Configure AD Authentication for AnyConnect Clients

Contents

Introduction

This document describes how to configure Active Directory (AD) authentication for AnyConnect clients that connect to Firepower Threat Defense (FTD).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- RA Virtual Private Network (VPN) configuration on Firepower Manage Center (FMC)
- Lightweight Directory Access Protocol (LDAP) server configuration on FMC
- Active Directory (AD)
- Fully Qualified Domain Name (FQDN)
- Intersight Infrastructure Services (IIS)
- Remote Desktop Protoco (RDP)

Components Used

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

- Microsoft 2016 Server
- FMCv running 6.5.0
- FTDv running 6.5.0

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.

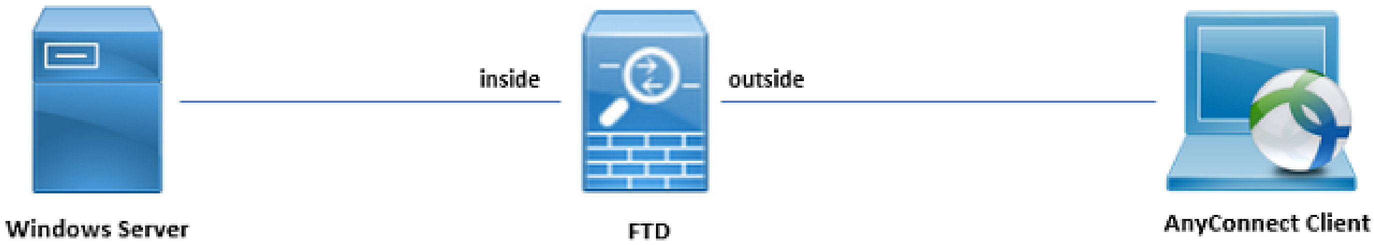
Background Information

This document describes how to configure Active Directory (AD) authentication for AnyConnect clients that connect to Firepower Threat Defense (FTD), managed by Firepower Management Center (FMC).

User identity is used in the access policies to restrict AnyConnect users to specific IP addresses and ports.

Configure

Network Diagram and Scenario



Windows server is pre-configured with IIS and RDP in order to test user identity. In this configuration guide, three user accounts and two groups are created.

User Accounts:

- FTD Admin: This is used as the directory account to allow the FTD to bind to the Active Directory server.
- IT Admin: A test administrator account used to demonstrate user identity.

- Test User: A test user account used to demonstrate user identity.

Groups:

- AnyConnect Admins: A test group that IT Admin is added to demonstrate user identity. This group only has RDP access to the Windows Server.
- AnyConnect Users: A test group that Test User is added to demonstrate user identity. This group only has HTTP access to the Windows Server.

Active Directory Configurations

In order to appropriately configure AD authentication and user identity on FTD, a few values are required.

All these details must be created or collected on the Microsoft Server before configuration can be done on FMC. The main values are:

- **Domain Name**:

This is the domain name of the server. In this configuration guide, **example.com** is the domain name.

- **Server IP/FQDN Address**:

The IP address or the FQDN used to reach the Microsoft server. If an FQDN is used, a DNS server must be configured within FMC and FTD to resolve the FQDN.

In this configuration guide, this value is win2016.example.com (which resolves to 192.168.1.1).

- **Server port**:

The port used by the LDAP service. By default, LDAP and STARTTLS uses TCP port 389 for LDAP, and LDAP over SSL (LDAPS) uses TCP port 636.

- **Root CA**:

If LDAPS or STARTTLS is used, the root CA used to sign the SSL certificate used by LDAPS is required.

- **Directory Username and Password**:

This is the account used by FMC and FTD to bind to the LDAP server and authenticate users and search for users and groups.

An account named FTD Admin is created for this purpose.

- **Base and Group Distinguished Name (DN)**:

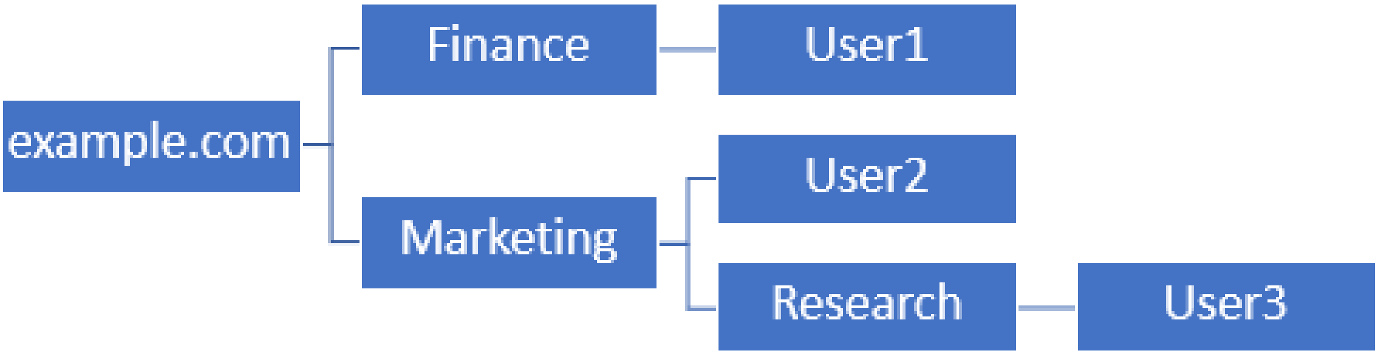
The Base DN is the starting point FMC and the FTD tells the Active Directory to begin the search for and authenticate users.

Similarly, the Group DN is the starting point FMC tells the Active Directory where to begin to search for groups for user identity.

In this configuration guide, the root domain example.com is used as the Base DN and Group DN.

However, for a production environment, using a **Base DN** and **Group DN** further within the LDAP hierarchy is better.

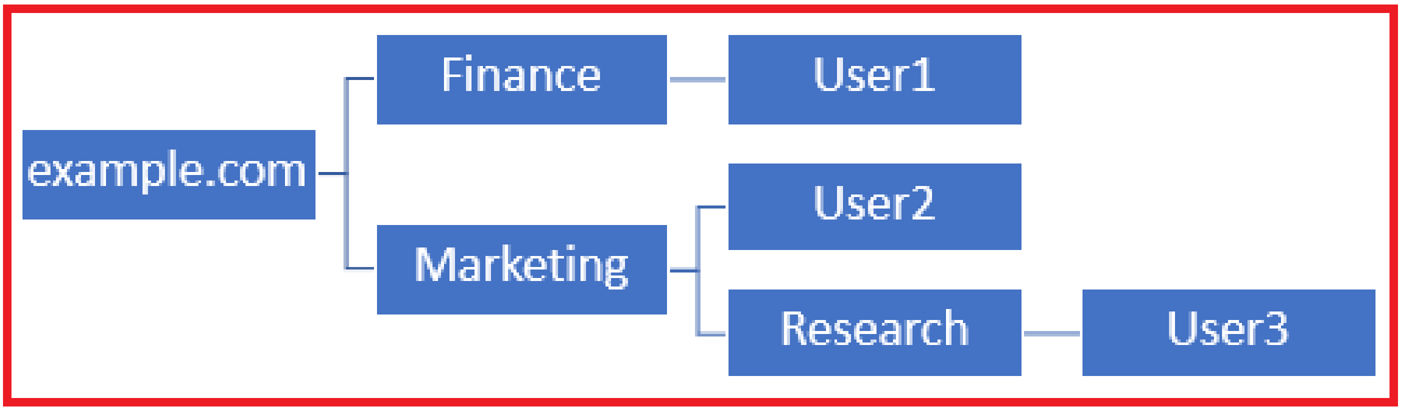
For example, this LDAP hierarchy:



If an administrator wants users within the **Marketing** organizational unit to be able to authenticate the base DN can be set to the root (example.com).

However, this also allows User1 under the **Finance** organizational unit to also log in since the user search begins at the root and go down to **Finance, Marketing,** and **Research**.

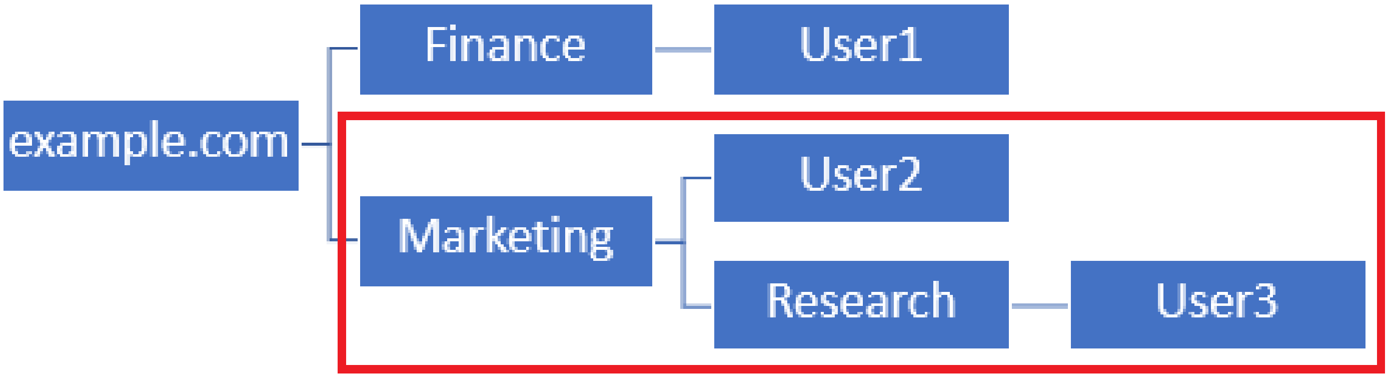
Base DN set to example.com



In order to restrict the log in to the only user in the **Marketing** organizational unit and below, the admin can instead set the Base DN to **Marketing**.

Now only User2 and User3 are able to authenticate because the search starts at **Marketing**.

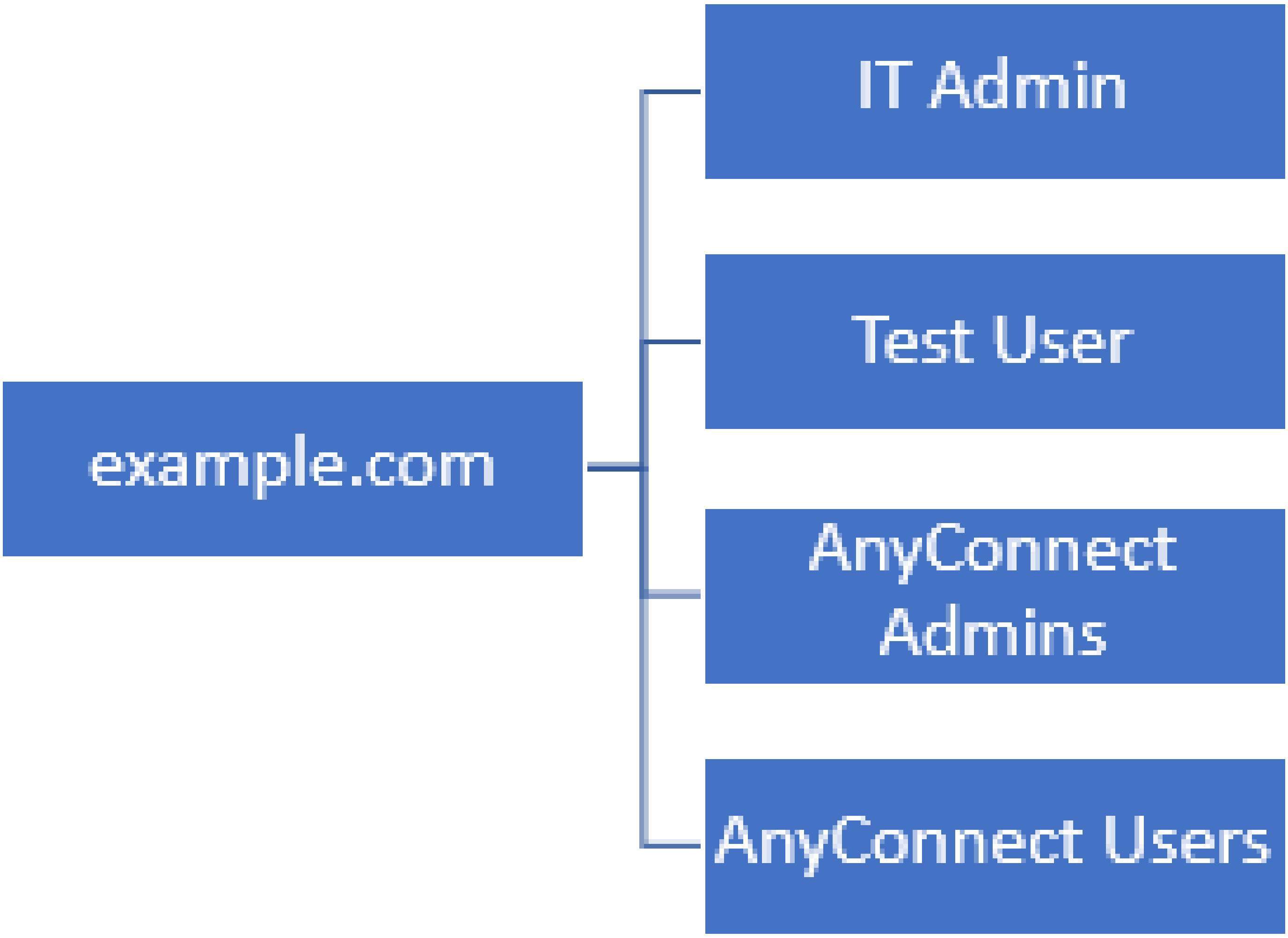
Base DN set to Marketing



Note that for more granular control within the FTD for which users are allowed to connect or assigning users different authorization based on their AD attributes, an LDAP authorization map needs to be configured.

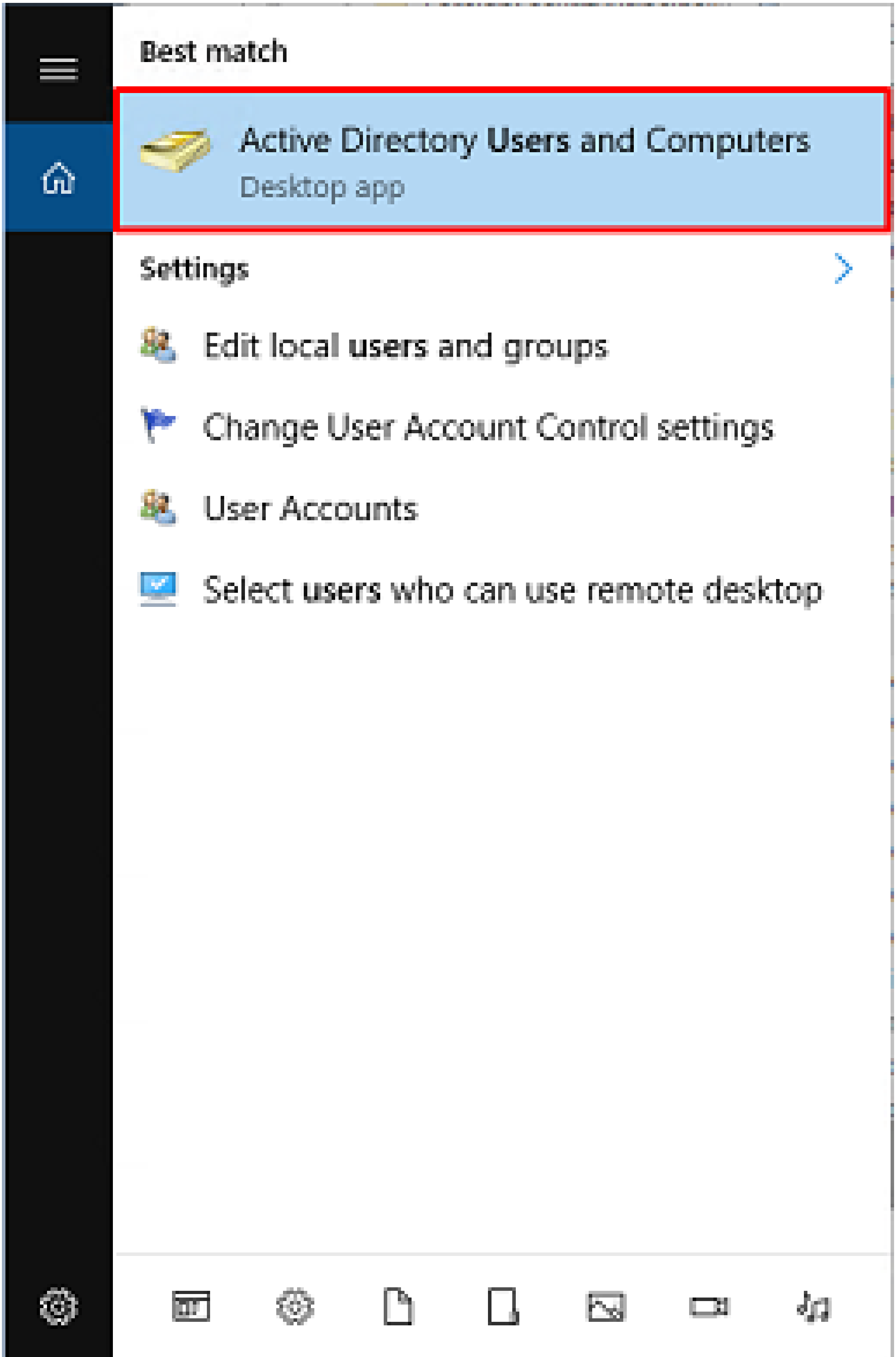
More information on this can be found here: Configure AnyConnect LDAP mapping on Firepower Threat Defense (FTD).

