Configure Certificate Authentication & DUO SAML Authentication

Contents

Introduction **Prerequisites Requirements Components Used** Configure Steps on DUO Create an Application Protection Policy **Create Application Policy** Configuration Steps for FMC **Deploy Identity Certificate to the FTD** Deploy IDP certificate to the FTD Creating the SAML SSO Object Create Remote Access Virtual Private Network (RAVPN) Configuration Verify Troubleshoot Issue 1: Certificate authentication failing. issue 2: SAML failures

Introduction

This document describes an example of the implementation of certificate-based authentication and duo SAML authentication.

Prerequisites

The tools and devices used in the guide are:

- Cisco Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- Internal Certificate Authority (CA)
- Cisco DUO Premier Account
- Cisco DUO Authentication Proxy
- Cisco Secure Client (CSC)

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic VPN,
- SSL/TLS
- Public Key Infrastucture
- Experience with FMC
- Cisco Secure Client
- FTD code 7.2.0 or Higher
- Cisco DUO Authentication Proxy

Components Used

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

- Cisco FTD (7.3.1)
- Cisco FMC (7.3.1)
- Cisco Secure Client (5.0.02075)
- Cisco DUO Authentication Proxy (6.0.1)
- Mac OS (13.4.1)
- Active Directory

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.

Configure Steps on DUO

This section describes the steps to configure Cisco DUO Single Sign-on (SSO). Before you begin, be sure to have the authentication proxy implemented.

Warning: If an authentication proxy has not been implemented, this link has the guide for this task. <u>DUO Authentication Proxy Guide</u>

Create an Application Protection Policy

Step 1. Sign on to the admin panel via this link Cisco Duo



Cisco DUO homepage

Step 2. Navigate to Dashboard > Applications > Protect an Application.

In the search bar, enter "Cisco Firepower Threat Defense VPN" and select "Protect".

	Bilt	Q Search for users, groups, applications, or devices		Cisco ID:			
	Dashboard	Dashboard > Applications > Protect an Application					
	Device Insight	Protect on Application					
	Policies						
ľ	Applications	Cisco Firepower Threat Defense VPN					
Į	Protect an Application						
	Single Sign-On	Application	Protection Type				
	Users						
	Groups	CISCO Cisco Firepower Threat Defense VPN	2FA	Documentat			
	Render allaka						

- Identity Provider Entity ID SSO URL
- Logout URL

See the Cisco ASA SSO documentation II to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID	Сору
Sign In URL	Сору
Sign Out URL	Сору

Example of information to copy

Note: The links have been omitted from the screenshot.

Step 4. Select "Download certificate" to download the Identity Provider Certificate under Downloads.

Step 5. Fill in the Service Provider Information

Cisco Firepower Base URL- The FQDN used to reach the FTD

Connection Profile Name- The Tunnel-Group Name

Create Application Policy

Step 1: To create an **Application Policy** under **Policy** Select "**Apply a policy to all users**" then select "**Or**, **create a new Policy**" as shown in the image.

Policy

Policy defines when and how users will authenticate when accessing this application. Your global policy always applies, but you can override its



: "Skip Check for CA flag in basic constraints of the CA Certificate" can be used if needed. Use this option with caution.

Step 4: Select the newly created certificate enrollment object under "**Cert Enrollment***:" then select "**Add**" as shown in the image.

Add New Certificate

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

Device*:									
HA •									
Cert Enrollment*:									
duocert	▼ +								
Cert Enrollment Details:									
Name: Enrollment Type: Enrollment URL:	duocert Manual (CA Only) N/A								

Screenshot of added certificate enrollment object and device

Note: Once added, the certificate deploys' immediately.

Creating the SAML SSO Object

This section describes the steps to configure SAML SSO via FMC. Before you begin, be sure to deploy all configurations.

Step 1. Navigate to **Objects > AAA Server > Single Sign-on Server** and select "**Add Single Sign-on Server**".

Objects

"Certificate Enrollment:*": Idenity certificate created during "Deploy Identity Certificate to the FTD" portion of this guide



Step 4 of RAVPN wizard

Tip: If this has not been created, add a new certificate enrollment object by selecting the "+."

Step 6. Summary

Verify all the information. If everything is correct, continue with 'Finish."

Firewall Management Center Devices / VPN / Serue Weard	Overview	Analysis	Policies	Devices	Objects	Integration				
Remote Access VPN Policy Wizard Policy Assignment ③ Connection Profile ③ Secure Client ④ Access & Certificate ④ Summary										
						Ramada Usar — Secur	e Giera Datasé	Ven. Prode Corporate Device Resources		
						Remote Access VPN Policy C	Configuration	AAA Additional Configuration Requirements		
						Name: Device Targets:	ngure an iou trins Policy with the following settings DUO HA	After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.		
						Connection Profile:	DUO	Access Control Policy Update		
						Connection Allas:	Duo	An Access Control rule must be defined to allow		
						Authoritation Mathedi	Class Castleone & SAME	VPN traffic on all targeted devices.		
						SIMI Login Experience:	VPN client embedded browser	NAT Exemption		
						Username From Certificate:		If NAT is enabled on the targeted devices, you		
						Authentication Server:	duosso (550)	must define a NAT Policy to exempt VPN traffic.		
						Authorization Server:		DNS Configuration		
						Accounting Server:		To resolve hostname specified in AAA Servers		
					Address Assignment: or CA		or CA Servers, configure DNS using RexConfig			
						Address from AAA:		Policy on the targeted devices.		
N						DHCP Servers:	Tcoutrie-SRV	Port Configuration		
						Address Pools (IPv4):		SSL will be enabled on port 443.		
						Address Pools (Pv6):	- Distantiation	Please ensure that these ports are not used in NAT Deliver or other particles before decipated		
						Group Policy:	clares secure class mana-5.0.02025 webdening	the configuration.		
						aecure Caent Images:	k9.pkg cisco-secure-client-win-5.0.02075-webdeploy-k9.	A Network Interface Configuration		