

Configure Dynamic Group Policy Assignment with SAML on Secure Firewall for Secure Client

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[Verify](#)

[Finance User](#)

[Sales User](#)

[Admin User](#)

[Troubleshoot](#)

Introduction

This document describes the process of dynamically assigning group policies using SAML authentication on the Cisco Secure Firewall.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic Remote Access VPN, SSL, and Certificate Knowledge
- Basic SAML Knowledge
- Experience with Firepower Management Center

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Firewall v7.2.0
- Cisco Secure Firewall Management Center (FMC) v7.2.0
- Cisco Secure Client 5.0.04032

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

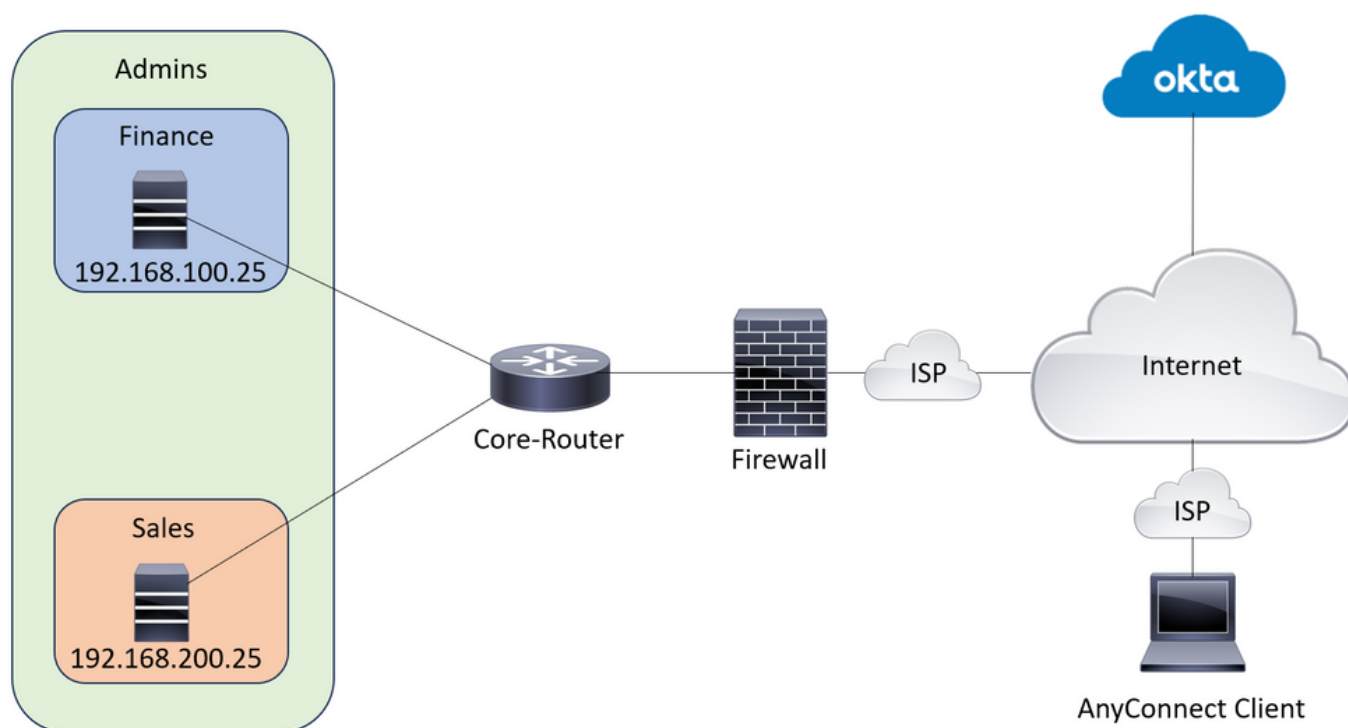
Background Information

In this document, Okta is used as the Identity Provider (IdP). However, it is essential to note that any IdP that allows for the customization of attributes sent in the SAML Assertion can be used.