This simplified LDAP hierarchy is used in this configuration guide and the DN for the root example.com is used for both the Base DN and the Group DN.



Determine LDAP Base DN and Group DN

1. Open **Active Directory Users and Computers**.



Best match

Active Directory Users and Computers

Desktop app

Settings

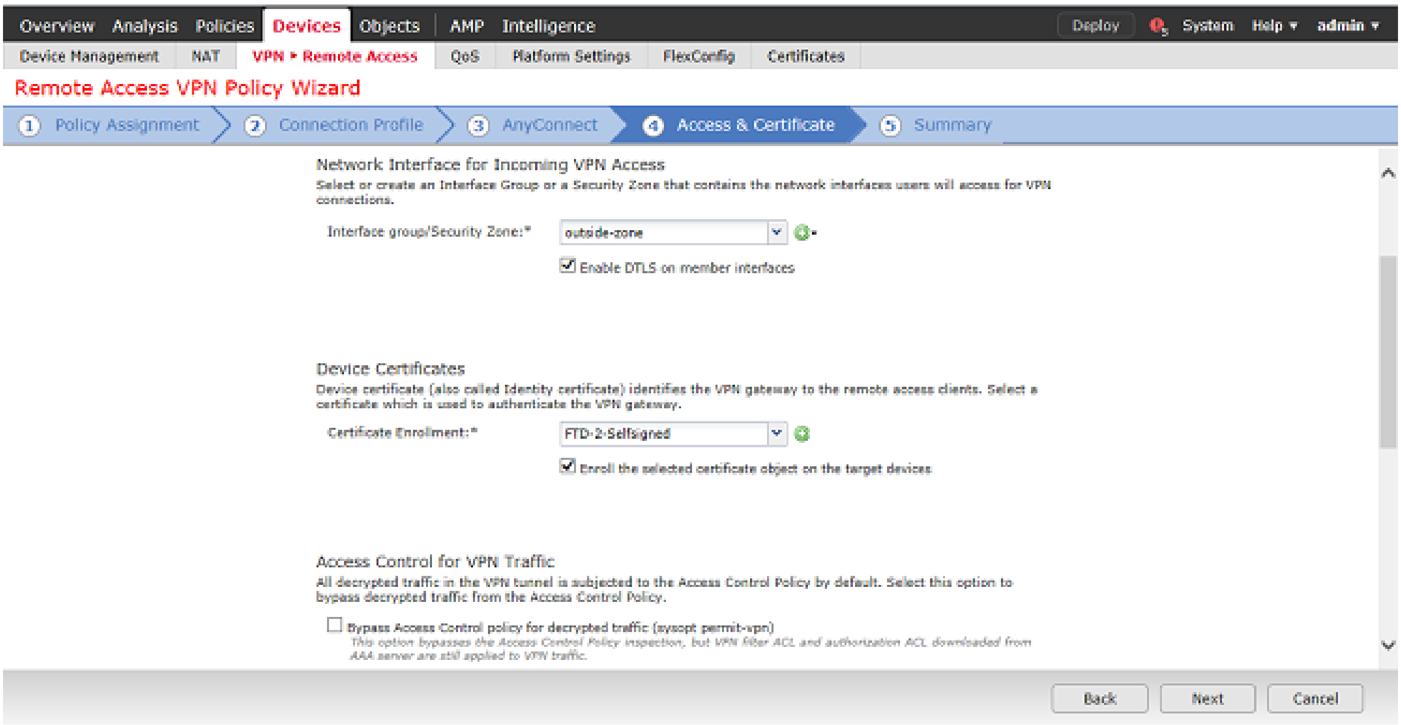
Edit local users and groups

Change User Account Control settings

User Accounts

Select users who can use remote desktop

for decrypted traffic (sysopt permit-vpn) is unchecked so that the user identity created later takes effect for RAVPN connections.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Device Management NAT VPN ▸ Remote Access QoS Platform Settings FlexConfig Certificates
1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary
Back Next Cancel

Remote Access VPN Policy Wizard

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:* FTD-2-Selfsigned

☑ Enroll the selected certificate object on the target devices

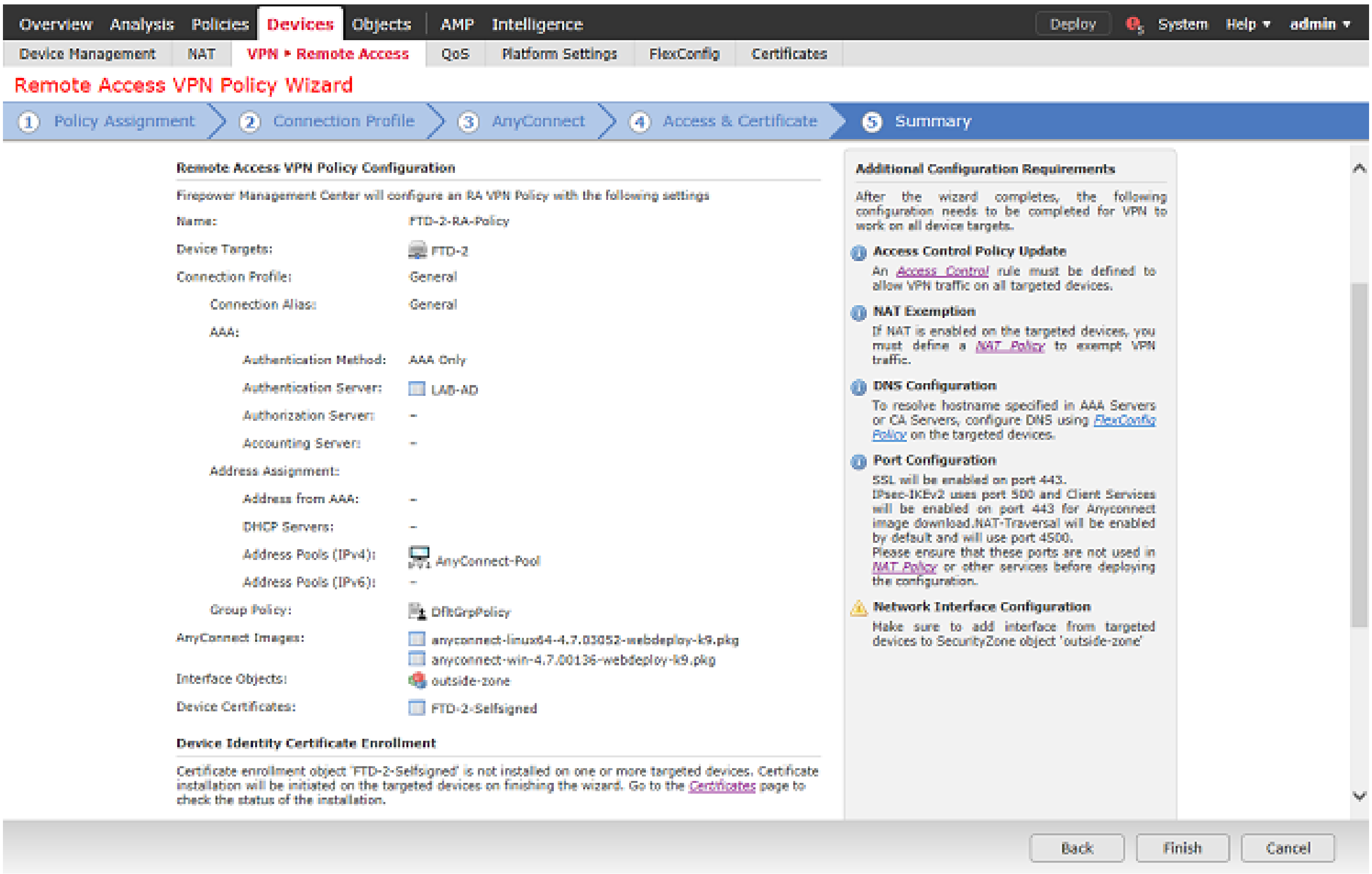
Access Control for VPN Traffic

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.

Under **Summary**, review the configuration the click **Finish**.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Device Management NAT VPN ▸ Remote Access QoS Platform Settings FlexConfig Certificates
1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary
Back Finish Cancel

Remote Access VPN Policy Wizard

Remote Access VPN Policy Configuration

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

Name: FTD-2-RA-Policy

Device Targets: FTD-2

Connection Profile: General

Connection Alias: General

AAA:

Authentication Method: AAA Only

Authentication Server: LAB-AD

Authorization Server: -

Accounting Server: -

Address Assignment:

Address from AAA: -

DHCP Servers: -

Address Pools (IPv4): AnyConnect-Pool

Address Pools (IPv6): -

Group Policy: DfltGrpPolicy

AnyConnect Images: anyconnect-linux64-4.7.03052-webdeploy-k9.pkg
anyconnect-win-4.7.00136-webdeploy-k9.pkg

Interface Objects: outside-zone

Device Certificates: FTD-2-Selfsigned

Device Identity Certificate Enrollment

Certificate enrollment object 'FTD-2-Selfsigned' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the Certificates page to check the status of the installation.

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.

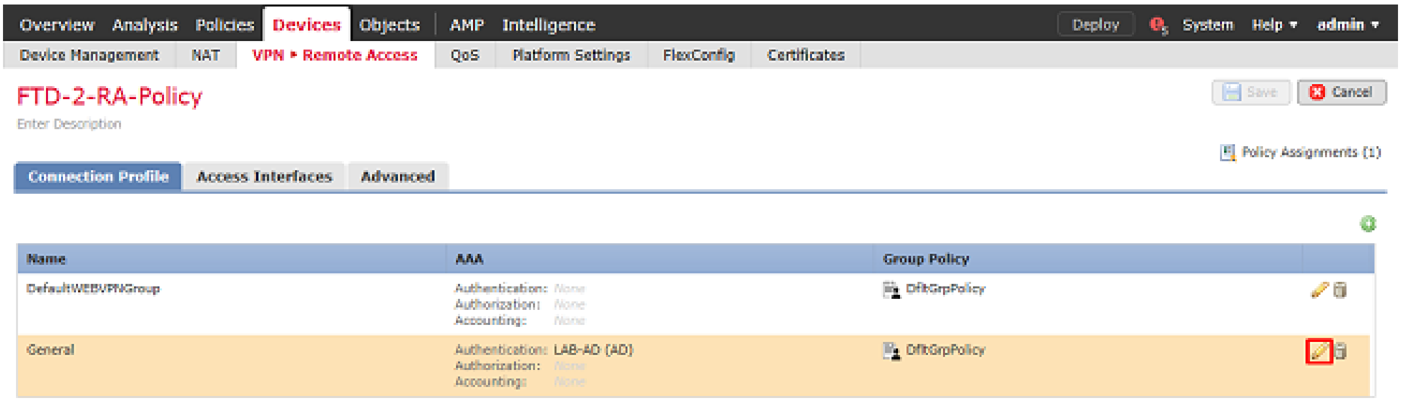
Port Configuration

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'

3. Under the **VPN > Remote Access** policy, click **Edit** icon (pencil) for the appropriate **Connection Profile**.



FTD-2-RA-Policy

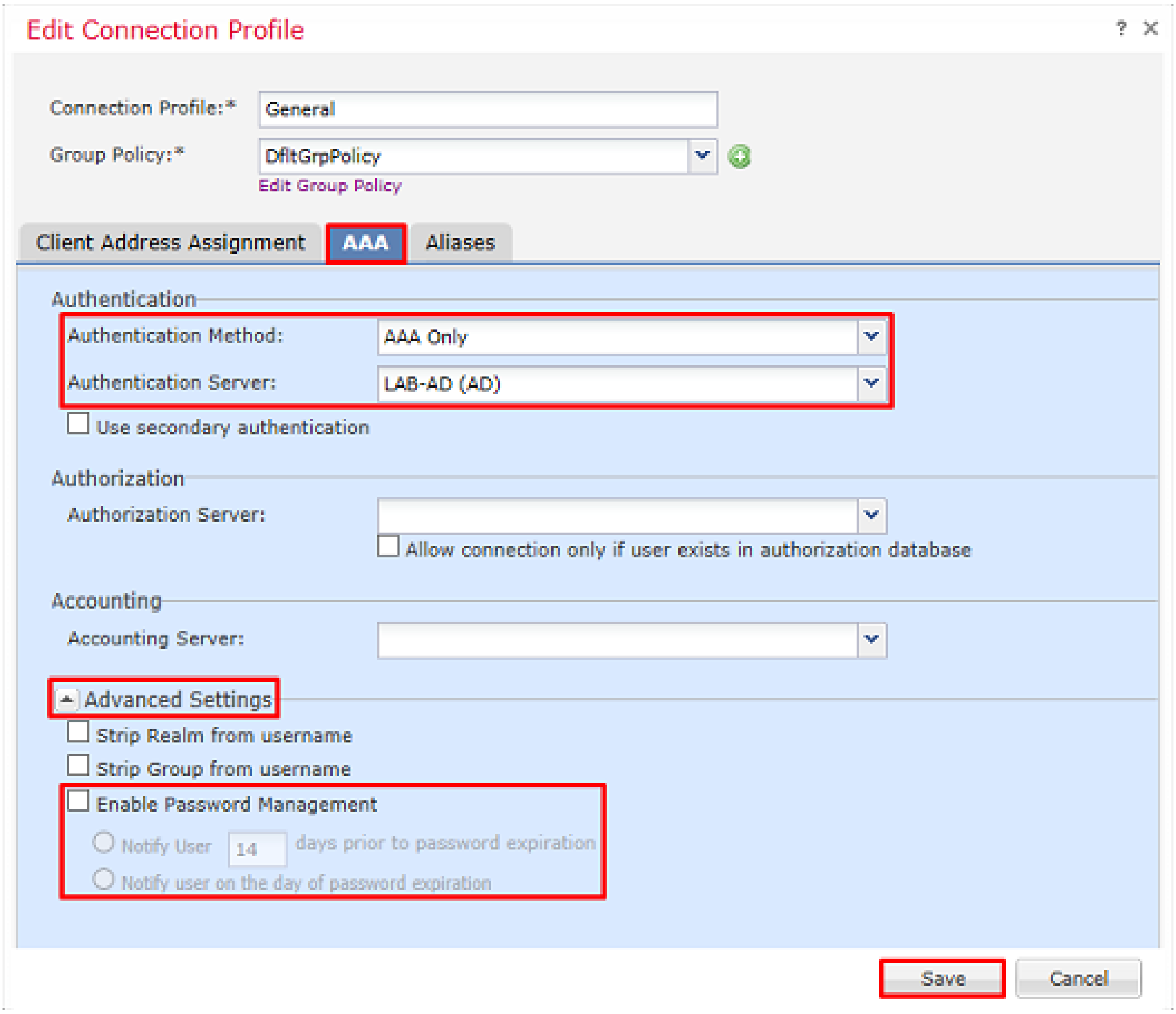
Enter Description

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
General	Authentication: LAB-AD (AD) Authorization: None Accounting: None	DfltGrpPolicy

Ensure that the Authentication Server is set to the realm created earlier.

Under **Advanced Settings**, **Enable Password Management** can be checked to allow users to change their password when or before it expires.

This setting requires that the realm use LDAPS, however. If any changes were made, click **Save**.



Edit Connection Profile

Connection Profile:* General

Group Policy:* DfltGrpPolicy

Authentication

Authentication Method: AAA Only

Authentication Server: LAB-AD (AD)

□ Use secondary authentication

Authorization

Authorization Server:

□ Allow connection only if user exists in authorization database

Accounting

Accounting Server:

Advanced Settings

□ Strip Realm from username

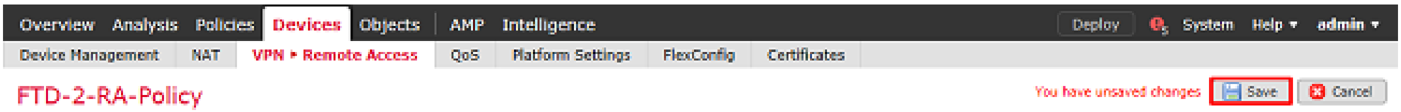
□ Strip Group from username

□ Enable Password Management

○ Notify User 14 days prior to password expiration

○ Notify user on the day of password expiration

When finished, click **Save**.

