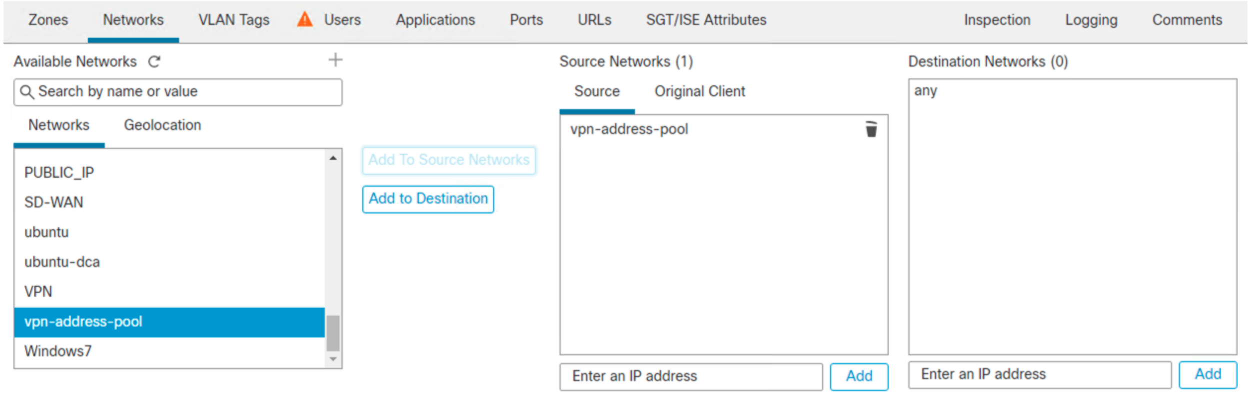
Enter an IP address — Add

Destination Networks (0)

any

Enter an IP address — Add

Step 5. For subsequent rules, in the **Networks** tab, add the VPN address pool for VPN users into the **source network** column. This means that the policy will match to any traffic originating from an IP address of a VPN user.



Zones | Networks | VLAN Tags | ⚠ Users | Applications | Ports | URLs | SGT/ISE Attributes | Inspection | Logging | Comments

Available Networks C +

Search by name or value

Networks | Geolocation

- PUBLIC_IP
- SD-WAN
- ubuntu
- ubuntu-dca
- VPN
- vpn-address-pool
- Windows7

Source Networks (1)

Source | Original Client

vpn-address-pool

Enter an IP address — Add

Destination Networks (0)

any

Enter an IP address — Add

Step 6. In the **Logging** tab, click **Log at Beginning of Connection** to ensure any attempted connections are logged.

Step 7. Click **Save**.

NAT Exemption

SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for AnyConnect image download. NAT-Traversal will be enabled by default and will use port 4500. Please ensure that these ports are not used in NAT Policy or other services before deploying the configuration.

For testing purposes, the FTD was connected directly to a public IP address so a NAT exemption policy was not needed. For more information visit Configure NAT Exemption.

DNS Policy

To resolve hostname specified in AAA Servers or CA Servers, configure DNS using FlexConfig Policy on the targeted devices. For testing purposes, all servers were addressed using their IP addresses within a private lab environment. If your network makes use of domain names, visit Configure DNS.

Split Tunnel

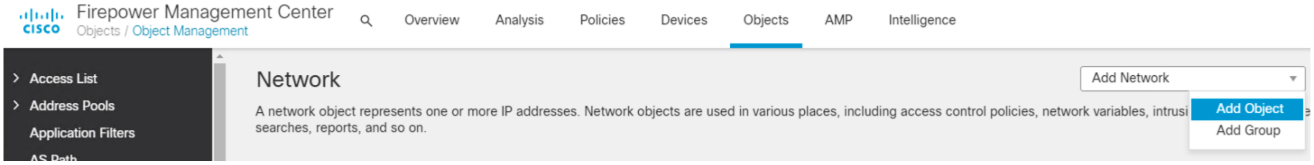
By default, all traffic is sent down the VPN tunnel. This is one of the deployments that is recommended by CISA for TIC protections, so if that is the desired outcome this becomes an optional step.

Static Split Tunnel

In this example we will create a rule that only sends internal traffic back to the data center. Static split tunneling is not recommended, but since it's a quick configuration option we will show its deployment.

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

Step 2. Create a network object using the **Add network > Add object** dropdown button for each network range that belongs to the internal network. The example below uses the network range 10.10.0.0/24.

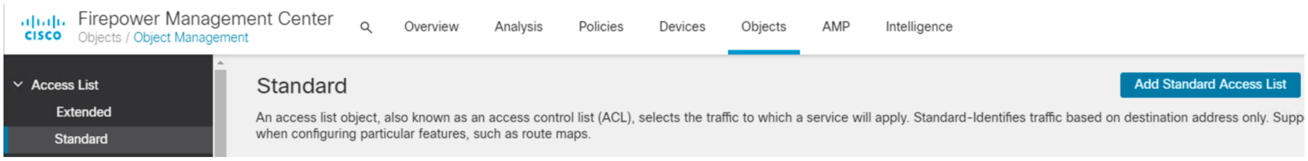


A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusi
searches, reports, and so on.

Step 3. If you have created more than one network object, create a network group using the **Add network > Add group** dropdown button and add all of the network objects from the previous step.

Step 4. Now that network objects have been created, navigate to **Object > Object Management > Access List > Standard**.

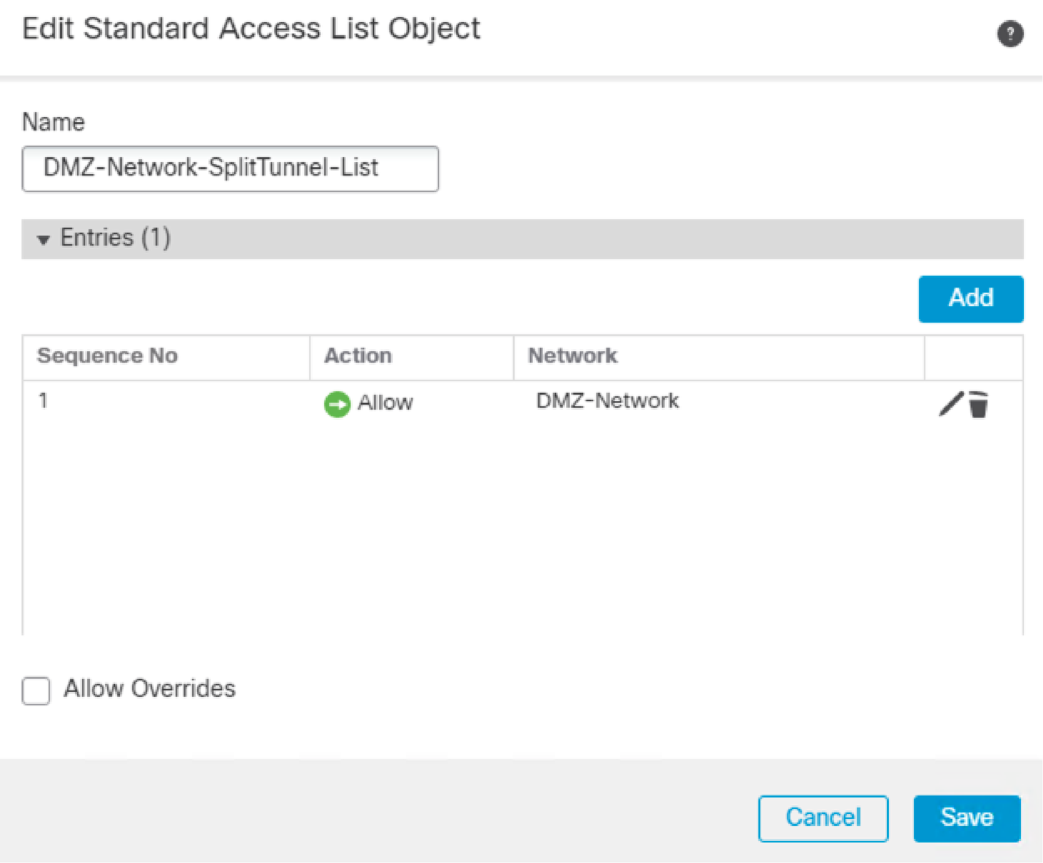
Step 5. Click **Add Standard Access List**.



An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on destination address only. Supp
when configuring particular features, such as route maps.

Step 6. Give a meaningful name to the entry and click **Add** to add the network group/object from the previous step.

Step 7. After adding all the network elements, click **Save**.



Edit Standard Access List Object

Name: DMZ-Network-SplitTunnel-List

Entries (1)

Sequence No	Action	Network
1	Allow	DMZ-Network

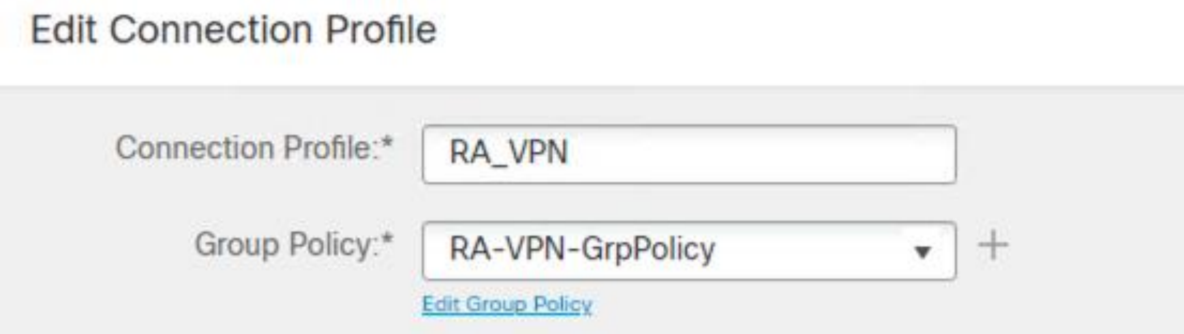
□ Allow Overrides

Step 8. Navigate to **Devices > VPN > Remote Access**.

Step 9. Click the **pencil icon** to edit the remote access vpn configuration that this split tunnel will apply to.

Step 10. Click the **pencil icon** to edit the remote access vpn connection profile that is used for this configuration.

Step 11. Click on **Edit Group Policy**.



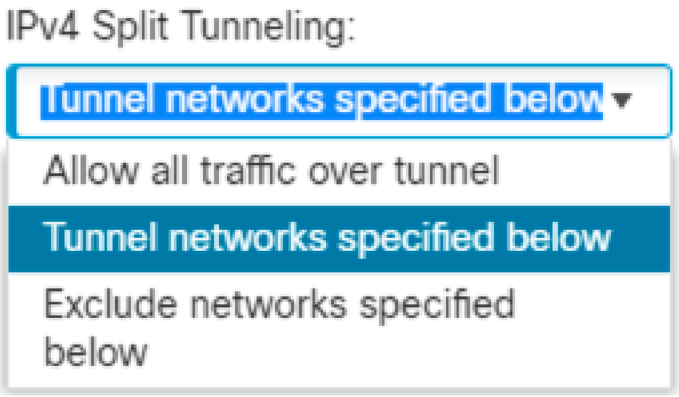
Edit Connection Profile

Connection Profile:* RA_VPN

Group Policy:* RA-VPN-GrpPolicy

Step 12. Navigate to **General > Split Tunneling**.

Step 13. Under **IPv4 Split Tunneling** choose **Tunnel networks specified below**. This is because we will only send internal traffic through the tunnel. In the dynamic split tunnel configuration, we will do the opposite, and choose networks not to send down the tunnel.

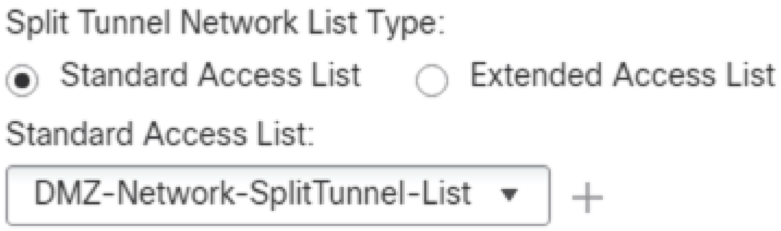


IPv4 Split Tunneling:

Tunnel networks specified below ▾

- Allow all traffic over tunnel
- Tunnel networks specified below
- Exclude networks specified below

Step 14. Click Split Tunnel **Network List Type > Standard Access List** checkbox and select the access list created in a previous step using the **Standard Access List** dropdown.



Split Tunnel Network List Type:

● Standard Access List ○ Extended Access List

Standard Access List:

DMZ-Network-SplitTunnel-List ▾ +

Step 15. Under **DNS Request Split Tunneling**, choose **Always send DNS requests over tunnel** unless you have another means of logging all DNS requests from roaming users (such as using Umbrella DNS as your DNS resolver).

Step 16. Click **Save** to save the group policy and then click **Save** again to save the VPN policy.

Step 17. **Deploy** all changes that were made so that policies can take effect.

Dynamic Split Tunnel

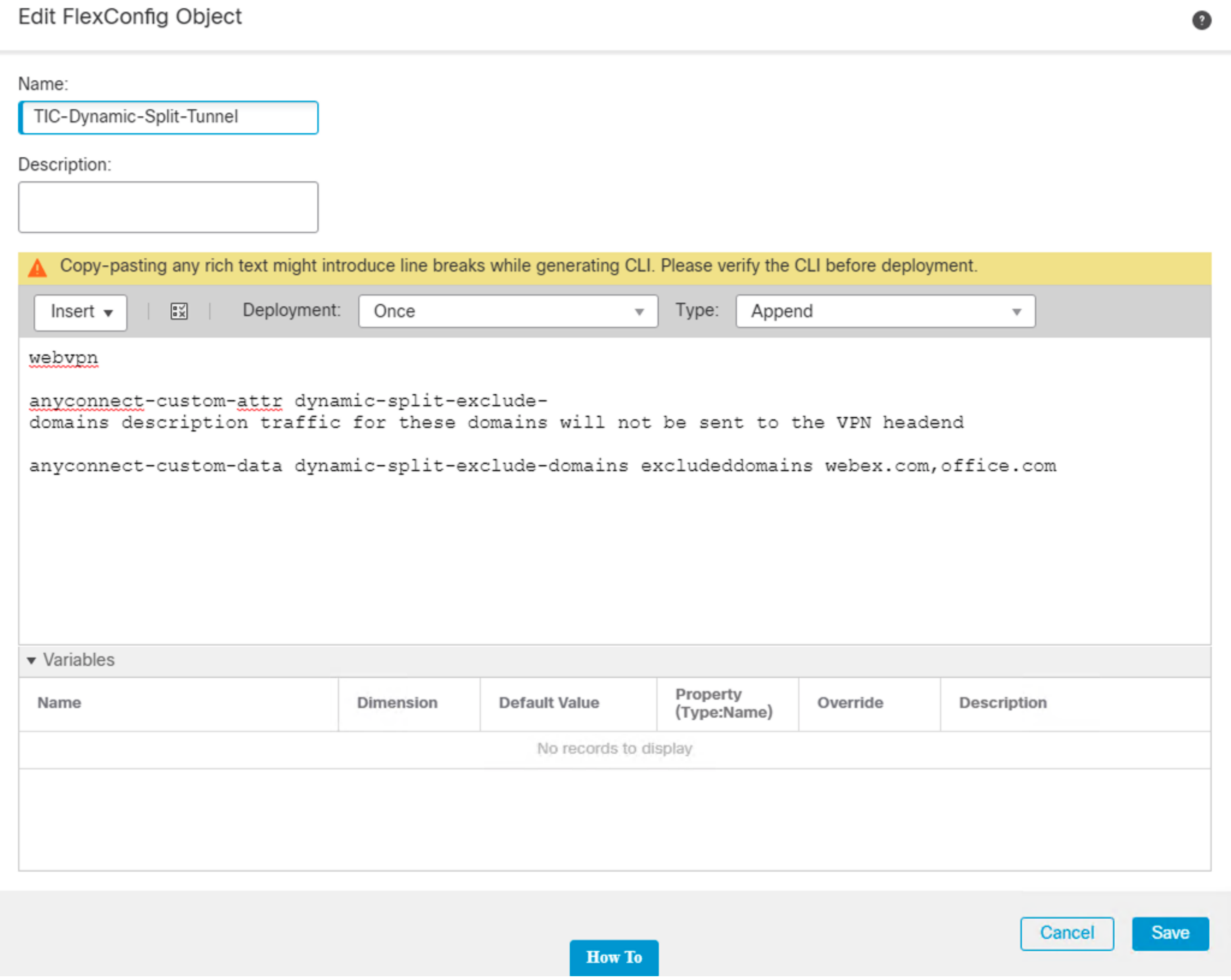
Dynamic split tunneling is more suitable to TIC since we want to break out trusted internet connections from the tunnel and typically not based on IP but on domain names. Dynamic split tunneling in FTD is done using FlexConfigs. Dynamic split tunnel configuration is based on creating a custom AnyConnect attribute of the type dynamic-split-exclude-domains, then adding that attribute to the group policies used in your RA VPN connection profiles. For more information, and for configuration options that deviate from this example, see Advanced AnyConnect VPN Deployments for Firepower Threat Defense with FMC.

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

Step 2. Click **Add FlexConfig Object**.

