



On-line dvakrát týdně

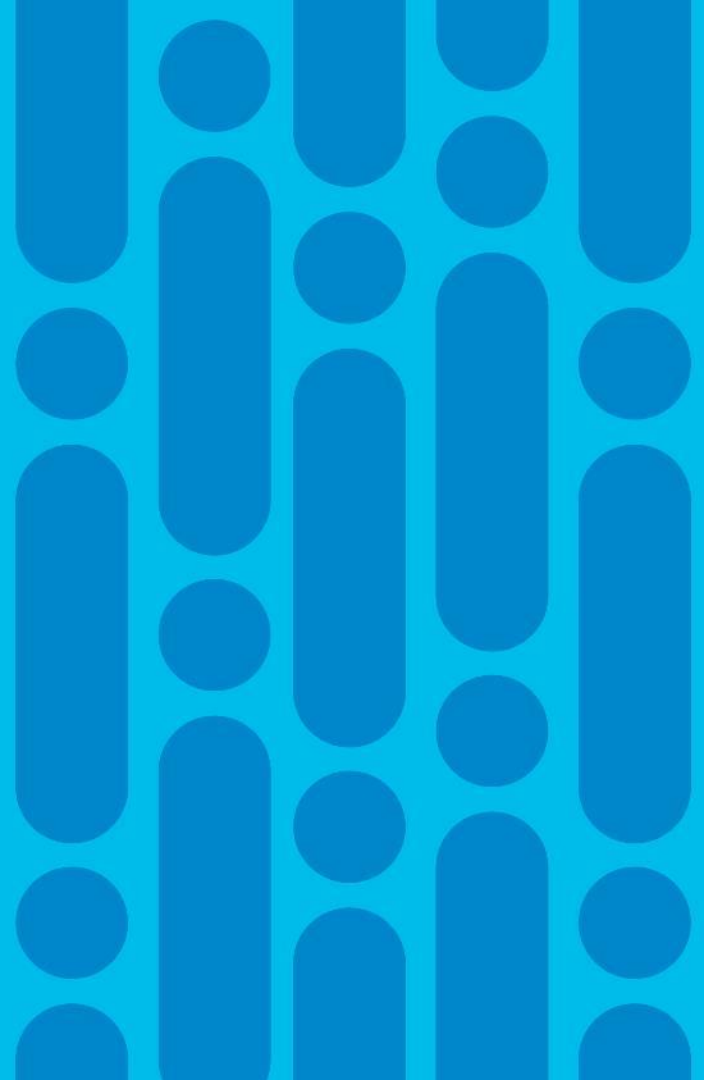
Cisco Tech Club Webinář:

VPN řešení a integrace s MFA (DUO), ASA, FTD

Přednášející: Jiří Tesař, Technical Solution Architect – Security

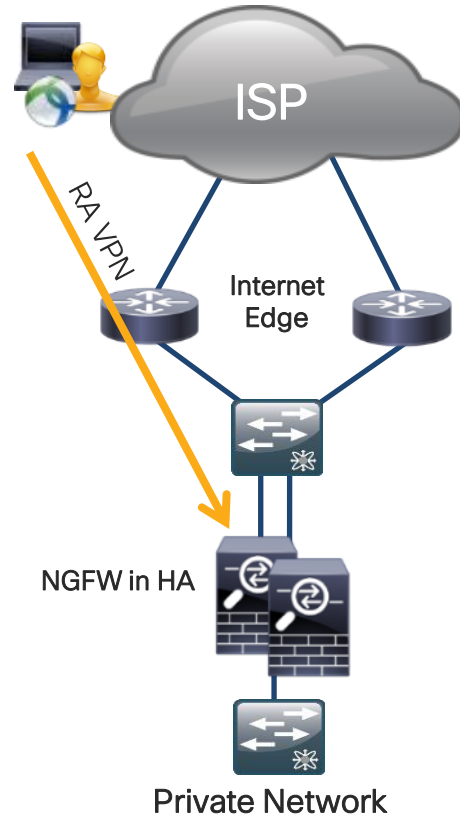
14.4. 2020

FTD Remote Access VPN (RA VPN) And Duo



Remote Access VPN - Use Case

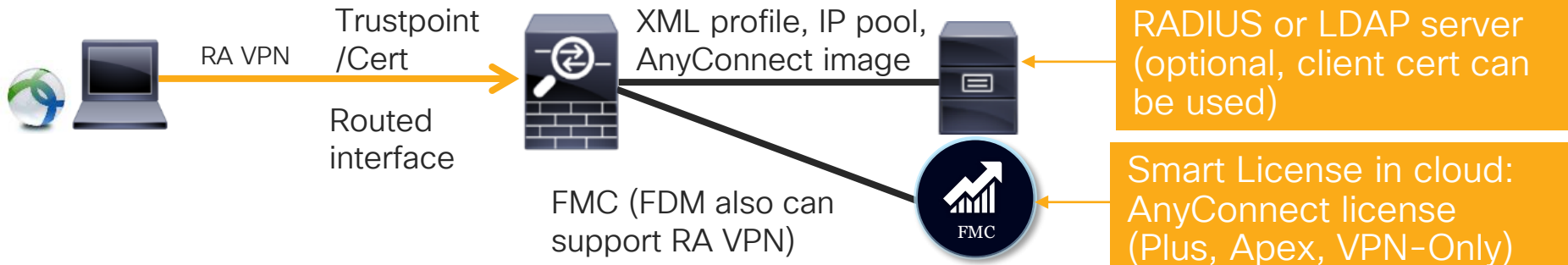
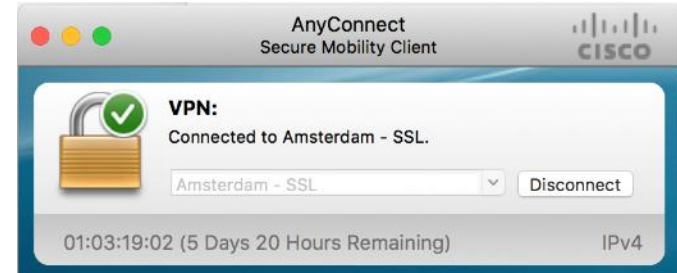
- **TLS/IPsec** AnyConnect access
- **Split Tunneling or Backhauling** to handle traffic from remote users to Internet
- **AMP/ File and IPS** inspection policies
- **Application** level inspection
- Easy **Wizard** to configure RA VPN



Remote Access VPN & FTD

- AMP/ File and IPS inspection policies
- Application level inspection
- FTD version 6.2.2 and later
- RA VPN protocols:
 - Transport Layer Security (TLS)
 - Internet Key Exchange version 2 (IKEv2)
- Service and code came from ASA

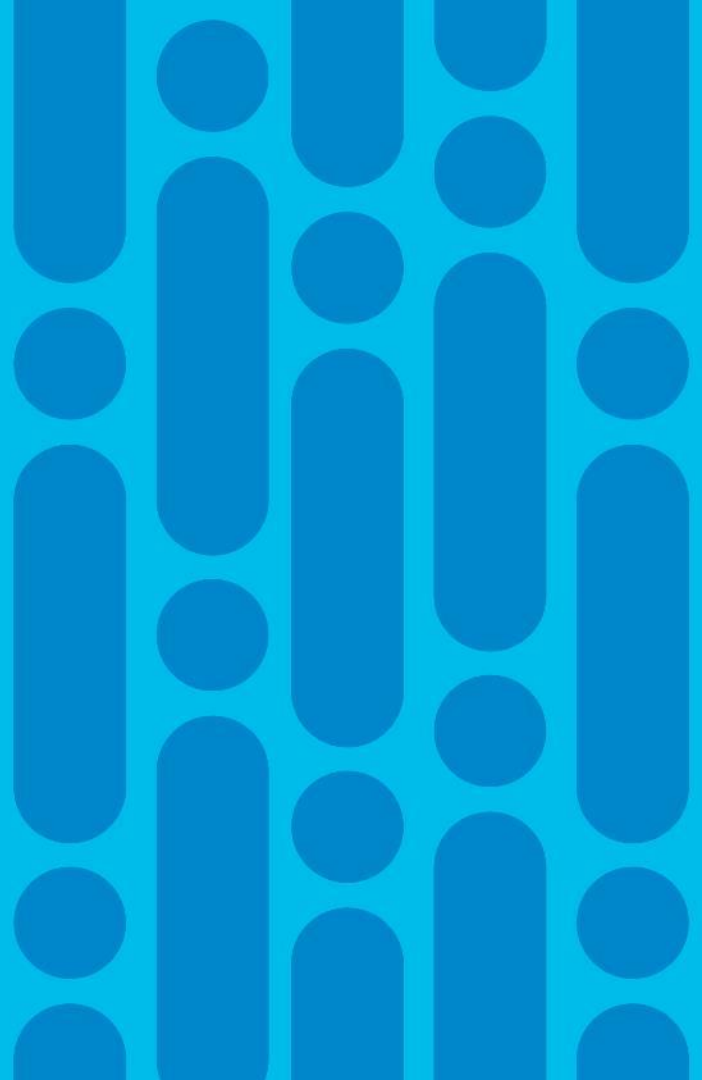
- Cisco AnyConnect from 4.x



Supported RA VPN Features on FTD

- IPv4 & IPv6. All combinations
- Both FMC and FDM, Device specific overrides
- Both FMC and FMC HA environments
- Multiple interfaces and multiple AAA servers
- From 6.3:
 - ISE posture, RADIUS CoA
 - RADIUS timeout (MFA with Duo)
- AAA
 - Server authentication using self-signed or CA-signed identity certificates
 - AAA username and password-based remote authentication using RADIUS or LDAP/AD
 - RADIUS group and user authorization attributes, and RADIUS accounting
 - NGFW Access Control integration using VPN Identity
- From: 6.4:
 - Secondary Authentication
- From 6.5:
 - Remote access VPN two-factor authentication using Duo LDAP
- VPN Tunneling
 - Address assignment
 - Split tunneling
 - Split DNS
 - Client Firewall ACLs
 - Session Timeouts for maximum connect and idle time
- Monitoring
 - VPN Dashboard Widget
 - RA VPN events including
 - Tunnel statistics available (CLI)

Pre-Configuration Before Remote Access VPN Wizard

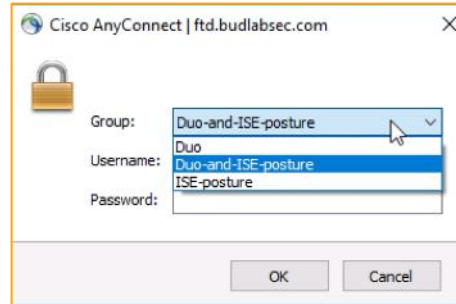
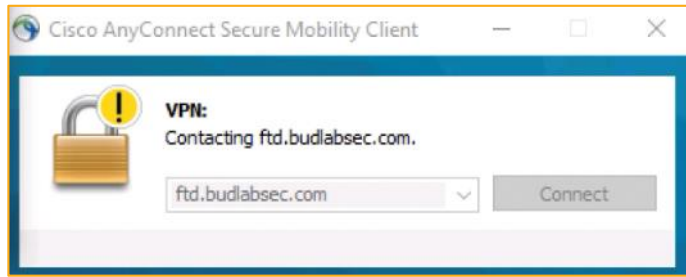


Tasks Before the Remote Access VPN Wizard

1. Create a **certificate** used for server authentication (for production)
2. Configure RADIUS or LDAP server for **user authentication** (no local auth yet, optional, client cert is supported)
3. Create **pool** of addresses for VPN users (optional, wizard helps)
4. Creating XML **profile** (optional, Profile Editor can be used)
5. Upload AnyConnect **images** for different platforms (optional, wizard helps)

RA VPN Components

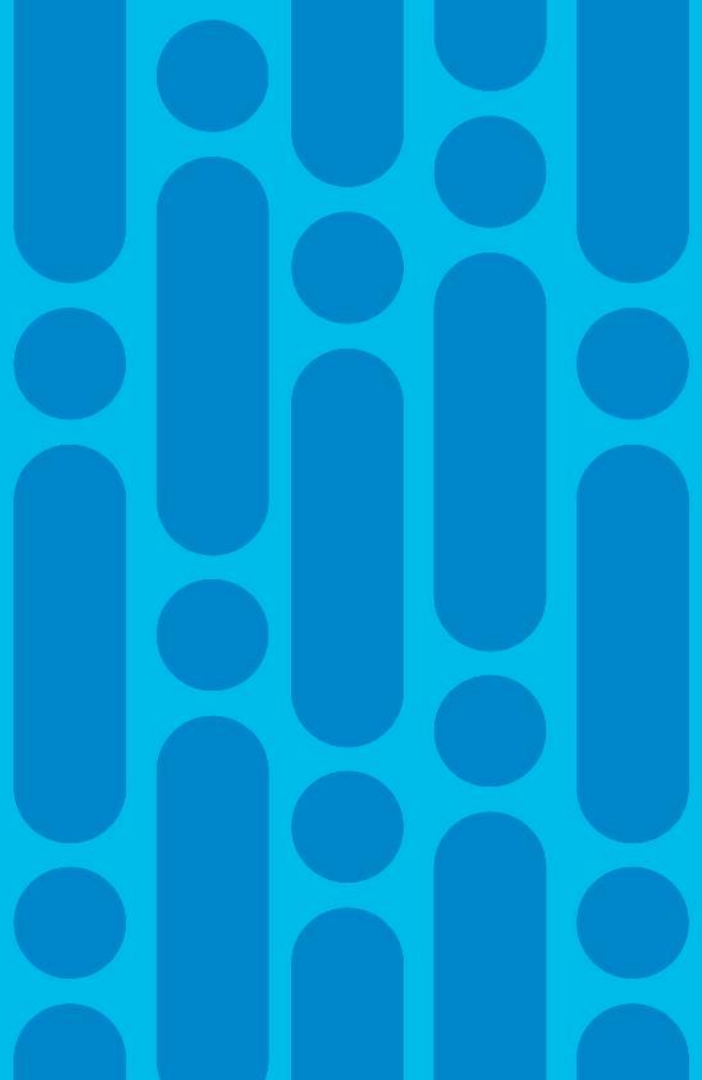
- **Connection profiles** – determine how **authentication** is performed



Connection Profiles

- **Group policies** – a set of user-oriented **attribute/value pairs** for RA VPN users
 - DNS/WINS, SSL/DTLS, timeouts, client bypass protocol and DHCP network scope
 - Split tunnel and split DNS configuration, VPN filter, **egress VLAN** and client firewall rules
 - AnyConnect client profile, SSL/DTLS settings and connection settings

Remote Access VPN Wizard



RA VPN Wizard

Pre-Configuration:
“Before You Start”

- Devices > VPN > Remote Access > Add

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

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

Targeted Devices and Protocols

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

Name:* VPN-profile

Description:

VPN Protocols: ☒ SSL ☒ IPsec-IKEv2

Targeted Devices: Available Devices Selected Devices

Search

10.62.42.99

Add

10.62.42.99

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure [Realm](#) or [RADIUS Server Group](#) to authenticate VPN clients.