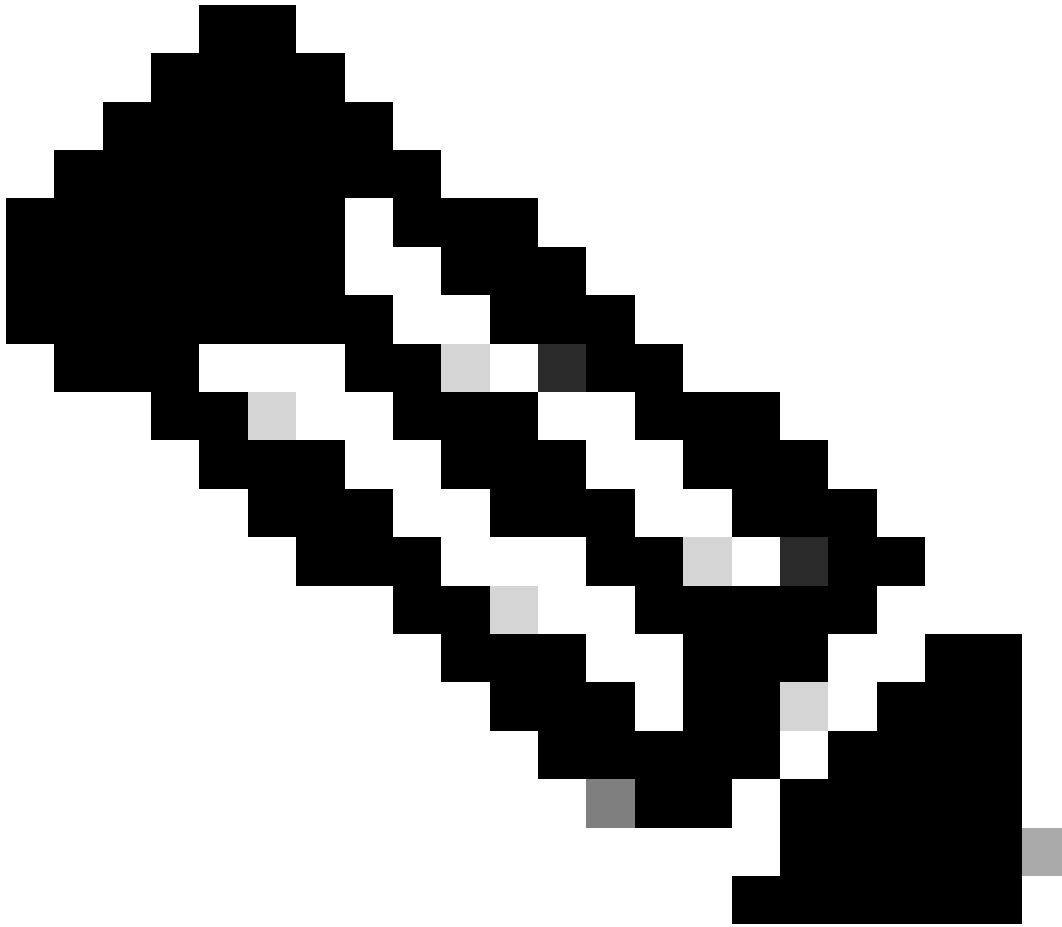
The SAML IdP can be configured in order to send assertions attributes in addition to the authentication assertion. The SAML Service Provider component in ASA/FTD interprets the SAML assertions received from IdP and makes policy selections based on them.

Configure

Network Diagram



Lab Topology



Note: This setup only works when a user is part of one and only one group, it does not work when a user is a part of multiple groups.

Configurations

Okta - SAML Configuration Part #1

1. Navigate to Applications > Applications and click Browse App Catalog. Search for Cisco in the catalog search bar and choose Cisco ASA VPN SAML, then click Add Integration.



Browse App Integration Catalog

Create New App

The screenshot shows the 'Browse App Integration Catalog' interface. On the left is a 'Use Case' sidebar with categories like 'All Integrations' (7660), 'Apps for Good' (9), 'Automation' (95), 'Centralized Logging' (24), 'Directory and HR Sync' (47), 'Bot or Fraud Detection' (5), 'Identity Proofing' (25), and 'Identity Governance and' (26). The main search area has a search bar containing 'Cisco' (labeled '4') and a 'POPULAR SEARCHES' section with 'Bookmark App', 'SCIM 2.0 Test App', 'Okta Org2Org', and 'Template App'. Search results are displayed in a grid, with 'Cisco ASA VPN (SAML) SAML' (labeled '5') highlighted by a red box. Other results include 'Cisco SWA', 'Cisco Webex SAML, SCIM, SWA', and 'Cisco Meraki Dashboard SAML SAML'. A 'See All Results' link is at the bottom right.

Okta ASA SAML App

Last updated: March 15, 2019

+ Add Integration

The 'Okta Application Add Button' for 'Cisco ASA VPN (SAML)'. It features the Cisco logo on the left, the application name 'Cisco ASA VPN (SAML)' in bold, and a 'SAML' tag below it.

Okta Application Add Button

2. Fill in the Application Label in the General Settings section and click Done.

Add Cisco ASA VPN (SAML)

1 General Settings

General settings · Required

Application label

Cisco Secure Firewall

This label displays under the app on your home page

Application Visibility

Do not display application icon to users

Cancel

Done

Okta general settings

3. In the Sign On, find the Metadata URL, copy it, and open it in a new tab. The Metadata XML file looks like as shown in this image:



Cisco Secure Firewall

Active ▾



[View Logs](#) [Monitor Imports](#)

- General
- Sign On**
- Import
- Assignments

Settings

[Edit](#)