Step 3. Give a meaningful name to the configuration and insert an **object body** similar to below (this example shows how to split traffic destined to webex.com and office.com). Keep **deployment** and **type** as default (**Once** and **Append** respectively). **Note: the description is optional, but if included, it is not a separate command but part of the anyconnect-custom-attr command. For the domain names, separate them with a comma but do not include spaces.**

```
webvpn
 anyconnect-custom-attr dynamic-split-exclude-domains description traffic for these domains will not be sent to the VPN headend
 anyconnect-custom-data dynamic-split-exclude-domains excludeddomains webex.com,office.com
```



Name: TIC-Dynamic-Split-Tunnel

Description:

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment: Once

Type: Append

```
webvpn
anyconnect-custom-attr dynamic-split-exclude-
domains description traffic for these domains will not be sent to the VPN headend
anyconnect-custom-data dynamic-split-exclude-domains excludeddomains webex.com,office.com
```

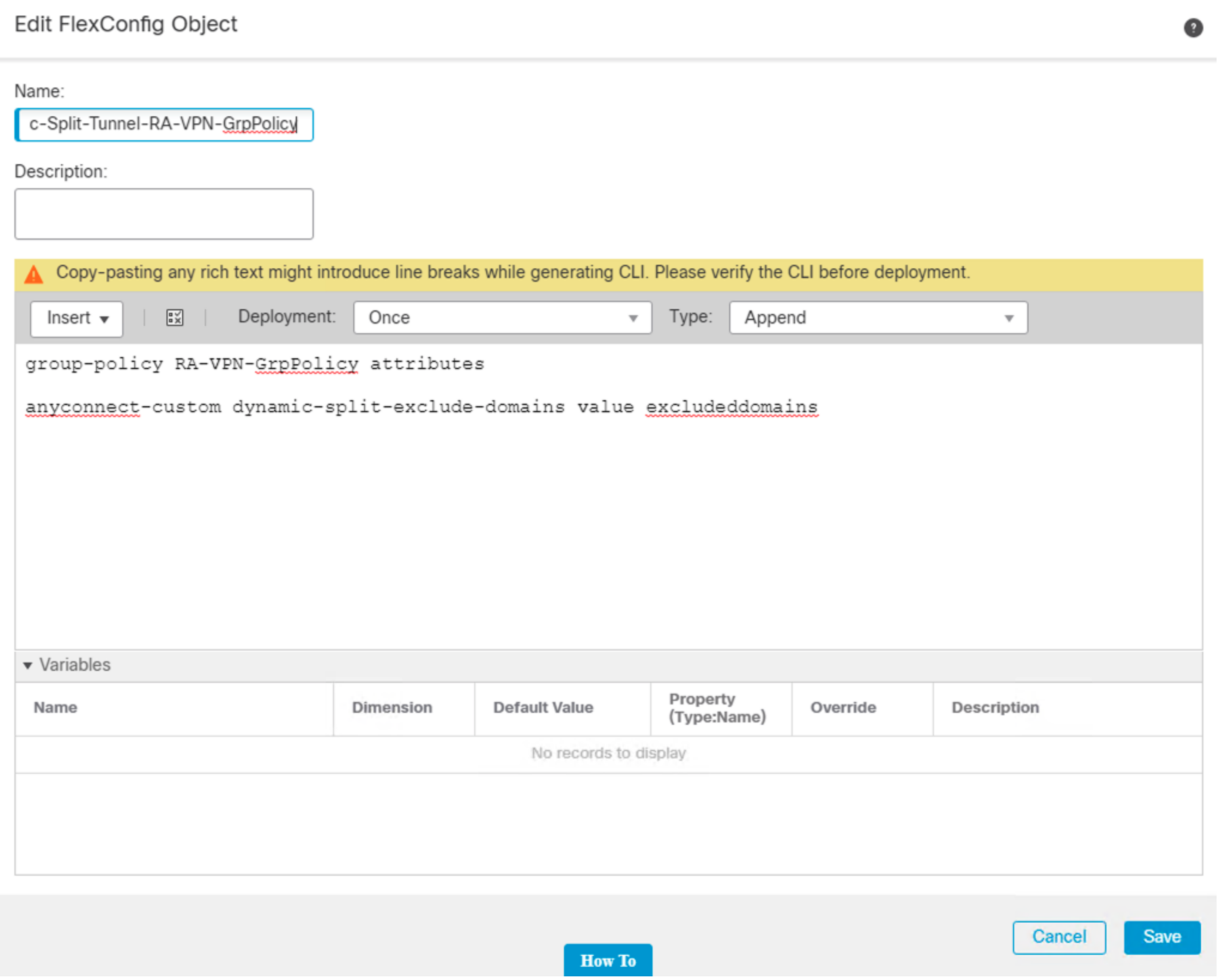
Variables

Name	Dimension	Default Value	Property (Type:Name)	Override	Description
No records to display					

Step 4. Click **Save**.

Step 5. Since we are using a custom group policy in our VPN configuration, we are going to reference that policy within this FlexConfig. On the FlexConfig Objects, click **Add FlexConfig Object.** Give a meaningful name to the configuration and insert an object body similar to below (this example references a group policy called RA-VPN-GrpPolicy). Keep **deployment** and **type** as default (**Once** and **Append** respectively).

```
group-policy RA-VPN-GrpPolicy attributes
   anyconnect-custom dynamic-split-exclude-domains value excludeddomains
```


Edit FlexConfig Object
Name:
c-Split-Tunnel-RA-VPN-GrpPolicy
Description:
Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.
Insert
Deployment:
Once
Type:
Append
Variables
Cancel
Save
How To

```
group-policy RA-VPN-GrpPolicy attributes

anyconnect-custom dynamic-split-exclude-domains value excludeddomains
```

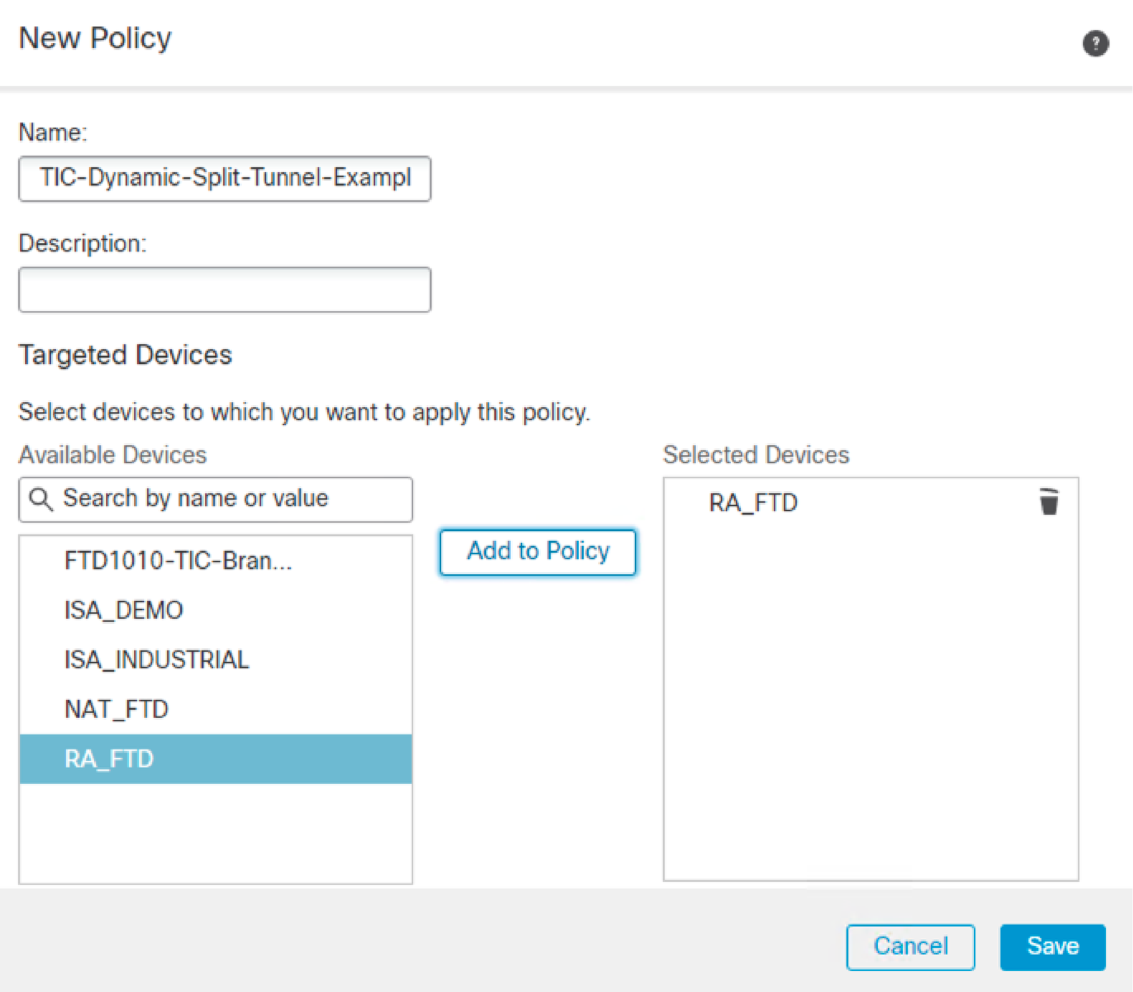
Name	Dimension	Default Value	Property (Type:Name)	Override	Description
No records to display					

Step 6. Click **Save**.

Step 7. Create the FlexConfig object that will deploy the above policies. In FMC, navigate to **Devices > FlexConfig**.

Step 8. Click **New Policy**.

Step 9. Add a meaningful name to the policy and add the FTD device that will be used for remote access. Click **Save**.



New Policy

Name: TIC-Dynamic-Split-Tunnel-Exampl

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Search by name or value

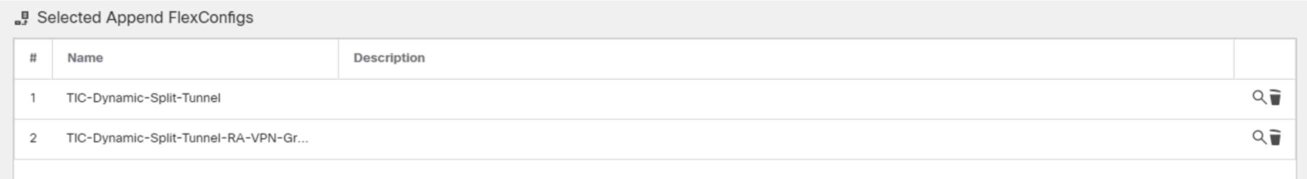
- FTD1010-TIC-Bran...
- ISA_DEMO
- ISA_INDUSTRIAL
- NAT_FTD
- RA_FTD

Selected Devices

- RA_FTD

Step 10. Select the FlexConfig objects previously created from the **User Defined** column.

Step 11. Use drag and drop to ensure that the objects are in the correct order. **Note: The object that creates the custom attribute object must come before the objects that assign that attribute to the group policies. Otherwise, if you try to add a custom attribute that does not yet exist, you will get an error.**



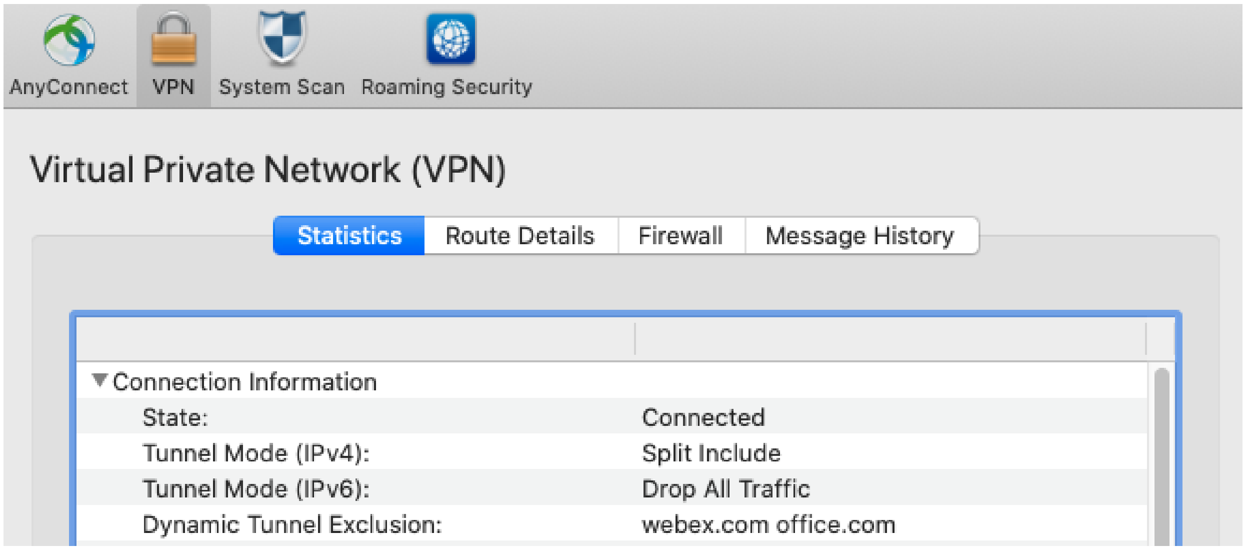
Selected Append FlexConfigs

#	Name	Description
1	TIC-Dynamic-Split-Tunnel	
2	TIC-Dynamic-Split-Tunnel-RA-VPN-Gr...	

Step 12. Click **Save**.

Step 13. **Deploy** the changes.

Step 14. To test, connect to the VPN via AnyConnect. In the **AnyConnect Statistics Window**, navigate to **Connection Information > Dynamic Tunnel Exclusion** and a list of all excluded domains will be shown in the window.



▼Connection Information

State:	Connected
Tunnel Mode (IPv4):	Split Include
Tunnel Mode (IPv6):	Drop All Traffic
Dynamic Tunnel Exclusion:	webex.com office.com

Duo Multi-Factor Authentication

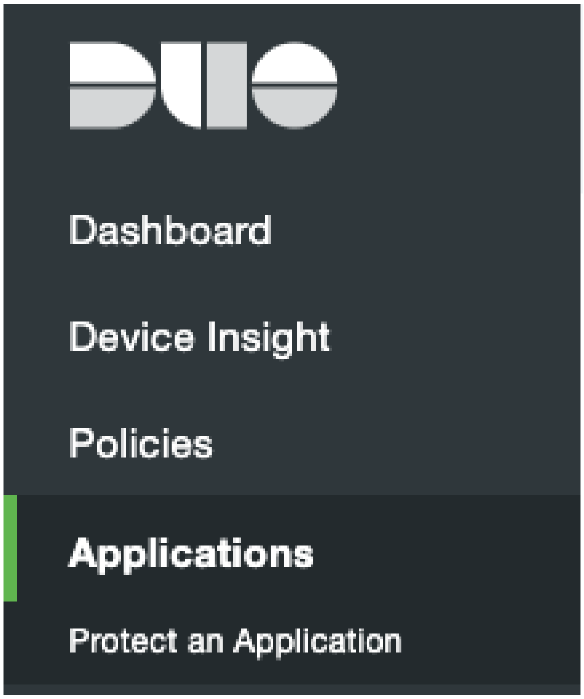
This guide will walk through a single example setup to add second factor authentication to remote access VPN users. For more details, such as how to deploy to a Cisco ASA device (which isn't covered in this guide), see the Duo documentation.

Pre-requisites

- A Duo Admin account
- Duo Authentication Proxy (install steps below) has a route to Duo Cloud, FTD and ISE (or Active Directory depending on your install)

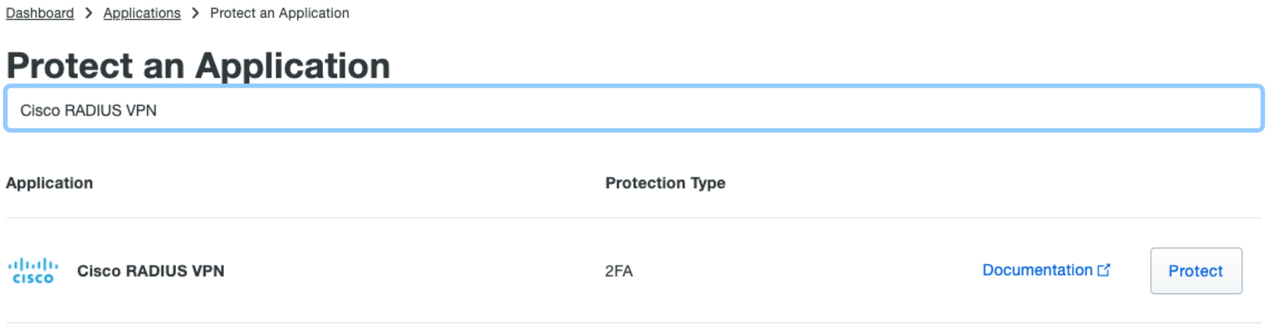
Add Application to Duo Account

Step 1. In the Duo Admin dashboard, navigate to **Applications**.



Step 2. Click **Protect an Application.**

Step 3. Search for Cisco **RADIUS** VPN and click **Protect**.


Dashboard > Applications > Protect an Application

Protect an Application

Cisco RADIUS VPN

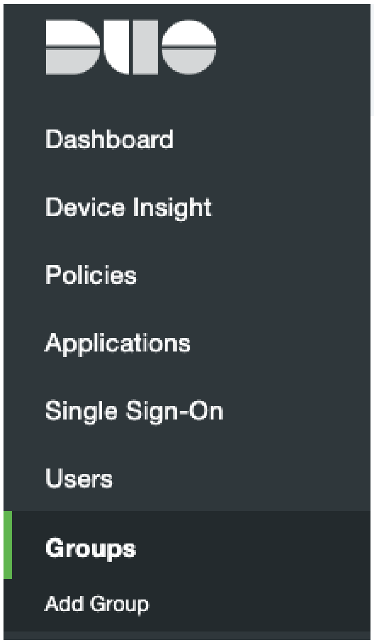
Application	Protection Type		
Cisco RADIUS VPN	2FA	Documentation	Protect

Step 4. Take note of the **Integration Key**, **Secret Key**, and **API hostname**.

Configure Duo User Groups

This setup assumes that users who require access to VPN already have their account details registered to Duo already. For more information on adding users to Duo see Enroll Users. Included in that redirect link is more information on importing an existing identity store, such as Active Directory.

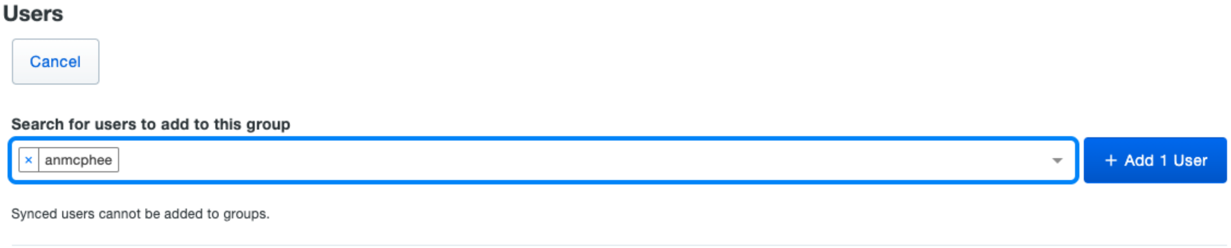
Step 1. In Duo, navigate to **Groups**.