AnyConnect Client Package

Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

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.

Remote Access VPN Policy Wizard

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

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:* VPN-profile

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:* AAA Only
Authorization Server: Client Certificate Only
Accounting Server: Client Certificate & AAA

+ (Realm or RADIUS)
+ (RADIUS)
+ (RADIUS)

Client Address Assignment:

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

- ☐ Use AAA Server (RADIUS only) i
☐ Use DHCP Servers
☒ Use IP Address Pools

IPv4 Address Pools: pool10

IPv6 Address Pools:

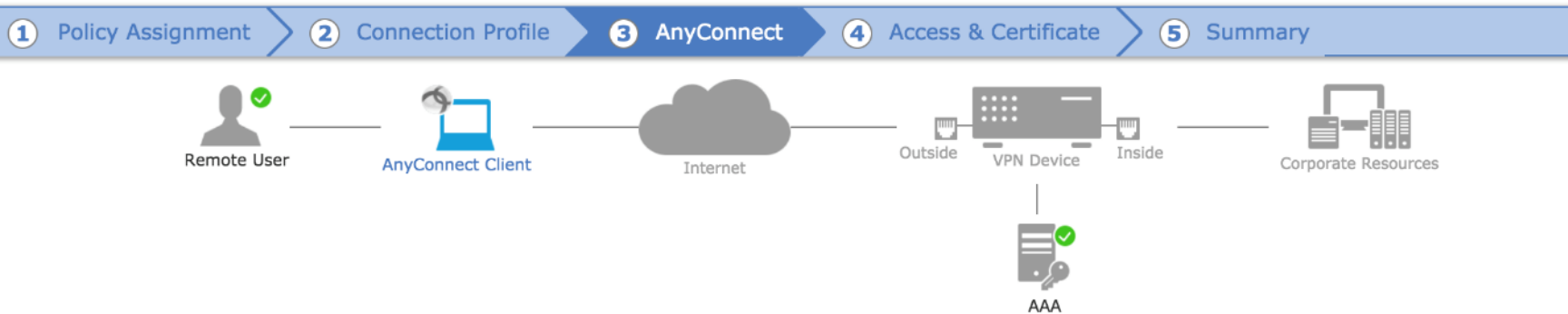
Group Policy:

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

Group Policy:* DfltGrpPolicy

RADIUS Server (like ISE) can change it with RADIUS CLASS attribute IETF-Class-25 (OU= group-policy-name)

Remote Access VPN Policy Wizard



Remote User

AnyConnect Client

Internet

VPN Device

Corporate Resources

AAA

AnyConnect Client Image

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

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

Show Re-order buttons

<input type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	AnyConnect-4.7	anyconnect-win-4.7.00136-webdeploy-k9.pkg	Windows
<input type="checkbox"/>	AnyCon	anyconnect-win-4.6.03049-webdeploy-k9.pkg	Windows

Add AnyConnect File

Name:*

AnyConnect-Win

File Name:*

anyconnect-win-4.6.03049-webdeploy-k9.pk

Browse..

File Type:*

AnyConnect Client Image

Description:

AnyConnect Windows

Save

Cancel

OverviewAnalysisPolicies**Devices**ObjectsAMPIntelligence

Device ManagementNAT**VPN > Remote Access**QoSPlatform SettingsFlexConfigCertificates

Remote Access VPN Policy Wizard

1 Policy Assignment2 Connection Profile3 AnyConnect4 Access & Certificate5 Summary

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:*

outside-zone

+

☒ Enable DTLS on member interfaces

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:*

outside-cert

+

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

☒ Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

“outside-zone” is a zone and FTD’s outside interface is a member

New in 6.3, earlier: configured ACL or “sysopt permit-vpn” command in FlexConfig

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public 13

Remote Access VPN Policy Wizard

1 Policy Assignment

2 Connection Profile










3 AnyConnect

4 Access & Certificate

5 Summary






Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name:	VPN-profile
Device Targets:	 10.62.42.99
Connection Profile:	VPN-profile
Connection Alias:	VPN-profile
AAA:	
Authentication Method:	AAA Only
Authentication Server:	 DuoRADIUS-Server-Group
Authorization Server:	 DuoRADIUS-Server-Group
Accounting Server:	 DuoRADIUS-Server-Group
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	 pool10
Address Pools (IPv6):	-
Group Policy:	 DfltGrpPolicy
AnyConnect Images:	 AnyConnect-Win
Interface Objects:	 outside-zone
Device Certificates:	 outside-cert

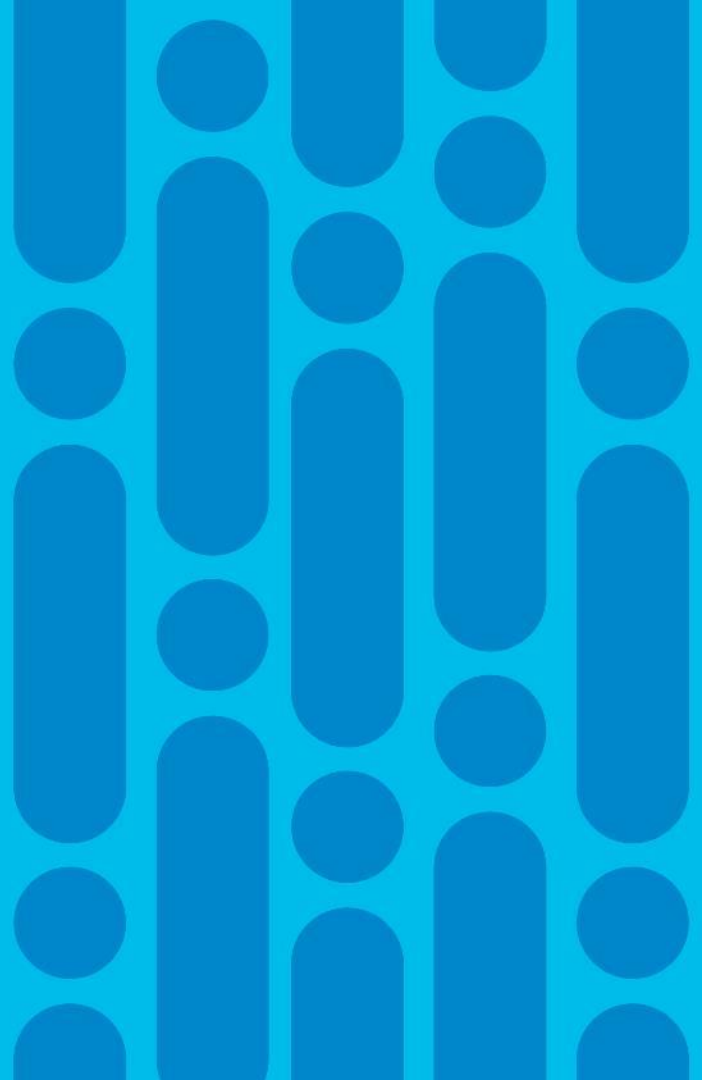
Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

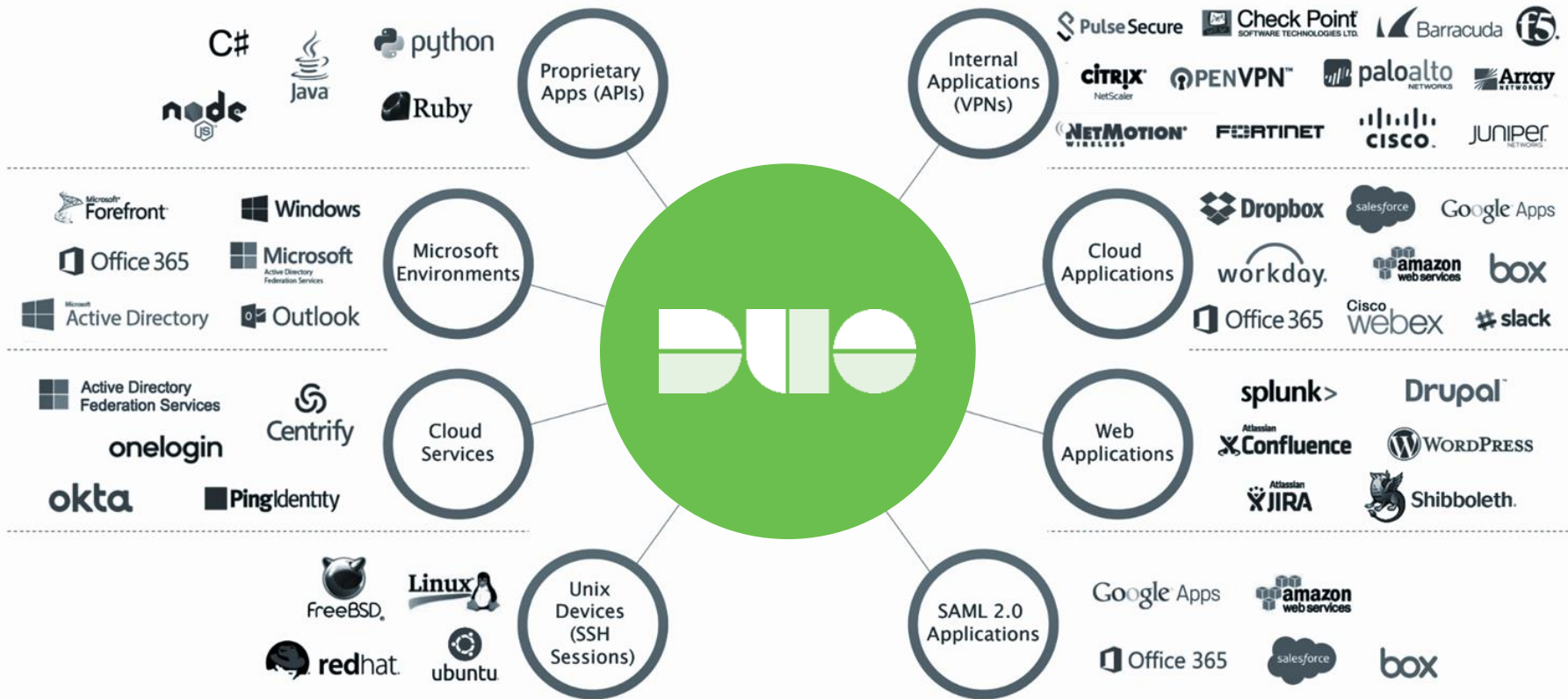
-  **Access Control Policy Update**
An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
-  **NAT Exemption**
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
-  **DNS Configuration**
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
-  **Port Configuration**
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.
-  **Network Interface Configuration**
Make sure to add interface from targeted devices to SecurityZone object 'outside-zone'

After Wizard Configuration

FTD RA VPN with Duo Security Multi-Factor Authentication (MFA)



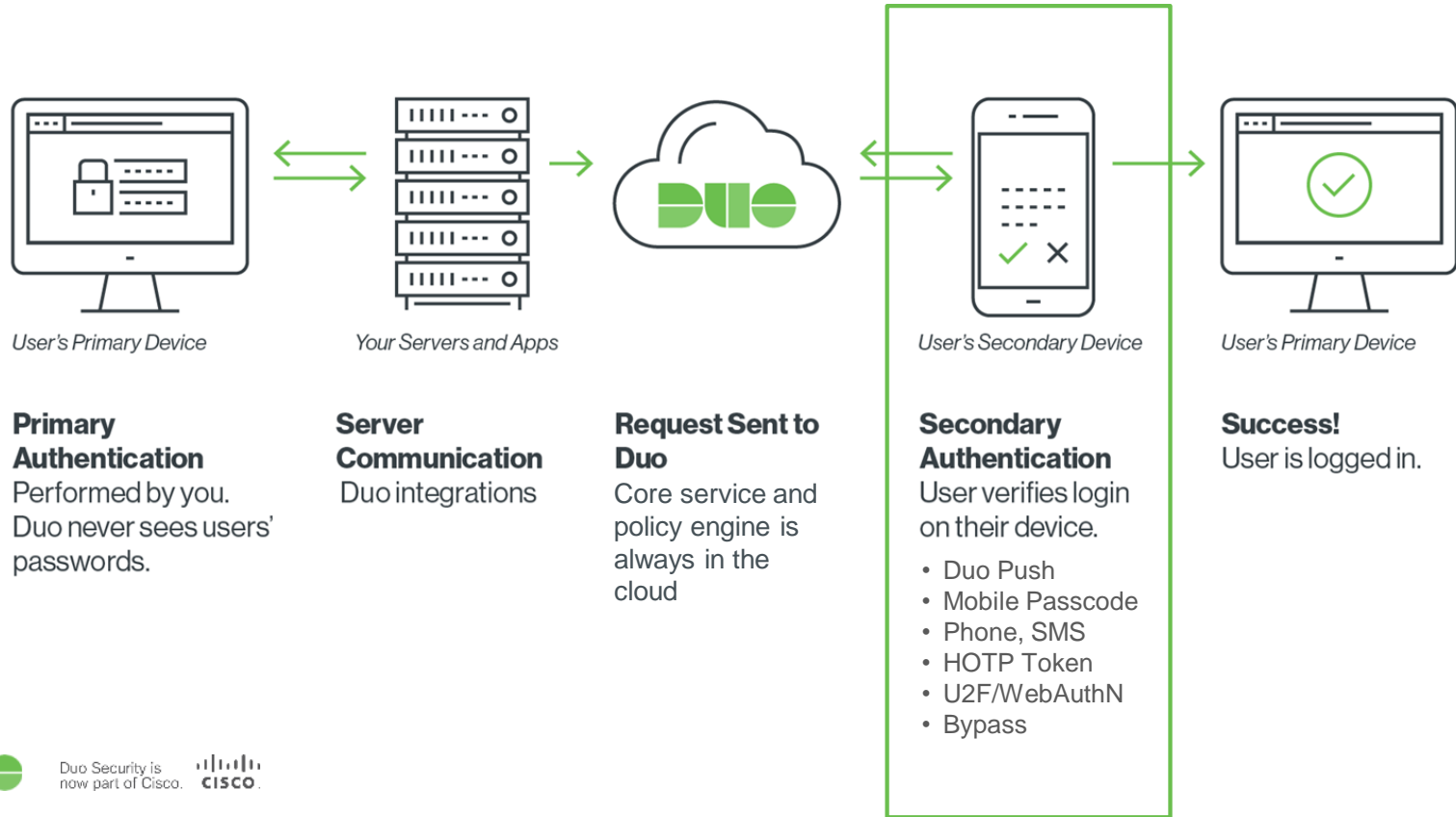
Secure Any Corporate Application



Duo Security is
now part of Cisco.