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

Disable Force Authentication

Enable Single Logout

Metadata details

Metadata URL

https://trial-

/sso/saml/
metadata

Copy

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="...">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Certificate>
          [REDACTED]
        </ds:X509Certificate>
      </ds:KeyInfo>
    </md:KeyDescriptor>
  </md:IDPSSODescriptor>
  <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format: unspecified /md:NameIDFormat>
  <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format: emailAddress /md:NameIDFormat>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://..." /sso:saml"/>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://..." /sso:saml"/>
</md:EntityDescriptor>
```

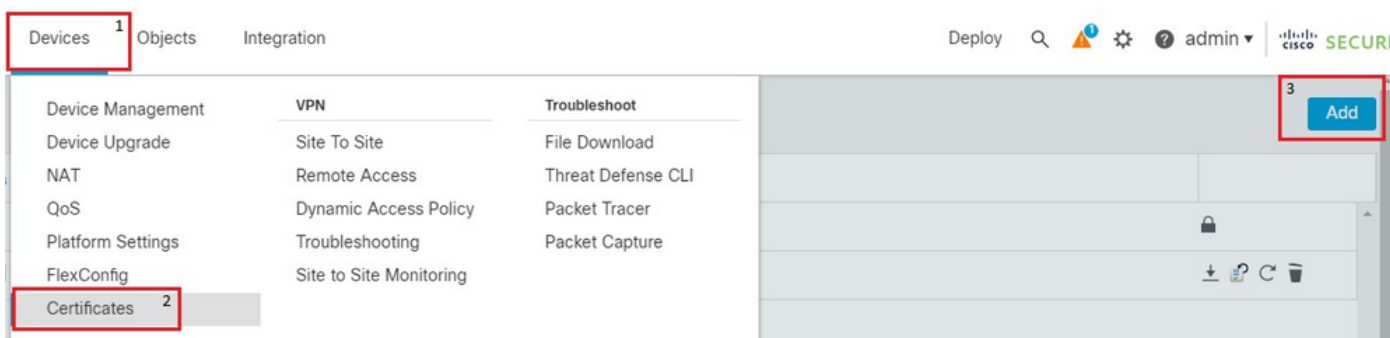
Metadata XML

4. Download the SAML Signing Certificate, from the same Sign On section. This is needed for configuring SSO in FMC.

5. Next, configure the SSO server on FMC. The assumption is made that the SSL certificate is configured and enrolled for FTD (here the trustpoint name is RAVPN-SSL).

FMC - SAML Configuration

1. In FMC, navigate to Devices > Certificates and click Add.



FMC devices nav

2. Choose the appropriate device and click + , next to Cert Enrollment. Give a name for the Cert Enrollment. Under CA Information, choose the Enrollment Type to be Manual. Check the CA Only checkbox and in the CA Certificate section paste the contents of the certificate you received earlier from the Okta SAML page. Once done, click Save.

Add New Certificate



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

Device* 1

FTD ▼

Cert Enrollment*:

Select a certificate enrollment object ▼ + 2

Cancel

Add

Add Cert Enrollment



Name* 3

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: 4
 CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate: 5