Step 2. Click **Add Group**.

Step 3. Add a meaningful name to the group and an optional description before clicking **Save**.

Step 4. Using the **+ Add User to Group** button, add all of the users who require access to the VPN. Click **Save Changes** when all users have been added.

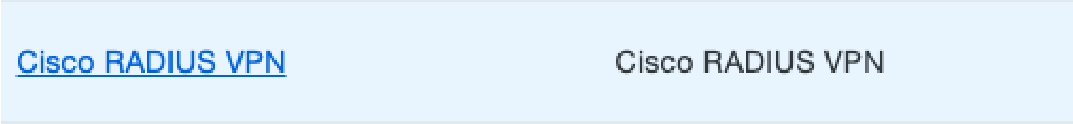

Users

Search for users to add to this group

× anmcphee

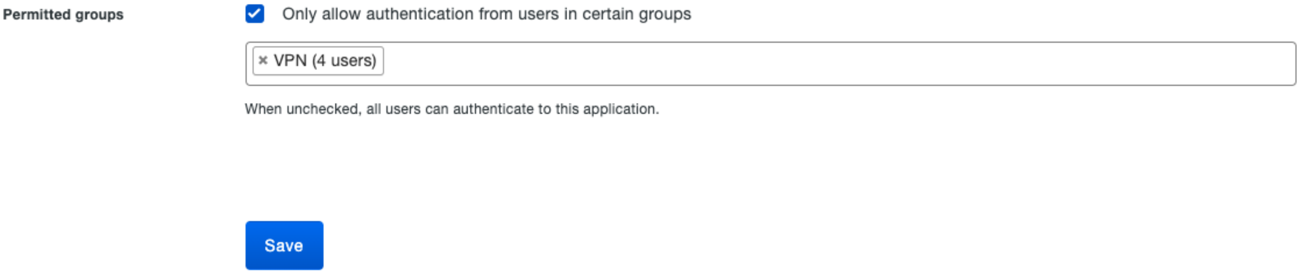
Synced users cannot be added to groups.

Step 5. Navigate to **Applications** and click on **Cisco RADIUS VPN**.



Cisco RADIUS VPN Cisco RADIUS VPN

Step 6. Scroll down to **permitted groups** and click the checkbox to **Only allow authentication from users in certain groups**. **Add** the VPN user group that was created in the previous step. This results in only allowing users who have been added to VPN group, instead of all users who may be registered to this Duo account for alternate reasons. Click **Save**.



Permitted groups

☑ Only allow authentication from users in certain groups

× VPN (4 users)

When unchecked, all users can authenticate to this application.

Configure Duo Authentication Proxy

Step 1. On a windows server (must have a route to the Duo API hostname and must be reachable from the remote access FTD), install and configure the Duo Application Proxy. All instruction can be found in the Duo documentation.

The configuration used in this example can be seen below.

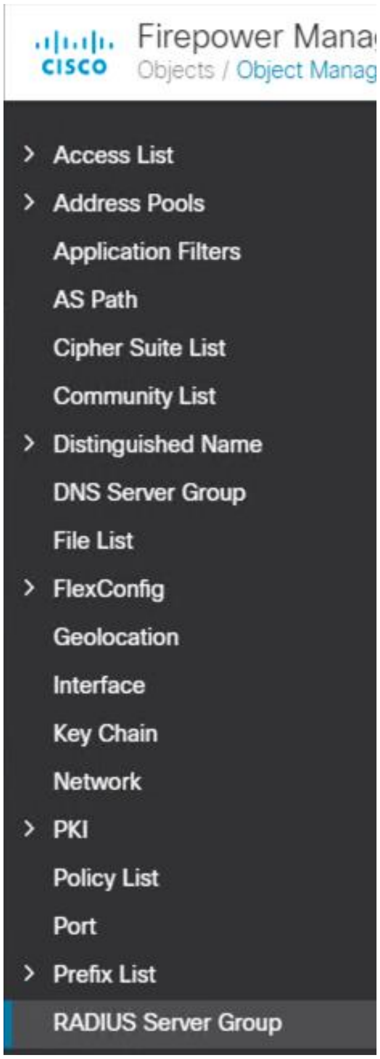
```
[duo_only_client]

[radius_client]
host=$ISE_IP
secret=$ISE_SECRET

[radius_server_auto]
ikey=$DUO_iKEY
skey=$DUO_sKEY
api_host=$DUO_HOST
radius_ip_1=$DUO_RADIUS_IP1
radius_secret_1=$DUO_SECRET1
radius_ip_2=$DUO_RADIUS_IP2
radius_secret_2=$DUO_SECRET2
failmode=safe
client=radius_client
port=1812
```

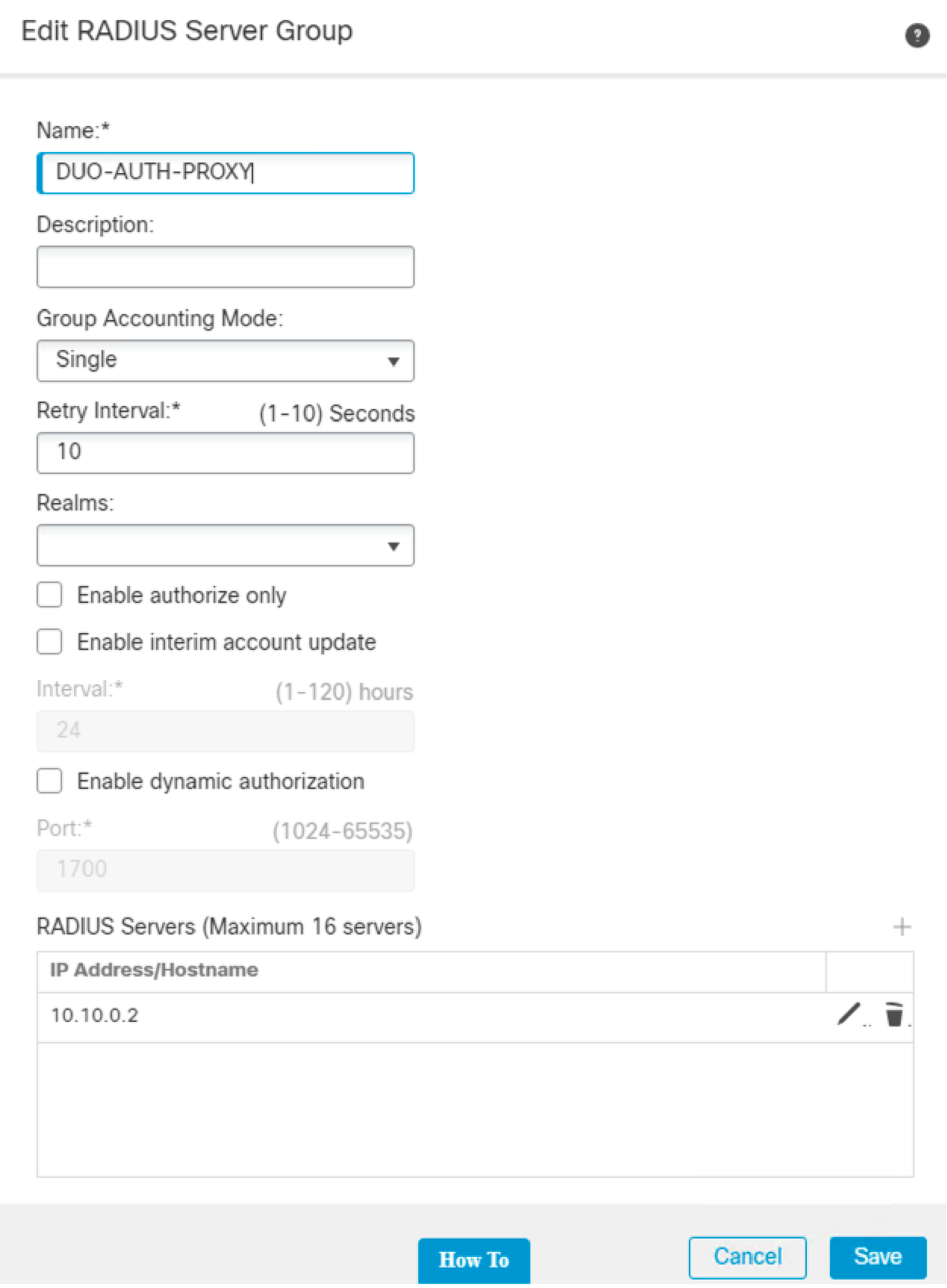
Add Duo Authentication Proxy to VPN Configuration

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



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

Step 3. Add a meaningful **name** and add the **IP address** that the Duo Authentication Proxy can be reached. Click **Save**.



Edit RADIUS Server Group

Name:*
DUO-AUTH-PROXY

Description:

Group Accounting Mode:
Single

Retry Interval:* (1-10) Seconds
10

Realms:

□ Enable authorize only

□ Enable interim account update

Interval:* (1-120) hours
24

□ Enable dynamic authorization

Port:* (1024-65535)
1700

RADIUS Servers (Maximum 16 servers)

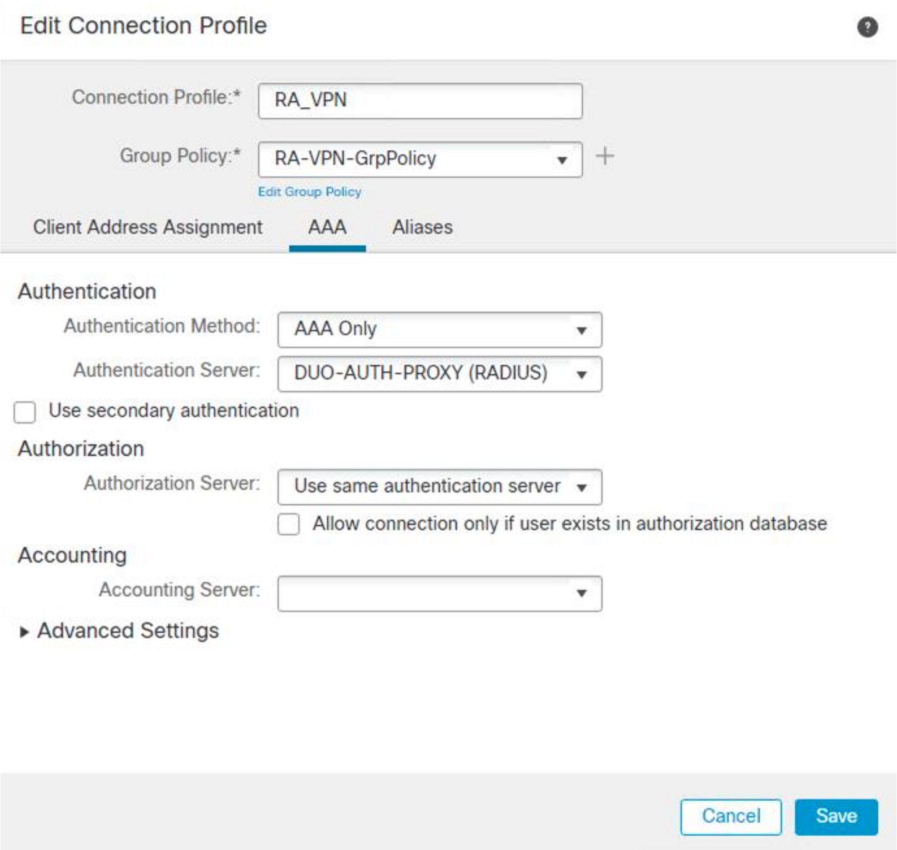
IP Address/Hostname
10.10.0.2

Step 4. In FMC, navigate to **Devices > VPN > Remote Access.**

Step 5. Click the **pencil icon** to configure the appropriate remote access VPN configuration.

Step 6. Click the **pencil icon** to configure the appropriate remote access connection profile.

Step 7. In the **AAA** tab, click the **Authentication Server** dropdown and choose the Duo Authentication Proxy RADIUS object. Click **Save.**



Edit Connection Profile

Connection Profile:* RA_VPN

Group Policy:* RA-VPN-GrpPolicy

Authentication

Authentication Method: AAA Only

Authentication Server: DUO-AUTH-PROXY (RADIUS)

□ Use secondary authentication

Authorization

Authorization Server: Use same authentication server

□ Allow connection only if user exists in authorization database

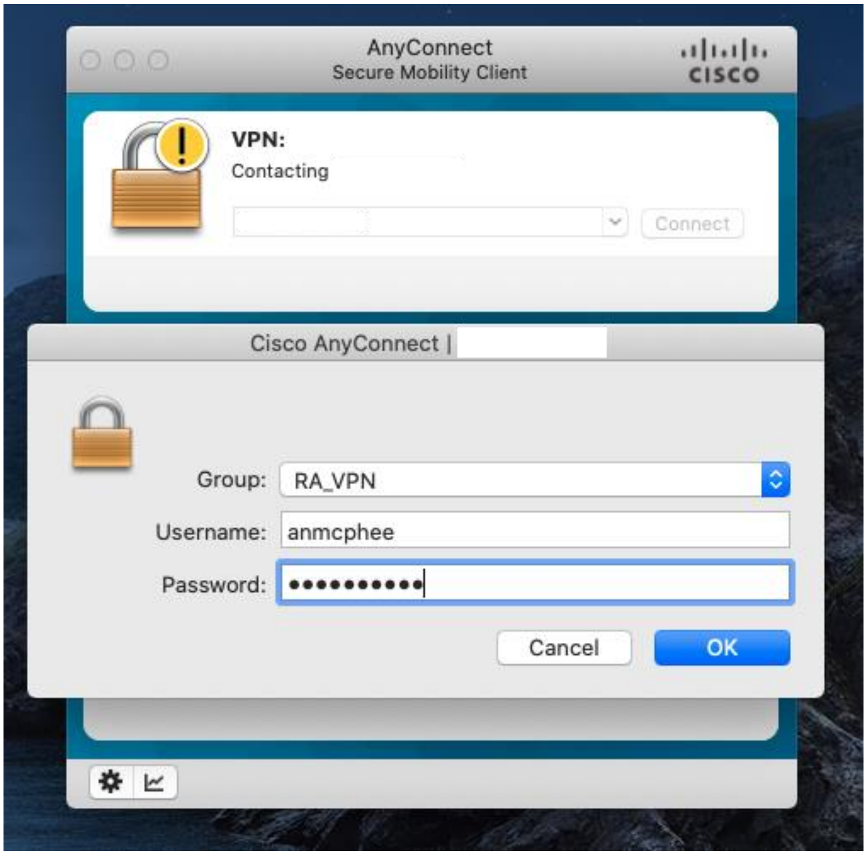
Accounting

Accounting Server:

Step 8. **Deploy** the changes.

Test the setup

Step 1. Using AnyConnect, type the FQDN/IP Address of the remote access firewall and press Connect.



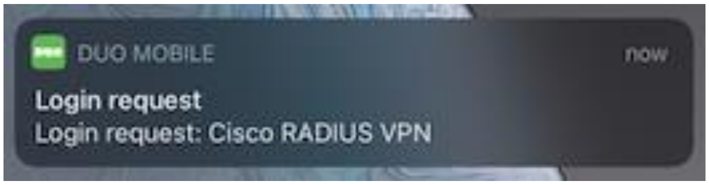
VPN:
Contacting

Cisco AnyConnect | [redacted]

Group: RA_VPN
Username: anmcphee
Password: ●●●●●●●●●●●

Step 2. Enter your username and password.

Step 3. If the credentials were accepted, a Duo prompt should have been received on the registered device. Accept the connection.


DUO MOBILE now
Login request
Login request: Cisco RADIUS VPN

Cisco AnyConnect Client Profile

The AnyConnect package includes modules for a variety of features, such as the AMP enabler, that you can optionally use to provide additional services to RA VPN connections. Each module includes a profile that you can edit to make the module work according to your requirements. To enable these modules and profiles on FTD, you need to use FlexConfig.

Create AnyConnect XML Templates

Step 1. Download and install the stand-alone AnyConnect Profile Editor (Windows only). You must also install Java JRE 6 (or higher) before installing the profile editor. Obtain the AnyConnect profile editor from software.cisco.com in the AnyConnect Secure Mobility Client category.

Step 2. Use the profile editors to create the profiles you need. For details on each of the AnyConnect options:

- VPN Profile – Enables the configuration of settings such as always on VPN or managing certificates.
- Network Visibility Module (NVM) – Use this configuration to get visibility into the device that the AnyConnect module resides on. This will be discussed further in the CESA section below.
- AMP Enabler – Used as a median for deploying AMP for endpoints.
- Umbrella Roaming Security – Provides DNS security when no VPN is active.

Step 3. Each configuration step creates a unique XML file. In a text editor of your choice and using the VPN profile XML as the master file, combine all modules into a single file. To do this, copy the full XML configuration from each configure module and place them within the **<AnyConnectProfile>** tag.

Step 4. **Save** the file.

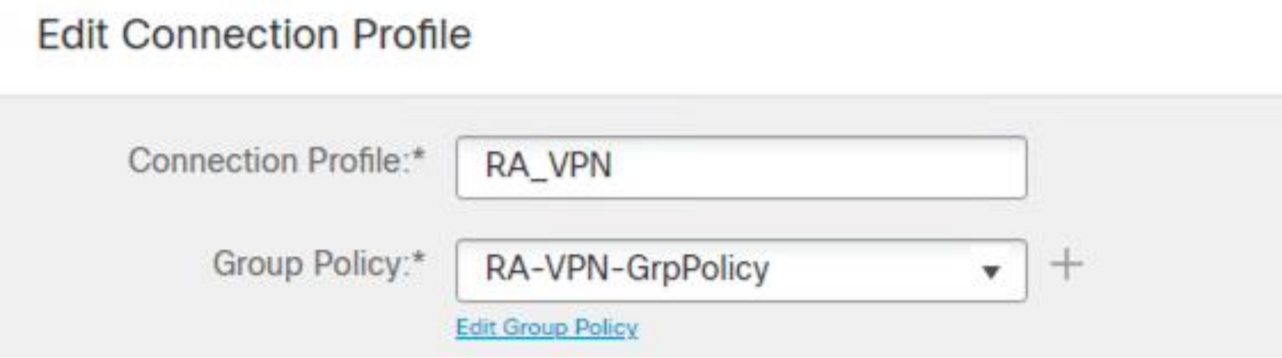
Add Template to VPN Configuration

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

Step 2. Click the **pencil icon** to edit the remote access VPN configuration that this profile will apply to.