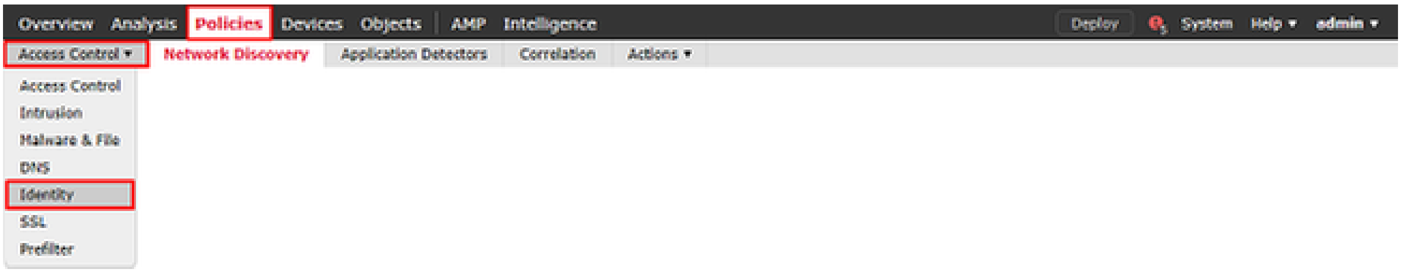


FTD-2-RA-Policy

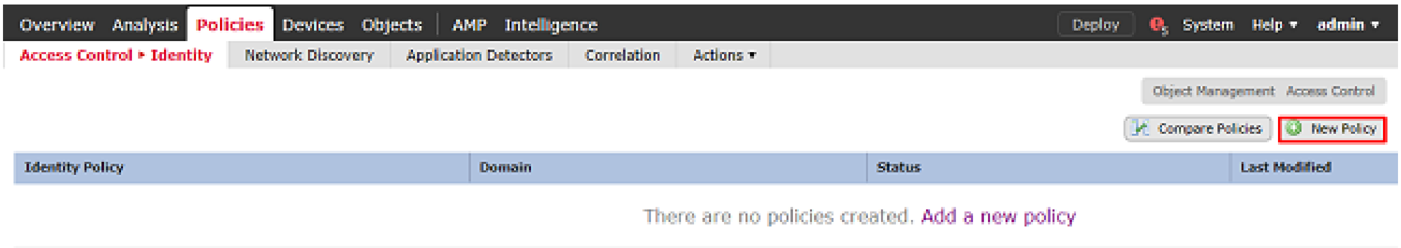
You have unsaved changes

Enable Identity Policy and Configure Security Policies for User Identity

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



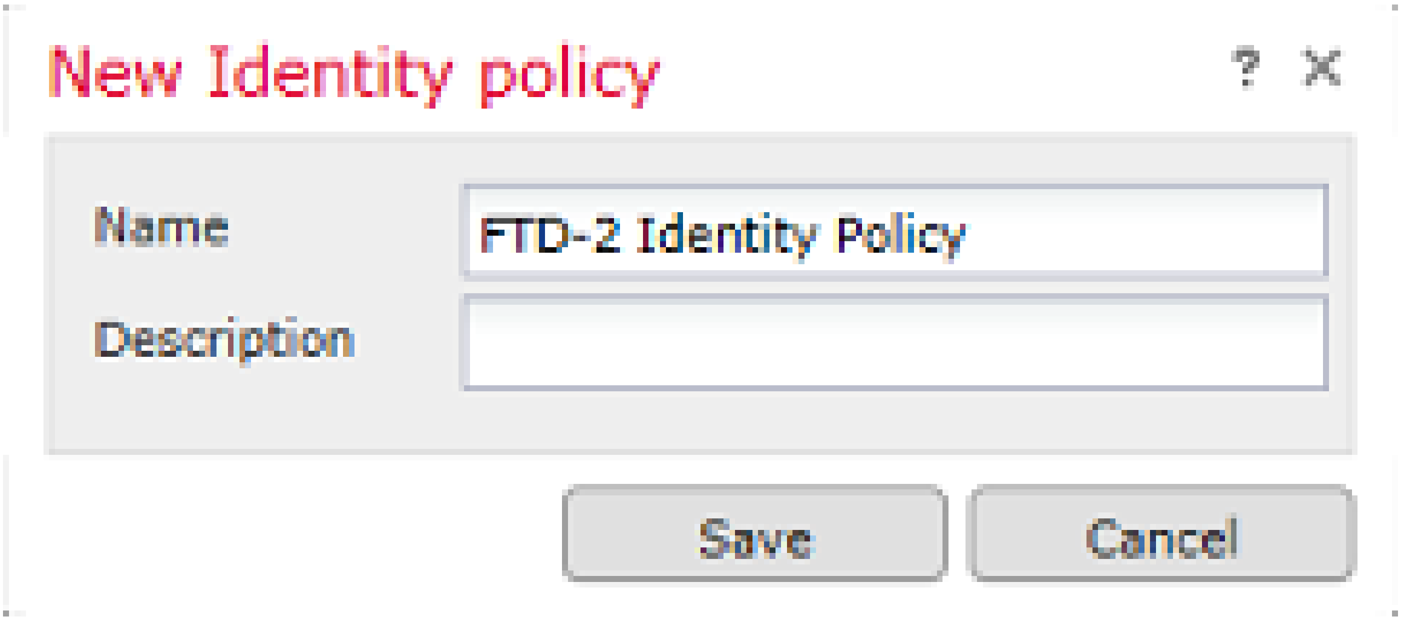
Create a new Identity Policy.



Identity Policy	Domain	Status	Last Modified

There are no policies created. Add a new policy

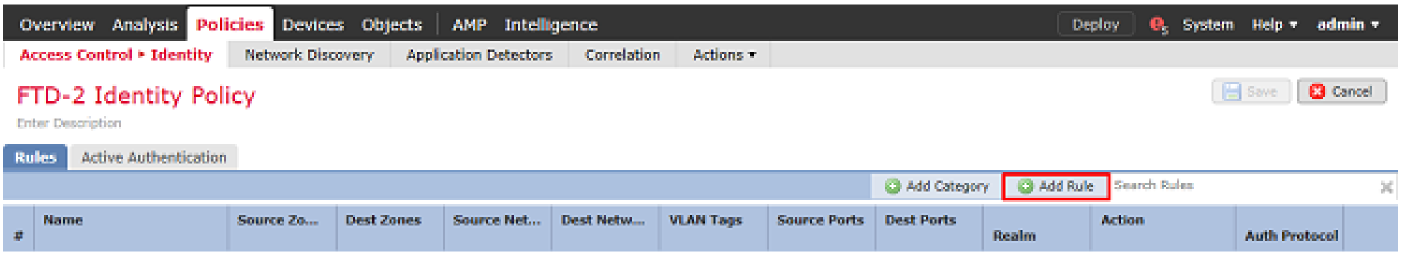
Specify a **Name** for the new **Identity Policy**.



Name: FTD-2 Identity Policy

Description:

2. Click **Add Rule**.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Access Control ▸ Identity Network Discovery Application Detectors Correlation Actions ▾
Save Cancel
Rules Active Authentication
Add Category Add Rule Search Rules

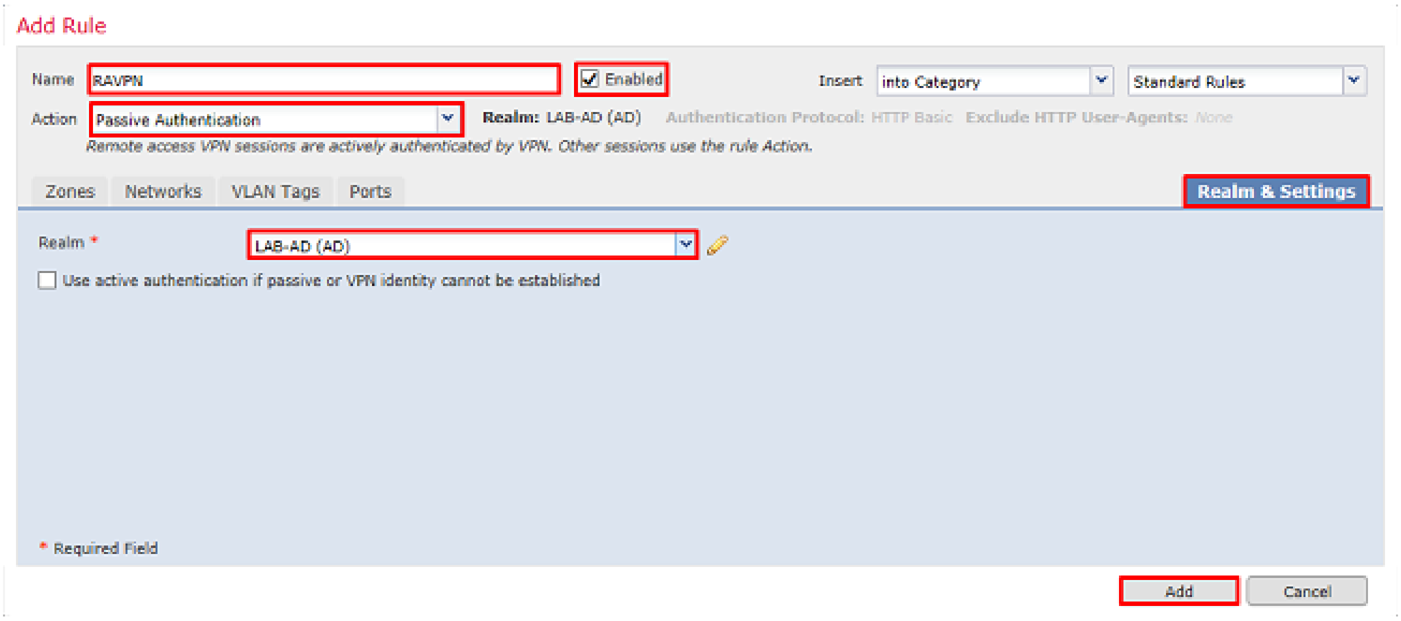
FTD-2 Identity Policy

Enter Description

#	Name	Source Zo...	Dest Zones	Source Net...	Dest Netw...	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol

3. Specify a **Name** for the new rule. Ensure that it is enabled and the action is set to **Passive Authentication**.

Click the **Realm & Settings** tab and select the realm created earlier. Click **Add** when finished.



Add Rule

Name RAVPN ☑ Enabled Insert into Category Standard Rules

Action Passive Authentication Realm: LAB-AD (AD) Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: *None*

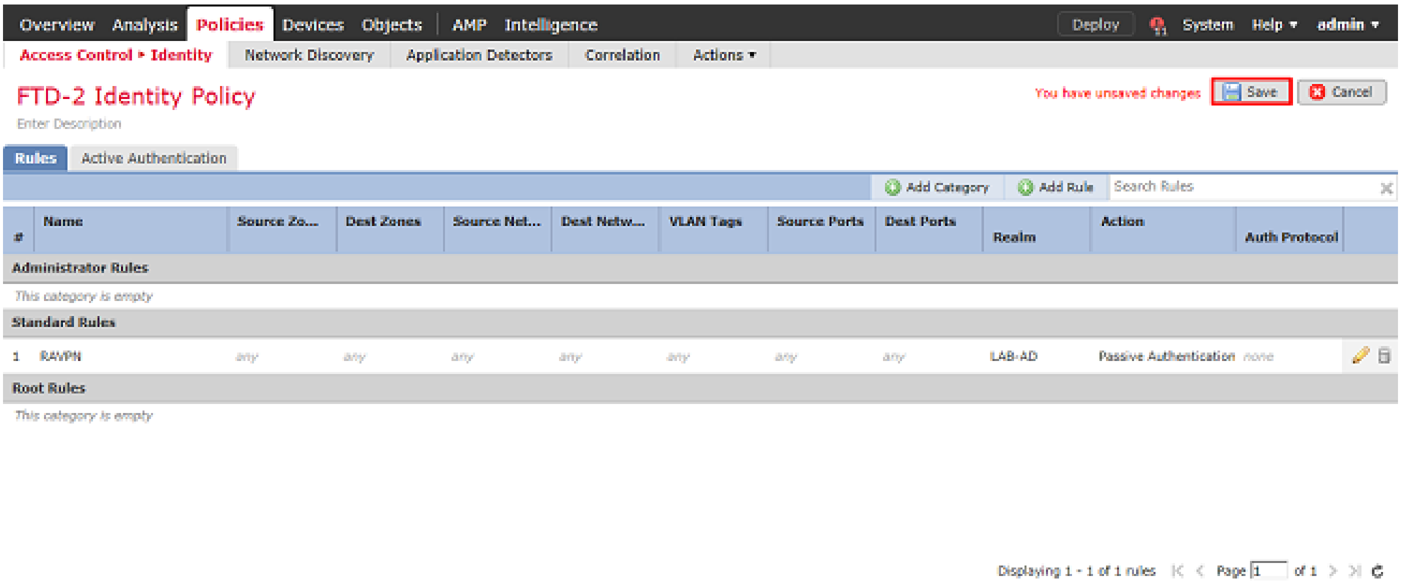
Remote access VPN sessions are actively authenticated by VPN. Other sessions use the rule Action.

Realm * LAB-AD (AD)

□ Use active authentication if passive or VPN identity cannot be established

* Required Field

4. Click **Save**.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Access Control ▸ Identity Network Discovery Application Detectors Correlation Actions ▾
Save Cancel
Rules Active Authentication
Add Category Add Rule Search Rules

FTD-2 Identity Policy

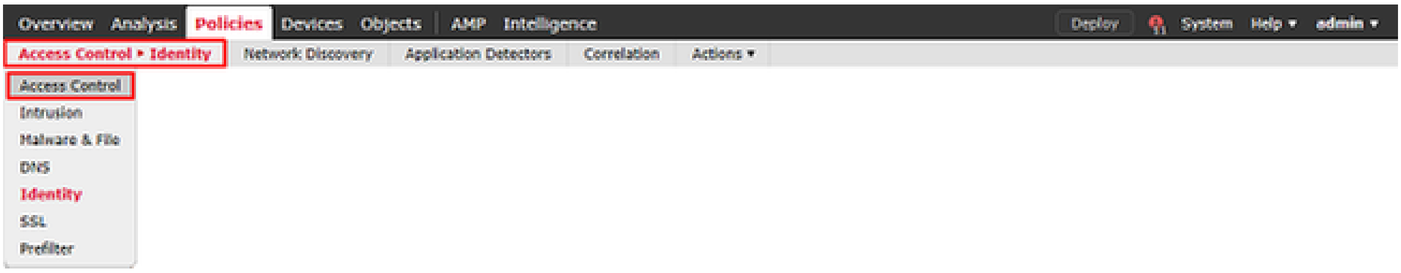
Enter Description

You have unsaved changes

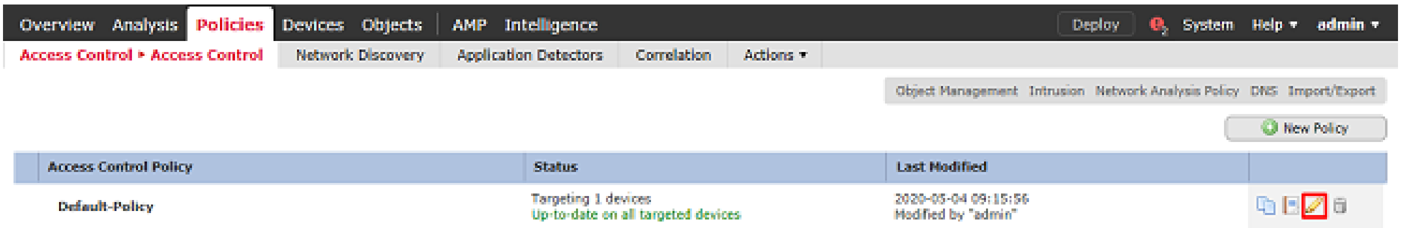
#	Name	Source Zo...	Dest Zones	Source Net...	Dest Netw...	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules											
This category is empty											
Standard Rules											
1	RAVPN	*any*	*any*	*any*	*any*	*any*	*any*	*any*	LAB-AD	Passive Authentication	*none*
Root Rules											
This category is empty											