```
cFS6x4Ff9AVd7Ys8Tpi9vezE
Wcu0fXieugZbEo+KAigx5n8y
G2tmM
oNAMLsfaLIG7P7SpiSxKNRqD
tGMCiSkAxXB8/4KG6SfKPluh
1GQwILT6k74jVg8neJ6gxWA
9fpI9
PUCZlrjO3kZ6LEYHg8bB7AAr
1N4tVwnG4LMFZMh
-----END CERTIFICATE-----
```

Validation Usage: IPsec Client SSL Client SSL Server

Skip Check for CA flag in basic constraints of the CA Certificate 6

Cancel

Save 7



Note: Check the option Skip Check for CA flag in basic constraints of the CA certificate, since the certificate provided by the IdP is usually self-signed.

3. Click Add in order to enroll in the certificate.

Add New Certificate



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

Device*:

Cert Enrollment*:

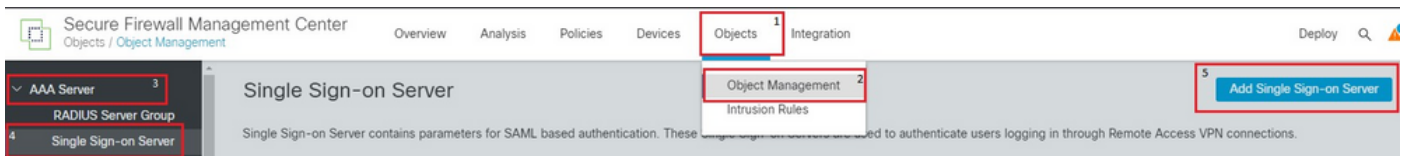
 +

Cert Enrollment Details:

Name: OktaSSO
Enrollment Type: Manual (CA Only)
Enrollment URL: N/A

fmc add cert enrollment

4. Navigate to Objects > Object Management > AAA Server > Single Sign-on Server and click Add Single Sign-on Server. Fill in the necessary information, from the Metadata XML (Entity ID and SSO URL), the base URL is the common name (CN) that you have for the FTD SSL Certificate. The IdP Certificate is OktaSSO which was enrolled earlier, and the Service Provider Certificate is the SSL certificate for FTD, which is RAVPN-SSL in this case. Leave everything else as default. Once you are done, click Save.



FMC object nav

New Single Sign-on Server



OktaSSO

Identity Provider Entity ID*

http://

SSO URL*

https://

Logout URL

Base URL

https://ftd.ciscolabs.com

Identity Provider Certificate*

OktaSSO



Service Provider Certificate

RAVPN-SSL



Request Signature

--No Signature--



Request Timeout

Use the timeout set by the provide

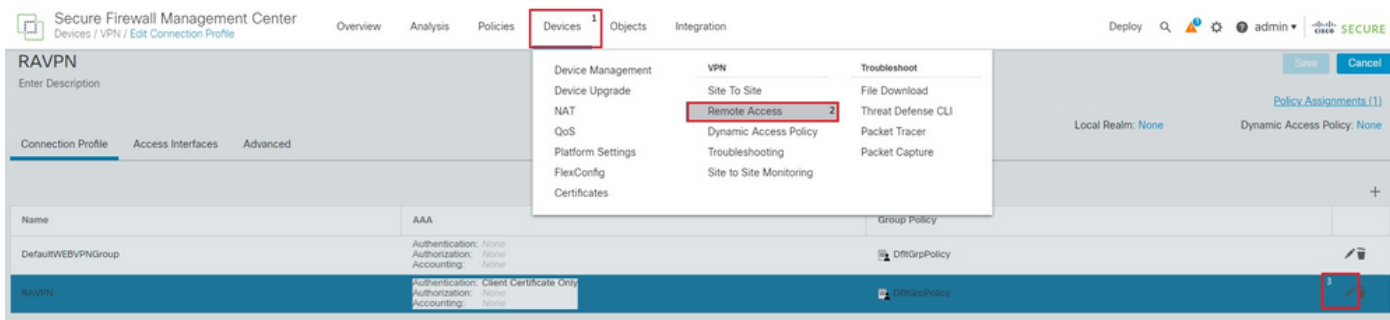
seconds (1-7200)

Enable IdP only accessible on Internal Network

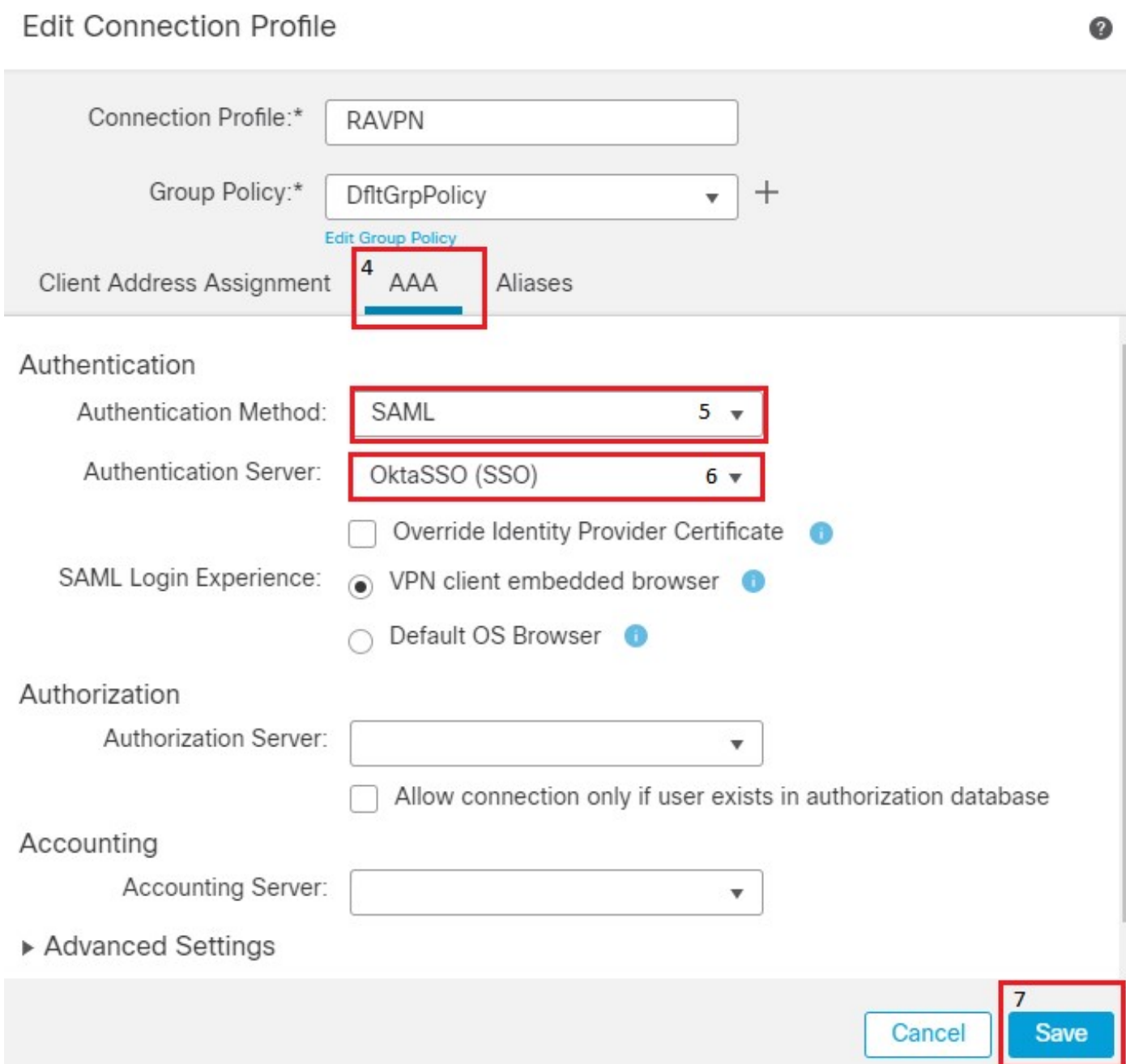
Request IdP re-authentication on Login

Allow Overrides

and edit the Connection Profile of Concern. Under the AAA Section, use the SSO server created earlier as the Authentication Method. Once done, click Save. Remember to save the changes by clicking Save on the top right corner.



FMC Devices RA nav



FMC Connection Profile settings

6. Next, create the three Group Policies named, Admins, Finance, and Sales.

7. The Group Policy DfltGrpPolicy has the Simultaneous Login Per User. value set to 0 so that it is not used by any user.

Edit Group Policy ?

Name:*
DfltGrpPolicy

Description:

General AnyConnect **Advanced**

Traffic Filter

Session Settings

Access Hours:
 +

Simultaneous Login Per User:
 (Range 0-2147483647)

Connection Time

Max Connection Time:
 Minutes (Range 1-4473924)

Alert Interval:
 Minutes (Range 1-30)

Idle Time

Idle Timeout:
 Minutes (Range 1-35791394)

Alert Interval:
 Minutes (Range 1-30)

FMC DfltGrpPolicy Settings

8. Navigate to Advanced Section > Group Policies and click +. Click + again in order to create a new group policy.

9. The image shows an example of the group Admins. Enter the name as Admins and this group has Welcome

Admins! as their banner value. This group also has Split Tunneling configured to Tunnel networks specified below which has access to both Finance and Sales team servers. Leave the rest of the options as defaults. Once you are done, click Save.

Secure Firewall Management Center
Devices / VPN / Edit Advanced

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin | **SECURE**

RAVPN
Enter Description Save Cancel

Policy Assignments (1)

Local Realm: None Dynamic Access Policy: None

Connection Profile Access Interfaces **Advanced** 1

AnyConnect Client Images
Address Assignment Policy
Certificate Maps
Group Policies 2
LDAP Attribute Mapping
Load Balancing
IPsec
Crypto Maps

Group Policies
Group policy can be assigned to VPN user through connection profile or by RADIUS server during authentication.
Following are the group policies that are associated with this Remote Access VPN configuration. Add a group policy if it is required to be assigned by RADIUS server during authentication.

Name	Protocol	DNS Servers	VPN Filter