Step 3. Click the **pencil icon** to edit the remote access VPN connection profile(s) that this configuration uses.

Step 4. Located directly under the Group Policy dropdown, click **Edit Group Policy**.

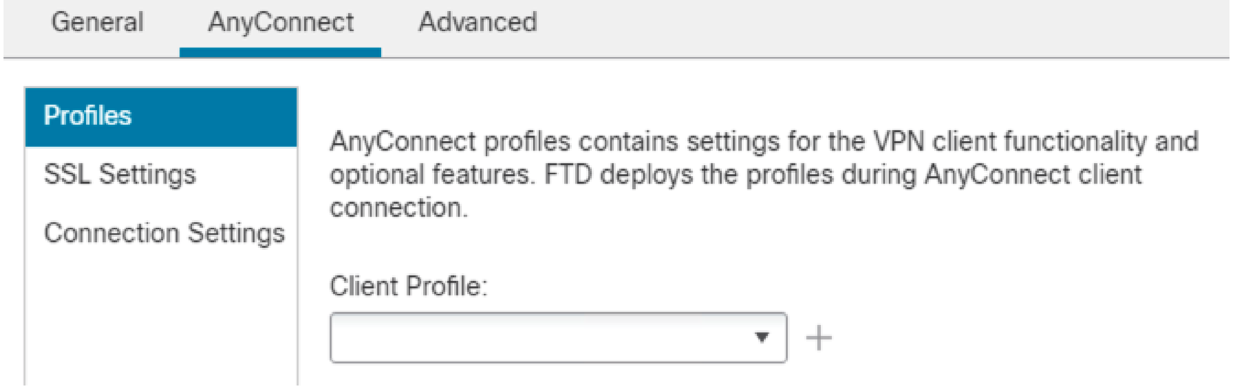


Edit Connection Profile

Connection Profile:* RA_VPN

Group Policy:* RA-VPN-GrpPolicy

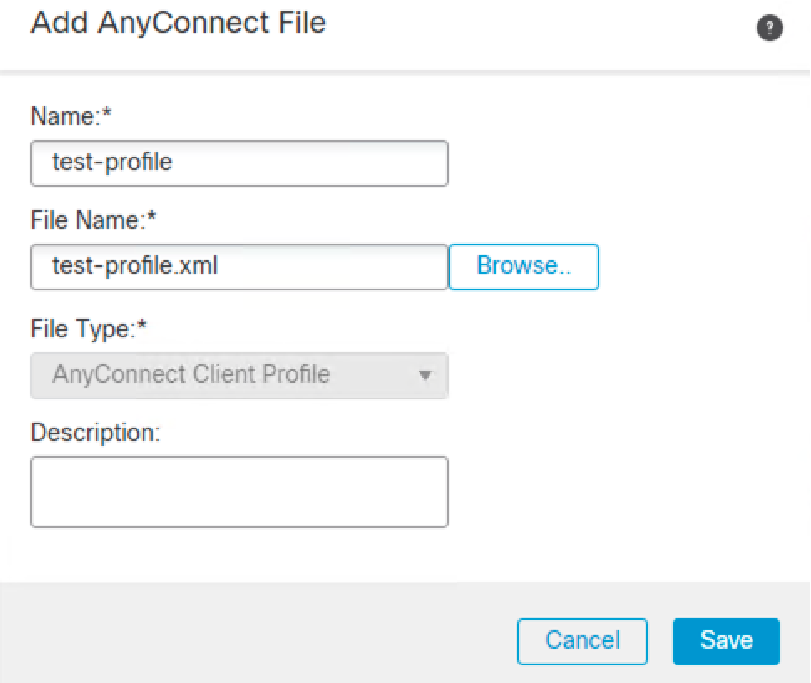
Step 5. In the **AnyConnect > Profiles** tab, click the **add (+)** button to add a new Client Profile.



AnyConnect profiles contains settings for the VPN client functionality and optional features. FTD deploys the profiles during AnyConnect client connection.

Client Profile:

Step 6. Browse for the newly created AnyConnect profile and click **Save**.



Add AnyConnect File

Name:* test-profile

File Name:* test-profile.xml

File Type:* AnyConnect Client Profile

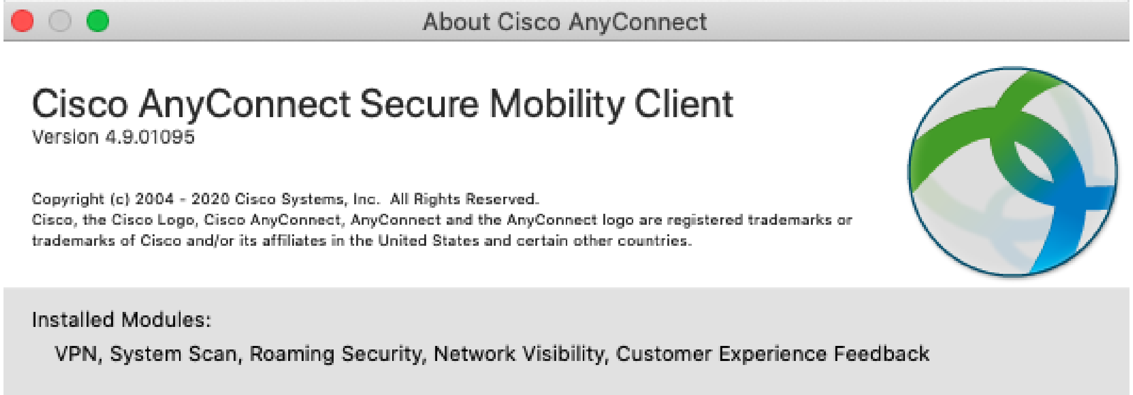
Description:

Step 7. Continue to **Save** until completion. **Deploy** the configuration.

Step 8. To test, connect to the VPN using AnyConnect.

Step 9. On the device connected via VPN, navigate to **About AnyConnect.**

Step 10. All modules installed on the device will be listed.



About Cisco AnyConnect

Cisco AnyConnect Secure Mobility Client

Version 4.9.01095

Copyright (c) 2004 - 2020 Cisco Systems, Inc. All Rights Reserved.
Cisco, the Cisco Logo, Cisco AnyConnect, AnyConnect and the AnyConnect logo are registered trademarks or trademarks of Cisco and/or its affiliates in the United States and certain other countries.

Installed Modules:
VPN, System Scan, Roaming Security, Network Visibility, Customer Experience Feedback

Cisco Endpoint Security Analytics (CESA)

Pre-requisites

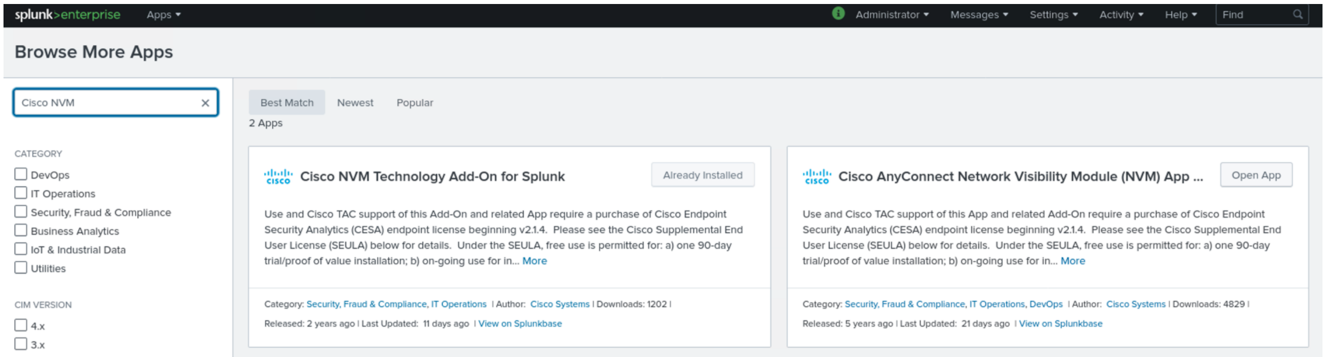
- Splunk Account
- For this specific deployment, Splunk Enterprise installed on a 64-bit Linux system.
- Cisco AnyConnect Apex license
- Cisco AnyConnect Profile Editor

Add Apps to Splunk

Step 1. In Splunk, navigate to **Apps > Find More Apps**.

Step 2. Download the following apps:

- Cisco AnyConnect Network Visibility (NVM) App for Splunk – https://splunkbase.splunk.com/app/2992/
- Cisco NVM Add-On for Splunk – https://splunkbase.splunk.com/app/4221/



2 Apps

Cisco NVM Technology Add-On for Splunk

Use and Cisco TAC support of this Add-On and related App require a purchase of Cisco Endpoint Security Analytics (CESA) endpoint license beginning v2.1.4. Please see the Cisco Supplemental End User License (SEULA) below for details. Under the SEULA, free use is permitted for: a) one 90-day trial/proof of value installation; b) on-going use for in... More

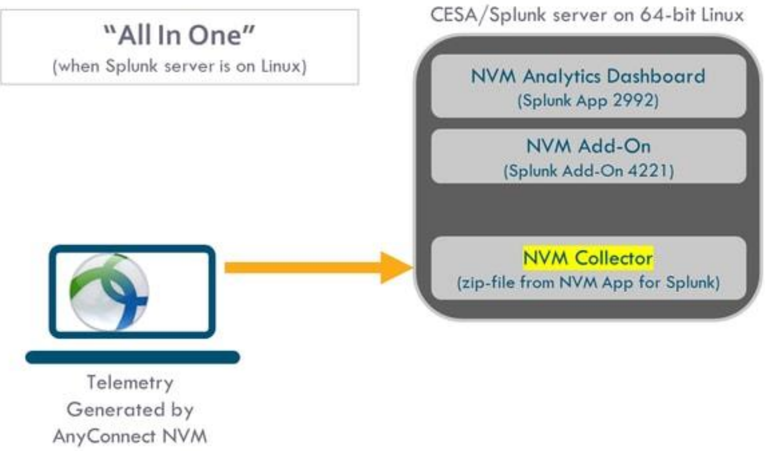
Category: Security, Fraud & Compliance, IT Operations | Author: Cisco Systems | Downloads: 1202 |
Released: 2 years ago | Last Updated: 11 days ago | View on Splunkbase

Cisco AnyConnect Network Visibility Module (NVM) App ...

Use and Cisco TAC support of this App and related Add-On require a purchase of Cisco Endpoint Security Analytics (CESA) endpoint license beginning v2.1.4. Please see the Cisco Supplemental End User License (SEULA) below for details. Under the SEULA, free use is permitted for: a) one 90-day trial/proof of value installation; b) on-going use for in... More

Category: Security, Fraud & Compliance, IT Operations, DevOps | Author: Cisco Systems | Downloads: 4829 |
Released: 5 years ago | Last Updated: 21 days ago | View on Splunkbase

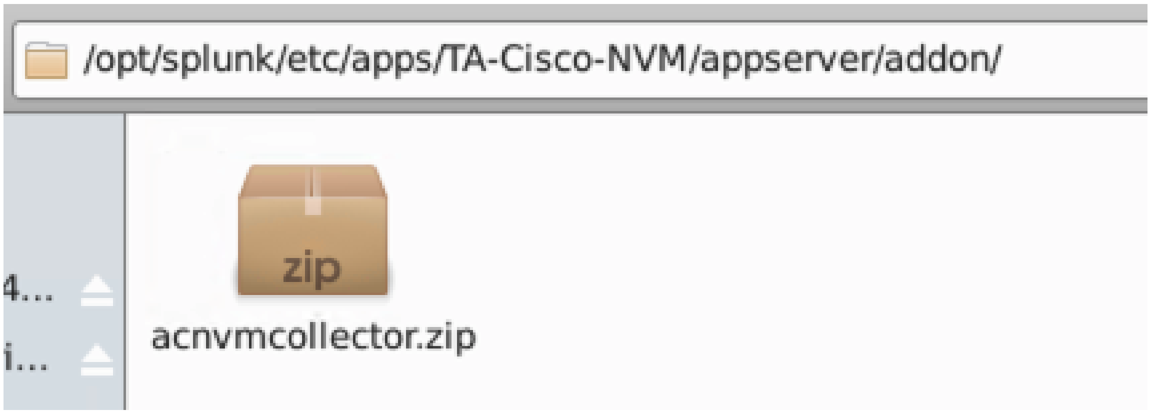
Install NVM Collector



The Collector Component is responsible for collecting and translating all IPFIX data from the endpoints and forwarding it to the Splunk Add-on. The NVM collector runs on 64-bit Linux. CentOS, Ubuntu and Docker configuration scripts are included. The CentOS install scripts and configuration files can also be used in Fedora and Redhat distributions as well.

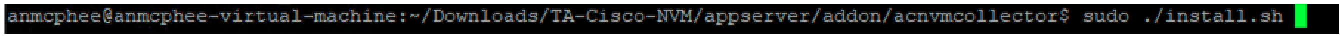
In a typical distributed Splunk Enterprise deployment, the collector should be run on either a standalone 64-bit Linux system or a Splunk Forwarder node running on 64-bit Linux. This guide shows the deployment of an 'all-in-one' configuration running on 64-bit Linux. For more information on additional installation guides see the CESA installation guide.

Step 1. In the Linux host where Splunk runs, unzip the **acnvmcollector.zip** file which is located in the **/opt/splunk/etc/apps/$APP_DIR/appserver/addon** folder.



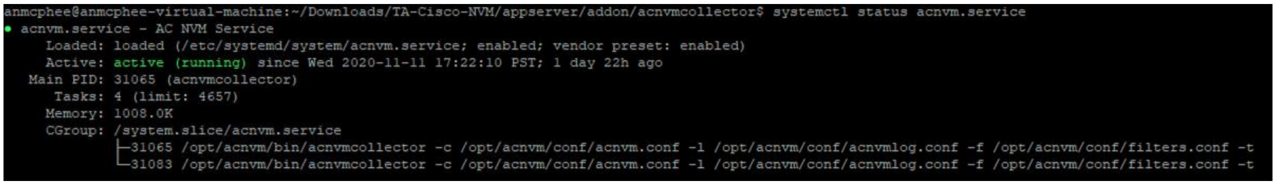
Step 2. It is recommended to read the **$PLATFORM$_README** file in the **.zip** bundle before moving on to the next step. The README file provides information on the relevant configuration settings that need to be verified and modified (if necessary). For this all-in-one deployment, the default configuration is sufficient.

Step 3. Open a terminal, navigate to the unzipped folder and run **sudo ./install.sh**.



```
anmcphee@anmcphee-virtual-machine:~/Downloads/TA-Cisco-NVM/appserver/addon/acnvmcollector$ sudo ./install.sh
```

Step 4. To verify that the collector is running successfully, run **systemctl status acnvm.service**.

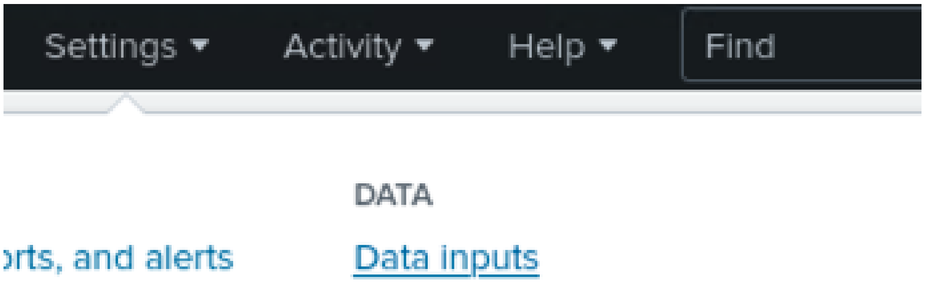


```
anmcphee@anmcphee-virtual-machine:~/Downloads/TA-Cisco-NVM/appserver/addon/acnvmcollector$ systemctl status acnvm.service
● acnvm.service - AC NVM Service
   Loaded: loaded (/etc/systemd/system/acnvm.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2020-11-11 17:22:10 PST; 1 day 22h ago
 Main PID: 31065 (acnvmcollector)
    Tasks: 4 (limit: 4657)
   Memory: 1008.0K
   CGroup: /system.slice/acnvm.service
           ├─31065 /opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/conf/filters.conf -t
           └─31083 /opt/acnvm/bin/acnvmcollector -c /opt/acnvm/conf/acnvm.conf -l /opt/acnvm/conf/acnvmlog.conf -f /opt/acnvm/conf/filters.conf -t
```

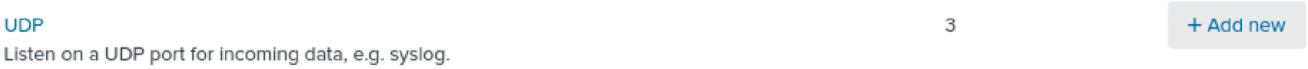
Enable UDP Inputs using Splunk Web

The default collector configuration uses UDP ports 20519, 20520 and 20521 to send data to Splunk. If the configuration changed in the above step, the port numbers listed here will have to change accordingly.

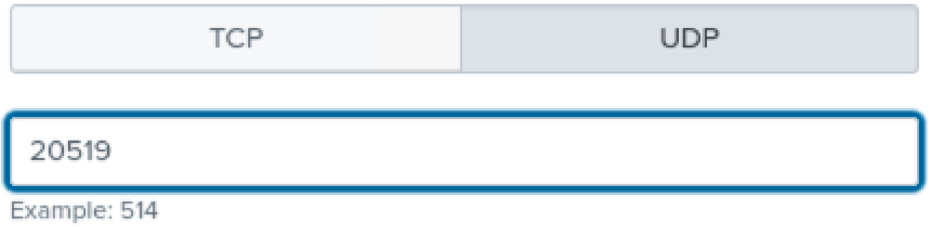
Step 1. In Splunk, navigate to **Settings > Data > Data Inputs.**



Step 2. Click **+ Add new** in the **UDP** row.