Duo never touches the primary authentication

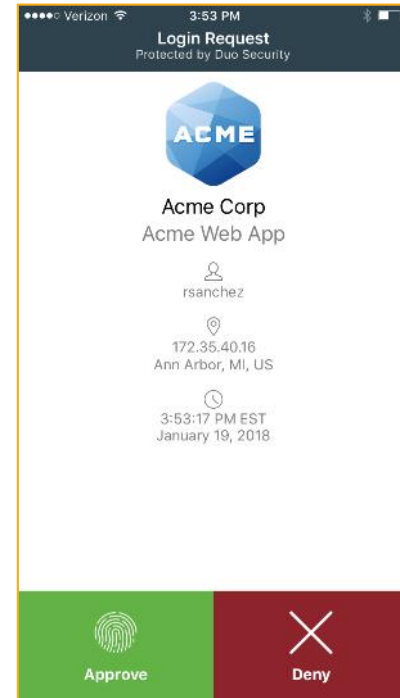


Duo Security is
now part of Cisco.



Duo Security Introduction

- Started as a multi-factor authentication (MFA) and later Zero Trust Security with device posture, adaptive authentication and SAML (Security Assertion Markup Language) support
- Policy decision point: cloud only
- 3 different methods for ASA RA VPN and FTD can support 2 methods from 6.3 (RADIUS proxy, LDAPs) now
- More information:
 - Application and User-centric Protection with Duo Security, BRKSEC-2382

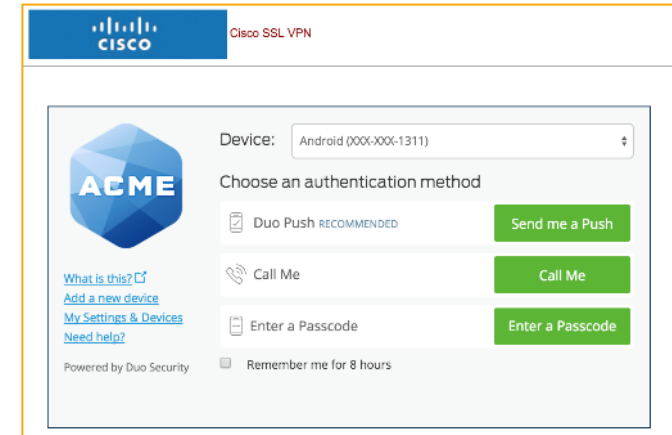


Duo Security with ASA Integration

- “**Modify the iframe**” and Secondary Auth.; push/phone or sms; but users do not like 2nd pass code on AnyConnect; <http://duo.com/docs/cisco>
- Alternative configuration: “auto-push” with **Duo Auth Proxy**, AnyConnect has only 2 fields only! <http://duo.com/docs/cisco-alt>
- **SAML integration**: no extra pass code field; easy, but it requires minimum ASA 9.7, <http://duo.com/docs/ciscoasa-ss0>

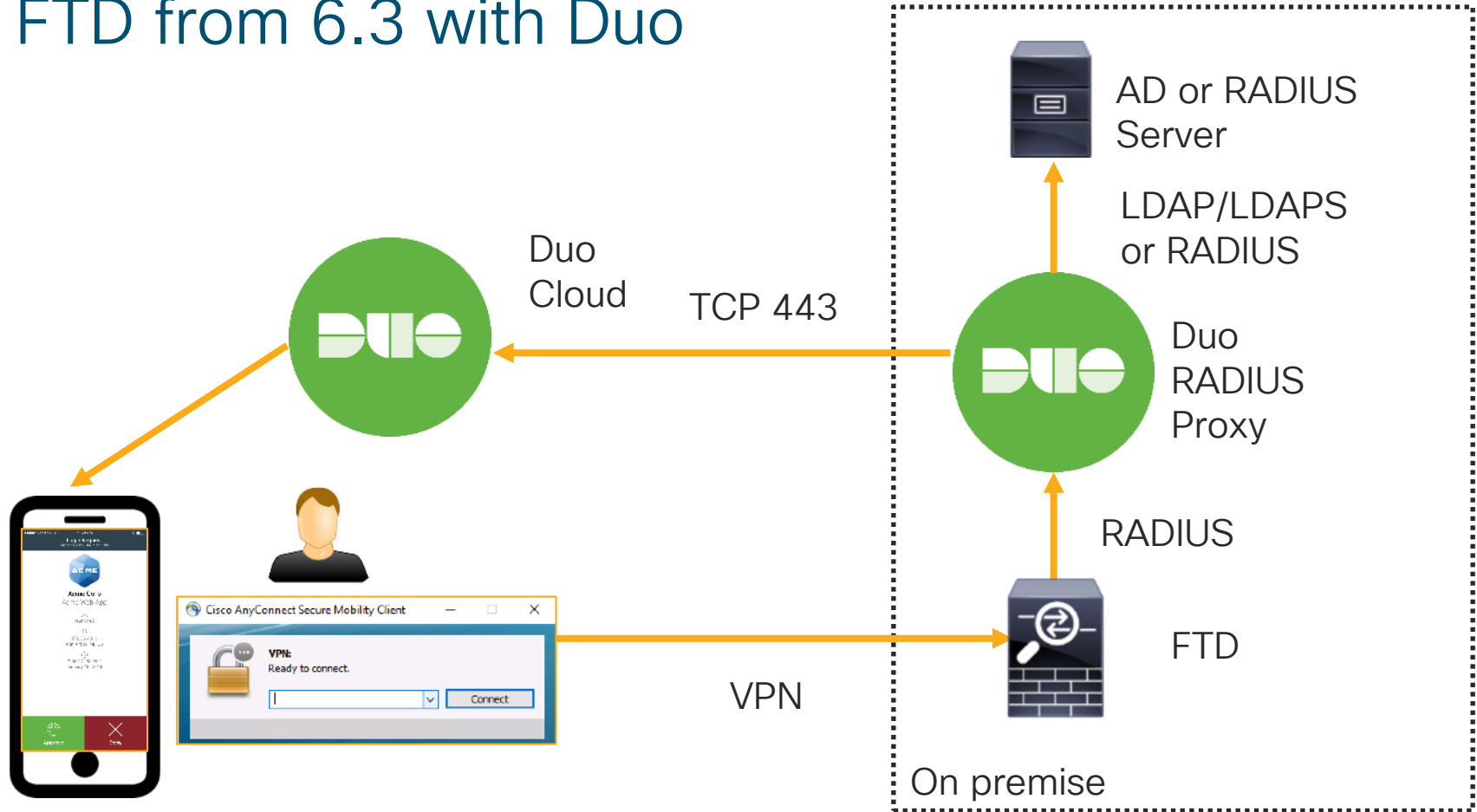


A screenshot of a mobile authentication interface. At the top, it says 'Authentication' with 'Cancel' and 'Connect' buttons. Below, it prompts 'Please enter your username and password.' There are three input fields: 'Username:', 'Password:', and 'Second Password:'. The 'Second Password:' field is highlighted with an orange border.



A screenshot of the Cisco AnyConnect Duo authentication interface. The top bar shows 'Cisco SSL VPN'. The main area has the Cisco logo and 'ACME' branding. It displays 'Device: Android (000-000-1311)'. Under 'Choose an authentication method', there are three options: 'Duo Push RECOMMENDED' with a 'Send me a Push' button, 'Call Me' with a 'Call Me' button, and 'Enter a Passcode' with an 'Enter a Passcode' button. There is also a 'Remember me for 8 hours' checkbox. On the left, there are links for 'What is this?', 'Add a new device', 'My Settings & Devices', and 'Need help?'. At the bottom left, it says 'Powered by Duo Security'.

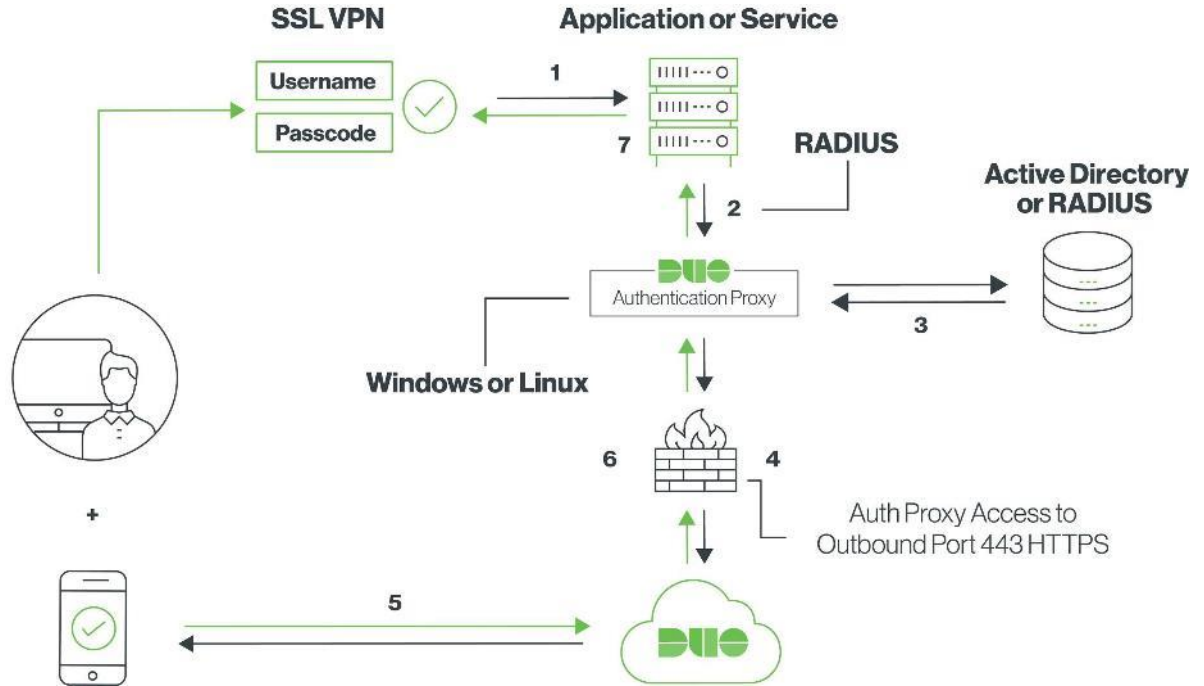
FTD from 6.3 with Duo



RADIUS: Available with Cisco ASA or FTD

Requirements

1. Cisco ASA 8.3 or later
2. Cisco FTD 6.3 or later
3. Duo Auth proxy



Duo Security is
now part of Cisco.



[Learn more about AnyConnect RADIUS integration](#)

Duo RADIUS Proxy

A Standalone Duo Software Acting as a RADIUS Server

- Install Windows or Linux as an **admin** account
 - Config file: conf\authproxy.cfg
 - Log file: log\authproxy.log

[ad_client]

```
host=<AD-IP-address>
service_account_username=admin
service_account_password=C1sco12345
search_dn=CN=Users,DC=mydomain,DC=com
```

[radius_server_auto]

```
ikey=D94FBB987I8KUTK5556Z
skey=F0E47ItOrET0c8jE7gxaxQcJnRb7VObjQc9rbOTw
api_host=api-1506c3ct.duosecurity.com
```

```
radius_ip_1=10.1.1.40
radius_secret_1=C1sco12345
```

Primary authentication options:

1. AD account (LDAP/LDAPS)
Port: 389 or 636 if using LDAPS
2. RADIUS: [radius_client] section
Port: Typically 1812, but any unused port is acceptable

Secondary authentication:
Duo account in the cloud

FTD as a RADIUS client

RADIUS Authentication Timeout from FMC/FTD 6.3

Users need longer Timeout

New RADIUS Server

IP Address/Hostname:* 10.
Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* 1812 (1-65535)

Key:*

Confirm Key:*

Accounting Port: 1813 (1-65535)

Timeout: 60 (1-300) Seconds

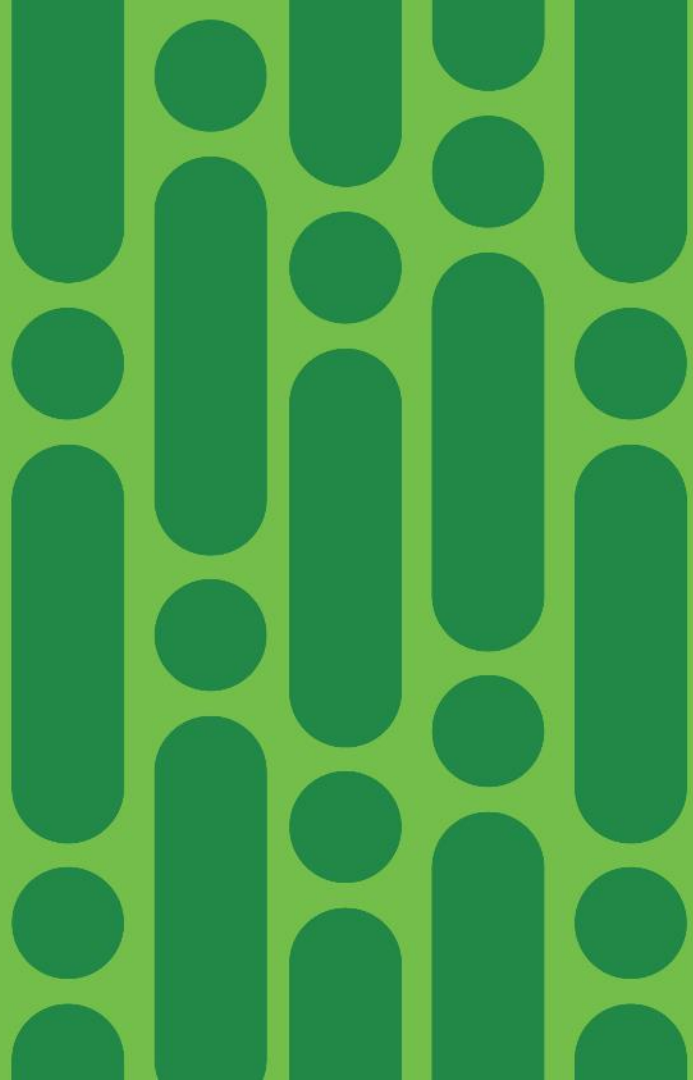
Connect using: ☒ Routing ☐ Specific Interface ⓘ

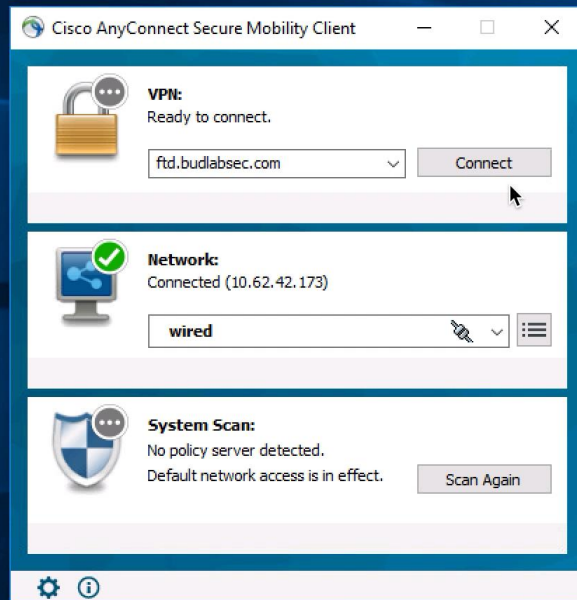
Default: Diagnostic Interface

Redirect ACL:

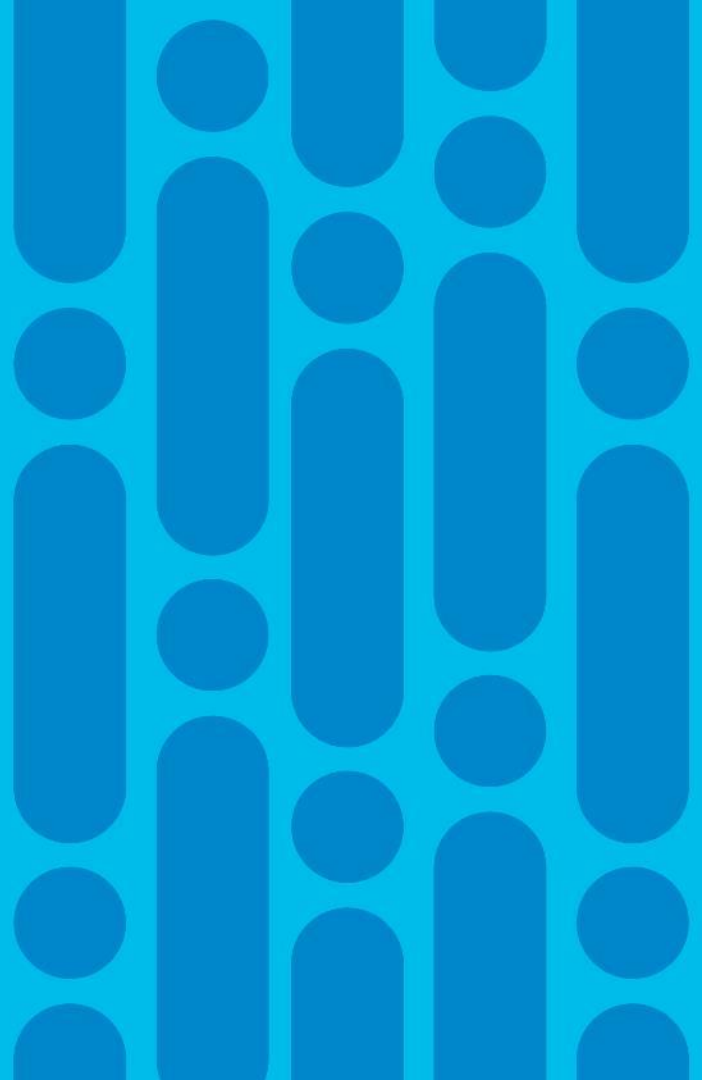
Save Cancel

FTD RA VPN with Duo Security Demo

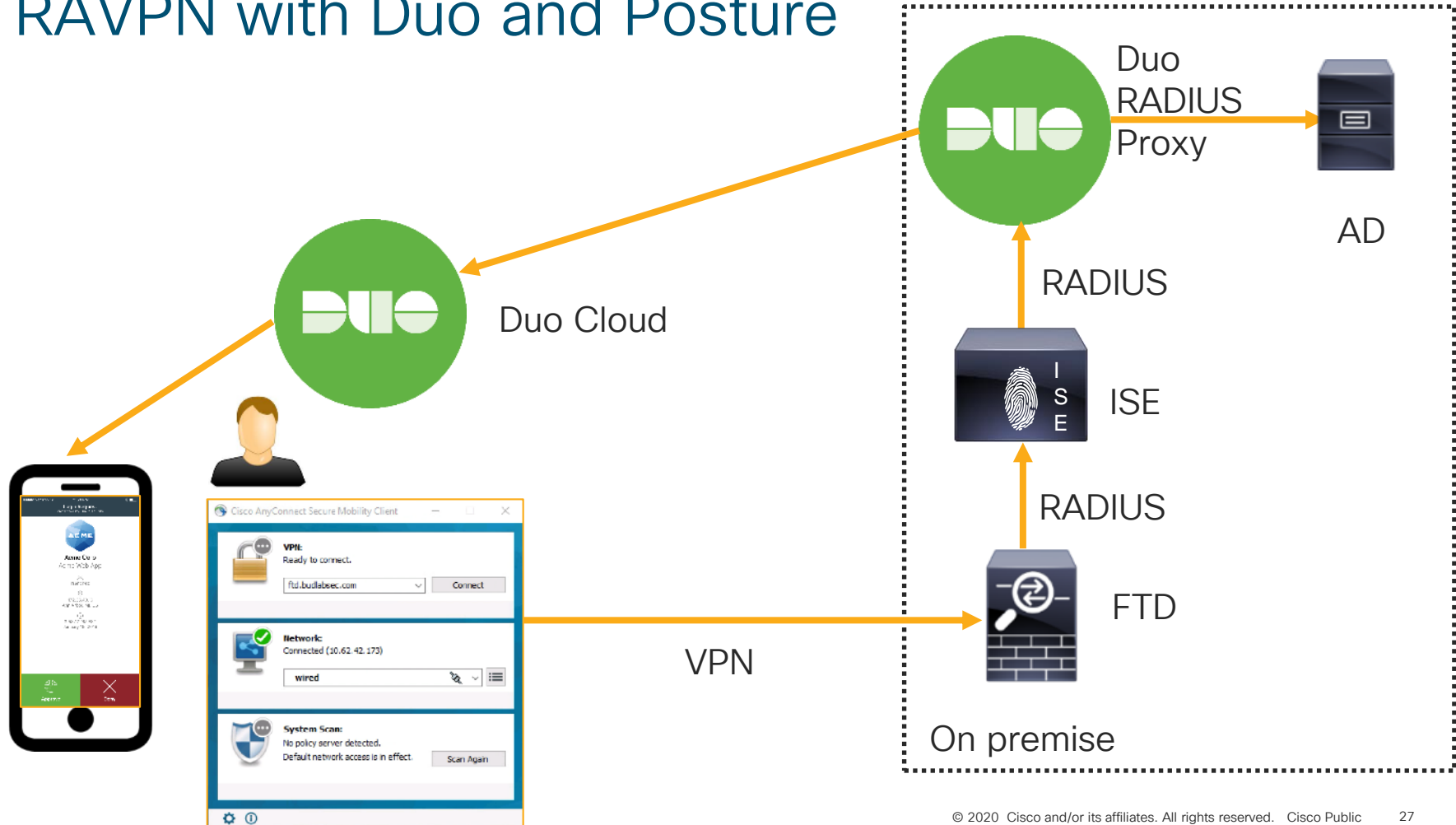




FTD RA VPN with Duo and RADIUS CoA



RAVPN with Duo and Posture



Authentication and Authorization Servers

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy 1 System Help admin

Device Management NAT **VPN ▶ Remote Access** QoS Platform Settings FlexConfig Certificates

FTD-RA-VPN-Profiles

Enter Description

Save Cancel

Policy Assignments (1)

Connection Profile Access Interfaces Advanced

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: <i>None</i> Authorization: <i>None</i> Accounting: <i>None</i>	DfltGrpPolicy
ISE-posture	Authentication: ISE-RADIUS (RADIUS) Authorization: ISE-RADIUS (RADIUS) Accounting: ISE-RADIUS (RADIUS)	DfltGrpPolicy
Duo	Authentication: Duo (RADIUS) Authorization: Duo (RADIUS) Accounting: Duo (RADIUS)	DfltGrpPolicy
Duo-and-ISE-posture	Authentication: ISE-RADIUS (RADIUS) Authorization: ISE-RADIUS (RADIUS) Accounting: ISE-RADIUS (RADIUS)	DfltGrpPolicy

ISE as an Authentication AND Authorization Server

ISE Authentication Configuration

Authentication Policy (2)

Status	Rule Name	Conditions	Use
	Duo	Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS Duo-and-ISE-posture	Duo Options Internal Users Options
	Default		

Tunnel-Group-Name equals Duo-and-ISE-posture

External Identity Sources

- Certificate Authentication Profile
- Active Directory
 - budlabsec.com
- LDAP
- ODBC
- RADIUS Token
 - Duo
- RSA SecurID
- SAML Id Providers
- Social Login

RADIUS Token List > Duo

RADIUS Token Identity Sources

General Connection Authentication Au

Server Connection

- ☐ Safeword Server
- ☐ Enable Secondary Server ☐ Always Access Primary Server First ☒ Failback to Primary Server after

Primary Server

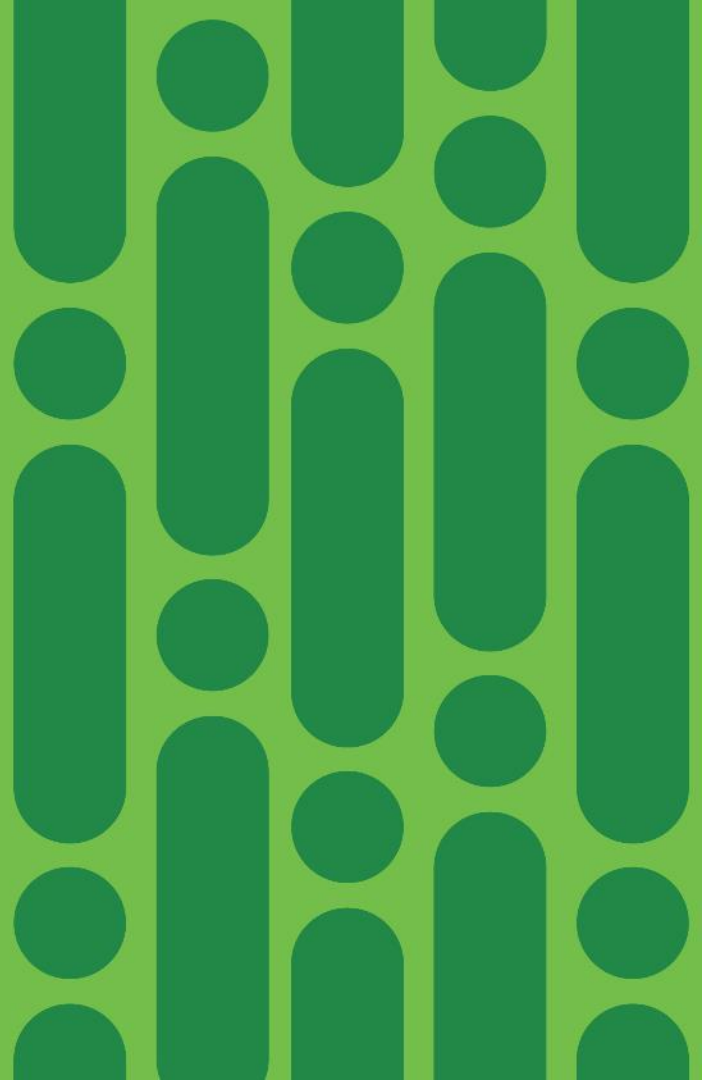
* Host IP 10.62

* Shared Secret

* Authentication Port 1812

“Duo” as an External Identity, RADIUS Token authentication pointing to Duo RADIUS proxy

FTD RA VPN with Duo MFA and ISE Posture Demo



gacs-Win10-jumphost - VMware Remote Console

VMRC

Windows Defender Security Center

Restore settings

Domain network
Firewall is off.
Turn on

Private network
Firewall is off.
Turn on

Cisco AnyConnect Secure Mobility Client

VPN:
Ready to connect.
ftd.budlabsec.com
Connect

Network:
Connected (10.62.42.173)
wired

System Scan:
No policy server detected.
Default network access is in effect.
Scan Again

Type here to search

11:32 PM
1/12/2019

9:41 100%

Edit

DUO ADMIN
Cisco Systems Hung...

DUO-PROTECTED
Duo Demo

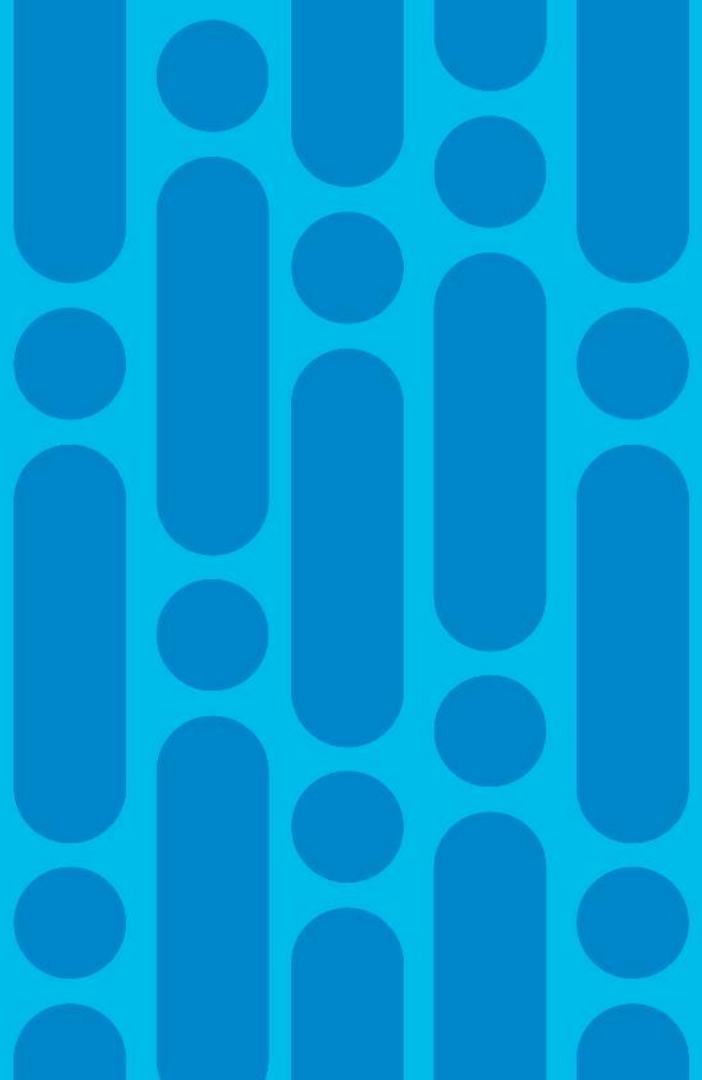
DUO-PROTECTED
Cisco Systems Hung...