Displaying 1 - 1 of 1 rules Page 1 of 1

5. Navigate to **Policies** > **Access Control** > **Access Control**.

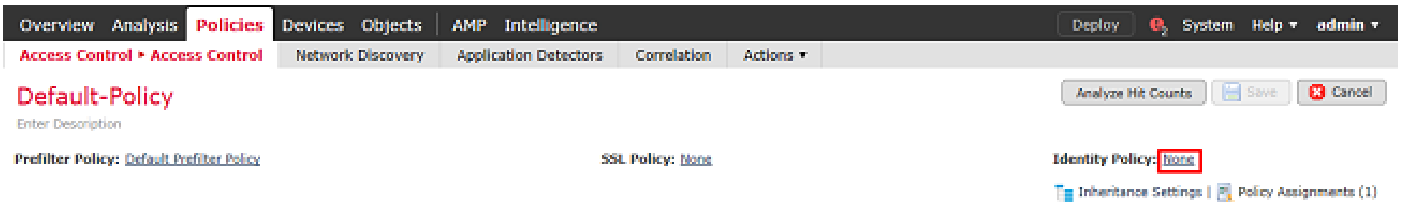


6. Edit the **Access Control Policy** the FTD is configured under.



Access Control Policy	Status	Last Modified
Default-Policy	Targeting 1 devices Up-to-date on all targeted devices	2020-05-04 09:15:56 Modified by "admin"

7. Click the value next to **Identity Policy**.



Default-Policy

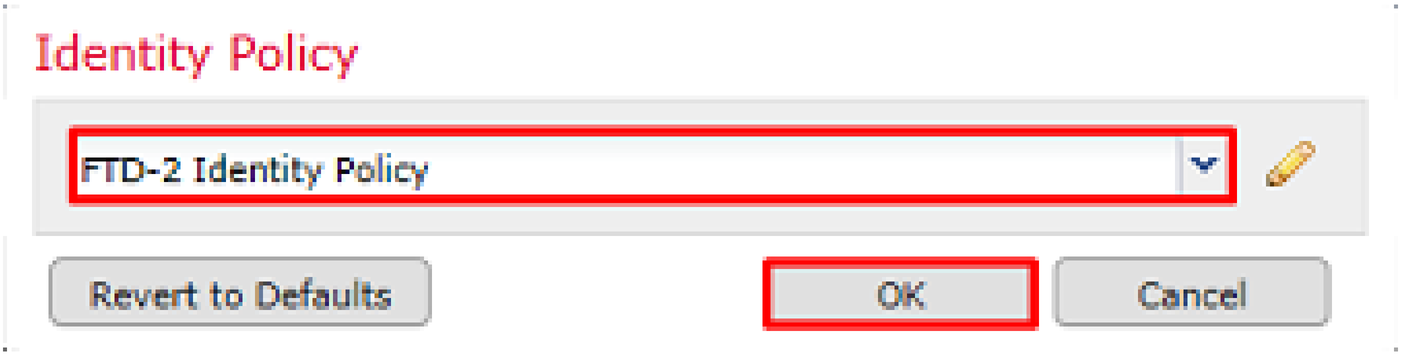
Enter Description

Prefilter Policy: Default Prefilter Policy

SSL Policy: None

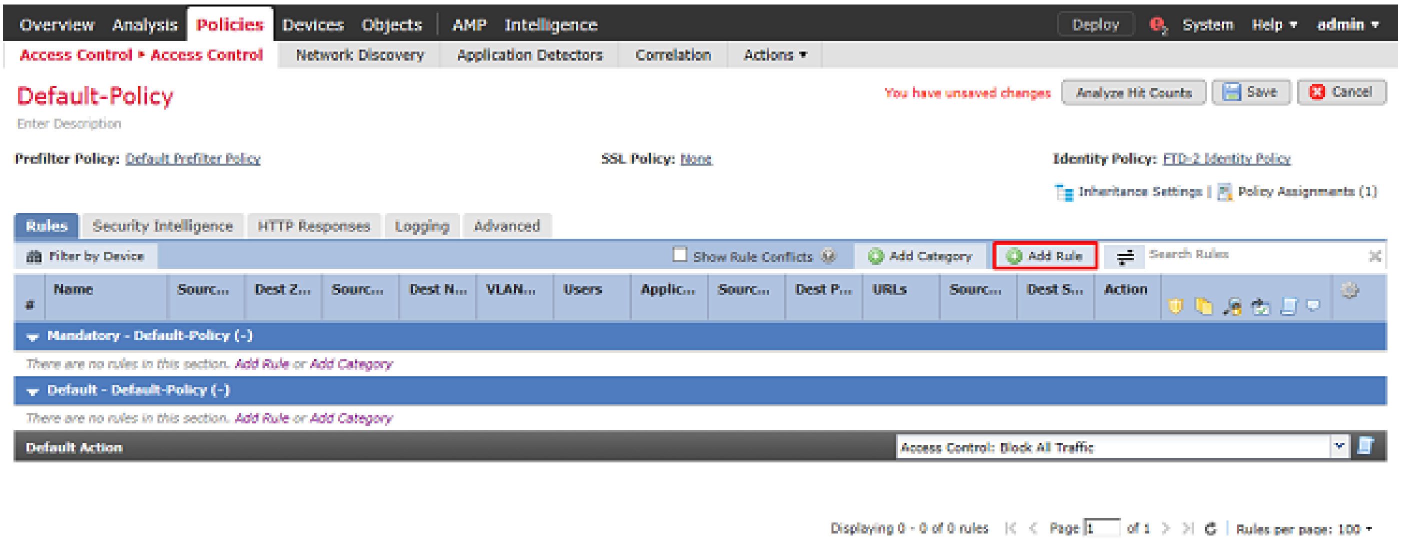
Identity Policy: None

Select the **Identity Policy** created earlier then click **OK**.



Identity Policy: FTD-2 Identity Policy

8. Click **Add Rule** to create an new ACP rule. These steps create a rule to allow the user within the AnyConnect Admins group to connect to devices within the inside network using RDP.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Access Control ▸ Access Control
Network Discovery Application Detectors Correlation Actions ▾
You have unsaved changes
Analyze Hit Counts
Save
Cancel
Inheritance Settings | Policy Assignments (1)
Rules Security Intelligence HTTP Responses Logging Advanced
Filter by Device
□ Show Rule Conflicts
Add Category
Add Rule
Search Rules
# Name Sourc... Dest Z... Sourc... Dest N... VLAN... Users Applic... Sourc... Dest P... URLs Sourc... Dest S... Action
Displaying 0 - 0 of 0 rules |< < Page 1 of 1 > >| Rules per page: 100 ▾

Default-Policy

Enter Description

Prefilter Policy: Default Prefilter Policy

SSL Policy: None

Identity Policy: FTD-2 Identity Policy

Mandatory - Default-Policy (-)

There are no rules in this section. Add Rule or Add Category

Default - Default-Policy (-)

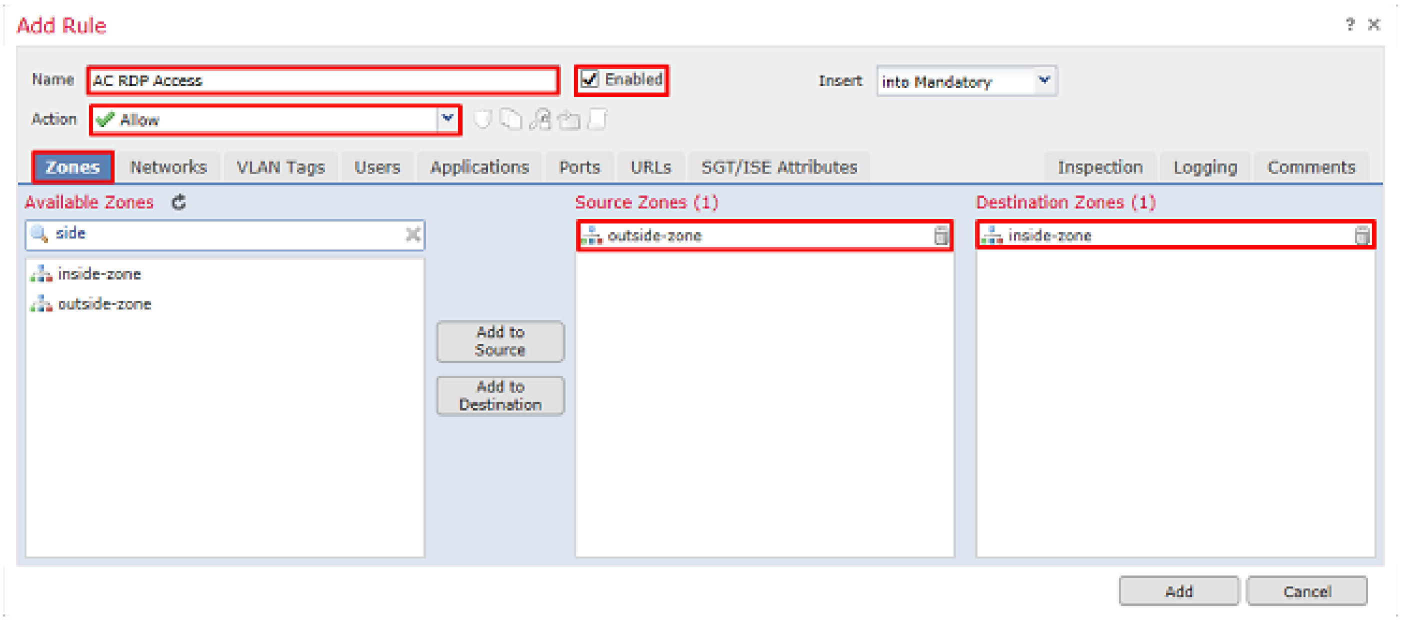
There are no rules in this section. Add Rule or Add Category

Default Action: Access Control: Block All Traffic

Specify a name for the rule. Ensure that the rule is **Enabled** and has the appropriate **Action**.

Under the **Zones** tab, specify the appropriate zones for the interesting traffic.

RDP traffic initiated by users come in to the FTD sourced from the outside-zone interface and egress the inside-zone.


Add Rule
? ✕
Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments
Add to Source
Add to Destination
Add
Cancel

Name: AC RDP Access

☑ Enabled

Insert: into Mandatory

Action: ✓ Allow

Available Zones

side

inside-zone

outside-zone

Source Zones (1)

outside-zone

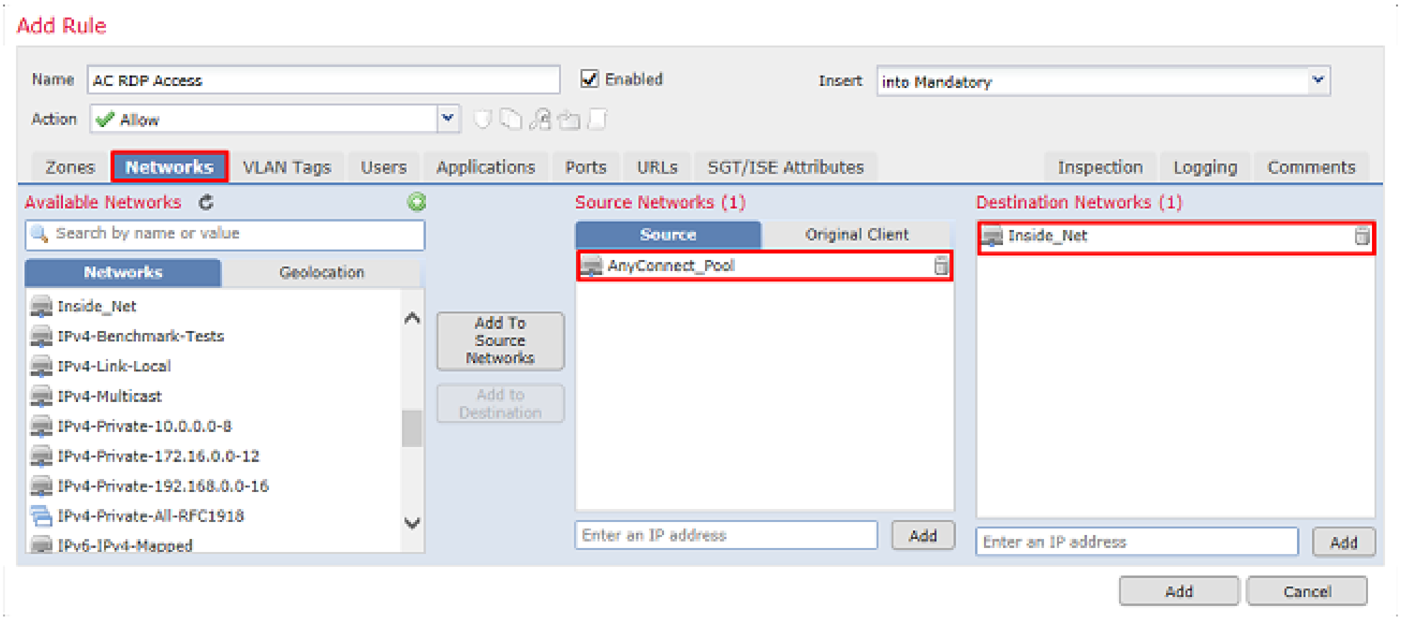
Destination Zones (1)

inside-zone

Under **Networks**, define the source and destination networks.

Object **AnyConnect_Pool** includes the IP addresses that is assigned to AnyConnect clients.

Object **Inside_Net** include the inside network subnet.



Add Rule

Name: AC RDP Access ☑ Enabled Insert: into Mandatory

Action: Allow

Source Networks (1): AnyConnect_Pool

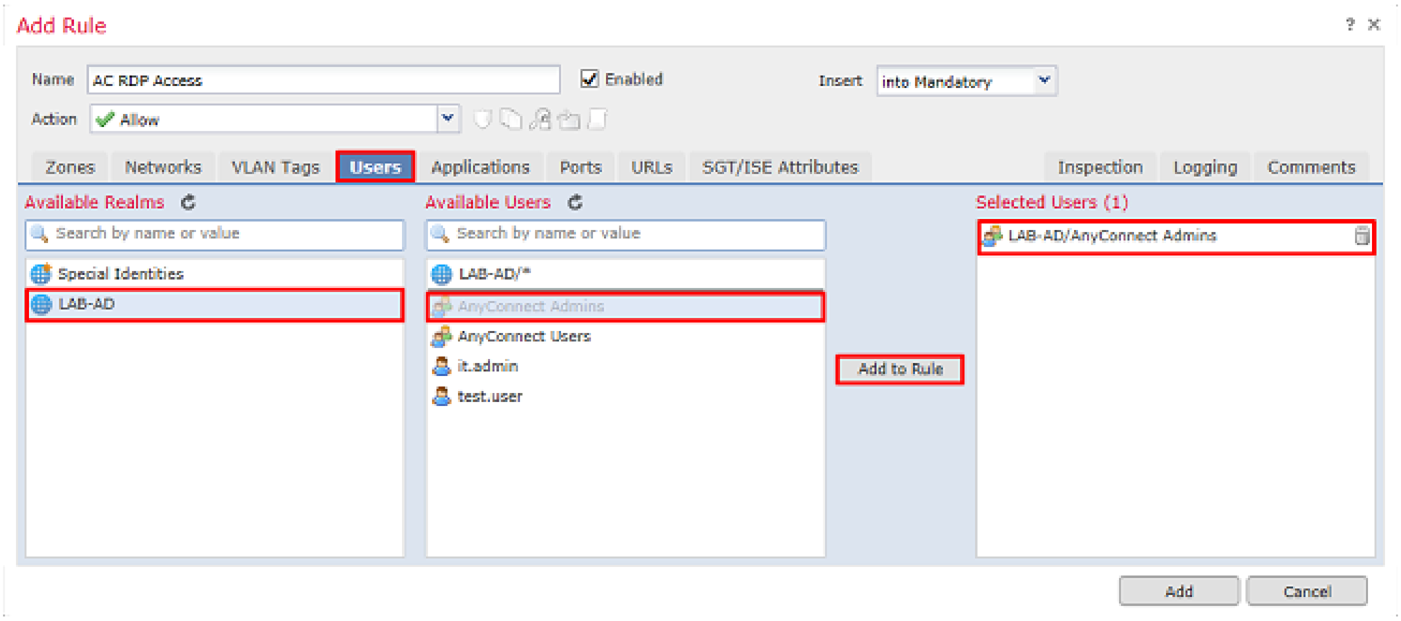
Destination Networks (1): Inside_Net

Under **Users**, click the realm created earlier under **Available Realms**, click the appropriate group/user under **Available Users**, then click **Add to Rule**.

If no users or groups are available under the **Available Users** section, ensure that FMC downloaded the **Users** and **Groups** under the realm section and that the appropriate **Groups/User** are included.

The **users/group** specified here is checked from the source perspective.

For example, with what has been defined in this rule so far, the FTD evaluates that the traffic is sourced from the outside-zone and destined to the inside-zone, sourced from the network in the AnyConnect_Pools object and destined to the network in the Inside_Net object, and the traffic is sourced from a user in the AnyConnect Admins group.