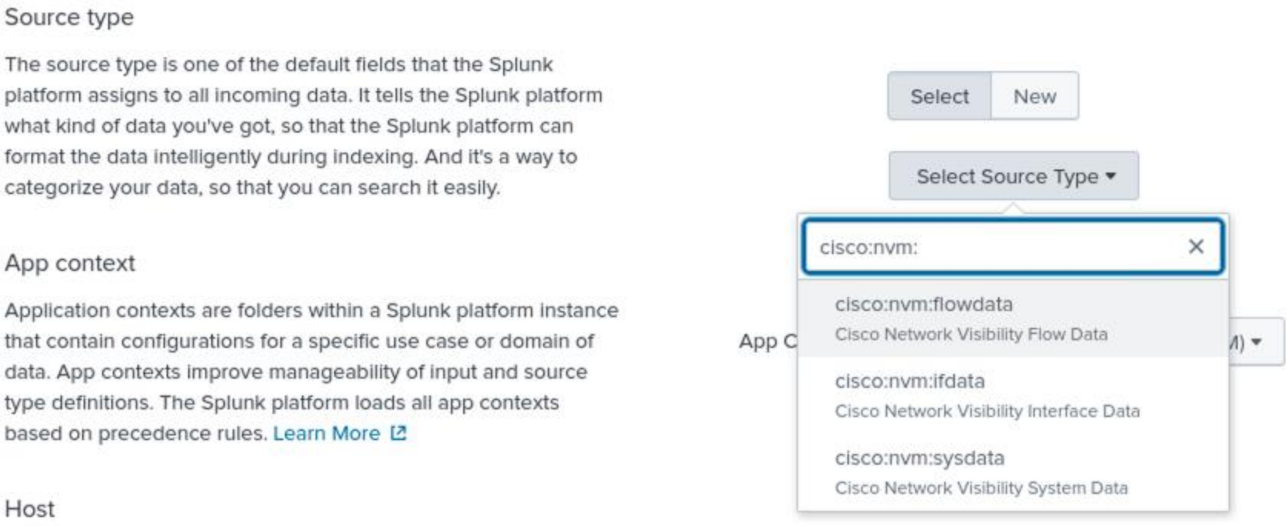
Step 3. Ensuring **UDP** is selected, enter **20519** into **Port**. Click **Next**.



Port ? 20519

Example: 514

Step 4. In the **Select Source Type** dropdown enter **cisco:nvm:flowdata.** Click **Review.**



Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More

Host

cisco:nvm: ✕

cisco:nvm:flowdata
Cisco Network Visibility Flow Data

cisco:nvm:ifdata
Cisco Network Visibility Interface Data

cisco:nvm:sysdata
Cisco Network Visibility System Data

Step 5. Click **Submit.**

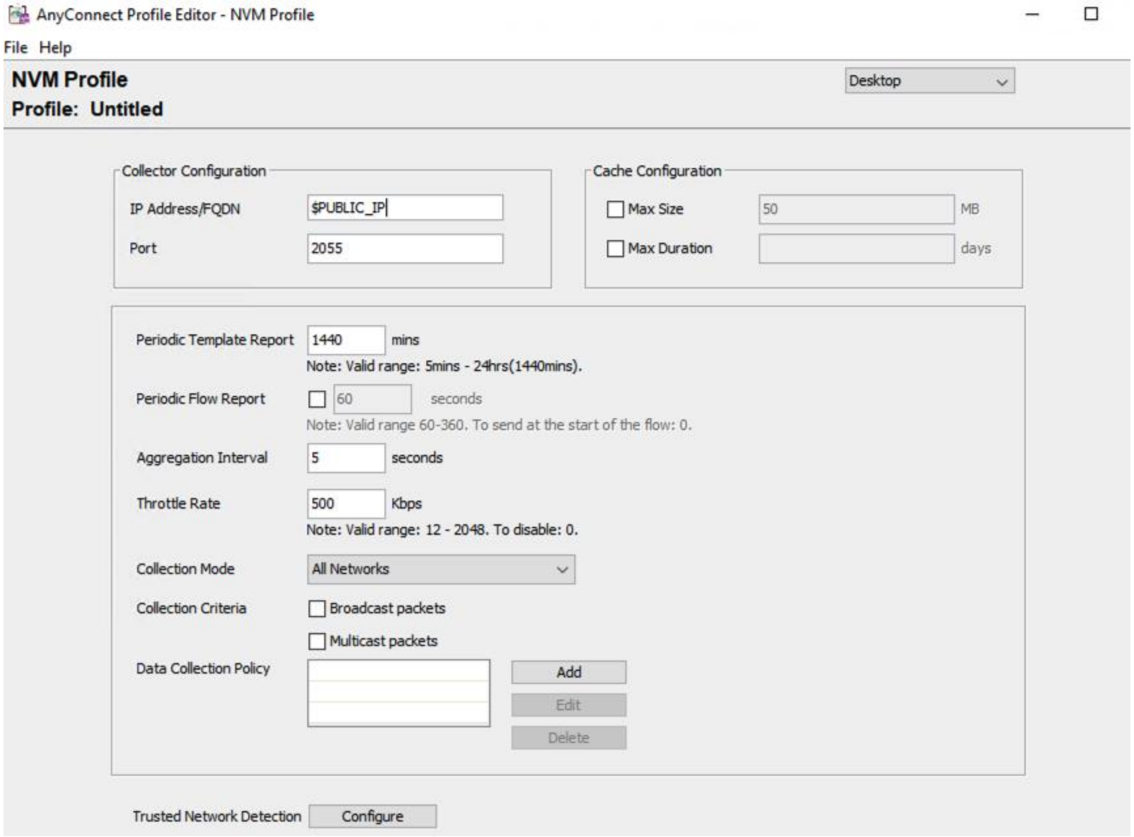
Step 6. Repeat steps 2 – 5 with the following mapping

- Port: **20520** | Source Type: **cisco:nvm:sysdata**
- Port: 20521 | Source Type: cisco:nvm:ifdata

Add Splunk Collector to AnyConnect Profile

The Cisco AnyConnect Secure Mobility Client software package contains a profile editor for all operating systems. If using a Cisco ASA in your VPN deployment, Cisco Adaptive Security Device Manager (ASDM) activates the profile editor when you load the AnyConnect client image on the ASA. As this deployment is using a Cisco Firepower device, the standalone AnyConnect Profile Editor will be used.

Step 1. In the AnyConnect NVM Profile Editor, enter the **IP Address/FQDN** and the **Port** that the collector is listening on. The default port is **2055** but it will depend on the configuration you did above.



NVM Profile
Profile: Untitled

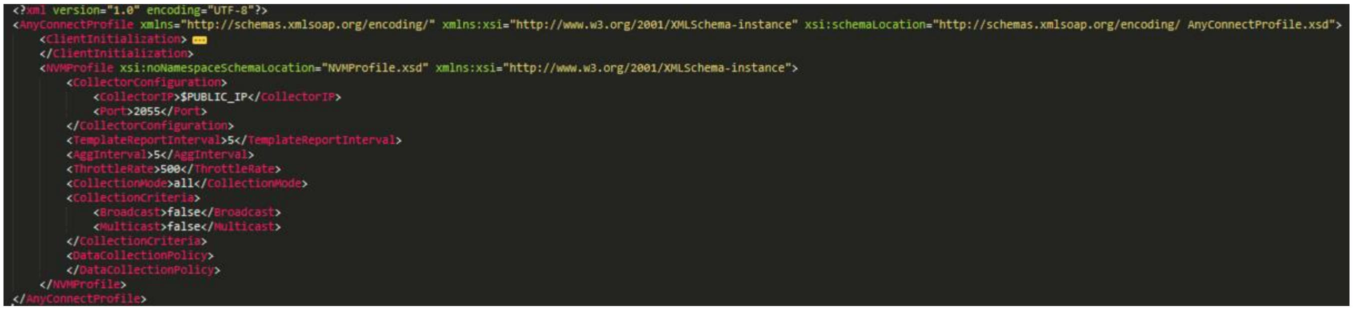
Collector Configuration
IP Address/FQDN: $PUBLIC_IP
Port: 2055

Cache Configuration
□ Max Size: 50 MB
□ Max Duration: days

Periodic Template Report: 1440 mins
Note: Valid range: 5mins - 24hrs(1440mins).
Periodic Flow Report: □ 60 seconds
Note: Valid range 60-360. To send at the start of the flow: 0.
Aggregation Interval: 5 seconds
Throttle Rate: 500 Kbps
Note: Valid range: 12 - 2048. To disable: 0.
Collection Mode: All Networks
Collection Criteria: □ Broadcast packets
□ Multicast packets
Data Collection Policy
Trusted Network Detection

Step 2. By default, the NVM collector will collect data from all networks and send logs every 24 hours. Details on how to change these configurations can be found in Configure Network Access Manager. **Save** the profile as an XML when finished.

Step 3. If applicable, add the XML to an existing XML profile containing all of the other AnyConnect config options such as the AMP enabler or VPN always on.



```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
    <ClientInitialization> ...
    </ClientInitialization>
    <NVMProfile xsi:noNamespaceSchemaLocation="NVMProfile.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <CollectorConfiguration>
            <CollectorIP>$PUBLIC_IP</CollectorIP>
            <Port>2055</Port>
        </CollectorConfiguration>
        <TemplateReportInterval>5</TemplateReportInterval>
        <AggInterval>5</AggInterval>
        <ThrottleRate>500</ThrottleRate>
        <CollectionMode>all</CollectionMode>
        <CollectionCriteria>
            <Broadcast>false</Broadcast>
            <Multicast>false</Multicast>
        </CollectionCriteria>
        <DataCollectionPolicy>
        </DataCollectionPolicy>
    </NVMProfile>
</AnyConnectProfile>
```

Step 4. In FMC, navigate to **Devices > Remote Access**.

Step 5. Click the **pencil icon** to edit the remote access VPN configuration that this profile will apply to.

Step 6. Click the **pencil icon** to edit the remote access VPN connection profile(s) that this configuration uses.

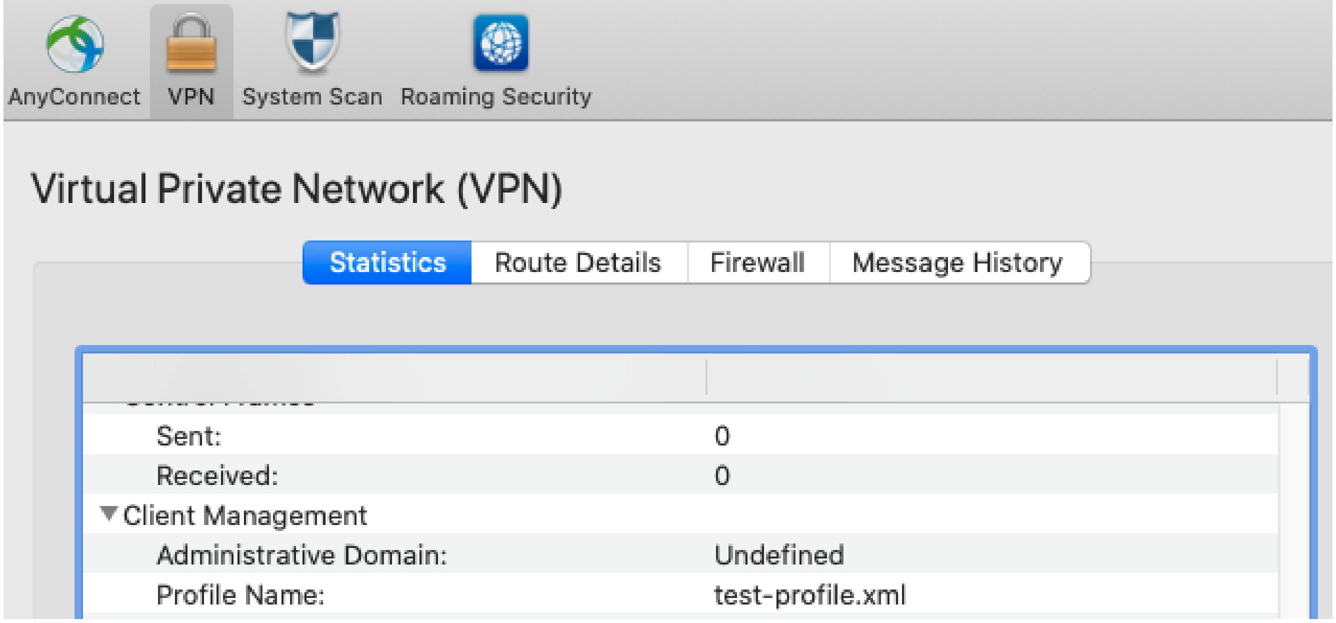
Step 7. Located directly under the Group Policy dropdown, click **Edit Group Policy**.

Step 8. In the **AnyConnect > Profiles** tab, click the **add (+)** button to add a new Client Profile.

Step 9. Browse for the newly created/modified NVM profile and click **Save**.

Step 10. Continue to **Save** until completion. **Deploy** the configuration.

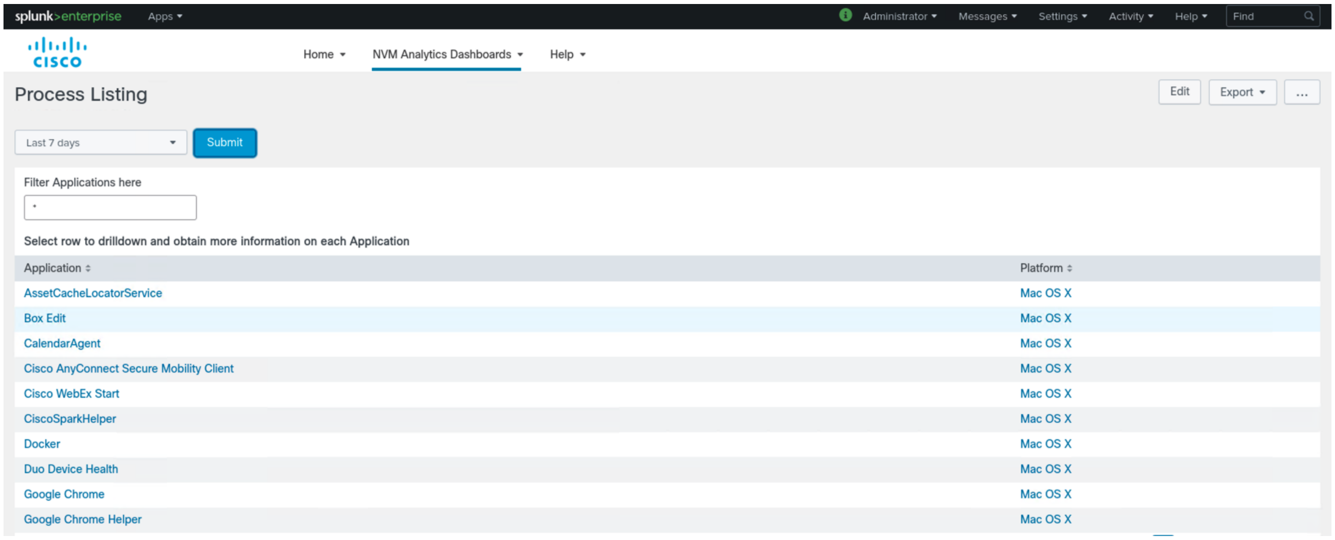
Step 11. To test deployment, disconnect and reconnect a device that uses this VPN headend. Open the AnyConnect Statistics Window and check that the **Profile Name** matches the one assigned in the policy.



Virtual Private Network (VPN)

Sent:	0
Received:	0
▼Client Management	
Administrative Domain:	Undefined
Profile Name:	test-profile.xml

Step 12. In Splunk, navigate to the Cisco NVM Dashboard to view AnyConnect data. **NOTE: It may take time for data to appear, with a delay depending on the configuration policy applied.**



Process Listing

Last 7 days

Filter Applications here: *

Select row to drilldown and obtain more information on each Application

Application	Platform
AssetCacheLocatorService	Mac OS X
Box Edit	Mac OS X
CalendarAgent	Mac OS X
Cisco AnyConnect Secure Mobility Client	Mac OS X
Cisco WebEx Start	Mac OS X
CiscoSparkHelper	Mac OS X
Docker	Mac OS X
Duo Device Health	Mac OS X
Google Chrome	Mac OS X
Google Chrome Helper	Mac OS X

Cisco Cloudlock

Pre-requisites

- The organization is using single sign on with an identity as a Service (IDaaS) provider such as Okta or OneLogin
- A Cloudlock account
- Cloudlock must be installed into all platforms that require protection. Quickstart guides can be found for the following platforms:
    - Active Directory Federation Services
    - Cisco Cloudlock App Discovery
    - Box
    - Dropbox
    - Google Suite
    - Office 365
    - Okta
    - OneLogin
    - Salesforce
    - ServiceNow
    - Slack (Enterprise)
    - Slack (Teams)
    - Webex Teams

Data Loss Protection – Create and Configure a Predefined Policy

Pre-defined policies are policies whose regular expressions are pre-written by Cisco Cloudlock engineers, some of which can be edited or customized in policy configuration. Some predefined policies typically used in the US Government industry include:

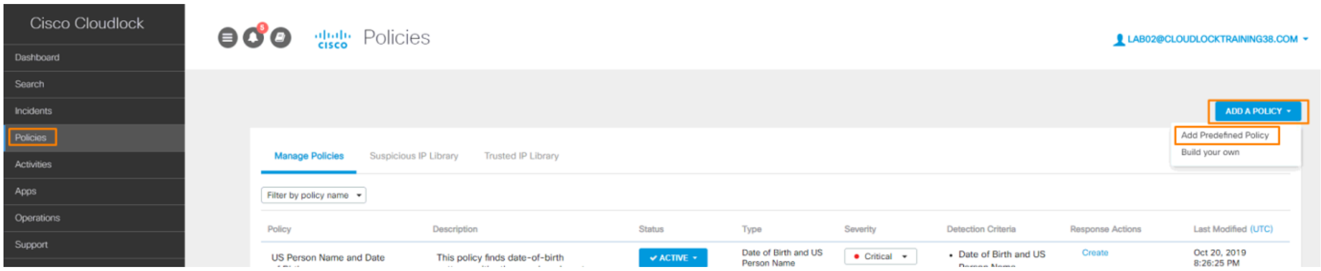
- Credit Card Number
- US Driver’s License Number
- US Personally Identifiable Information (PII) such as birth date or heath condition
- US Passport Number
- US Social Security Number

For a full list of all pre-written policies see pre-defined policies.

This example will show how Credit card numbers can be identified in both files uploaded to Box and within a Webex chat room.