DUO-PROTECTED
Cisco

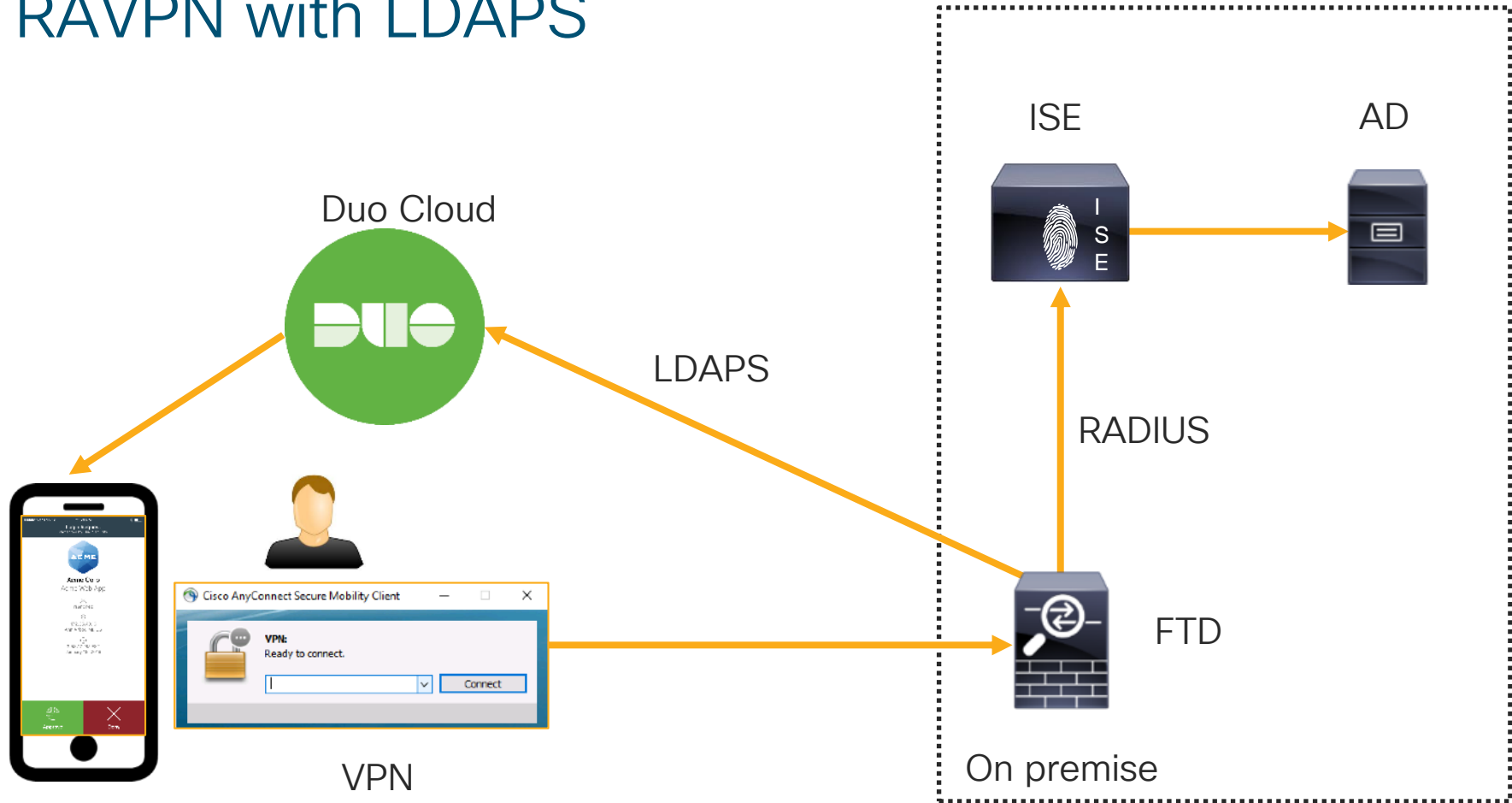
THIRD-PARTY
Umbrella

[About passcodes](#)

RA VPN with Duo and LDAPS

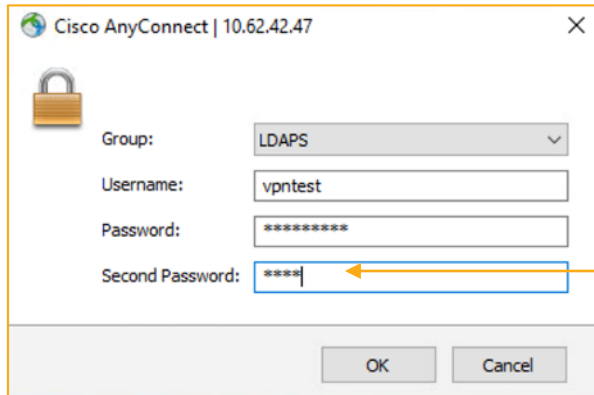


RAVPNN with LDAPS

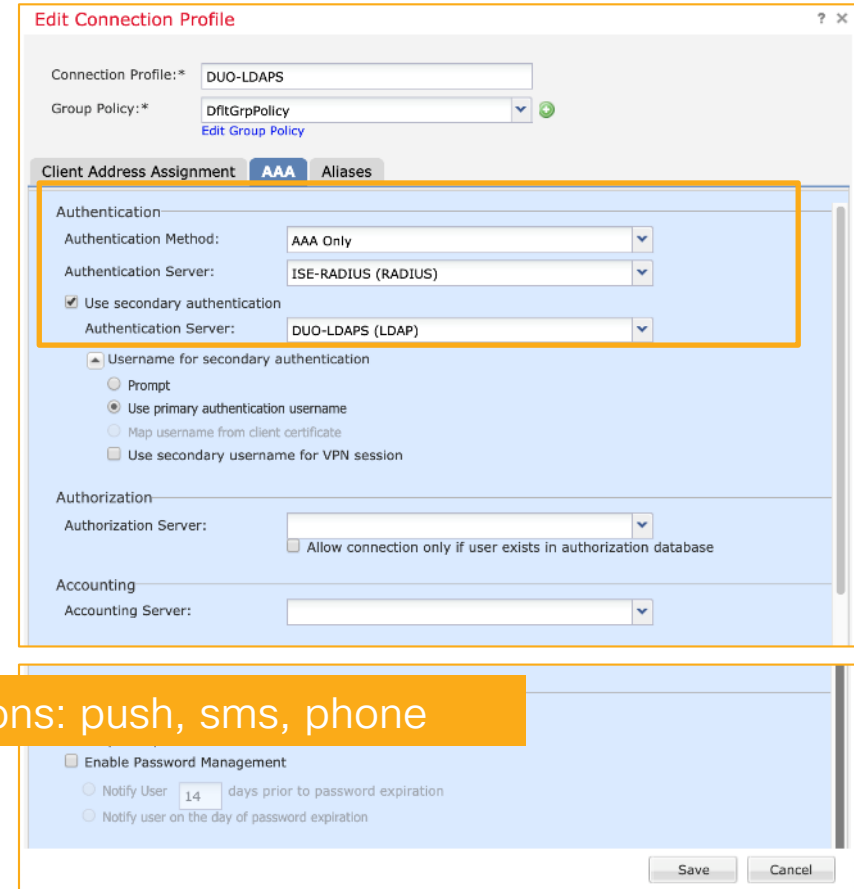


RA VPN Secondary Authentication from 6.4

- Like with ASA, in connection Profile > AAA tab, option to enable **secondary authentication**
- It can be either **Realm** (AD/LDAP) or **RADIUS** Server Group



Duo options: push, sms, phone



Username for Secondary Authentication

- Username for the secondary authentication can be provided in one of three ways:
 - **Prompt** (User should enter the username upon login)
 - Use the username provided in the **primary authentication**
 - Prefill the username from the **client certificate**
- You can choose between **primary and secondary username** as VPN session username

Edit Connection Profile

Connection Profile:* DUO-LDAPS

Group Policy:* DfltGrpPolicy [Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method: AAA Only

Authentication Server: ISE-RADIUS (RADIUS)

☒ Use secondary authentication

Authentication Server: DUO-LDAPS (LDAP)

Username for secondary authentication

- ☐ Prompt
- ☒ Use primary authentication username
- ☐ Map username from client certificate
- ☐ Use secondary username for VPN session

Authorization

Authorization Server:

☐ Allow connection only if user exists in authorization database

Accounting

Accounting Server:

LDAPS as a Realm

System > Integration > Realms

DUO-LDAPS
Enter Description

Directory **Realm Configuration** User Download

Directory Username * ex: uid=user,dc=example,dc=com

Directory Password *

Base DN * ex: ou=user,dc=cisco,dc=com

Group DN * ex: ou=group,dc=cisco,dc=com

Group Attribute ▼

User Session Timeout

User Agent and ISE/ISE-PIC Users	<input type="text" value="1440"/>	minutes until session released.
TS Agent Users	<input type="text" value="1440"/>	minutes until session released.
Captive Portal Users	<input type="text" value="1440"/>	minutes until session released.
Failed Captive Portal Users	<input type="text" value="1440"/>	minutes until session released.
Guest Captive Portal Users	<input type="text" value="1440"/>	minutes until session released.

Directory Username, Base DN and Group DN:
dc=INTEGRATION_KEY,dc=duosecurity,dc=com
Directory Password will be the Secret Key.

Edit directory ? x

Hostname / IP Address

Port

Encryption ☐ STARTTLS ☒ LDAPS ☐ None

SSL Certificate +

OK Test Cancel

Encryption: LDAPS,
“Test”

FlexConfig

Edit FlexConfig Object

Name: Duo-LDAP-FlexConfig

Description:

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

Insert ⌨ Deployment: Everytime Type: Append

```
aaa-server DUO-LDAPS host api-1302c8df.duosecurity.com  
ldap-naming-attribute on
```

Variables

Name	Dimension	Default Value	Property (Typ...	Override	Description
No records to display					

Deployment: Every
time

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings **FlexConfig** Certificates

Duo-LDAPS-Flexconfig

Enter Description

Available FlexConfig FlexConfig Object

- User Defined
 - Duo-LDAP-FlexConfig
- System Defined
 - Default_DNS_Configure
 - Default_Inspection_Protocol_Disable
 - Default_Inspection_Protocol_Enable
 - DHCPv6_Prefix_Delegation_Configure
 - DHCPv6_Prefix_Delegation_UnConfigure
 - DNS_Configure
 - DNS_UnConfigure
 - Eigrp_Configure
 - Eigrp_Interface_Configure
 - Eigrp_UnConfigure
 - Eigrp_UnConfigure_All
 - Inspect_IPv6_Configure
 - Inspect_IPv6_UnConfigure
 - ISIS_Configure
 - ISIS_Interface_Configuration

Selected Prepend FlexConfigs

#	Name
---	------

Selected Append FlexConfigs

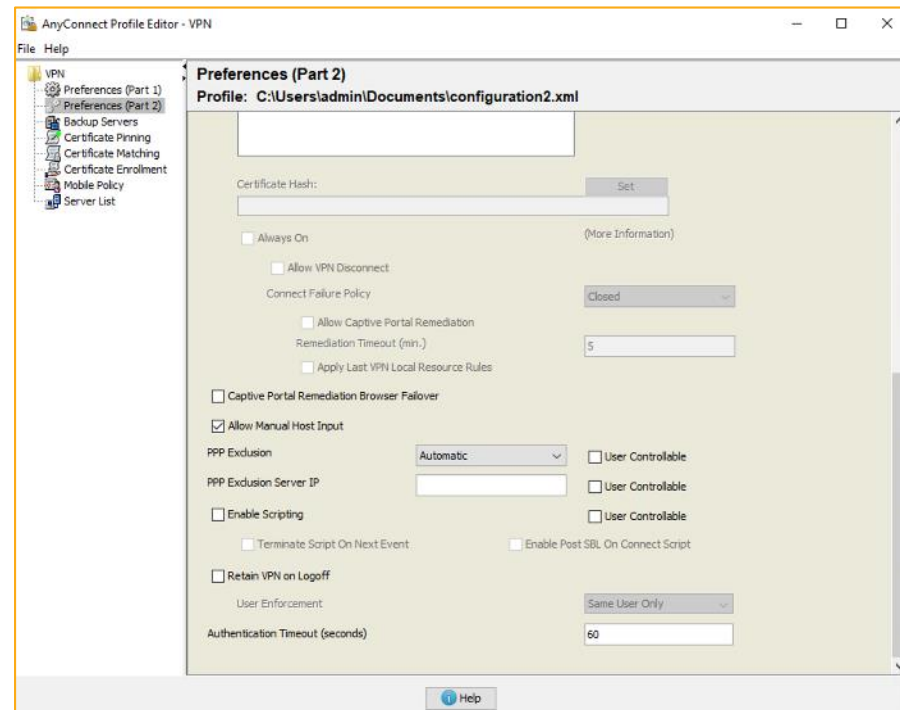
#	Name
1.	Duo-LDAP-FlexConfig

Append FlexConfig

Timeout

- Set the timeout to 60 instead of 12
- show aaa-server

```
Server Group:    DUO-LDAPS
Server Protocol: ldap
Server Hostname: api-1302c8df.duosecurity.com
Server Address:  52.19.127.204
Server port:     636
Server status:   ACTIVE, Last transaction at unknown
Number of pending requests      0
Average round trip time        0ms
Number of authentication requests 14
Number of authorization requests 0
Number of accounting requests   0
Number of retransmissions       0
Number of accepts               0
Number of rejects               0
Number of challenges            0
Number of malformed responses   0
Number of bad authenticators    0
Number of timeouts              14
Number of unrecognized responses 0
```



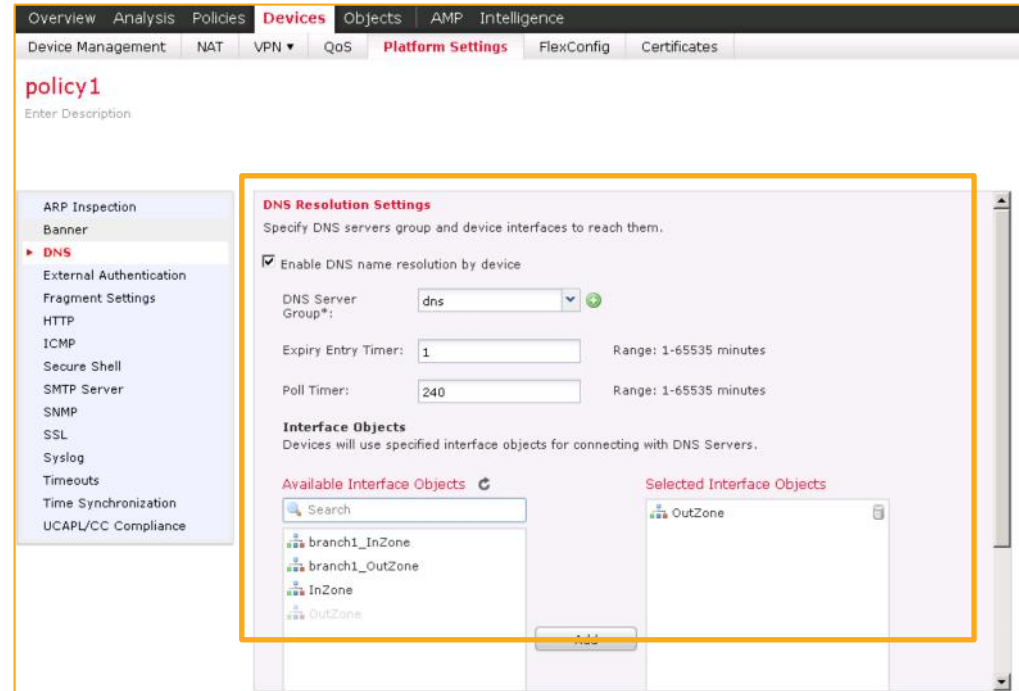
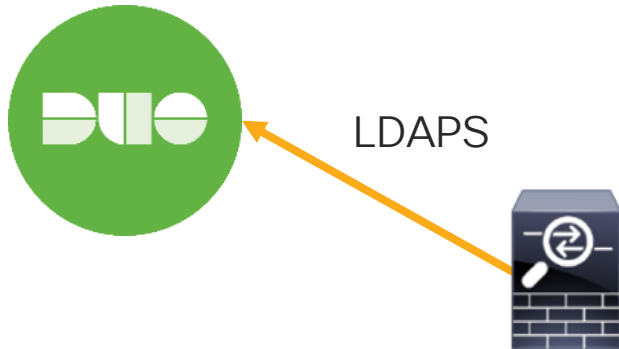
Authentication Timeout (seconds)