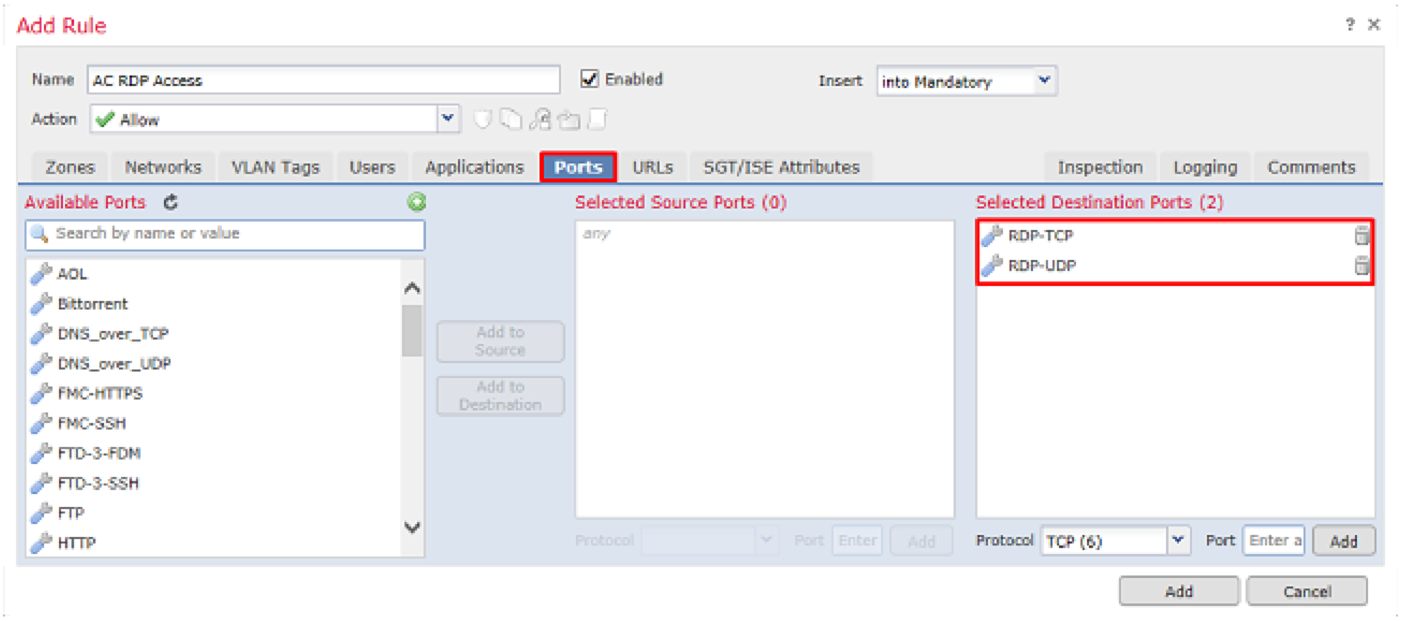
Add Rule

Name: AC RDP Access ☑ Enabled Insert: into Mandatory

Action: Allow

Selected Users (1): LAB-AD/AnyConnect Admins

Under **Ports**, custom RDP objects were created and added to allow TCP and UDP port 3389. Notice that RDP could have been added under the **Applications** section but for simplicity, only the ports are checked.


Add Rule

Name: AC RDP Access ☑ Enabled Insert: into Mandatory

Action: ✓ Allow

Available Ports

AOL
Bittorrent
DNS_over_TCP
DNS_over_UDP
FMC-HTTPS
FMC-SSH
FTD-3-FDM
FTD-3-SSH
FTP
HTTP

Selected Source Ports (0)

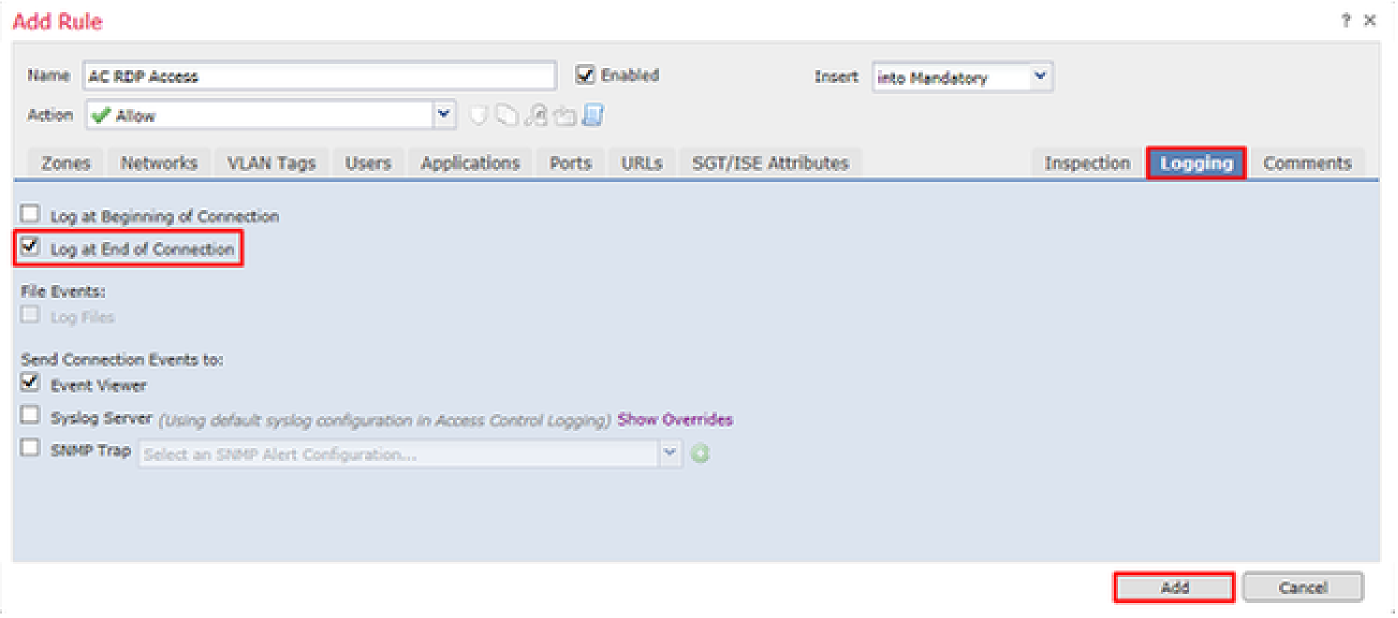
any

Selected Destination Ports (2)

RDP-TCP
RDP-UDP

Protocol: TCP (6) Port: Enter a

Finally, ensure that under **Logging**, **Log at End of Connection** is checked for additional verification later on. Click **Add** when done.


Add Rule

Name: AC RDP Access ☑ Enabled Insert: into Mandatory

Action: ✓ Allow

□ Log at Beginning of Connection

☑ Log at End of Connection

File Events:

□ Log Files

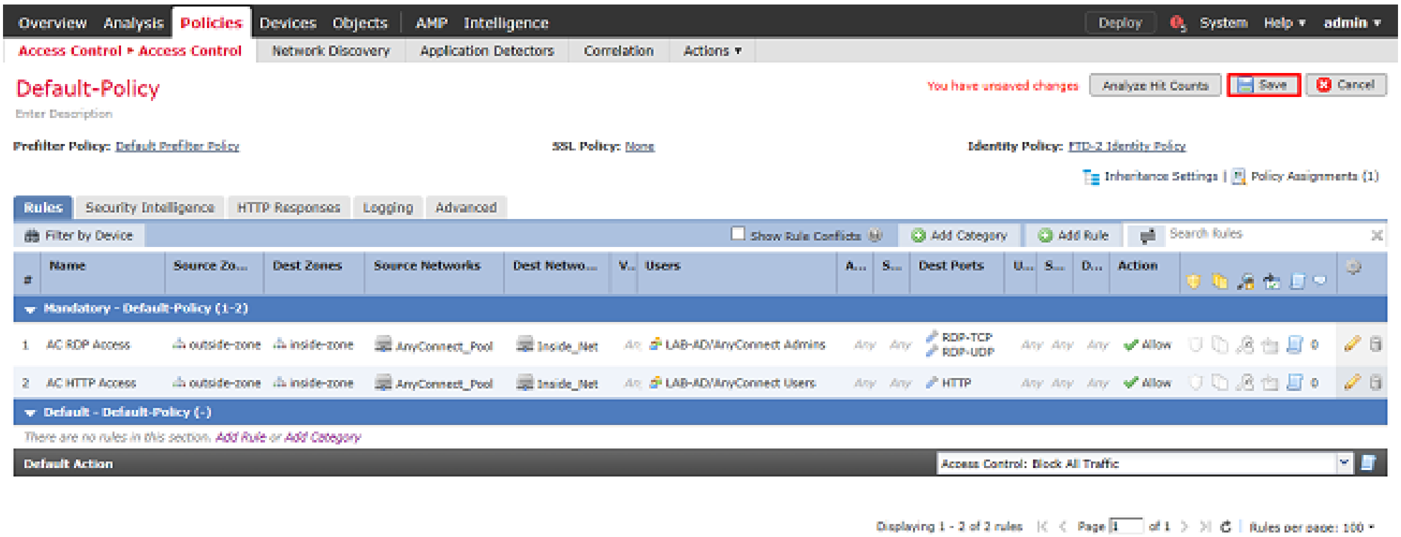
Send Connection Events to:

☑ Event Viewer

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

□ SNMP Trap Select an SNMP Alert Configuration...

9. An additional rule is created for HTTP access to allow users within the group **AnyConnect User** access to the **Windows Server IIS** website. Click **Save**.



Default-Policy

Enter Description

Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: FTD-2 Identity Policy

Inheritance Settings | Policy Assignments (1)

#	Name	Source Zo...	Dest Zones	Source Networks	Dest Netwo...	V...	Users	A...	S...	Dest Ports	U...	S...	D...	Action
Mandatory - Default-Policy (1-2)														
1	AC RDP Access	outside-zone	inside-zone	AnyConnect_Pool	Inside_Net	An	LAB-AD/AnyConnect Admins	Any	Any	RDP-TCP RDP-UDP	Any	Any	Any	✓ Allow
2	AC HTTP Access	outside-zone	inside-zone	AnyConnect_Pool	Inside_Net	An	LAB-AD/AnyConnect Users	Any	Any	HTTP	Any	Any	Any	✓ Allow
Default - Default-Policy (-)														

There are no rules in this section. Add Rule or Add Category

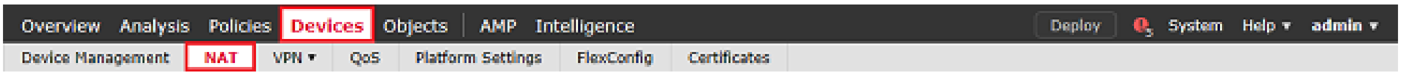
Default Action: Access Control: Block All Traffic

Displaying 1 - 2 of 2 rules Page 1 of 1 Rules per page: 100

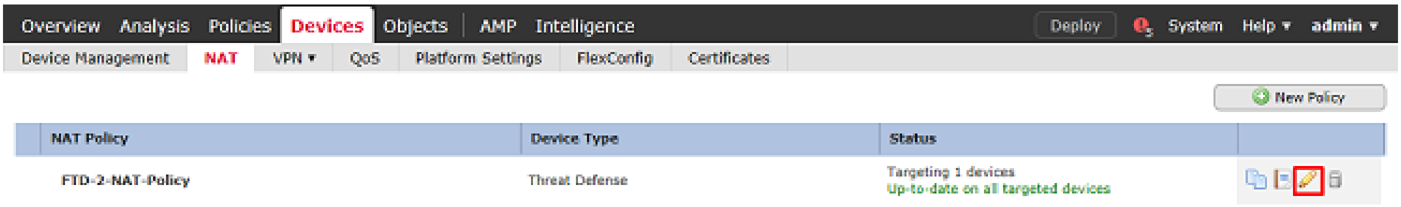
Configure NAT Exemption

If there are NAT rules that affect AnyConnect traffic, such as Internet PAT rules, it is important to configure NAT Exemption rules so that AnyConnect traffic is not NAT-affected.

1. Navigate to **Devices** > **NAT**.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates

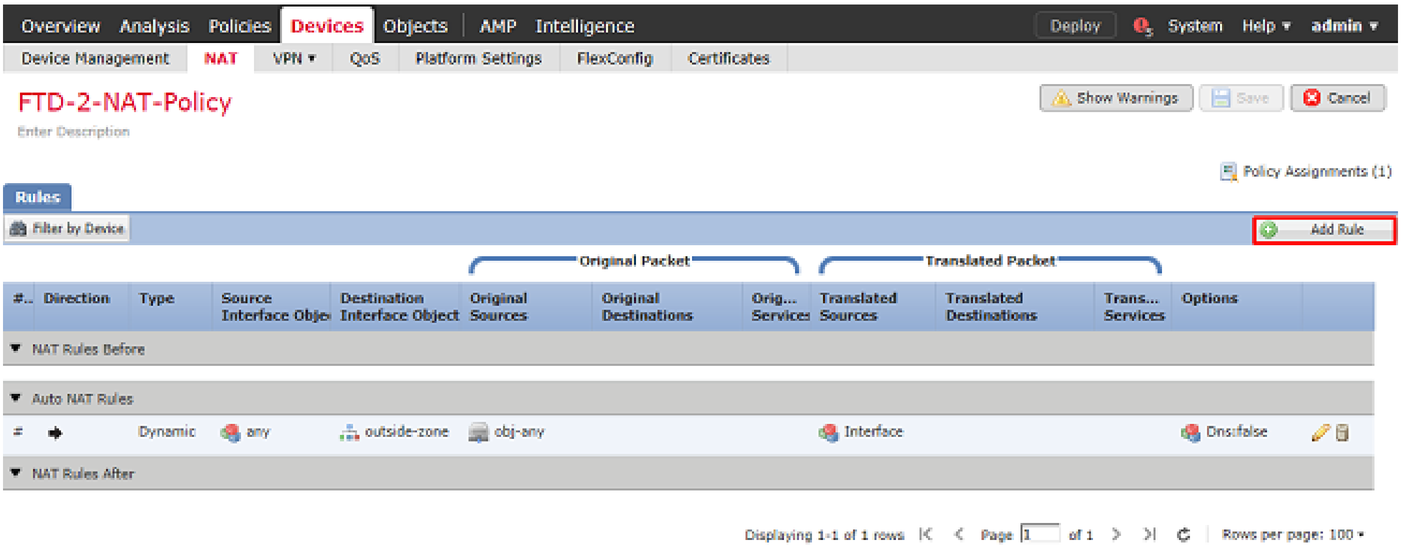
Select the **NAT Policy** applied to the FTD.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates
New Policy

NAT Policy	Device Type	Status
FTD-2-NAT-Policy	Threat Defense	Targeting 1 devices Up-to-date on all targeted devices

2. In this NAT Policy, there is a Dynamic PAT at the end which PAT-affects all traffic (including AnyConnect traffic) that egresses the outside interface to the outside interface.

To prevent AnyConnect traffic from being NAT-affected, click **Add Rule**.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates
Show Warnings
Save
Cancel
Policy Assignments (1)
Rules
Filter by Device
Add Rule

FTD-2-NAT-Policy

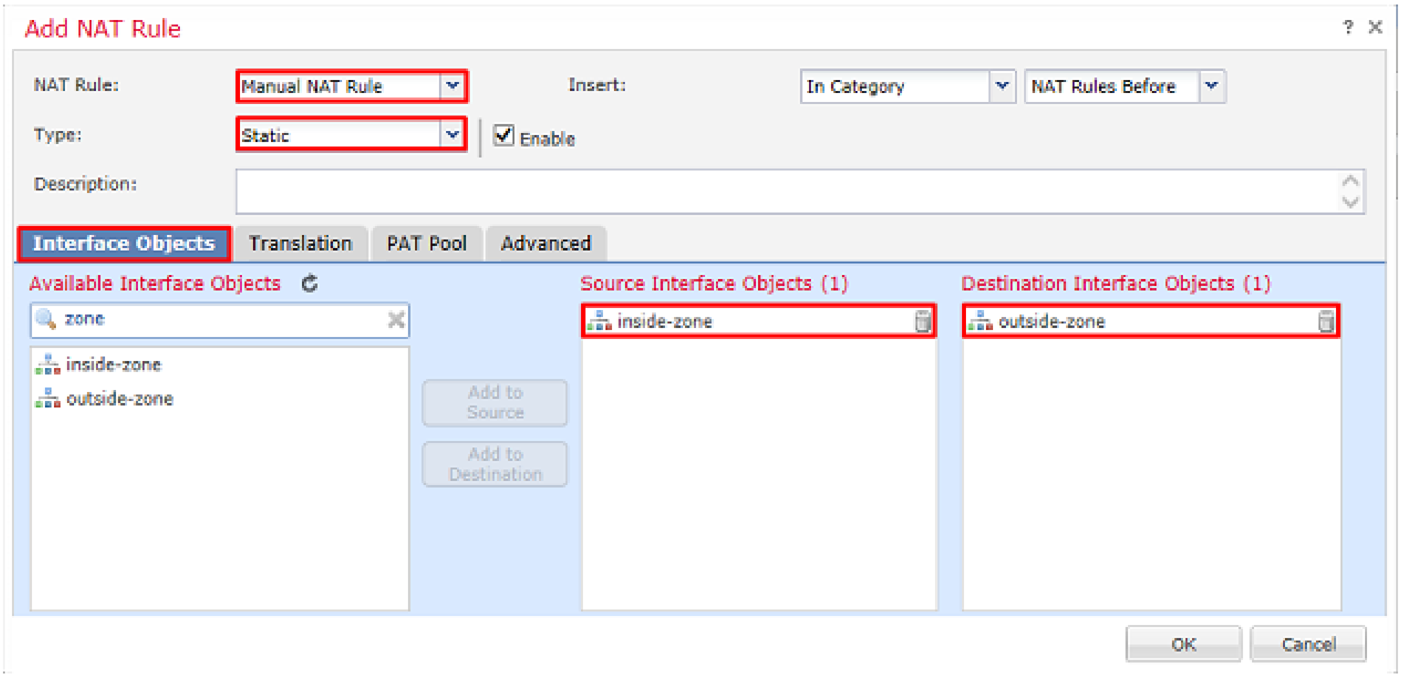
Enter Description

					Original Packet			Translated Packet			
#...	Direction	Type	Source Interface Obje	Destination Interface Object	Original Sources	Original Destinations	Orig... Services	Translated Sources	Translated Destinations	Trans... Services	Options
NAT Rules Before											
Auto NAT Rules											
#	➔	Dynamic	any	outside-zone	obj-any			Interface			Dns:false
NAT Rules After											

Displaying 1-1 of 1 rows Page 1 of 1 Rows per page: 100

3. Configure a NAT exemption rule, make sure that the rule is a **Manual NAT Rule** with **Type Static**. This is a bidirectional NAT rule that applies to AnyConnect traffic.