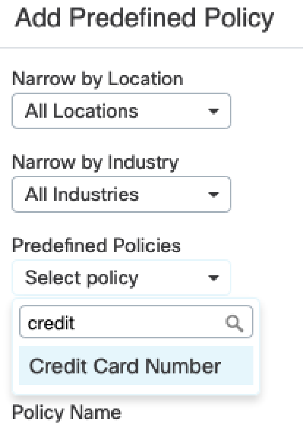
Step 1. In Cloudlock, navigate to **Policies**.

Step 2. Click **Add a Policy**. In the dropdown, click **Add Predefined Policy**.



Policy	Description	Status	Type	Severity	Detection Criteria	Response Actions	Last Modified (UTC)
US Person Name and Date	This policy finds date-of-birth	✓ ACTIVE	Date of Birth and US Person Name	● Critical	• Date of Birth and US	Create	Oct 20, 2019 8:26:25 PM

Step 3. Policies can be narrowed with location or industry filters. For this example, use the **Predefined Policies** dropdown and select **Credit Card Number**.



Add Predefined Policy

Narrow by Location: All Locations

Narrow by Industry: All Industries

Predefined Policies: Select policy

credit

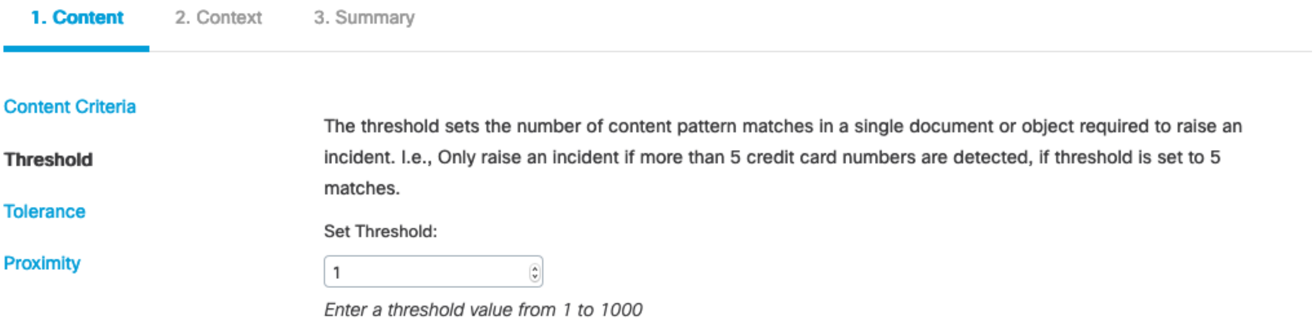
Credit Card Number

Policy Name

Step 4. Select **Alert** for the Severity. **Note: The severity level controls how an incident generated by the policy is displayed in the Cloudlock interface. The severity is meant to influence the priority given to incidents by security admins but will not affect the way the policy behaves.**

Step 5. Add a meaningful name and description to the policy and click **Configure Policy**.

Step 6. Click **Threshold**. Keep the threshold set to **1**. **Note: The threshold is the number of content pattern matches in a single document or object that are required to raise an incident.**

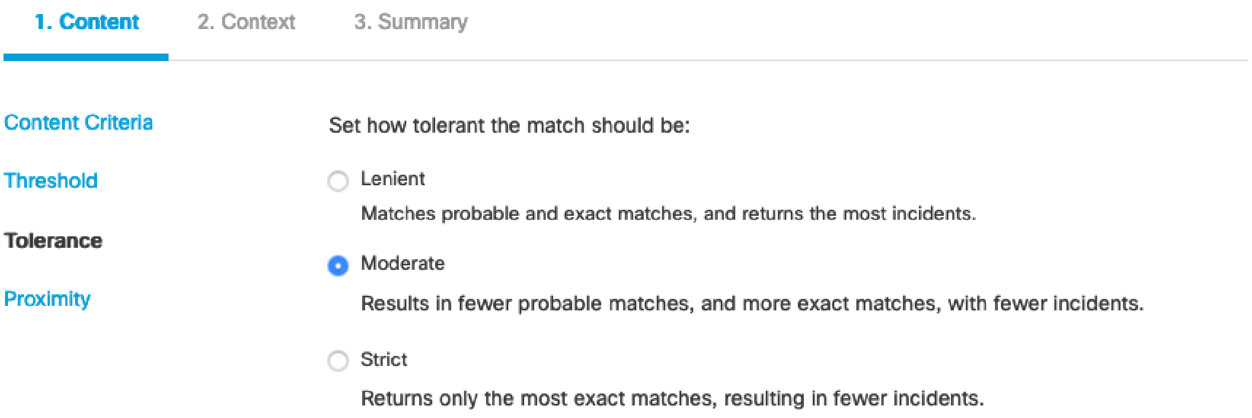


The threshold sets the number of content pattern matches in a single document or object required to raise an incident. I.e., Only raise an incident if more than 5 credit card numbers are detected, if threshold is set to 5 matches.

Set Threshold: 1

Enter a threshold value from 1 to 1000

Step 7. Click **Tolerance**. Set the tolerance to **Moderate**. **Note: Cisco Cloudlock has several content and contextual criteria that can be adjusted when building DLP policies. This allows for a reduction in false positives when applying policy within an organizations public cloud environment. The ability to tune out these false positives and reduce the incident counts allows a security admin to focus on mitigating real threats and exposures and helps strengthen the confidence the security admin has in the solution. For more information see Predefined Policy Configuration.**



Set how tolerant the match should be:

○ Lenient

Matches probable and exact matches, and returns the most incidents.

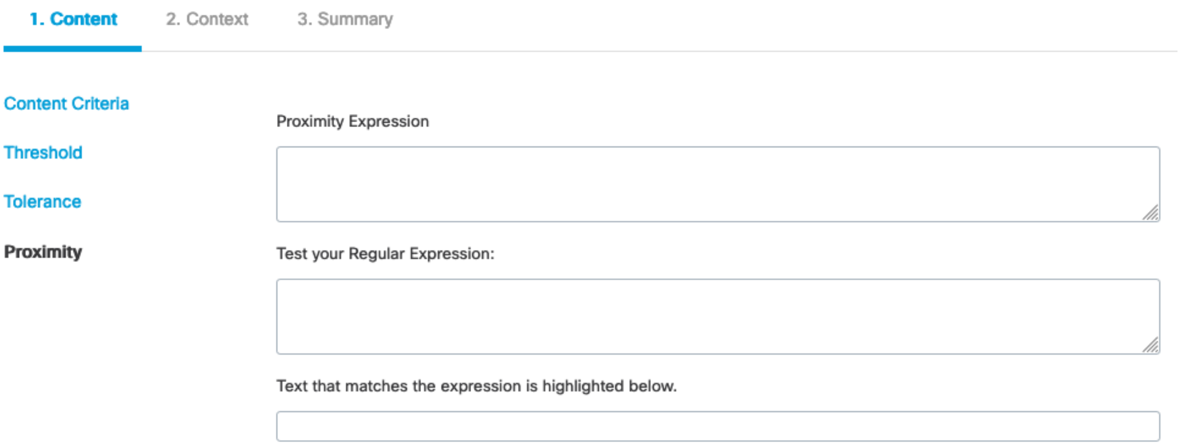
● Moderate

Results in fewer probable matches, and more exact matches, with fewer incidents.

○ Strict

Returns only the most exact matches, resulting in fewer incidents.

Step 8. Select **Proximity**. Leave the **Proximity Expression** field blank. **Note: Proximity is an optional regular expression that contains keywords or patterns that must be found within 100 terms (or in the same row or column of a spreadsheet) of the detected content. In many predefined policies, the Proximity will be pre-populated, but you can always edit this field depending on the need.**

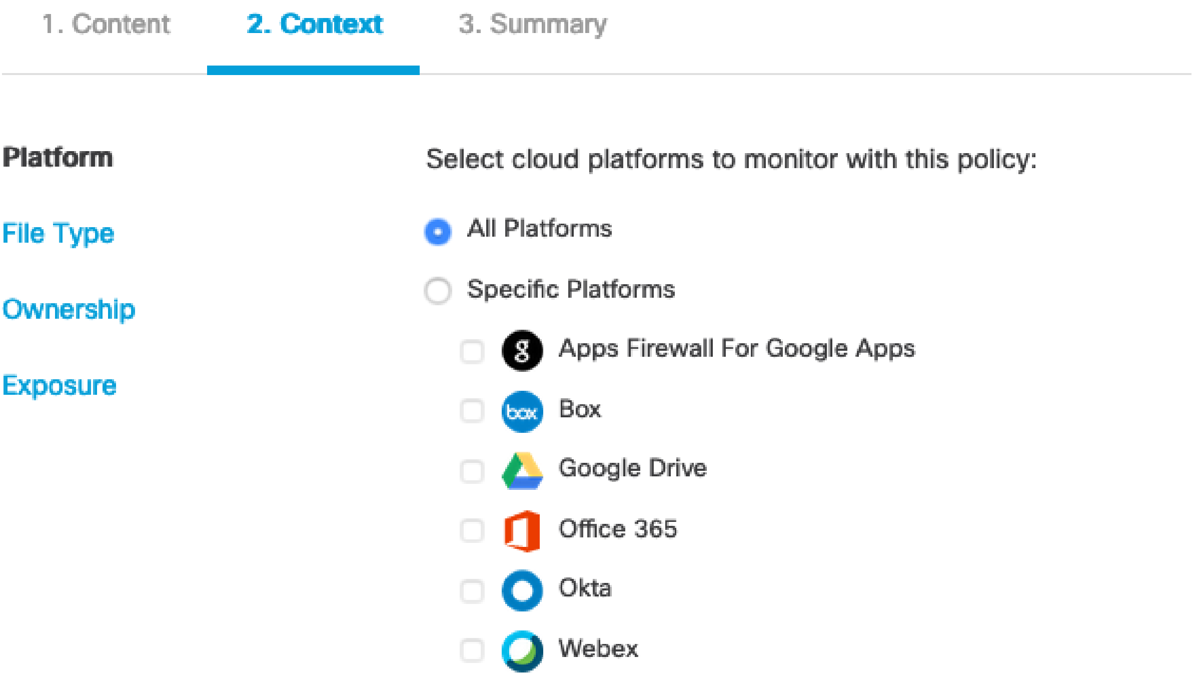


Proximity Expression

Test your Regular Expression:

Text that matches the expression is highlighted below.

Step 9. From the top level, select **Context**. Select **Platform** and set the policy to **All Platforms**. **Note: the platform setting defined the platform(s) to which the policy applies. This allows creation of one policy across multiple platforms or break out different policies to be applied to individual platforms.**



1. Content | **2. Context** | 3. Summary

Platform
File Type
Ownership
Exposure

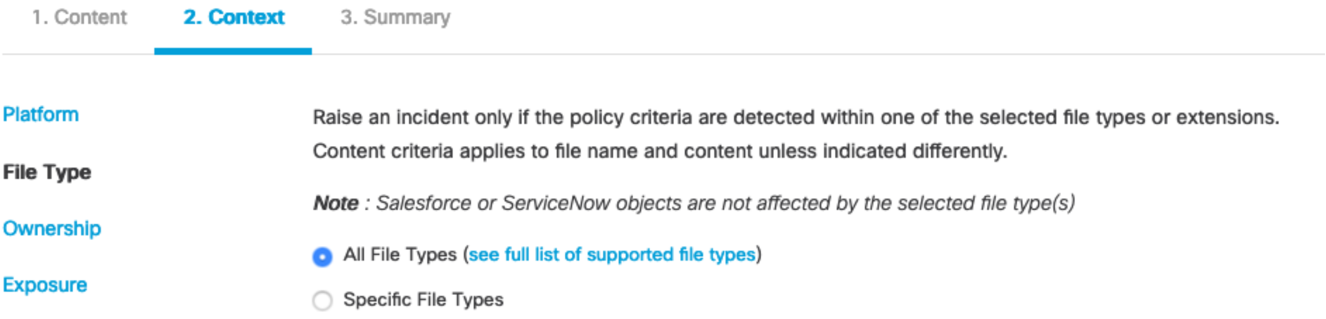
Select cloud platforms to monitor with this policy:

● All Platforms

○ Specific Platforms

- □ Apps Firewall For Google Apps
- □ Box
- □ Google Drive
- □ Office 365
- □ Okta
- □ Webex

Step 10. Select **File Type** and choose **All File Types.** For a list of supported file types see [Filetypes Supported in Content Policies](#).



1. Content | **2. Context** | 3. Summary

Platform
File Type
Ownership
Exposure

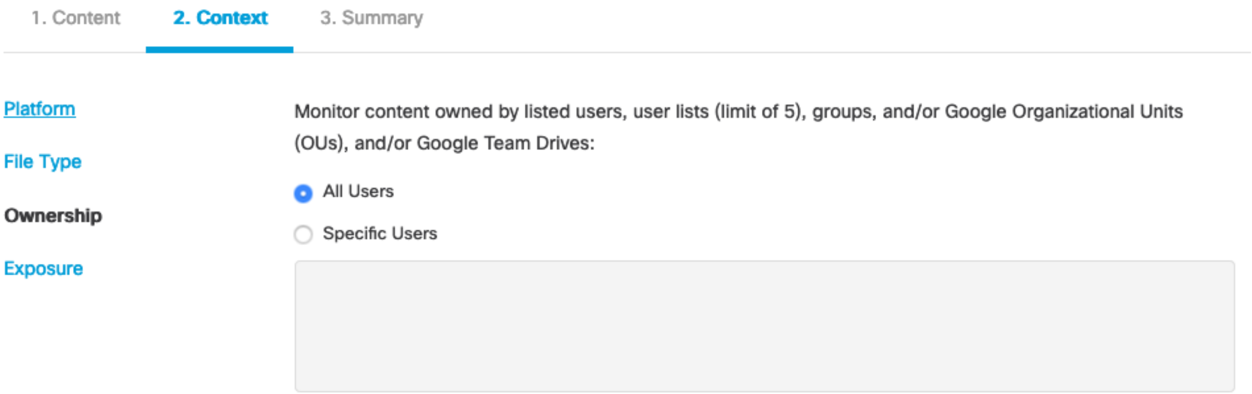
Raise an incident only if the policy criteria are detected within one of the selected file types or extensions. Content criteria applies to file name and content unless indicated differently.

Note *: Salesforce or ServiceNow objects are not affected by the selected file type(s)*

● All File Types (see full list of supported file types)

○ Specific File Types

Step 11. Select **Ownership** and choose **All Users**. **Note: Ownership refers to the users, groups or Organizational Units to which the policy applies. In certain cases, you may want to only look for Credit Card Numbers in files that are owned by members of specific groups, such as the finance team. For other organizations, you may want to exempt members of certain groups from the policy through an exception.**



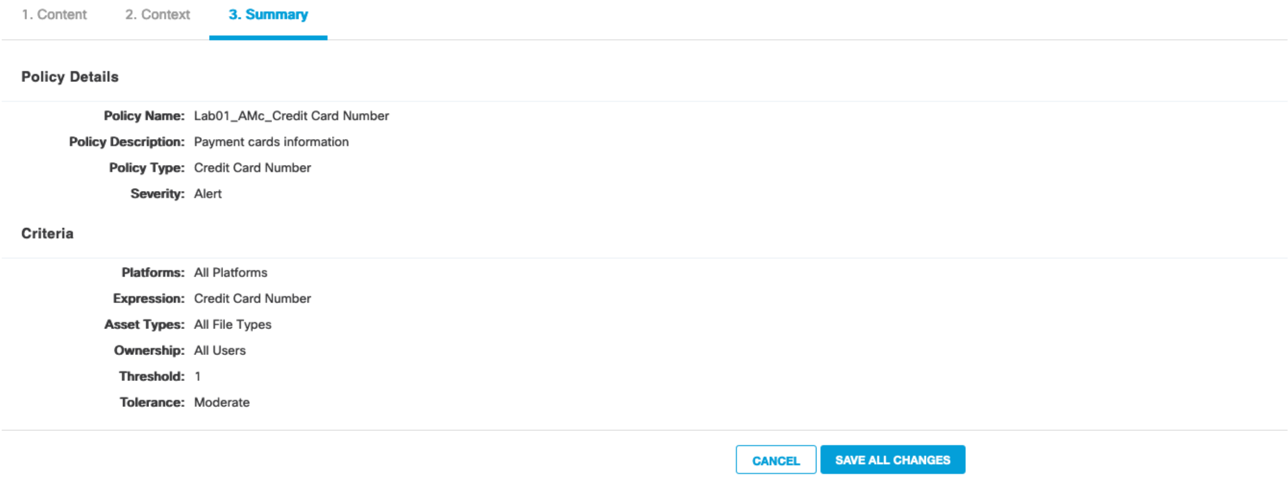
Monitor content owned by listed users, user lists (limit of 5), groups, and/or Google Organizational Units (OUs), and/or Google Team Drives:

● All Users

○ Specific Users

Step 12. **Exposure** will not be modified in this example. **Note: The Exposure criteria surfaces an incident based on the sharing / collaboration of the file. Choose the exposure level based on the platform(s) being monitored. If all exposures are left blank, the policy will raise an incident any time it finds a match for the content criteria, regardless of how the file was shared. When specific exposures are checked off, the policy will respect the choices made, and only raise incidents for the files that contain the content AND are shared in this manner.**

Step 13. Select Summary to view a summary of the policy configuration. Select **Save All Changes**.