DfltGrpPolicy	SPLIT		

FMC RAVPN Adv GP

Group Policy ?

Available Group Policy ↻ +

Search

DfltGrpPolicy

Add

Add

Selected Group Policy

DfltGrpPolicy 🗑️

Cancel OK

GP Add dialog

Edit Group Policy



Name:*

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

Banner:

Maximum total size: 3999, Maximum characters in a line : 497.

In case of a line spanning more than 497 characters, split the line into multiple lines.

** Only plain text is supported (symbols '<' and '>' are not allowed)

Welcome Admins!

Cancel

Save

New Standard Access List Object



Name

Admins-ACL

▼ Entries (1)

Add

Sequence No	Action	Network	
1	Allow	FinanceServer SalesServer	

Allow Overrides

Cancel

Save

Edit Group Policy



Name:*

Admins

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IPv4 Split Tunneling:

Tunnel networks specified below ▼

IPv6 Split Tunneling:

Allow all traffic over tunnel ▼

Split Tunnel Network List Type:

Standard Access List Extended Access List

Standard Access List:

Admins-ACL ▼



DNS Request Split Tunneling

DNS Requests:

Send DNS requests as per split t ▼

Domain List:

Cancel

Save

Admin GP ACL dialog

9. Similarly, create the remaining two groups `Finance` and `Sales`. In this lab, they are configured with banner values `Welcome Finance Team!` and `Welcome Sales Team!` respectively. They are also configured with split tunneling like the `Admins` group with them accessing only their servers, that is, the `Finance` group can access only `FinanceServer` and the `Sales` group can only access `SalesServer`.

10. Once created, add all of them and click OK.

Group Policy



Available Group Policy

Admins


DfltGrpPolicy

Finance

Sales

Add

Selected Group Policy

DfltGrpPolicy 

Finance 

Sales 

Admins 

Cancel

OK

Add All GP

11. Ensure to click **Save** on the top right corner and deploy the changes.

12. The required configurations on FTD/FMC are completed. The remaining SAML configuration on Okta is configured in the next section.

Okta - SAML Configuration Part #2

1. Navigate to **Applications > Applications** and click **Application > Sign on Section > Edit**.

2. The custom group attribute configured in Okta - SAML Config Part #1 which is `cisco_group_policy`, must be sent in the SAML assertion. Click the dropdown arrow to the left of **Attributes (Optional)** and in the **Group Attributes Statements (Optional)**, use the group as **Name** and `cisco_group_policy` as **Filter** which matches the regex `^(?!Everyone).*` as shown.

- Dashboard
- Directory
- Customizations
- Applications** ¹
- Applications ²
- Self Service
- API Service Integrations
- Security

[← Back to Applications](#)



Cisco Secure Firewall

Active



[View Logs](#) [Monitor Imports](#)

[General](#) [Sign On](#) [Import](#) [Assignments](#)

Settings

³

[Edit](#)

Sign on methods

Okta Sign on Settings

Attributes (Optional) [Learn More](#)

Attribute Statements (optional)

Name	Value
------	-------

Group Attribute Statements (optional)

Name	Filter
------	--------

cisco_group_policy	Matches regex <code>^(?!Everyone).*</code>
--------------------	--

Okta App attribute



Note: The Regex filter `^(?!Everyone).*`, gives the groups assigned to the user (which is only one per user in this lab) except Everyone, and send it as a value of `cisco_group_policy` in the SAML assertion.

4. Click **Preview SAML** in order to see what the assertion looks like.

5. Under **Advanced Settings** fill the values in the field, in order to complete the SAML configuration on Okta. Once done, click **Save**.

Entity ID: `https://<VPN Base URL>/saml/sp/metadata/<Connection Profile Name>`

Assertion Consumer URL: `https://<VPN Base URL>/+CSCOE+/saml/sp/acs?tname=<Connection Profile Name>`

Single Logout Service URL: `https://<VPN Base URL>/+CSCOE+/saml/sp/logout`

Advanced Sign-on Settings

These fields may be required for a Cisco ASA VPN (SAML) proprietary sign-on option or general setting.

Assertion Consumer Service URL

`https://ftd.ciscolabs.com/+CSCOE+/saml/sp/acs?tgname=`