With these settings, when the FTD detects traffic sourced from Inside_Net and destined to AnyConnect IP address (defined by AnyConnect_Pool), the source is translated to the same value (Inside_Net) and the destination is translated to the same value (AnyConnect_Pool) when traffic ingresses the **inside_zone** and egresses the **outside_zone**. This essentially bypasses NAT when these conditions are met.



Add NAT Rule

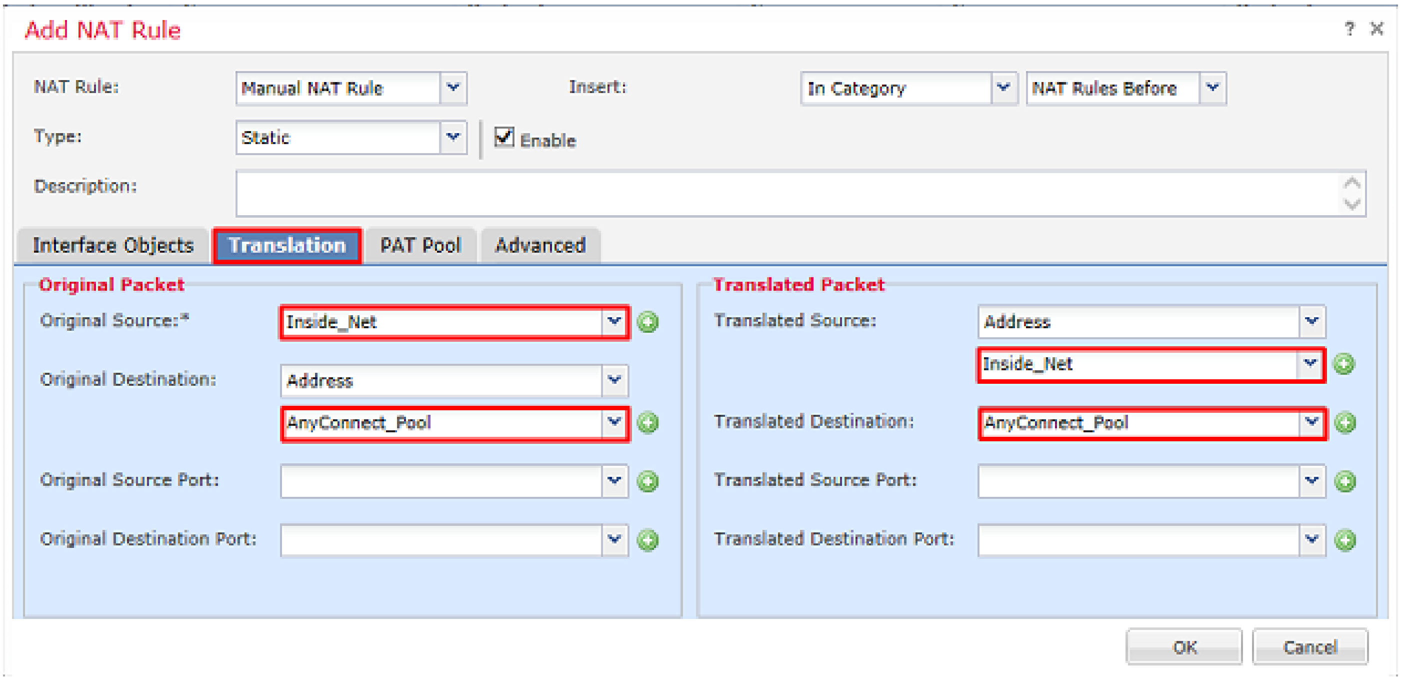
NAT Rule: Manual NAT Rule
Insert: In Category | NAT Rules Before
Type: Static
☑ Enable
Description:

Interface Objects | Translation | PAT Pool | Advanced

Available Interface Objects: zone
- inside-zone
- outside-zone

Source Interface Objects (1): inside-zone

Destination Interface Objects (1): outside-zone



Add NAT Rule

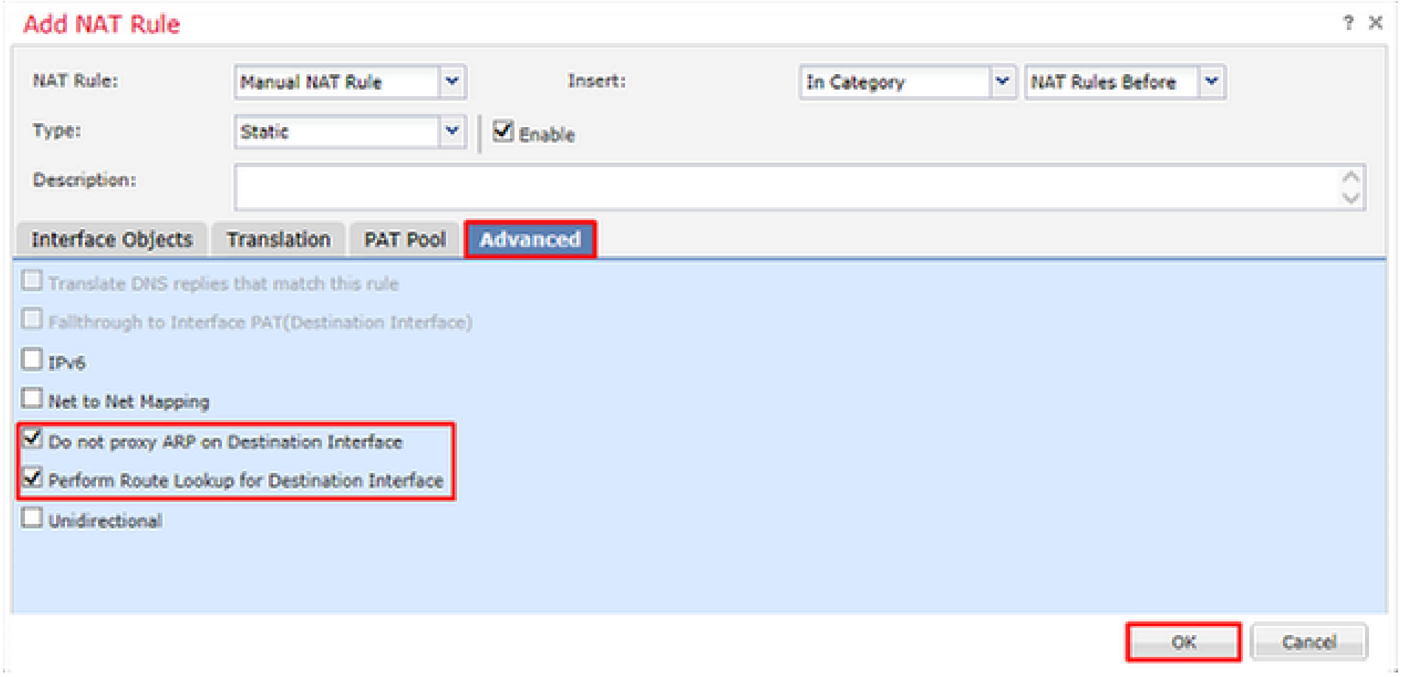
NAT Rule: Manual NAT Rule
Insert: In Category | NAT Rules Before
Type: Static
☑ Enable
Description:

Interface Objects | Translation | PAT Pool | Advanced

Original Packet
Original Source:* Inside_Net
Original Destination: Address
AnyConnect_Pool
Original Source Port:
Original Destination Port:

Translated Packet
Translated Source: Address
Inside_Net
Translated Destination: AnyConnect_Pool
Translated Source Port:
Translated Destination Port:

Additionally, the FTD is set to perform a route lookup on this traffic and not proxy ARP. Click **OK** when done.



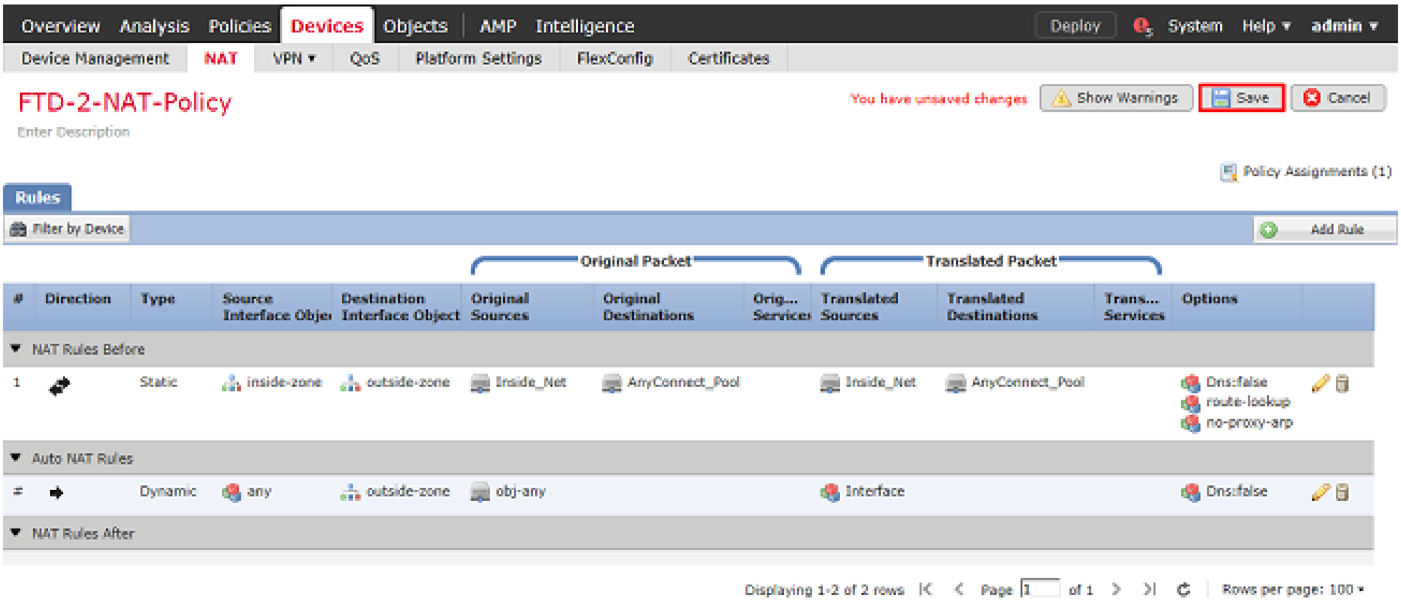
Add NAT Rule

NAT Rule:	Manual NAT Rule	Insert:	In Category / NAT Rules Before
Type:	Static	☑ Enable	
Description:			

Interface Objects | Translation | PAT Pool | Advanced

- □ Translate DNS replies that match this rule
- □ Fallthrough to Interface PAT(Destination Interface)
- □ IPv6
- □ Net to Net Mapping
- ☑ Do not proxy ARP on Destination Interface
- ☑ Perform Route Lookup for Destination Interface
- □ Unidirectional

4. Click **Save**.



FTD-2-NAT-Policy

Enter Description

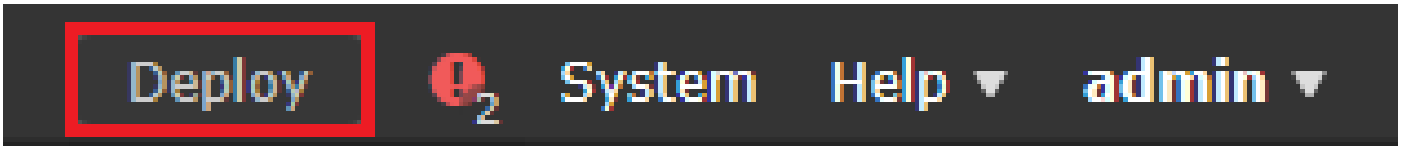
You have unsaved changes

					Original Packet			Translated Packet			
#	Direction	Type	Source Interface Obje	Destination Interface Object	Original Sources	Original Destinations	Orig... Services	Translated Sources	Translated Destinations	Trans... Services	Options
▼ NAT Rules Before											
1	⇄	Static	inside-zone	outside-zone	Inside_Net	AnyConnect_Pool		Inside_Net	AnyConnect_Pool		Dns:false route-lookup no-proxy-arp
▼ Auto NAT Rules											
#	➔	Dynamic	any	outside-zone	obj-any			Interface			Dns:false
▼ NAT Rules After											

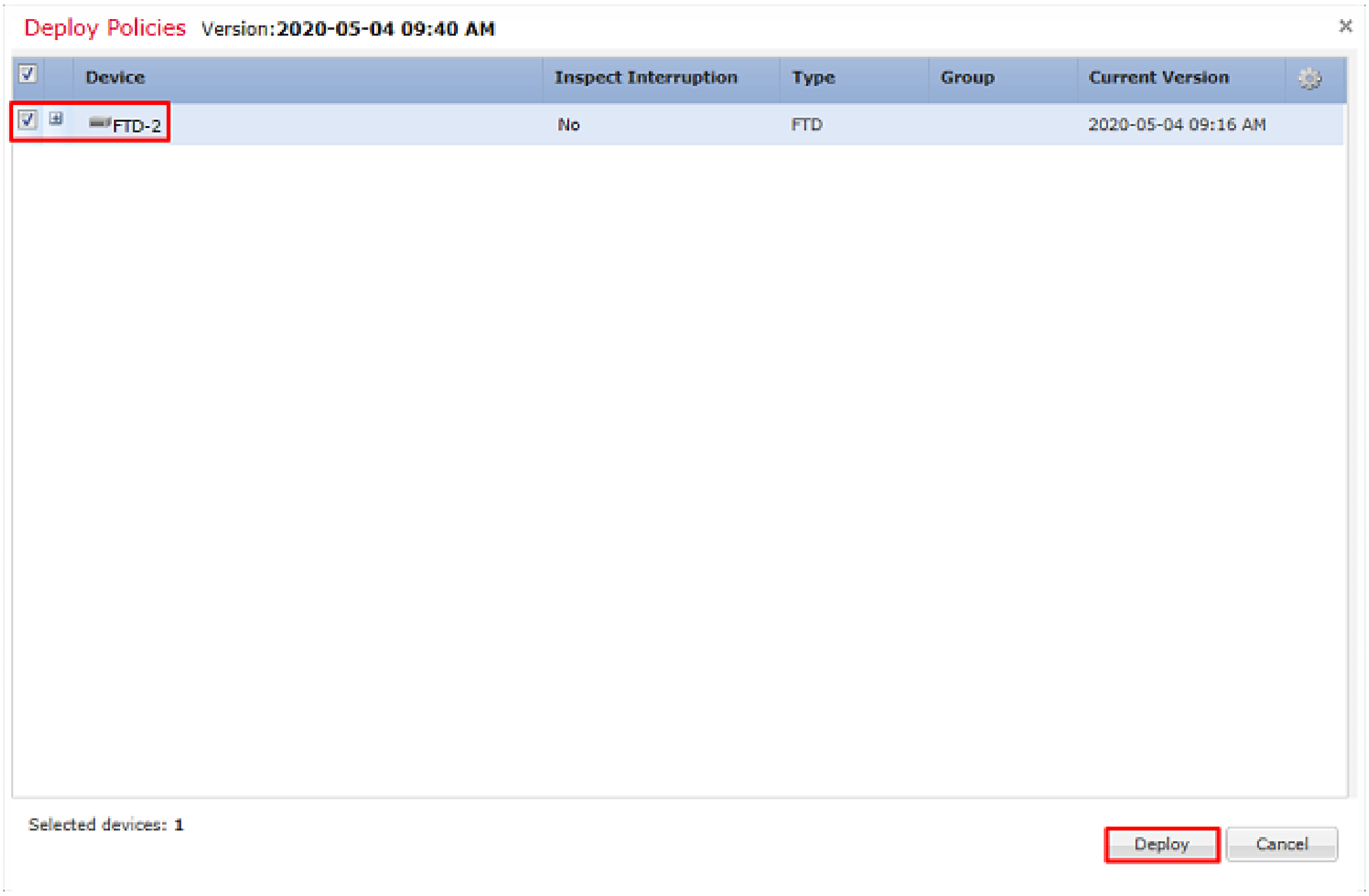
Displaying 1-2 of 2 rows | Page 1 of 1 | Rows per page: 100 ▾