Policy Details

Policy Name: Lab01_AMc_Credit Card Number
Policy Description: Payment cards information
Policy Type: Credit Card Number
Severity: Alert

Criteria

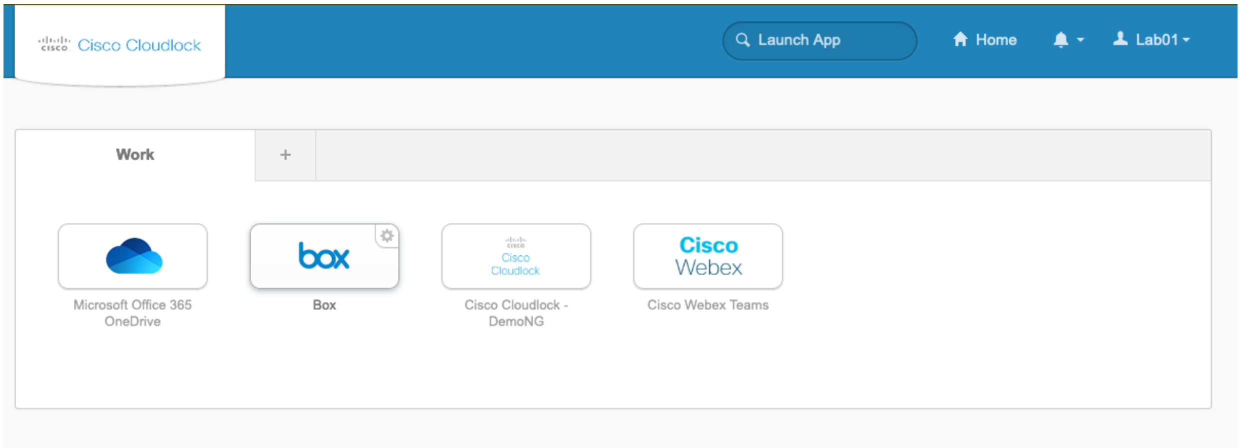
Platforms: All Platforms
Expression: Credit Card Number
Asset Types: All File Types
Ownership: All Users
Threshold: 1
Tolerance: Moderate

Data Loss Protection – Testing the Credit Card Number Policy

In this example, Okta is used as an IDaaS provider and Cloudlock has already been integrated into both Box and Webex Teams.

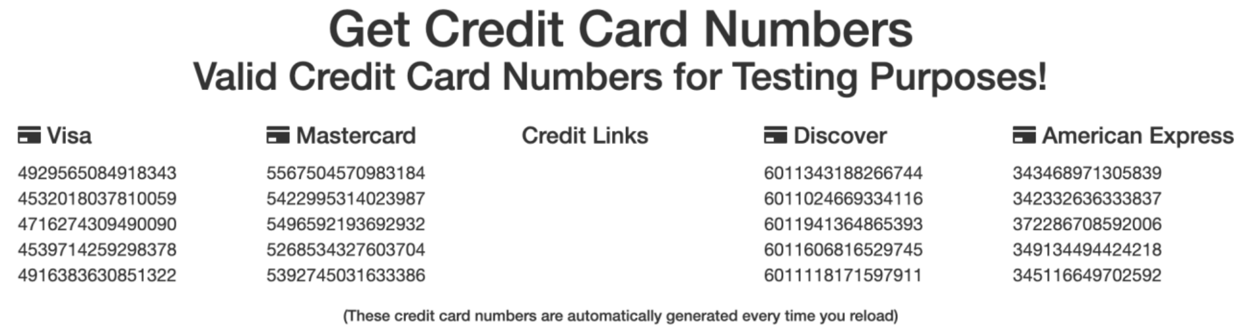
Procedure 4. Testing file policies using Box

Step 1. From the Okta dashboard, open **Box**.



Step 2. From a workstation, create a Word document and give it any name.

Step 3. In a web browser, navigate to https://www.getcreditcardnumbers.com.

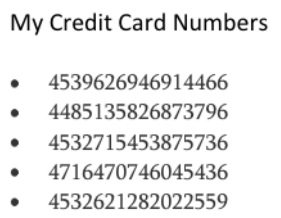


Get Credit Card Numbers
Valid Credit Card Numbers for Testing Purposes!

Visa	Mastercard	Credit Links	Discover	American Express
4929565084918343	5567504570983184		6011343188266744	343468971305839
4532018037810059	5422995314023987		6011024669334116	342332636333837
4716274309490090	5496592193692932		6011941364865393	372286708592006
4539714259298378	5268534327603704		6011606816529745	349134494424218
4916383630851322	5392745031633386		6011118171597911	345116649702592

(These credit card numbers are automatically generated every time you reload)

Step 4. Copy one or more of the credit card numbers and paste them to the word document created in a previous step. Save the word file.

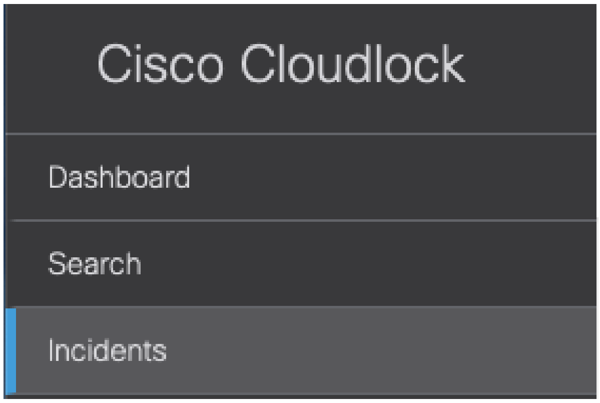


My Credit Card Numbers

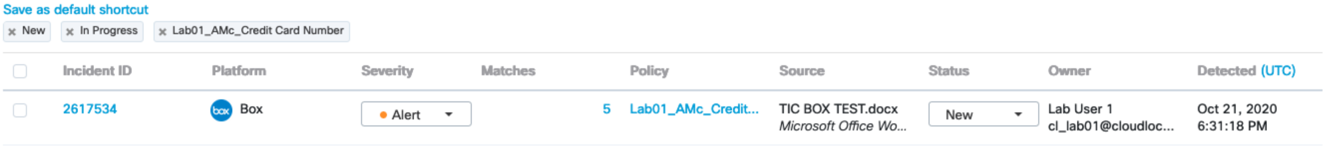
- 4539626946914466
- 4485135826873796
- 4532715453875736
- 4716470746045436
- 4532621282022559

Step 5. Upload the file to the box folder.

Step 6. In Cloudlock, navigate to **Incidents**.



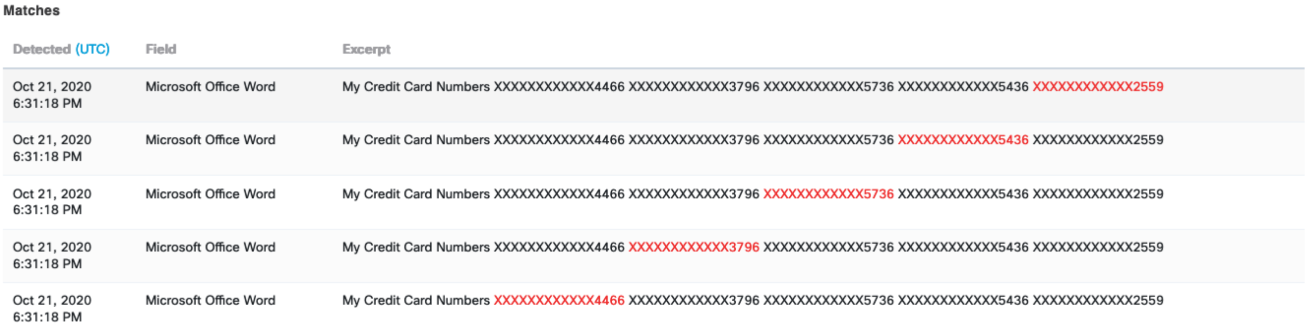
Step 7. At the bottom of the page, click on the incident for more information.


Save as default shortcut

× New × In Progress × Lab01_AMc_Credit Card Number

□	Incident ID	Platform	Severity	Matches	Policy	Source	Status	Owner	Detected (UTC)
□	2617534	Box	● Alert	5	Lab01_AMc_Credit...	TIC BOX TEST.docx *Microsoft Office Wo...*	New	Lab User 1 cl_lab01@cloudloc...	Oct 21, 2020 6:31:18 PM

Step 8. A match will appear for each credit card number in the word file.


Matches

Detected (UTC)	Field	Excerpt
Oct 21, 2020 6:31:18 PM	Microsoft Office Word	My Credit Card Numbers XXXXXXXXXXXX4466 XXXXXXXXXXXX3796 XXXXXXXXXXXX5736 XXXXXXXXXXXX5436 XXXXXXXXXXXX2559
Oct 21, 2020 6:31:18 PM	Microsoft Office Word	My Credit Card Numbers XXXXXXXXXXXX4466 XXXXXXXXXXXX3796 XXXXXXXXXXXX5736 XXXXXXXXXXXX5436 XXXXXXXXXXXX2559
Oct 21, 2020 6:31:18 PM	Microsoft Office Word	My Credit Card Numbers XXXXXXXXXXXX4466 XXXXXXXXXXXX3796 XXXXXXXXXXXX5736 XXXXXXXXXXXX5436 XXXXXXXXXXXX2559
Oct 21, 2020 6:31:18 PM	Microsoft Office Word	My Credit Card Numbers XXXXXXXXXXXX4466 XXXXXXXXXXXX3796 XXXXXXXXXXXX5736 XXXXXXXXXXXX5436 XXXXXXXXXXXX2559
Oct 21, 2020 6:31:18 PM	Microsoft Office Word	My Credit Card Numbers XXXXXXXXXXXX4466 XXXXXXXXXXXX3796 XXXXXXXXXXXX5736 XXXXXXXXXXXX5436 XXXXXXXXXXXX2559

Procedure 5. Testing policies in Webex Teams

Step 1. From the Okta dashboard, open **WebEx Teams**.

Single Sign-on succeeded.

Step 2. In a web browser, navigate to https://teams.webex.com. If not automatically logged in, do so with your domain account.

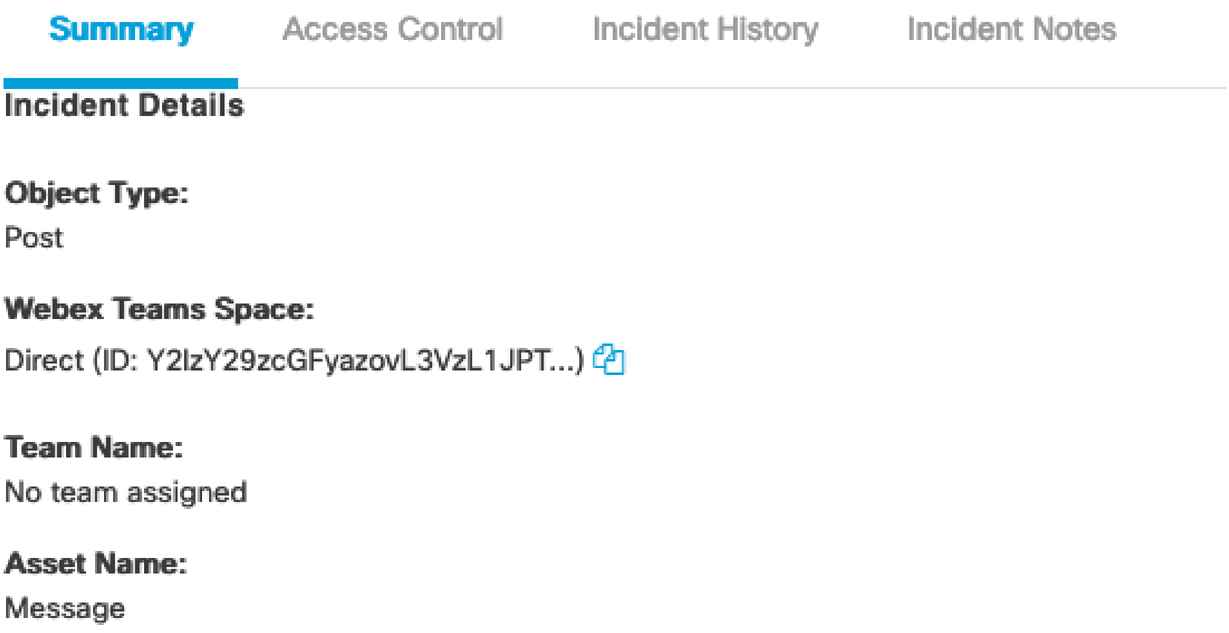
Step 3. In Webex Teams, click on the plus symbol to start a new chat and select a contact person.

Step 4. In the chat field, copy one or more of the credit card numbers from https://getcreditcardnumbers.com.

Step 5. In Cloudlock, navigate to **Incidents**.

Step 6. At the bottom of the page, click on the incident for more information.

Step 7. A match will appear for each credit card number found in the chat, along with details such as what team space the message was sent in.



Incident Details

Object Type:
Post

Webex Teams Space:
Direct (ID: Y2lzY29zcGFyazovL3VzL1JPT...)

Team Name:
No team assigned

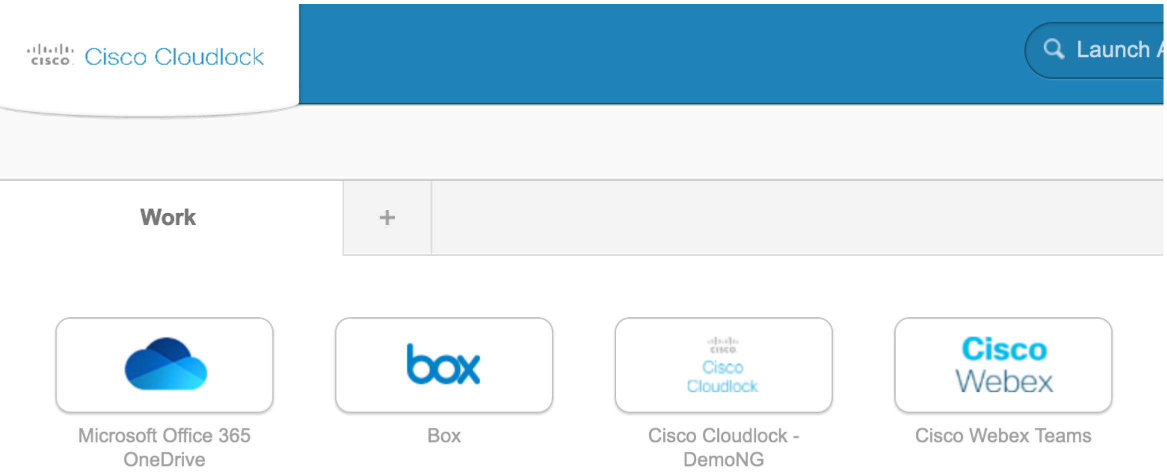
Asset Name:
Message

Shadow IT – Cloudlock Apps Firewall

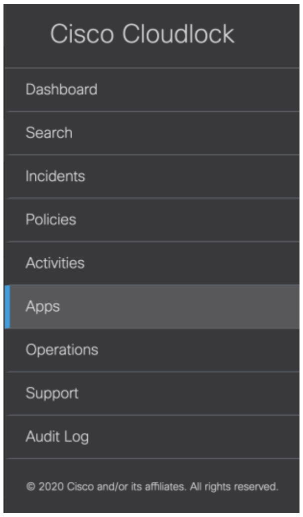
Cisco Cloudlock Apps Firewall discovers connected 3rd party apps that have been granted access to Google or Microsoft Office 365 via Oauth. Oauth, or open standard for authorization, is a standardized way for internet accounts to link with third-party applications. It is universally adopted by almost all web-based applications and platforms – including consumer as well as enterprise applications such as Google G-Suite, Microsoft Office 365, Salesforce, and many others. As more businesses adopt cloud platforms, the employees authorize apps using their corporate credentials, giving these apps programmatic (API) access to their corporate data, introducing millions of back doors into corporate environments. If you have ever come across the buttons below when viewing a website or logging into a cloud service e.g. Spotify, Facebook, you will have an option to sign in via Oauth.

Procedure 1. Application Visibility

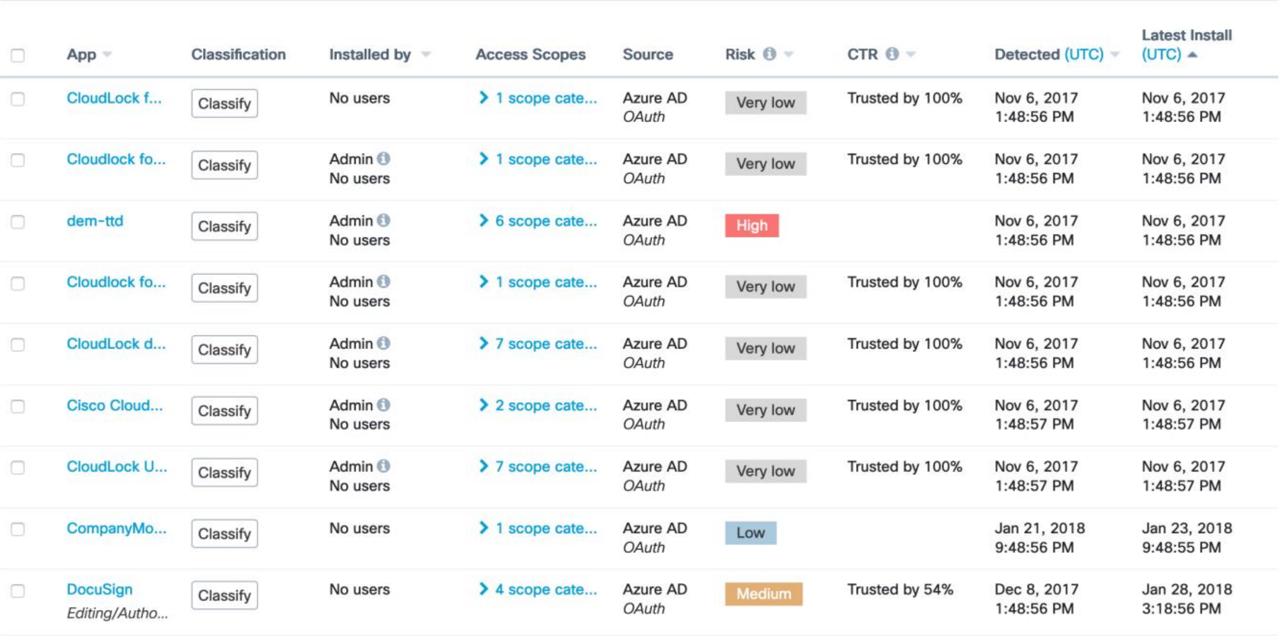
Step 1. In the Okta dashboard, open Cisco Cloudlock.



Step 2. Navigate to **Apps**.