Please enter your Assertion Consumer Service URL. Refer to the Setup Instructions above to obtain this value.

SP Entity ID

`https://ftd.ciscolabs.com/saml/sp/metadata/RAVPN`

Please enter your SP Entity ID. Refer to the Setup Instructions above to obtain this value.

Single Logout Service URL

`https://ftd.ciscolabs.com/+CSCOE+/saml/sp/logout`

Please enter your Single Logout Service URL (optional). Refer to the Setup Instructions above to obtain this value.

Credentials Details

Application username format

Okta username



Update application username on

Create and update



Password reveal

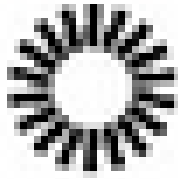
Allow users to securely see their password
(Recommended)



Password reveal is disabled, since this app is using SAML with no password.

Save

1. Start by configuring the groups, create three groups based on the Network Diagram, Admins, Finance, and Sales.
2. Log in to Okta Admin Dashboard. Navigate to Directory > Groups.



okta

Dashboard



Directory

1



People

Groups

2

Devices

Profile Editor

Directory Integrations

and fill in the value with the name of the Group Policy you want that group to be assigned. Configure the value Sales in order to keep it simple. Once done, click Save.

Sales

Actions ▾

Sales Team

Created: 9/3/2023 Last modified: 9/3/2023 [View logs](#)

People Applications **Profile**¹ Directories Admin roles

Profile

Attributes Cancel

Name
name

Description
description

Cisco AnyConnect Group Policy
cisco_group_policy ²

³

Okta Sales Group

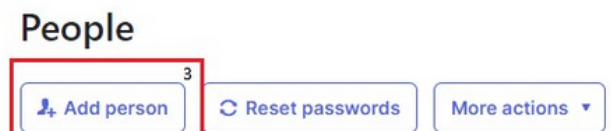
11. Repeat the same steps for the groups Admins and Finance. Configure the value for cisco_group_policy to Admins and Finance respectively.



Note: The value of `cisco_group_policy` must be exactly the same as the group policy name configured earlier.


12. Next, create some users and assign them to the groups created in the previous steps. Navigate to `Directory > People` and click `Add Person`.

13. Create three users to test the lab, `FinanceUser`, `SalesUser`, and `AdminUser` that belong to `Finance`, `Sales`, and `Admins` groups respectively. The image shows an example for `FinanceUser` groups.



Okta add person

Add Person

User type 

First name

Last name

Username

Primary email

Secondary email (optional)

Groups (optional)

Activation

I will set password

To create new users with password, enrollment policy must set password as required

User must change password on first login

Do not send unsolicited or unauthorized activation emails. [Read more](#)

Okta finance user

14. Repeat the same steps for the remaining two users; AdminUser and SalesUser.

15. The final step is to add the groups created to the SAML application. Navigate to Applications > Applications >

Edit > Assignments. Click Assign > Assign to Groups. Assign to the three groups created earlier and click Done.

The screenshot shows the Okta administration interface. On the left, a navigation menu has 'Applications' (1) selected under 'Customizations', and a sub-menu 'Applications' (2) is open. The main area shows the 'Cisco Secure Firewall' configuration page. The 'Assignments' tab (3) is active. An 'Assign' button (4) is highlighted, and its dropdown menu is open, showing 'Assign to Groups' (5) as the selected option. Other options in the dropdown include 'Assign to People'.

Okta assign user to group

The dialog box is titled 'Assign Cisco Secure Firewall to Groups' and features a search bar at the top. Below the search bar, there is a list of groups with their status:

Group Name	Status
Admins Admin Team	Assigned
Everyone All users in your organization	Assign
Finance Finance Team	Assigned
Sales Sales Team	Assigned

A blue 'Done' button is located at the bottom right of the dialog box.

Okta group assign

Verify

Finance User

Banner

Cisco Secure Client

Welcome Finance Team!

Finance team banner

Secured Routes

Virtual Private Network (VPN)

Non-Secured Routes (IPv4) _____
0.0.0.0/0

Secured Routes (IPv4) _____
192.168.100.25/32

Server Reachability