Deploy

1. When the configuration is finished, click **Deploy**.



2. Click the checkbox next to the FTD the configuration is applied to it and then click **Deploy**.



Deploy Policies Version:2020-05-04 09:40 AM

☑	Device	Inspect Interruption	Type	Group	Current Version
☑ ⊞	FTD-2	No	FTD		2020-05-04 09:16 AM

Selected devices: 1

Verify

Final Configuration

AAA Configuration

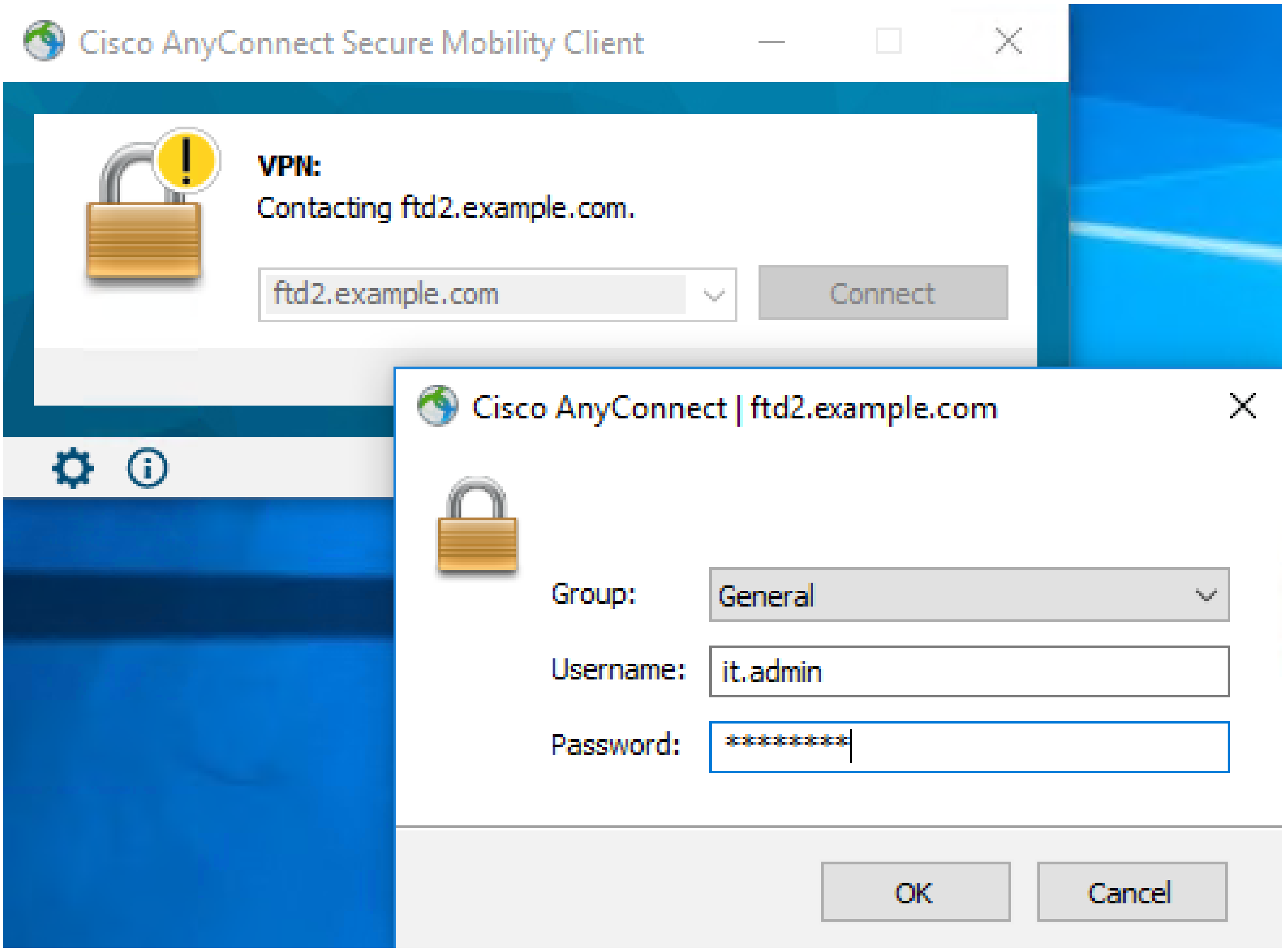
```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
 max-failed-attempts 4
 realm-id 5
aaa-server LAB-AD host win2016.example.com
 server-port 389
 ldap-base-dn DC=example,DC=com
 ldap-group-base-dn DC=example,DC=com
 ldap-scope subtree
 ldap-naming-attribute samaccountname
 ldap-login-password *****
 ldap-login-dn ftd.admin@example.com
 server-type microsoft
```

AnyConnect Configuration

```
> show running-config webvpn
webvpn
```

```
 enable Outside
 anyconnect image disk0:/csm/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1 regex "Linux"
 anyconnect image disk0:/csm/anyconnect-win-4.7.00136-webdeploy-k9.pkg 2 regex "Windows"
 anyconnect profiles Lab disk0:/csm/lab.xml
 anyconnect enable
 tunnel-group-list enable
 cache
  no disable
 error-recovery disable

> show running-config tunnel-group
tunnel-group General type remote-access
tunnel-group General general-attributes
 address-pool AnyConnect-Pool
 authentication-server-group LAB-AD
tunnel-group General webvpn-attributes
 group-alias General enable

> show running-config group-policy
group-policy DfltGrpPolicy attributes
 vpn-simultaneous-logins 10
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Lab
 user-authentication-idle-timeout none
 webvpn
  anyconnect keep-installer none
  anyconnect modules value dart
  anyconnect ask none default anyconnect
  http-comp none
  activex-relay disable
  file-entry disable
  file-browsing disable
  url-entry disable
  deny-message none
  anyconnect ssl df-bit-ignore enable

> show running-config ssl
ssl trust-point FTD-2-SelfSigned outside
```

Connect with AnyConnect and Verify Access Control Policy Rules



Cisco AnyConnect Secure Mobility Client

VPN:
Contacting ftd2.example.com.

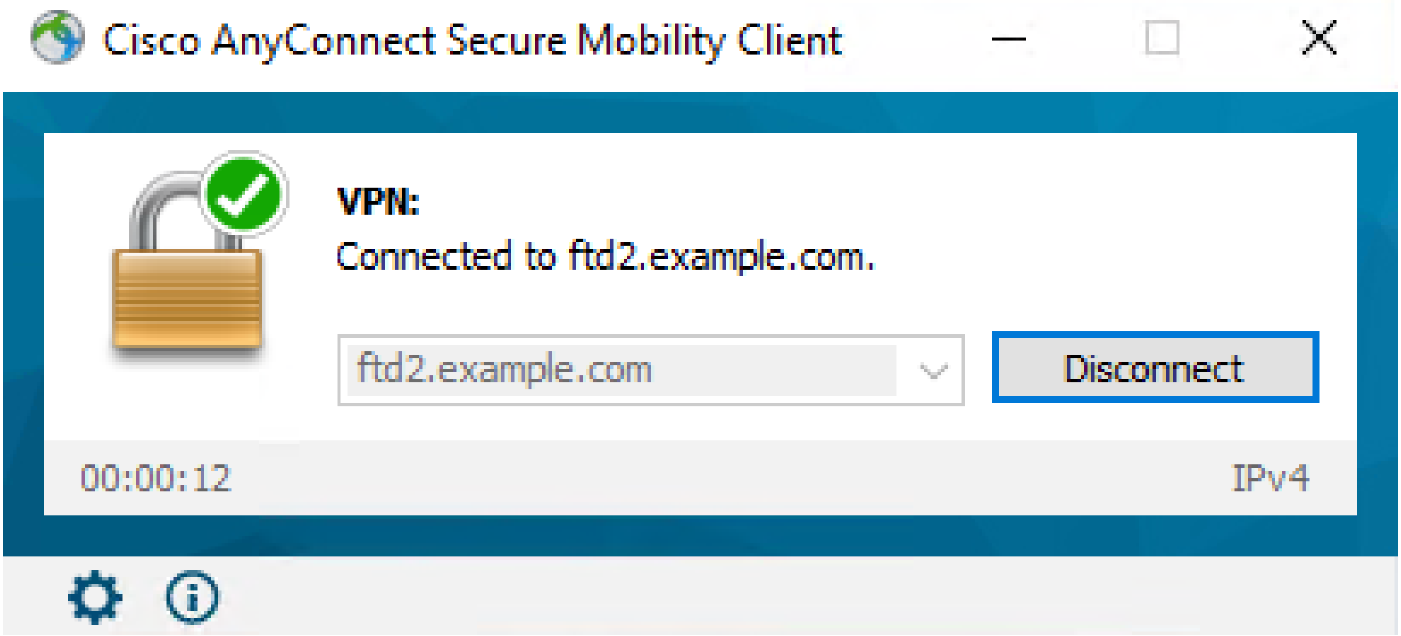
ftd2.example.com

Cisco AnyConnect | ftd2.example.com

Group: General

Username: it.admin

Password: *********



Cisco AnyConnect Secure Mobility Client

VPN:
Connected to ftd2.example.com.

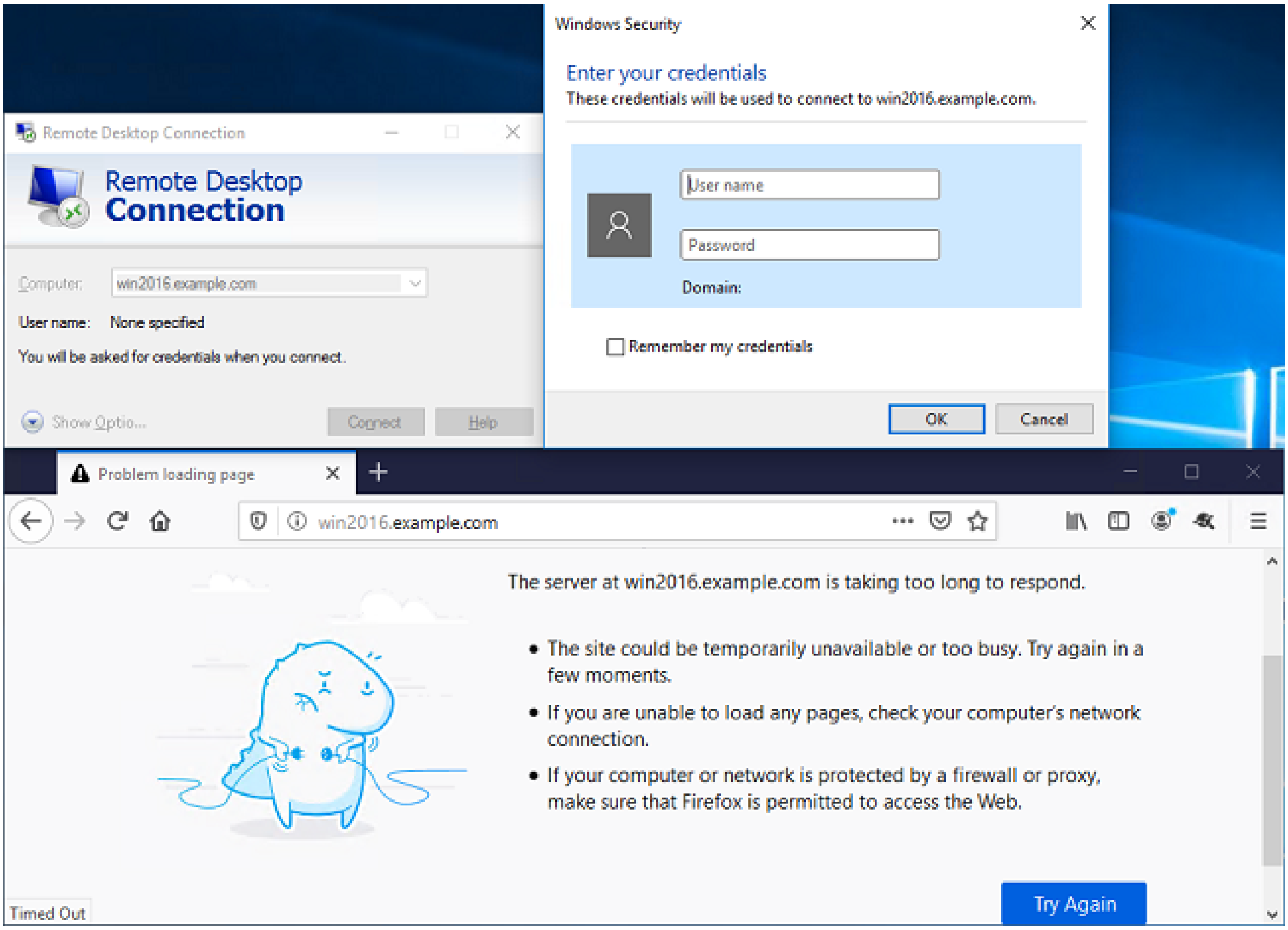
ftd2.example.com

00:00:12

IPv4

User IT Admin is in the group AnyConnect Admins which has RDP access to the Windows Server. However it does not have access to HTTP.

Opening an RDP and Firefox session to this server verifies that this user can only access the server via RDP.

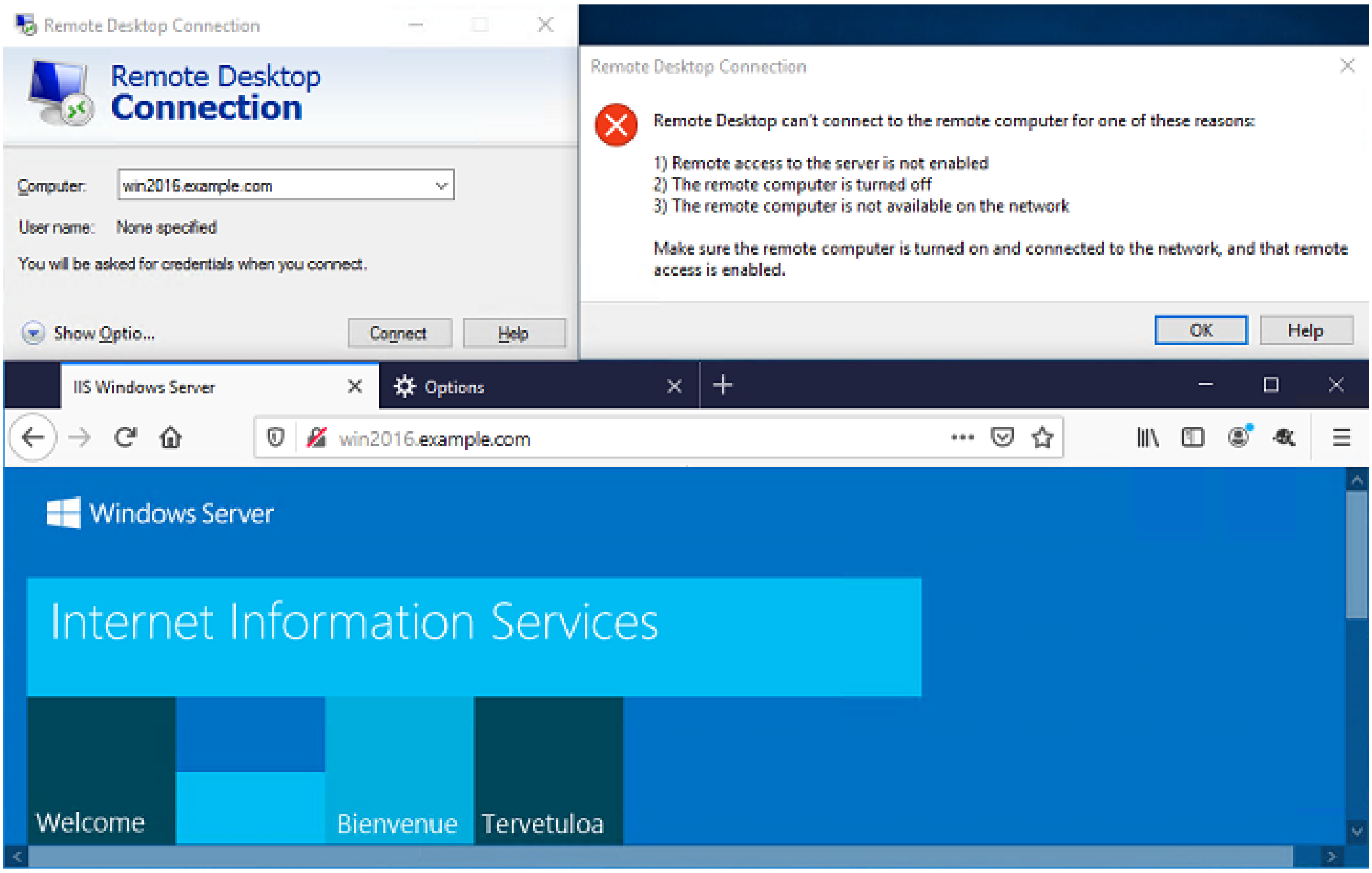


Remote Desktop Connection
Remote Desktop Connection
Computer: win2016.example.com
User name: None specified
You will be asked for credentials when you connect.
Show Optio...
Connect
Help
Windows Security
Enter your credentials
These credentials will be used to connect to win2016.example.com.
User name
Password
Domain:
Remember my credentials
OK
Cancel
Problem loading page
win2016.example.com
Try Again
Timed Out

The server at win2016.example.com is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

If logged in with user Test User who is in the group AnyConnect Users which as HTTP access but not RDP access, you are able to verify that the access control policy rules are taking effect.