60

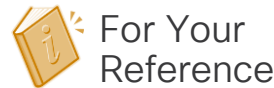
Authentication timeout: 60

FTD DNS Configuration

- FTD should resolve duosecurity.com domain alone, therefore DNS configuration is needed



Troubleshooting Secondary Authentication

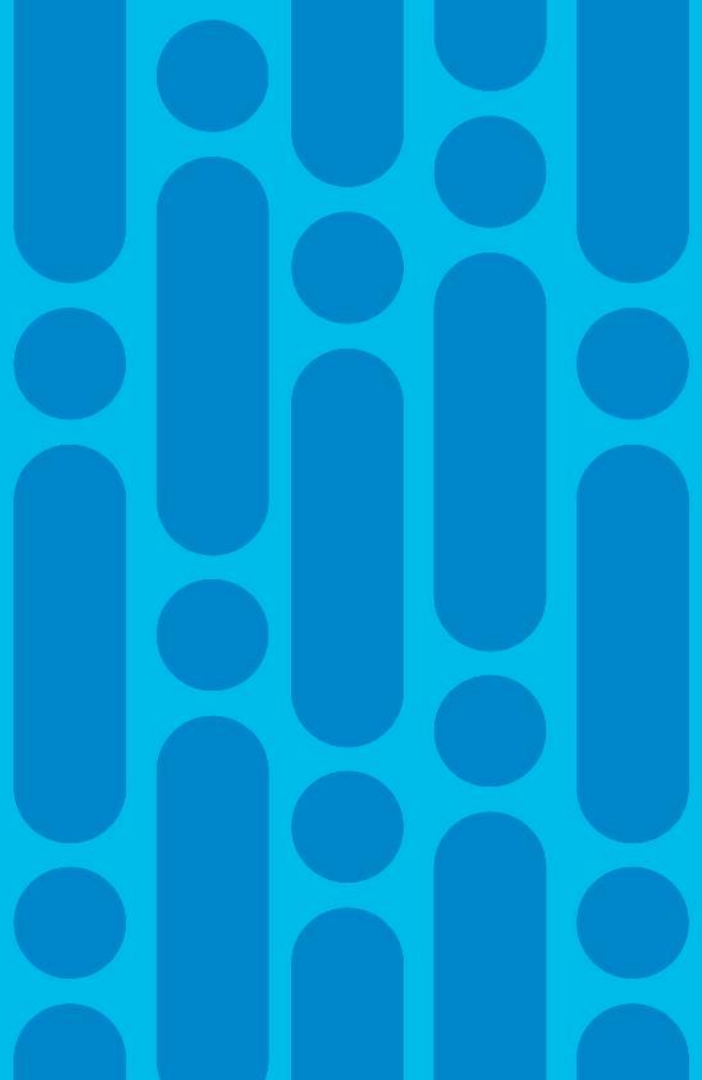


- **Verify** the AAA server using the test command on FTD

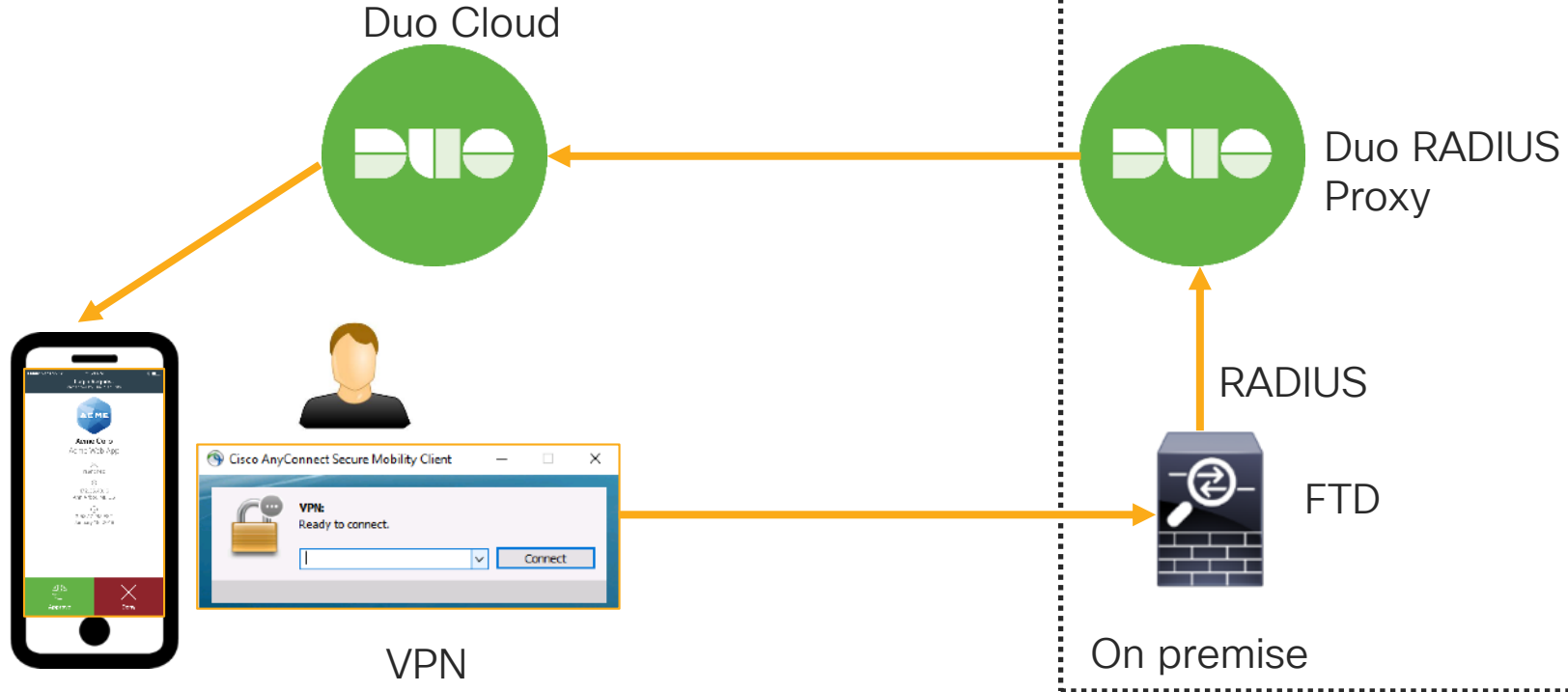
```
test aaa-server authentication <AAA-Server>
```

- AD/LDAP configured via Realms uses the **routing table** to reach the AD/LDAP server, verify the route
- RADIUS Server configured in RADIUS Server group uses routing table by default, **change the configuration** in RADIUS Server group if the server is reachable via an interface

RA VPN with Certificate and Duo MFA



RAVPNN with Certificate and Duo MFA



Certificate Based Authentication with Duo

- Authentication: Client AND AAA
- AAA: Duo Auth Proxy
- Prefill username from certificate
- Hide username in login window

The screenshot shows the 'Add Connection Profile' window with the following configuration:

- Connection Profile:** Duo
- Group Policy:** DftGrpPolicy (with an 'Edit Group Policy' link)
- Tabs:** Client Address Assignment, **AAA**, Aliases
- Authentication Section:**
 - Authentication Method:** Client Certificate & AAA
 - Authentication Server:** Duo_Auth_Proxy (RADIUS)
 - Map username from client certificate:** (expanded)
 - Map specific field:** (selected)
 - Primary Field:** CN (Common Name)
 - Secondary Field:** OU (Organisational Unit)
 - Use entire DN (Distinguished Name) as username:** (unselected)
 - Prefill username from certificate on user login window:** ☒ (highlighted with an orange box)
 - Hide username in login window:** ☒ (highlighted with an orange box)
 - Use secondary authentication:** (unselected)
- Authorization Section:**
 - Authorization Server:** ISE_RADIUS (RADIUS)
 - Allow connection only if user exists in authorization database:** (unselected)
- Accounting Section:**
 - Accounting Server:** ISE_RADIUS (RADIUS)
- Advanced Settings:** (collapsed)

Buttons at the bottom: Save, Cancel

Duo RADIUS Proxy – Duo Only Client

A Standalone Duo Software Acting as a RADIUS Server

```
[duo_only_client]
```

There is NO primary authentication

```
[radius_server_auto]
```

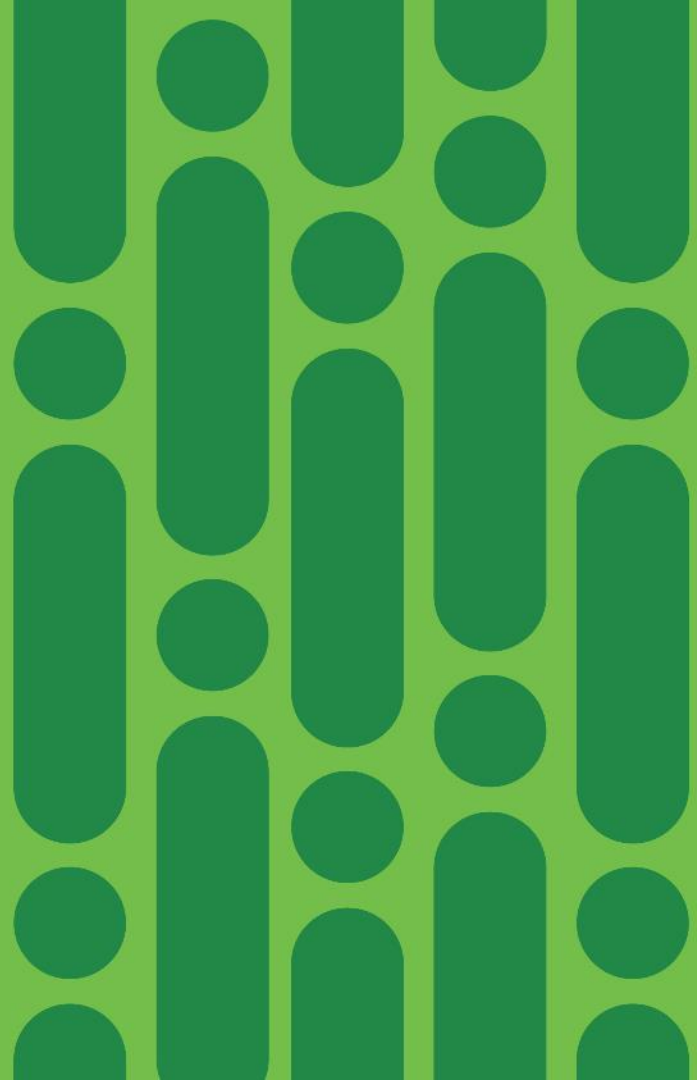
Secondary authentication:
Duo account in the cloud

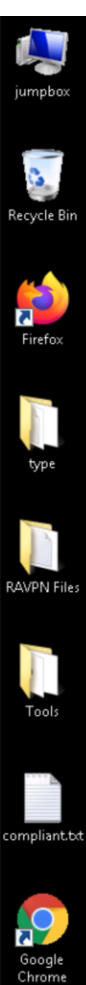
```
ikey=DIAHEPCGVZFPDLVHH9PL  
skey=g4VC01AqffKnH9pxEwfvvg8SFsaBu3ot6FY  
api_host=api-1301c7df.duosecurity.com
```

```
radius_ip_1=198.19.10.1  
radius_secret_1=C1sco12345  
failmode=safe  
client=duo_only_client
```