```
C:\Users\user>ping 192.168.100.25

Pinging 192.168.100.25 with 32 bytes of data:
Reply from 192.168.100.25: bytes=32 time=3ms TTL=255
Reply from 192.168.100.25: bytes=32 time=10ms TTL=255
Reply from 192.168.100.25: bytes=32 time=2ms TTL=255
Reply from 192.168.100.25: bytes=32 time=7ms TTL=255

Ping statistics for 192.168.100.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 10ms, Average = 5ms

C:\Users\user>ping 192.168.200.25

Pinging 192.168.200.25 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.200.25:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

ICMP to destination

Session on FTD

<#root>

```
firepower# sh vpn-sessiondb anyconnect filter name FinanceUser@xxxxxxx
Username : FinanceUser@xxxxxxx      Index : 14
Assigned IP : 10.72.1.1                Public IP : 10.106.68.246
```

----- OUTPUT OMITTED -----

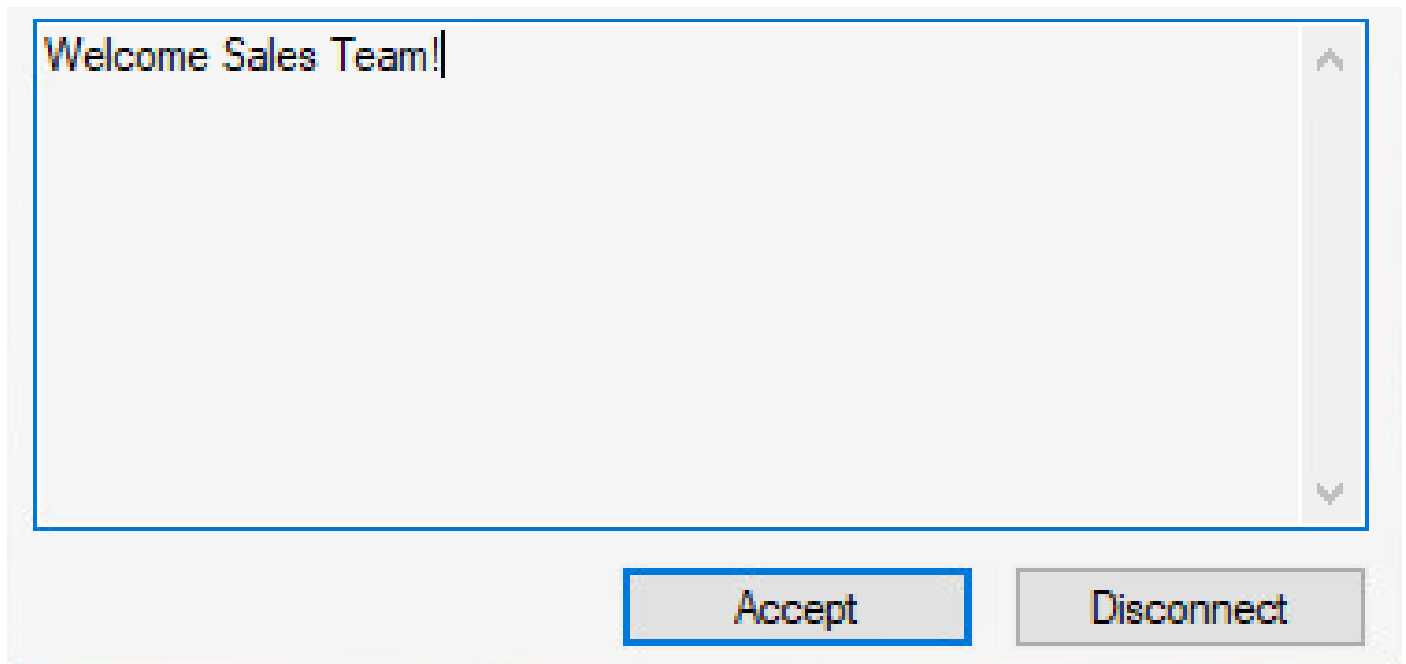
```
Group Policy : Finance                Tunnel Group : RAVPN
```

Duration : 0h:03m:26s

Sales User

Banner

Cisco Secure Client



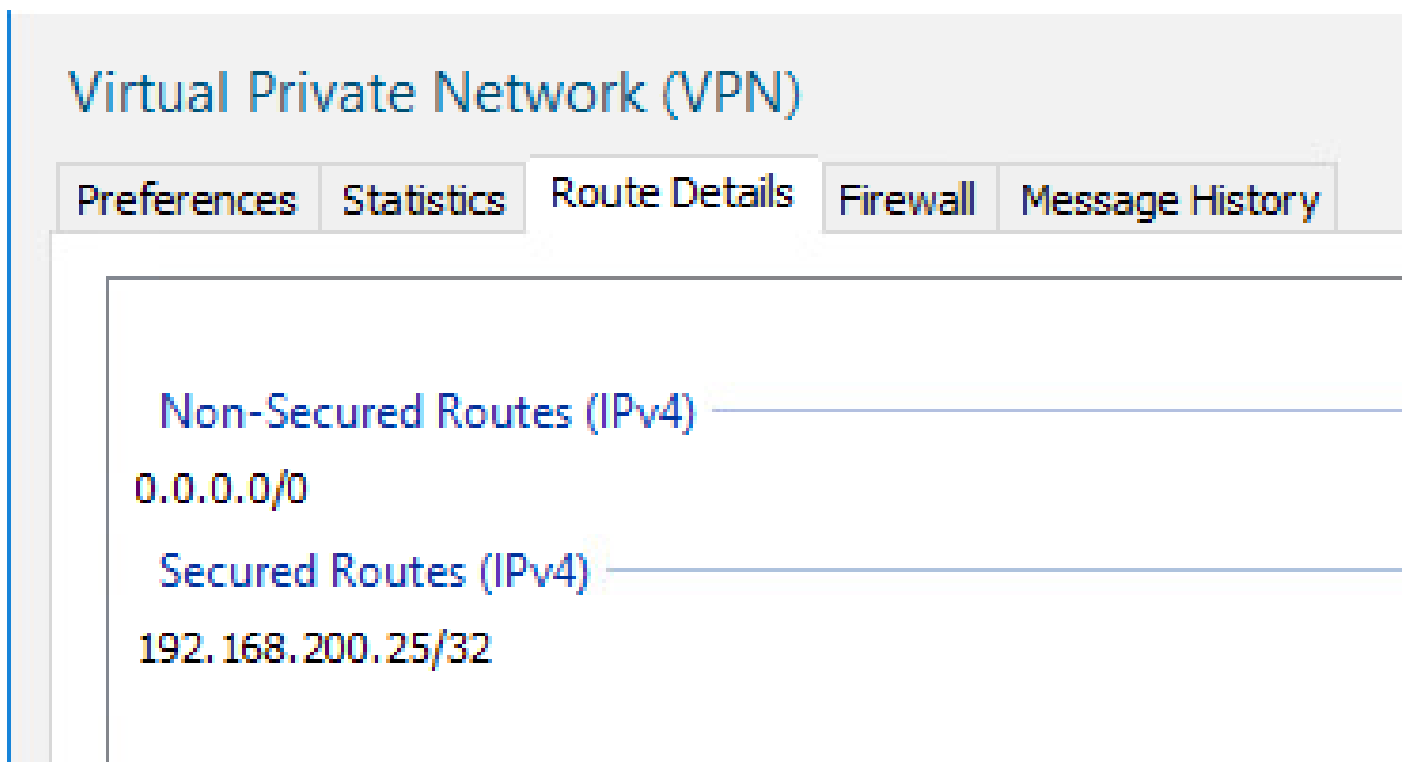
>Welcome Sales Team!