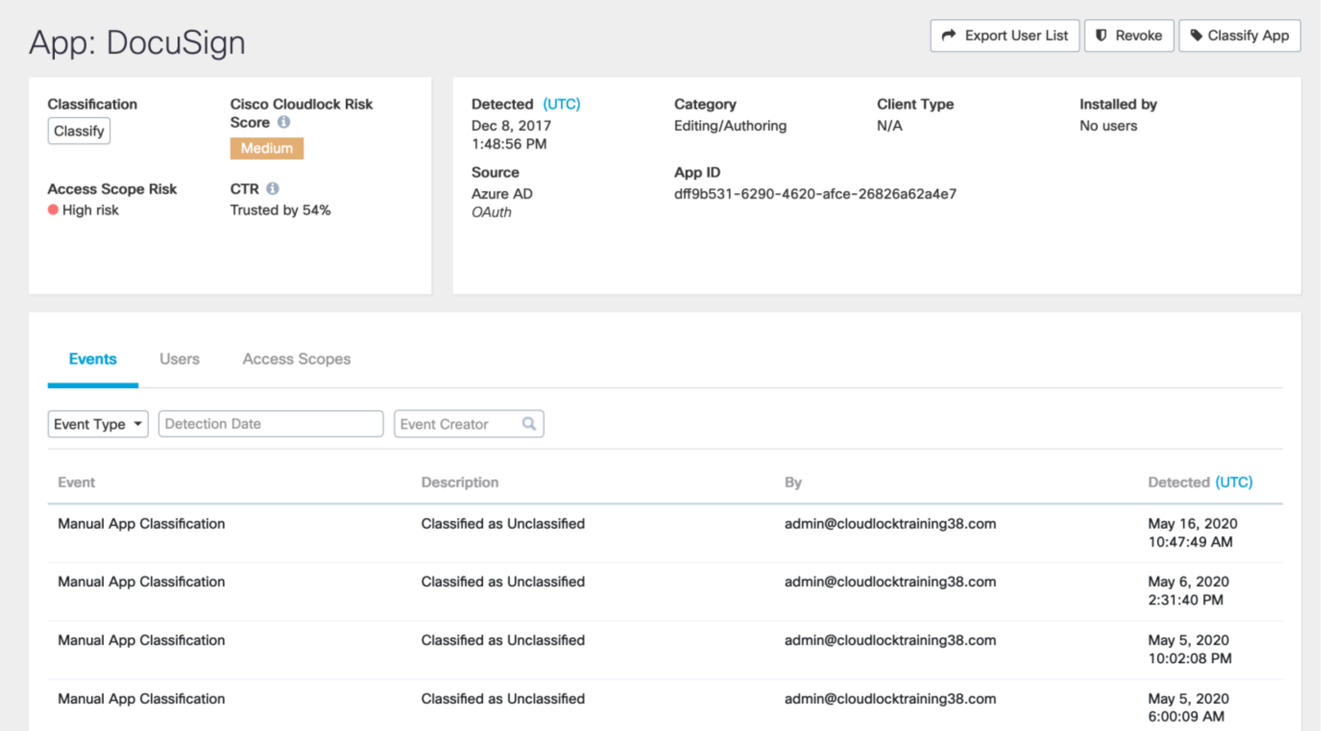


Step 3. The apps list is displayed at the bottom of the Apps Panel. Each installed app is listed along with the access scopes it requests, the Cloudlock Risk Score, Community Trust Rating (CTR) i.e. crowdsourced rating based on Cloudlock users of the specified app. Other information including the number of users in the domain who have installed the app, the date when the app was detected and the source of the app (i.e. Google OAuth or Azure AD).



□	App	Classification	Installed by	Access Scopes	Source	Risk	CTR	Detected (UTC)	Latest Install (UTC)
□	CloudLock f...	Classify	No users	› 1 scope cate...	Azure AD *OAuth*	Very low	Trusted by 100%	Nov 6, 2017 1:48:56 PM	Nov 6, 2017 1:48:56 PM
□	Cloudlock fo...	Classify	Admin No users	› 1 scope cate...	Azure AD *OAuth*	Very low	Trusted by 100%	Nov 6, 2017 1:48:56 PM	Nov 6, 2017 1:48:56 PM
□	dem-ttd	Classify	Admin No users	› 6 scope cate...	Azure AD *OAuth*	High		Nov 6, 2017 1:48:56 PM	Nov 6, 2017 1:48:56 PM
□	Cloudlock fo...	Classify	Admin No users	› 1 scope cate...	Azure AD *OAuth*	Very low	Trusted by 100%	Nov 6, 2017 1:48:56 PM	Nov 6, 2017 1:48:56 PM
□	CloudLock d...	Classify	Admin No users	› 7 scope cate...	Azure AD *OAuth*	Very low	Trusted by 100%	Nov 6, 2017 1:48:56 PM	Nov 6, 2017 1:48:56 PM
□	Cisco Cloud...	Classify	Admin No users	› 2 scope cate...	Azure AD *OAuth*	Very low	Trusted by 100%	Nov 6, 2017 1:48:57 PM	Nov 6, 2017 1:48:57 PM
□	CloudLock U...	Classify	Admin No users	› 7 scope cate...	Azure AD *OAuth*	Very low	Trusted by 100%	Nov 6, 2017 1:48:57 PM	Nov 6, 2017 1:48:57 PM
□	CompanyMo...	Classify	No users	› 1 scope cate...	Azure AD *OAuth*	Low		Jan 21, 2018 9:48:56 PM	Jan 23, 2018 9:48:55 PM
□	DocuSign *Editing/Autho...*	Classify	No users	› 4 scope cate...	Azure AD *OAuth*	Medium	Trusted by 54%	Dec 8, 2017 1:48:56 PM	Jan 28, 2018 3:18:56 PM

Step 4. Click the name of an app to open the details page for that app to view Details, History, and Access Scopes.

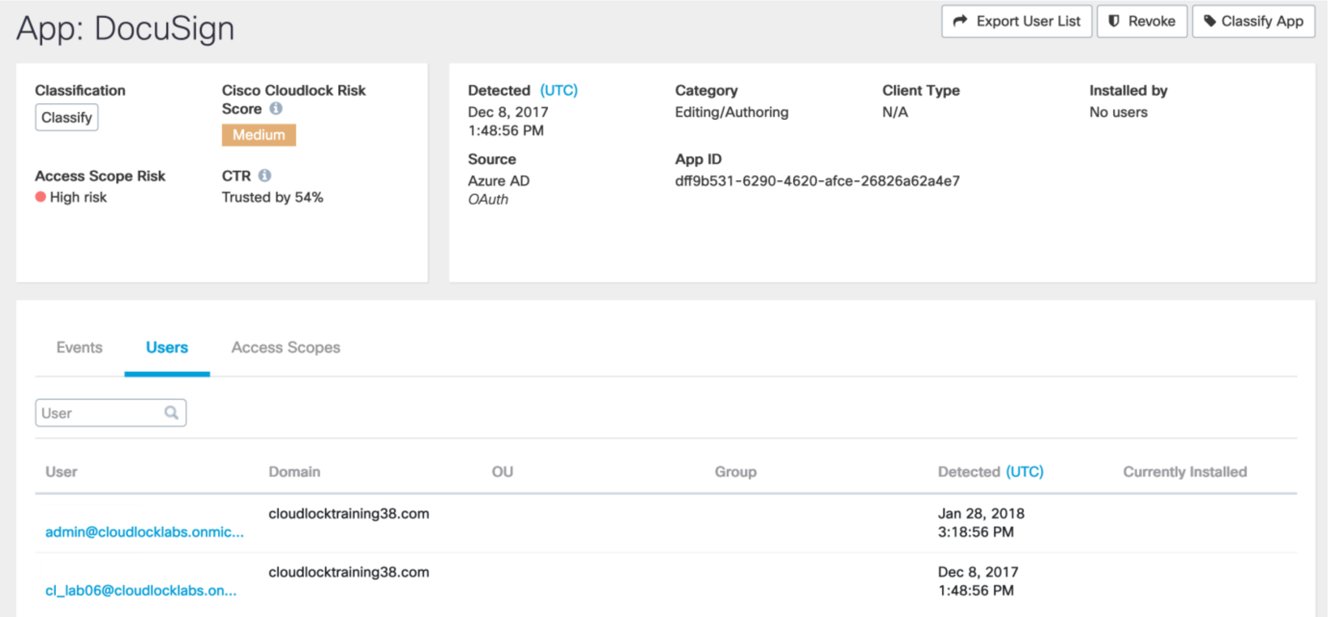


App: DocuSign

Classification: Classify
Cisco Cloudlock Risk Score: Medium
Access Scope Risk: ● High risk
CTR: Trusted by 54%
Detected (UTC): Dec 8, 2017 1:48:56 PM
Category: Editing/Authoring
Client Type: N/A
Installed by: No users
Source: Azure AD *OAuth*
App ID: dff9b531-6290-4620-afce-26826a62a4e7

Event	Description	By	Detected (UTC)
Manual App Classification	Classified as Unclassified	admin@cloudlocktraining38.com	May 16, 2020 10:47:49 AM
Manual App Classification	Classified as Unclassified	admin@cloudlocktraining38.com	May 6, 2020 2:31:40 PM
Manual App Classification	Classified as Unclassified	admin@cloudlocktraining38.com	May 5, 2020 10:02:08 PM
Manual App Classification	Classified as Unclassified	admin@cloudlocktraining38.com	May 5, 2020 6:00:09 AM

Step 5. In Users tab, you can see the users who have installed the application using their corporate credentials.



App: DocuSign

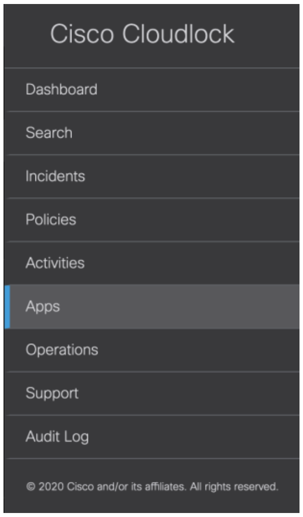
Classification: Classify
Cisco Cloudlock Risk Score: Medium
Access Scope Risk: ● High risk
CTR: Trusted by 54%
Detected (UTC): Dec 8, 2017 1:48:56 PM
Category: Editing/Authoring
Client Type: N/A
Installed by: No users
Source: Azure AD *OAuth*
App ID: dff9b531-6290-4620-afce-26826a62a4e7

User	Domain	OU	Group	Detected (UTC)	Currently Installed
admin@cloudlocklabs.onmic...	cloudlocktraining38.com			Jan 28, 2018 3:18:56 PM	
cl_lab06@cloudlocklabs.on...	cloudlocktraining38.com			Dec 8, 2017 1:48:56 PM	

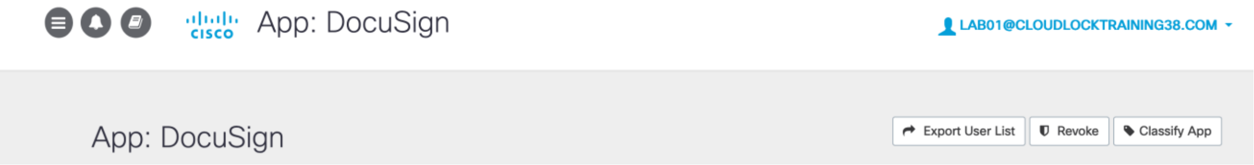
Procedure 2. Application Access Scopes

Access Scopes are the permissions apps request to interact with data and other apps on a platform in a given domain. The range of available access scopes depends on the capabilities made available by the underlying platform. The total number of access scopes available in a platform may be very large. When that is the case, the scopes are categorized to make them easier to work with. For example, in the Google platform the category access personal information can include personal information from other apps including calendar, email and full data access.

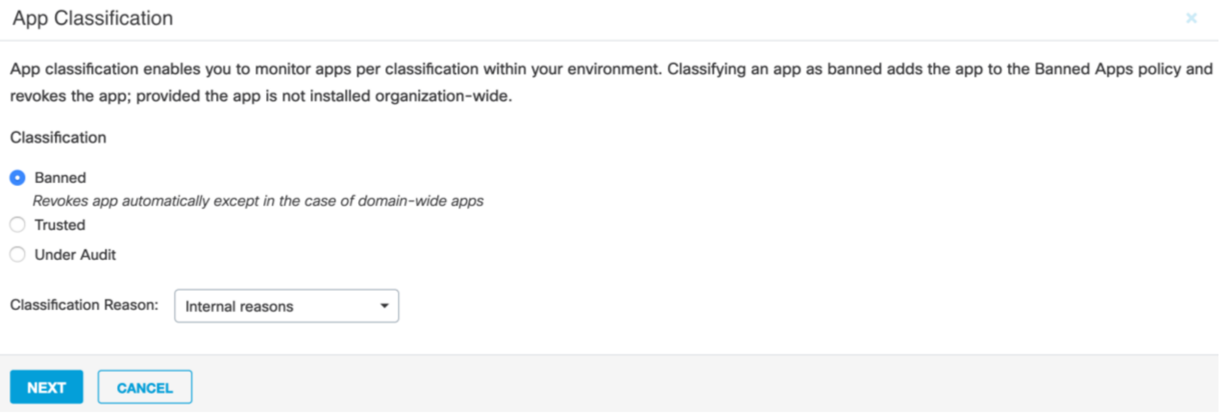
Step 1. In Cloudlock, navigate to **Apps** and click on an application that you would like to revoke. DocuSign will be revoked for demonstration purposes.



Step 2. Click on **Classify App**.



Step 3. Select **Banned** in the dropdown menu and choose a reason that most fits your requirement. Click **Next. NOTE: Classifying an app requires a reason, particularly if the classification is Banned or Under Audit. Banning an app enables you to add it to the default Banned Apps policy. Adding an app to that policy means all future installations of the app will be monitored and disallowed. For more details on classifying applications, see [Classifying Apps](#).**



App Classification

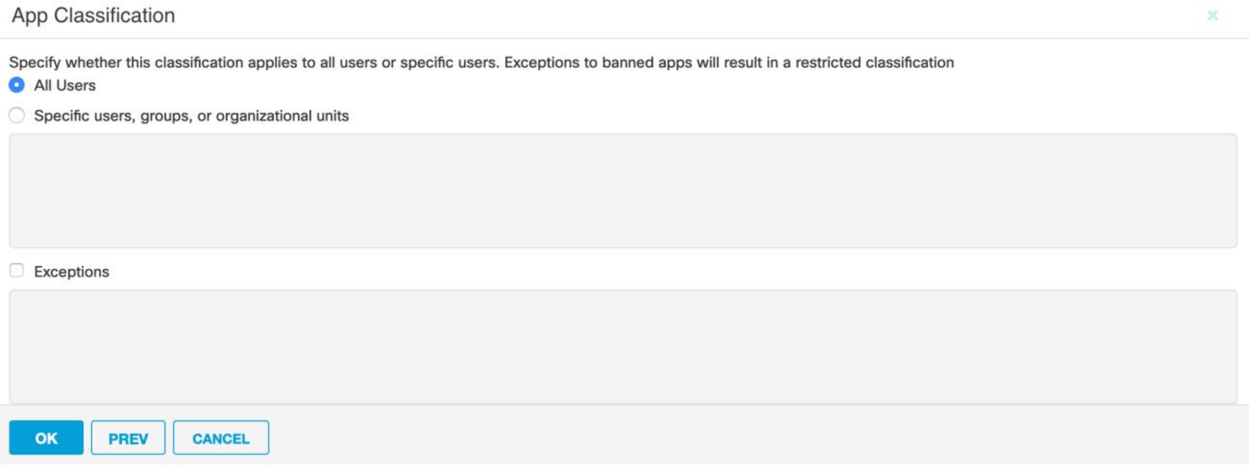
App classification enables you to monitor apps per classification within your environment. Classifying an app as banned adds the app to the Banned Apps policy and revokes the app; provided the app is not installed organization-wide.

Classification

● Banned
Revokes app automatically except in the case of domain-wide apps
○ Trusted
○ Under Audit

Classification Reason: Internal reasons

Step 4. App classification can be applied to all users or specific users, groups and organizational units (OUs). For this example, select **All Users**.



App Classification

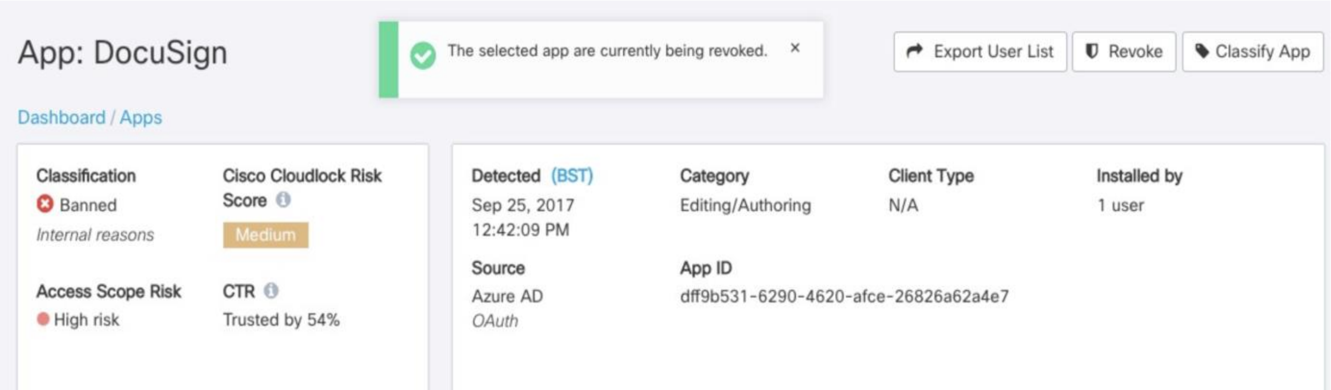
Specify whether this classification applies to all users or specific users. Exceptions to banned apps will result in a restricted classification

● All Users

○ Specific users, groups, or organizational units

□ Exceptions

Step 5. Click **OK**. **Note: it takes approximately 5 minutes for the Oauth token of the specified app to be automatically revoked. No Admin or user intervention is required.**



App: DocuSign

The selected app are currently being revoked.

Dashboard / Apps

Classification: Banned, *Internal reasons*

Cisco Cloudlock Risk Score: Medium

Access Scope Risk: High risk

CTR: Trusted by 54%

Detected (BST): Sep 25, 2017 12:42:09 PM

Category: Editing/Authoring

Client Type: N/A

Installed by: 1 user

Source: Azure AD *OAuth*

App ID: dff9b531-6290-4620-afce-26826a62a4e7

Americas Headquarters	Asia Pacific Headquarters	Europe Headquarters
Cisco Systems, Inc. San Jose, CA	Cisco Systems (USA) Pte. Ltd. Singapore	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**.