FTD as a RADIUS client

FTD RA VPN with Certificate and Duo MFA Demo

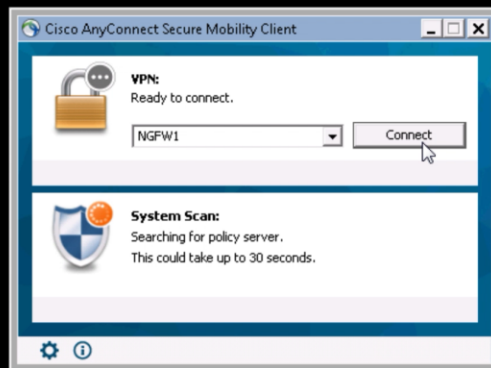


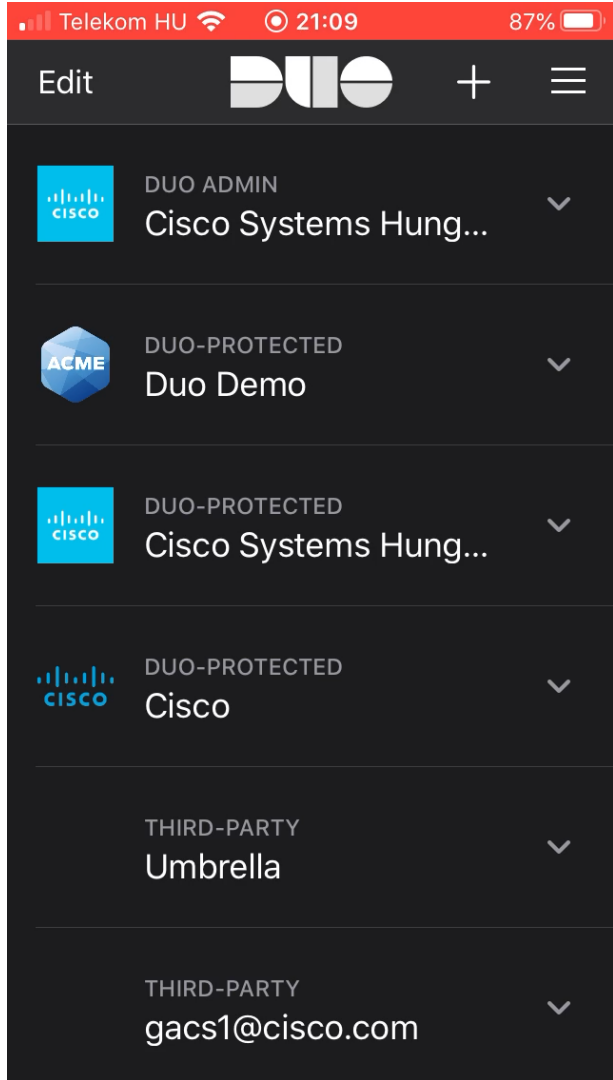


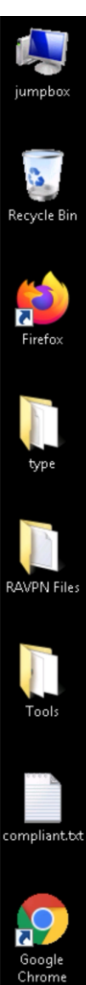
Untitled - Notepad

File Edit Format View Help

push



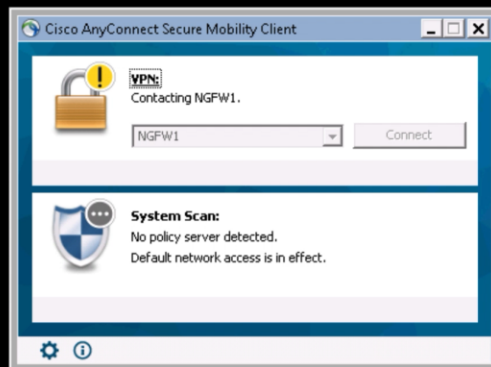




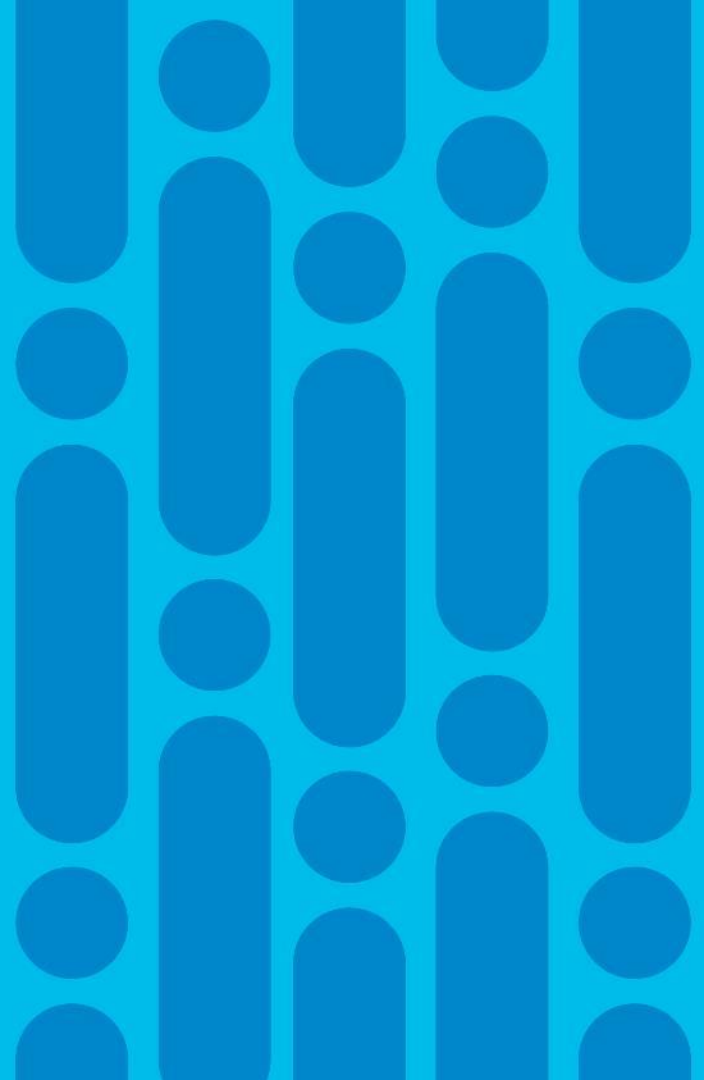
Untitled - Notepad

File Edit Format View Help

push



Monitoring of RA VPN Connections



Monitoring of RA VPN Connections

- VPN Server side monitoring: show commands

```
> show running-config tunnel-group
tunnel-group DefaultWEBVPNGroup general-attributes
  address-pool VPN-Pool1
  authentication-server-group RADIUS_SERVERS
  authorization-server-group RADIUS_SERVERS
  accounting-server-group RADIUS_SERVERS
tunnel-group VPN-profile type remote-access
tunnel-group VPN-profile general-attributes
  address-pool VPN-Pool1
  authentication-server-group RADIUS_SERVERS
  authorization-server-group RADIUS_SERVERS
  accounting-server-group RADIUS_SERVERS
tunnel-group VPN-profile webvpn-attributes
  group-alias VPN-profile enable
```

```
> show vpn-sessiondb anyconnect
```

Session Type: AnyConnect

Username	: remotel	Index	:
	27432		
Assigned IP	: 10.1.1.121	Public IP	:
	10.61.97.108		
Protocol	: AnyConnect-Parent SSL-Tunnel DTLS-Tunnel		
License	: AnyConnect Premium		
Encryption	: AnyConnect-Parent: (1)none	SSL-Tunnel:	
	(1)AES-GCM-256	DTLS-Tunnel:	(1)AES256
Hashing	: AnyConnect-Parent: (1)none	SSL-Tunnel:	
	(1)SHA384	DTLS-Tunnel:	(1)SHA1
Bytes Tx	: 31690	Bytes Rx	: 1



10.1.1.121



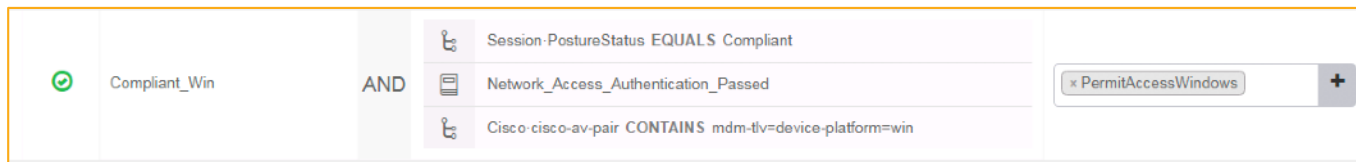
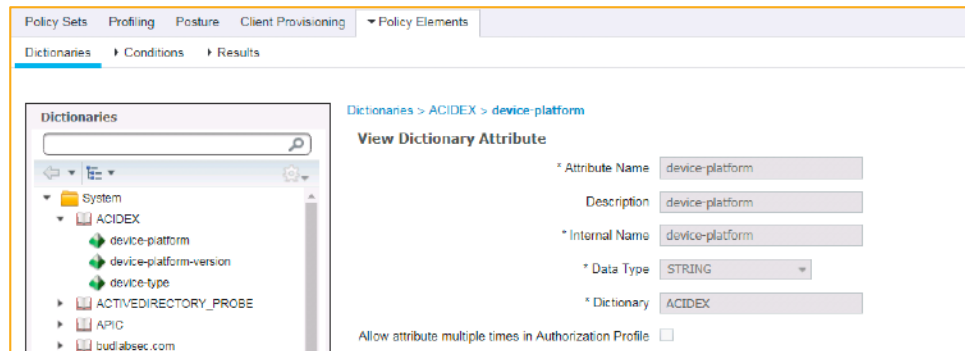
10.1.1.90

VPN_SERVER

INSIDE_ROUTED

AnyConnect Identity Extensions (ACIDex)

- FTD provides ACIDex, like ASA does
- It is used by ISE as a profiling information and authentication and authorization policy element



Device MAC address, platform and agent versions, device type and other information as AV pair sent by FTD

CiscoAVPair

```
mdm-tlv=device-platform=win,  
mdm-tlv=device-mac=00-50-56-ae-d6-4b,  
mdm-tlv=device-platform-version=10.0.17134,  
mdm-tlv=device-public-mac=00-50-56-ae-d6-4b,  
mdm-tlv=ac-user-agent=AnyConnect Windows 4.7.00136,  
mdm-tlv=device-type=VMware, Inc. VMware Virtual Platform,  
mdm-tlv=device-  
uid=51E751ED491618BCA76689C82A168D25143FCE5433A0171963E2EAC  
F0DE60F11,  
audit-session-id=0a3e2afd000010005c422933,  
ip:source-ip=10. [REDACTED]  
coa-push=true
```

Active Sessions

The screenshot shows the Cisco Active Sessions interface. The top navigation bar includes tabs for Overview, Analysis (selected), Policies, Devices, Objects, AMP, and Intelligence. Below this is a secondary navigation bar with links like Context Explorer, Connections, Intrusions, Files, Hosts, Users > Active Sessions (highlighted), Vulnerabilities, Correlation, Custom, Lookup, and Search. A dropdown menu for 'Active Sessions' is open, showing options: Active Sessions, Users, User Activity, and Indications of Compromise. The main content area is titled 'Active Sessions' and includes a 'Table View of Active Sessions' link and a search bar. Below the search bar is a table with columns: Login Time, Last Seen, User, Authentication Type, Current IP, Realm, Username, First Name, Last Name, and E-Mail. The table contains two rows: one for 'remote1' with 'VPN Authentication' and IP '10.1.1.121', and another for 'anonymous' with 'No Authentication' and IP '10.1.1.90'. An orange box at the bottom right contains the text 'VPN Authentication' with an arrow pointing to the 'VPN Authentication' entry in the table.

Overview **Analysis** Policies Devices Objects AMP Intelligence

Context Explorer Connections ▼ Intrusions ▼ Files ▼ Hosts ▼ **Users > Active Sessions** Vulnerabilities ▼ Correlation ▼ Custom ▼ Lookup ▼ Search

Active Sessions

[Table View of Active Sessions](#) > Active Sessions

► Search Constraints ([Edit Search](#))

Jump to... ▼

	▼ Login Time ×	Last Seen ×	User ×	Authentication × Type	Current × IP	Realm ×	Username ×	First × Name	Last × Name	E-Ma
↓	2017-12-10 22:34:53	2017-12-10 22:34:53	Discovered Identities\remote1 (LDAP)	VPN Authentication	10.1.1.121	Discovered Identities	remote1			
↓	2017-12-07 23:27:24	2017-12-07 23:27:24	Discovered Identities\anonymous (FTP)	No Authentication	10.1.1.90	Discovered Identities	anonymous			

Page 1 of 1 | Displaying rows 1–2 of 2 rows

View Logout

View All

VPN Authentication

User Activity

Overview **Analysis** Policies Devices Objects AMP Intelligence Deploy 1 System Help **admin**

Context Explorer Connections Intrusions Files Hosts **Users > User Activity** Vulnerabilities Correlation Custom Lookup Search

Bookmark This Page Report Designer Dashboard View Bookmarks Search

User Activity

[Table View of Events](#) > [Users](#)

2017-11-10 22:36:00 - 2017-12-10 22:42:27 Expanding

No Search Constraints ([Edit Search](#))

	Time	Event	Username	Realm	Discovery Application	Authentication Type	IP Address	Start Port	End Port	Description	VPN Session Type
2017-12-10 22:34:53	VPN User Login	remote1	Discovered Identities	LDAP	VPN Authentication	10.1.1.121				AnyConnect SSL	

- Detailed User information, like logon, logoff, bytes, duration

VPN Group Policy	VPN Connection Profile	VPN Client Public IP	VPN Client Country	VPN Client OS	VPN Client Application	VPN Connection Duration	VPN Bytes Out	VPN Bytes In
DfltGrpPolicy	VPN-profile	10.61.211.6		win	Cisco AnyConnect VPN Agent for Windows 4.5.02036	44 minutes	357,090	118,738

Access Controlled User Statistics

Provides traffic and intrusion event statistics by user

Show the Last 6 hours

Add Widgets

Connections Intrusion Events VPN +

Active VPN Sessions by Duration	
User	Session Duration
Discovered Identities\remote1 (LDA)	1 hour
Discovered Identities\remote2 (LDA)	5 minutes

Last updated 1 minute ago

Active VPN Sessions by Device	
Device	Count
10.62.42.54	3

Last updated 1 minute ago

VPN Users by Duration	
No Data	

Last updated 1 minute ago

Active VPN Sessions by Client Application	
VPN Client Application	Count
Cisco AnyConnect VPN Agent for Windows 4.5.02036	2
Cisco AnyConnect VPN Agent for Linux 4.5.03040	1

VPN Users by Data Transferred	
-------------------------------	--

Different Operating Systems and AnyConnect Versions

VPN Users by Client Application	
VPN Client Application	Count
Cisco AnyConnect VPN Agent for Windows 4.5.02036	2
Cisco AnyConnect VPN Agent for Linux 4.5.03040	1

Troubleshooting

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy 1 System Help **admin**

Device Management NAT **VPN Troubleshooting** QoS Platform Settings FlexConfig Certificates

Bookmark This Page Report Designer Dashboard View Bookmarks Search

VPN Troubleshooting

[Table View of VPN Troubleshooting](#)

2017-11-10 22:36:00 - 2017-12-10 22:36:26 Expanding

Search Constraints ([Edit Search](#)) Disabled Columns

	Time	Severity	Message	Message Class	Username	Device
↓	2017-12-04 16:58:30	Error	Local:10.62.42.47:4500 Remote:10.61.228.208:61113 Username:Unknown IKEv2 AnyConnect client reconnect authentication failed. Session ID: 75218944, Error: 75218944	IKE and IPsec	Unknown IKEv2	10.62.42.54
↓	2017-12-03 23:26:45	Critical	AAA Marking RADIUS server 10.62.42.169 in aaa-server group RADIUS_SERVERS as ACTIVE	User Authentication		10.62.42.54
↓	2017-12-03 23:26:45	Critical	AAA Marking RADIUS server 10.62.42.169 in aaa-server group RADIUS_SERVERS as failed	User Authentication		10.62.42.54
↓	2017-12-03 23:20:37	Critical	AAA Marking RADIUS server 10.62.42.169 in aaa-server group RADIUS_SERVERS as ACTIVE	User Authentication		10.62.42.54
↓	2017-12-03 23:20:37	Critical	AAA Marking RADIUS server 10.62.42.169 in aaa-server group RADIUS_SERVERS as failed	User Authentication		10.62.42.54