Accept Disconnect

The screenshot shows a Cisco Secure Client interface. At the top, the text "Cisco Secure Client" is displayed. Below it is a large text area containing the banner message "Welcome Sales Team!". At the bottom of the interface, there are two buttons: "Accept" and "Disconnect".

Sales Team banner

Secured Routes



Virtual Private Network (VPN)

Preferences Statistics Route Details Firewall Message History

Non-Secured Routes (IPv4)

0.0.0.0/0

Secured Routes (IPv4)

192.168.200.25/32

The screenshot displays the "Secured Routes" configuration page within a VPN client. The page title is "Virtual Private Network (VPN)". Below the title, there are five tabs: "Preferences", "Statistics", "Route Details", "Firewall", and "Message History". The "Route Details" tab is currently selected. The main content area is divided into two sections. The first section is titled "Non-Secured Routes (IPv4)" and lists the route "0.0.0.0/0". The second section is titled "Secured Routes (IPv4)" and lists the route "192.168.200.25/32".

Server Reachability

```
C:\Users\user>ping 192.168.100.25

Pinging 192.168.100.25 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.100.25:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\user>ping 192.168.200.25

Pinging 192.168.200.25 with 32 bytes of data:
Reply from 192.168.200.25: bytes=32 time=4ms TTL=255
Reply from 192.168.200.25: bytes=32 time=2ms TTL=255
Reply from 192.168.200.25: bytes=32 time=3ms TTL=255
Reply from 192.168.200.25: bytes=32 time=3ms TTL=255

Ping statistics for 192.168.200.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 3ms
```

ICMP to destination

Session on FTD

<#root>

```
firepower# sh vpn-sessiondb anyconnect filter name SalesUser@xxxxxxx
Username : SalesUser@xxxxxxx Index : 15
```

```
Assigned IP : 10.72.1.1          Public IP : 10.106.68.246
```

----- OUTPUT OMMITTED -----

```
Group Policy : Sales          Tunnel Group : RAVPN
```

```
Duration : 0h:02m:57s
```


Admin User

Banner

Cisco Secure Client

Welcome Admins!

Accept

Disconnect

Admin team banner

Secured Routes

Virtual Private Network (VPN)

Preferences

Statistics

Route Details

Firewall

Message History

Non-Secured Routes (IPv4)

0.0.0.0/0

Secured Routes (IPv4)

192.168.100.25/32

192.168.200.25/32

Server Reachability

```
C:\Users\user>ping 192.168.100.25

Pinging 192.168.100.25 with 32 bytes of data:
Reply from 192.168.100.25: bytes=32 time=2ms TTL=255
Reply from 192.168.100.25: bytes=32 time=2ms TTL=255
Reply from 192.168.100.25: bytes=32 time=2ms TTL=255
Reply from 192.168.100.25: bytes=32 time=3ms TTL=255

Ping statistics for 192.168.100.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\user>ping 192.168.200.25

Pinging 192.168.200.25 with 32 bytes of data:
Reply from 192.168.200.25: bytes=32 time=2ms TTL=255
Reply from 192.168.200.25: bytes=32 time=2ms TTL=255
Reply from 192.168.200.25: bytes=32 time=2ms TTL=255
Reply from 192.168.200.25: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.200.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

ICMP to destination

Session on FTD

<#root>

```
firepower# sh vpn-sessiondb anyconnect filter name AdminUser@xxxxxxx
```

```
Username : AdminUser@xxxxxxx Index : 16
```

```
Assigned IP : 10.72.1.1
```

```
Public IP : 10.106.68.246
```

```
----- OUTPUT OMMITTED -----
```

```
Group Policy : Admins
```

```
Tunnel Group : RAVPN
```

Duration : 0h:03m:05s

Troubleshoot

1. Ensure the time is synchronized on FTD and Okta. Check the same using `show clock` on the FTD CLI.

```
firepower# sh clock
05:14:52.494 UTC Mon Sep 4 2023
```

2. Apply SAML debugs in order to confirm if the SAML assertion is a Success.

<#root>

```
firepower# debug webvpn saml 255
----- OUTPUT OMMITTED -----
```

```
Sep 04 05:20:42
[SAML] consume_assertion:
http://www[.]okta[.]com/XXXXXXXXXXXXXXXX FinanceUser@xxxxxxx

[saml] webvpn_login_primary_username: SAML assertion validation succeeded
```

```
----- OUTPUT OMMITTED -----
```

3. Refer to [this](#) document in order to troubleshoot common issues found on the client side.