Page 1 of 1 Displaying rows 1-5 of 5 rows

View Delete View All Delete All

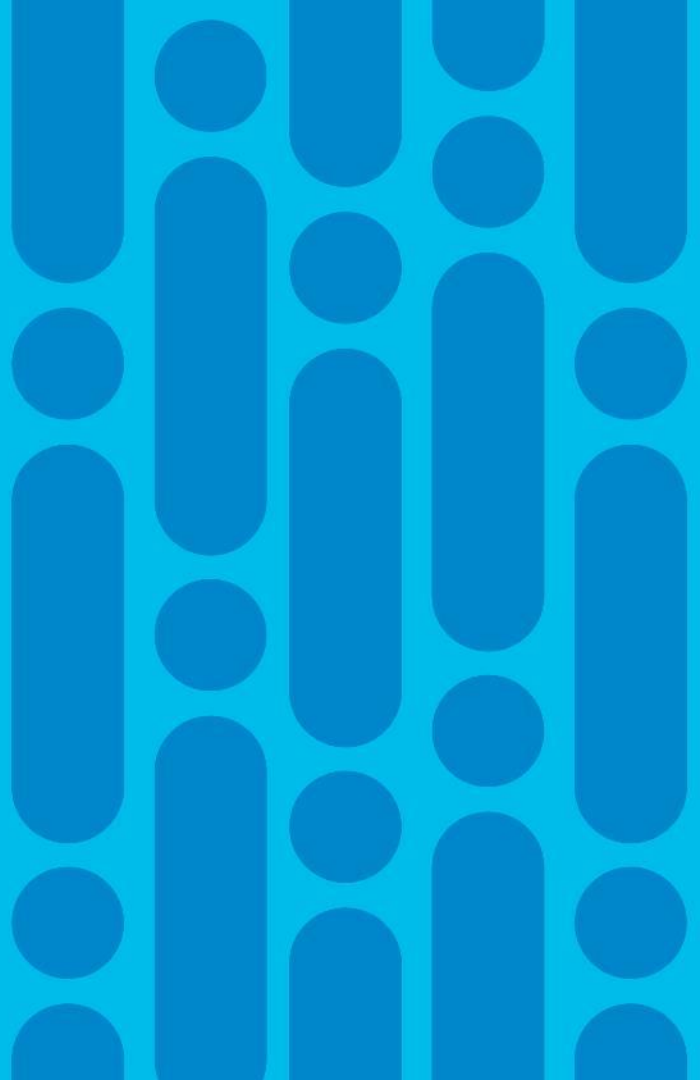
Wrongly configured RADIUS Server

RA VPN Summary

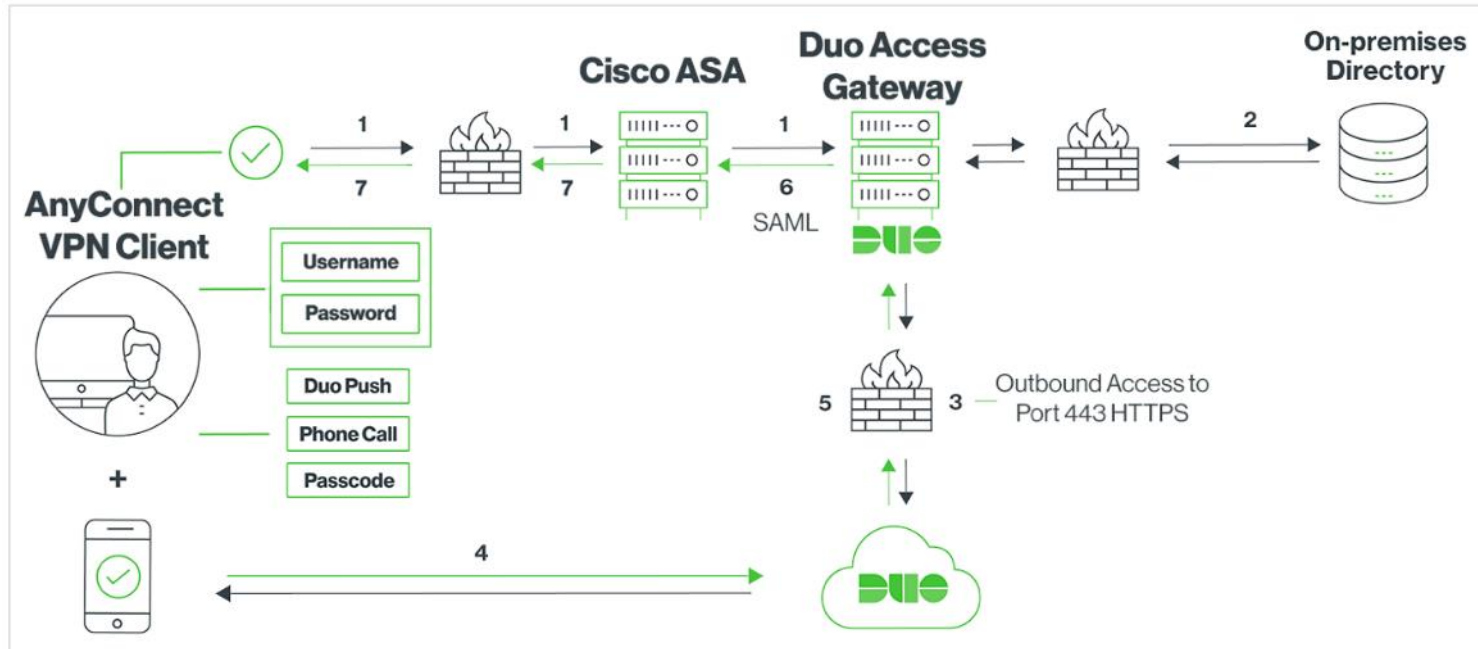
- RA VPN
 - It was introduced in version 6.2.2
 - Both IKEv2 and TLS
 - Wizard
- From 6.3:
 - RADIUS timeout (MFA)
 - RADIUS CoA
- From 6.4:
 - Secondary Authentication
- From 6.5:
 - Two-factor authentication using Duo LDAP

RA VPN with SAML

Duo Access Gateway



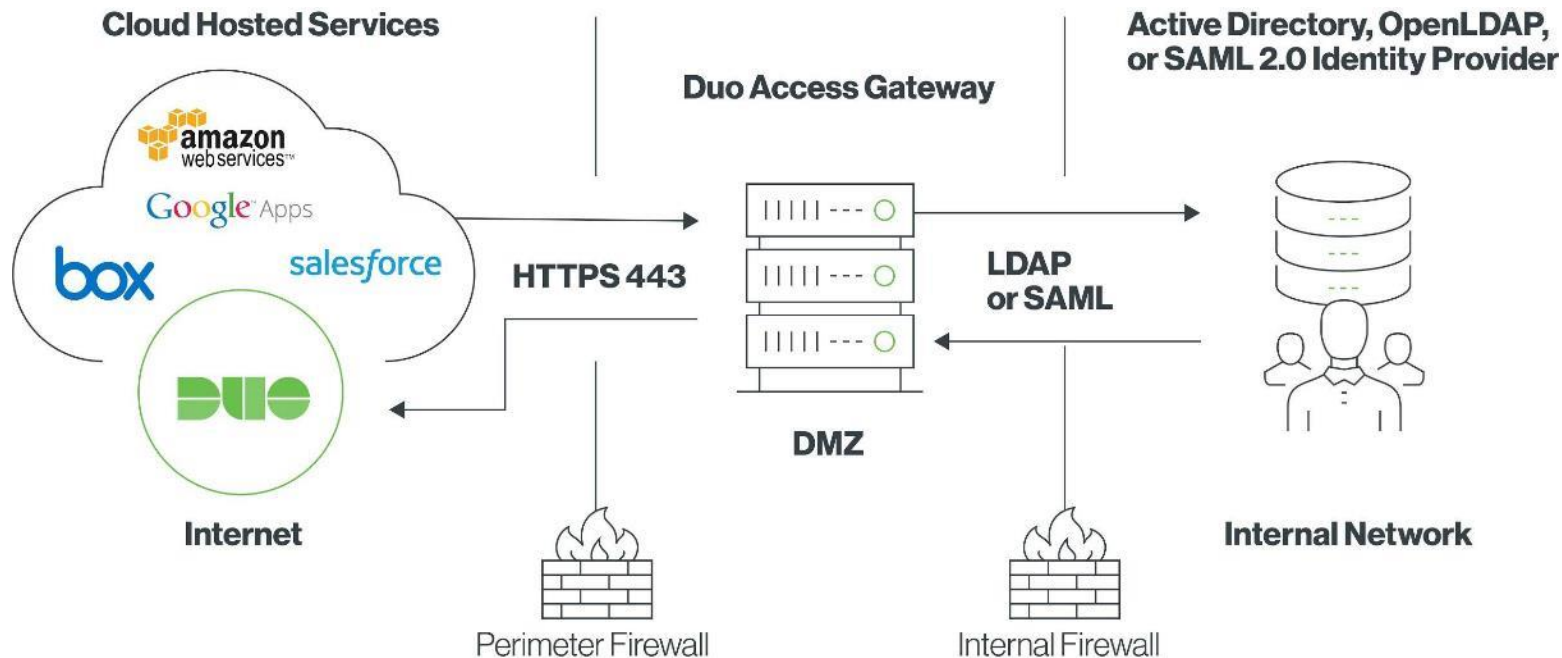
Duo Access Gateway (SAML): Cisco ASA only



- 1) VPN connection initiated to Cisco ASA, which redirects to the Duo Access Gateway for SAML authentication
- 2) AnyConnect client performs primary authentication via the Duo Access Gateway using an on-premises directory (example)
- 3) Duo Access Gateway establishes connection to Duo Security over TCP port 443 to begin 2FA
- 4) User completes Duo two-factor authentication.
- 5) Duo receives authentication response and returns that information to the Duo Access Gateway
- 6) Duo Access Gateway returns a SAML token for access
- 7) Cisco ASA VPN access granted



Duo Access Gateway Setup (DAG)

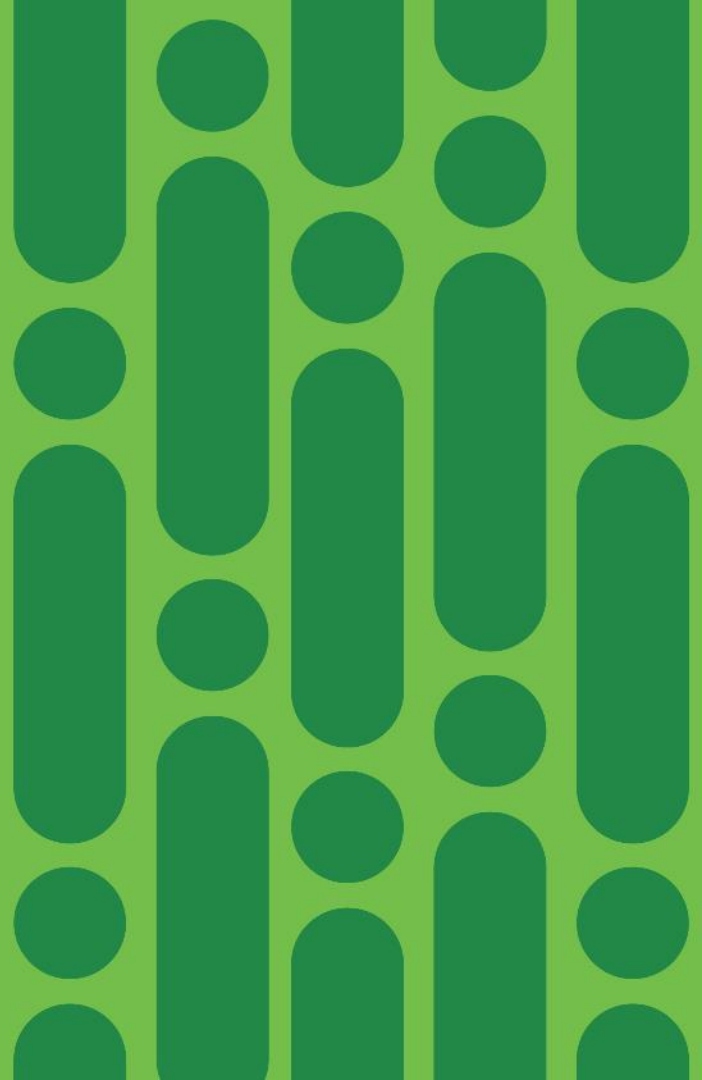


Duo Security is
now part of Cisco.



[Duo Access Gateway Documentation](#)

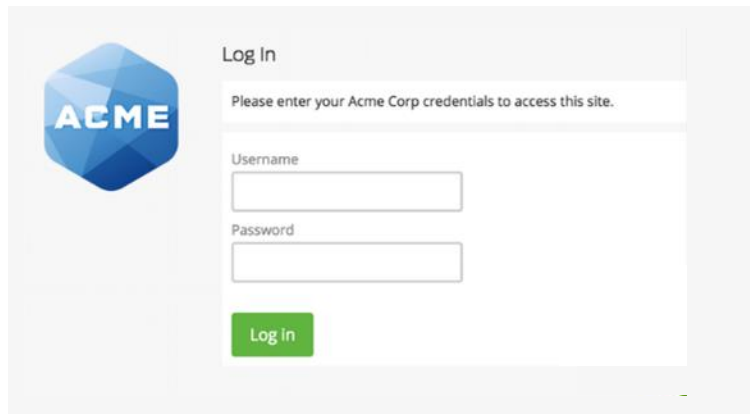
FTD RA VPN with Certificate and Duo MFA Demo



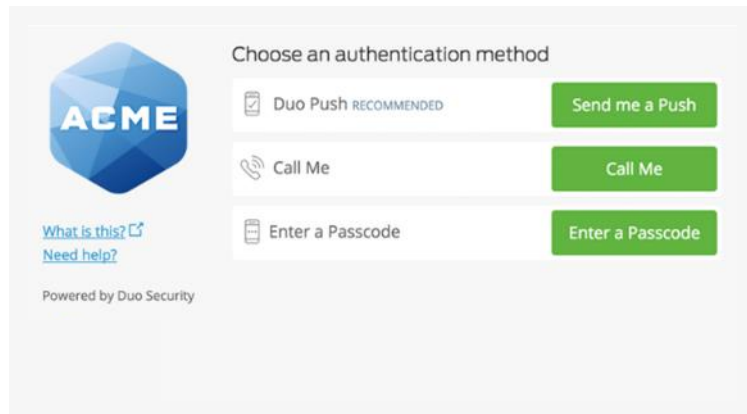
Duo Access Gateway (SAML): Cisco ASA only

Requirements:

1. A SAML gateway such as Duo Access Gateway (DAG) for SSO. [Read more here.](#)
2. ASA version of 9.7.1.24, 9.8.2.28, 9.9.2.1 or higher of each release
3. AnyConnect 4.6 or later.



The image shows the 'Log In' screen of the Duo Access Gateway (DAG). It features the ACME logo on the left. The main content area has the heading 'Log In' and a prompt: 'Please enter your Acme Corp credentials to access this site.' Below this are two input fields: 'Username' and 'Password'. At the bottom right of the form is a green 'Log In' button.



The image shows the 'Choose an authentication method' screen of the Duo Access Gateway (DAG). It features the ACME logo on the left. The main content area has the heading 'Choose an authentication method' and three options: 'Duo Push RECOMMENDED' with a 'Send me a Push' button, 'Call Me' with a 'Call Me' button, and 'Enter a Passcode' with an 'Enter a Passcode' button. Below these options are links for 'What is this?' and 'Need help?'. At the bottom left is the text 'Powered by Duo Security'.



Duo Security is
now part of Cisco.



[Learn more about AnyConnect SAML integration](#)