Remote Desktop Connection

Computer: win2016.example.com

User name: None specified

You will be asked for credentials when you connect.

Remote Desktop Connection

Remote Desktop can't connect to the remote computer for one of these reasons:

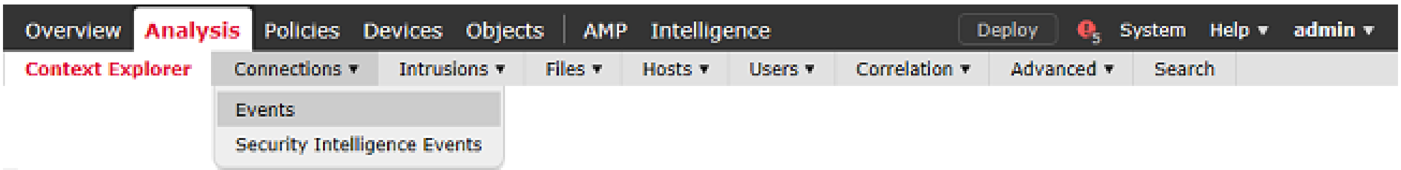
1) Remote access to the server is not enabled
2) The remote computer is turned off
3) The remote computer is not available on the network

Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.

Verify with FMC Connection Events

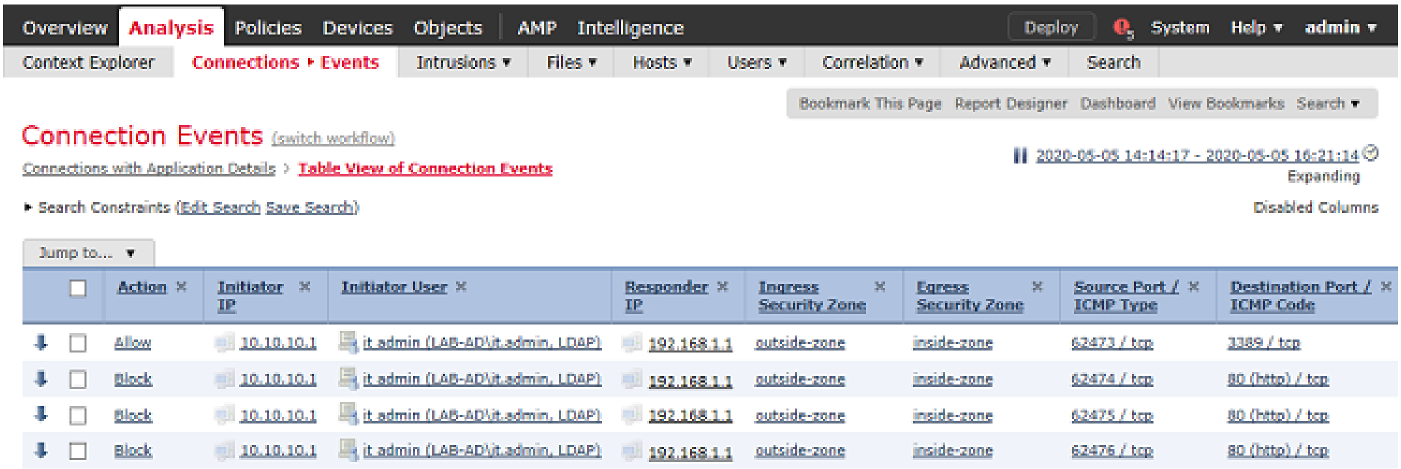
Since logging was enabled in the **Access Control Policy** rules, the connection events can be checked for any traffic that matches those rules.

Navigate to **Analysis** > **Connections** > **Events**.



Under the **Table View of Connection Events**, the logs are filtered to only show connection events for IT Admin.

Here, you can verify that RDP traffic to the server (TCP and UDP 3389) is allowed, however, port 80 traffic is blocked.



Connection Events (switch workflow)

Connections with Application Details › Table View of Connection Events

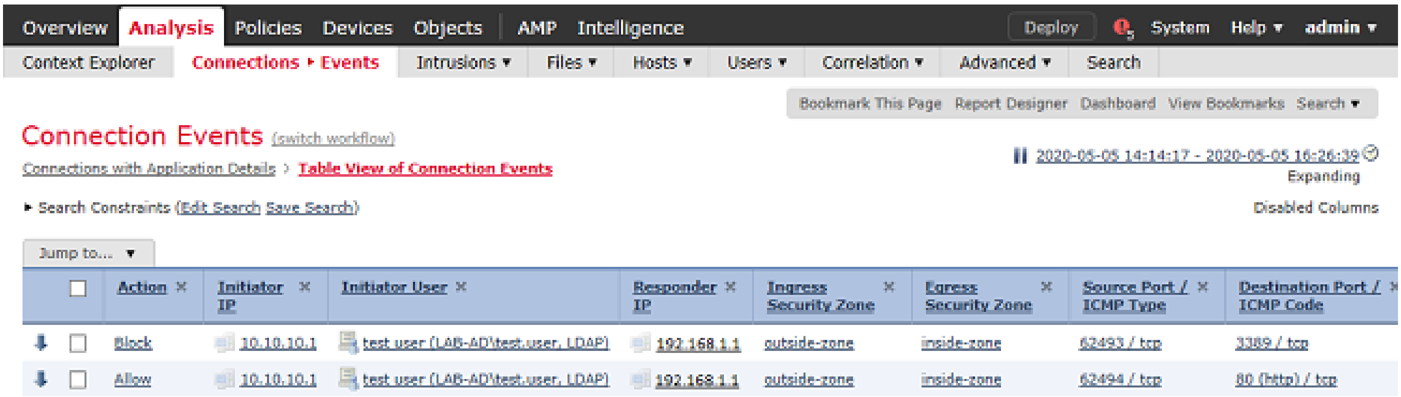
2020-05-05 14:14:17 - 2020-05-05 16:21:14
Expanding

▸ Search Constraints (Edit Search Save Search)

Disabled Columns

	□	Action	Initiator IP	Initiator User	Responder IP	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
⬇	□	Allow	10.10.10.1	it admin (LAB-AD\it.admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62473 / tcp	3389 / tcp
⬇	□	Block	10.10.10.1	it admin (LAB-AD\it.admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62474 / tcp	80 (http) / tcp
⬇	□	Block	10.10.10.1	it admin (LAB-AD\it.admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62475 / tcp	80 (http) / tcp
⬇	□	Block	10.10.10.1	it admin (LAB-AD\it.admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62476 / tcp	80 (http) / tcp

For user **Test User**, you can verify that RDP traffic to the server is blocked and port 80 traffic is allowed.



Connection Events (switch workflow)

Connections with Application Details › Table View of Connection Events

2020-05-05 14:14:17 - 2020-05-05 16:26:39
Expanding

▸ Search Constraints (Edit Search Save Search)

Disabled Columns

	□	Action	Initiator IP	Initiator User	Responder IP	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
⬇	□	Block	10.10.10.1	test user (LAB-AD\test.user, LDAP)	192.168.1.1	outside-zone	inside-zone	62493 / tcp	3389 / tcp
⬇	□	Allow	10.10.10.1	test user (LAB-AD\test.user, LDAP)	192.168.1.1	outside-zone	inside-zone	62494 / tcp	80 (http) / tcp

Troubleshoot

Debugs

This debug can be run in diagnostic CLI to troubleshoot LDAP authentication-related issues: **debug ldap 255**.

To troubleshoot user identity **Access Control Policy** issues, the **system support firewall-engine-debug** can be run in clish to determine why traffic is being allowed or blocked unexpectedly.

Working LDAP Debugs

```
[53] Session Start
[53] New request Session, context 0x00002b1d13f4bbf0, reqType = Authentication
[53] Fiber started
[53] Creating LDAP context with uri=ldap://192.168.1.1:389
[53] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] LDAP server 192.168.1.1 is Active directory
[53] Binding as ftd.admin@example.com
[53] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[53] LDAP Search:
        Base DN = [DC=example,DC=com]
        Filter  = [sAMAccountName=it.admin]
        Scope   = [SUBTREE]
```

```
[53] User DN = [CN=IT Admin,CN=Users,DC=example,DC=com]
[53] Talking to Active Directory server 192.168.1.1
[53] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[53] Read bad password count 6
[53] Binding as it.admin
[53] Performing Simple authentication for it.admin to 192.168.1.1
[53] Processing LDAP response for user it.admin
[53] Message (it.admin):
[53] Authentication successful for it.admin to 192.168.1.1
[53] Retrieved User Attributes:
[53]    objectClass: value = top
[53]    objectClass: value = person
[53]    objectClass: value = organizationalPerson
[53]    objectClass: value = user
[53]    cn: value = IT Admin
[53]    sn: value = Admin
[53]    givenName: value = IT
[53]    distinguishedName: value = CN=IT Admin,CN=Users,DC=example,DC=com
[53]    instanceType: value = 4
[53]    whenCreated: value = 20200421025811.0Z
[53]    whenChanged: value = 20200421204622.0Z
[53]    displayName: value = IT Admin
[53]    uSNCreated: value = 25896
[53]    memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
[53]    uSNChanged: value = 26119
[53]    name: value = IT Admin
[53]    objectGUID: value = &...J..O..2w...c
[53]    userAccountControl: value = 512
[53]    badPwdCount: value = 6
[53]    codePage: value = 0
[53]    countryCode: value = 0
[53]    badPasswordTime: value = 132320354378176394
[53]    lastLogoff: value = 0
[53]    lastLogon: value = 0
[53]    pwdLastSet: value = 132319114917186142
[53]    primaryGroupID: value = 513
[53]    objectSid: value = ............{I...;.....j...
[53]    accountExpires: value = 9223372036854775807
[53]    logonCount: value = 0
[53]    sAMAccountName: value = it.admin
[53]    sAMAccountType: value = 805306368
[53]    userPrincipalName: value = it.admin@example.com
[53]    objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=example,DC=com
[53]    dSCorePropagationData: value = 16010101000000.0Z
[53]    lastLogonTimestamp: value = 132319755825875876
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End
```

Unable to Establish a Connection with LDAP Server

<#root>

```
[-2147483611] Session Start
[-2147483611] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483611] Fiber started
[-2147483611] Creating LDAP context with uri=ldap://171.16.1.1:389
[-2147483611]
```

Connect to LDAP server: ldap://172.16.1.1:389, status = Failed

```
[-2147483611] Unable to read rootDSE. Can't contact LDAP server.
[-2147483611] Fiber exit Tx=0 bytes Rx=0 bytes, status=-2
[-2147483611] Session End
```

Potential Solutions:

- Check routing and ensure the FTD is receiving a response from the LDAP server.
- If LDAPS or STARTTLS is used, make sure that the correct root CA certificate is trusted so that the SSL handshake can complete successfully.
- Verify that the correct IP address and port are used. If a hostname is used, verify that DNS is able to resolve it to the correct IP address.

Binding Log in DN and/or Password Incorrect

<#root>

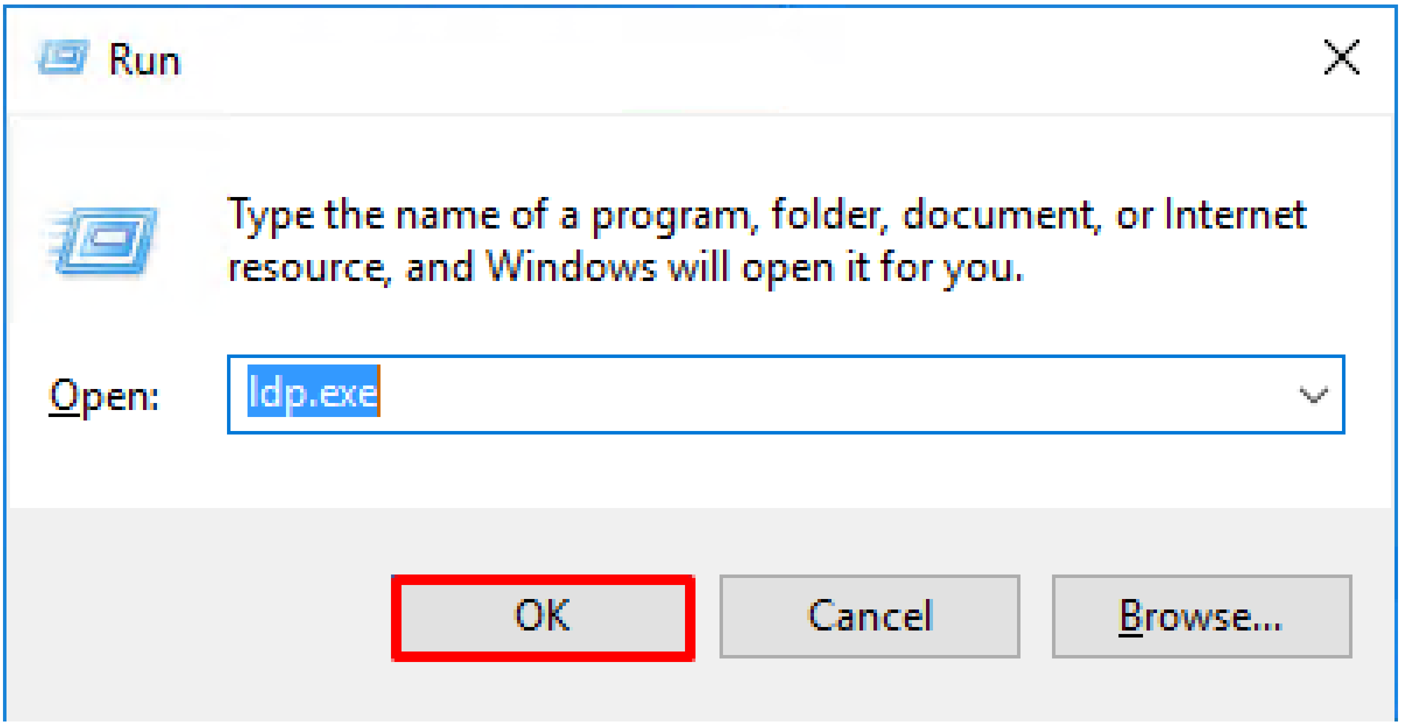
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] defaultNamingContext: value = DC=example,DC=com
[-2147483615] supportedLDAPVersion: value = 3
[-2147483615] supportedLDAPVersion: value = 2
[-2147483615] LDAP server 192.168.1.1 is Active directory
[-2147483615] supportedSASLMechanisms: value = GSSAPI
[-2147483615] supportedSASLMechanisms: value = GSS-SPNEGO
[-2147483615] supportedSASLMechanisms: value = EXTERNAL
[-2147483615] supportedSASLMechanisms: value = DIGEST-MD5
[-2147483615] Binding as ftd.admin@example.com
[-2147483615] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483615] Simple authentication for ftd.admin@example.com returned code (49) Invalid credentials
[-2147483615]
```

Failed to bind as administrator returned code (-1) Can't contact LDAP server

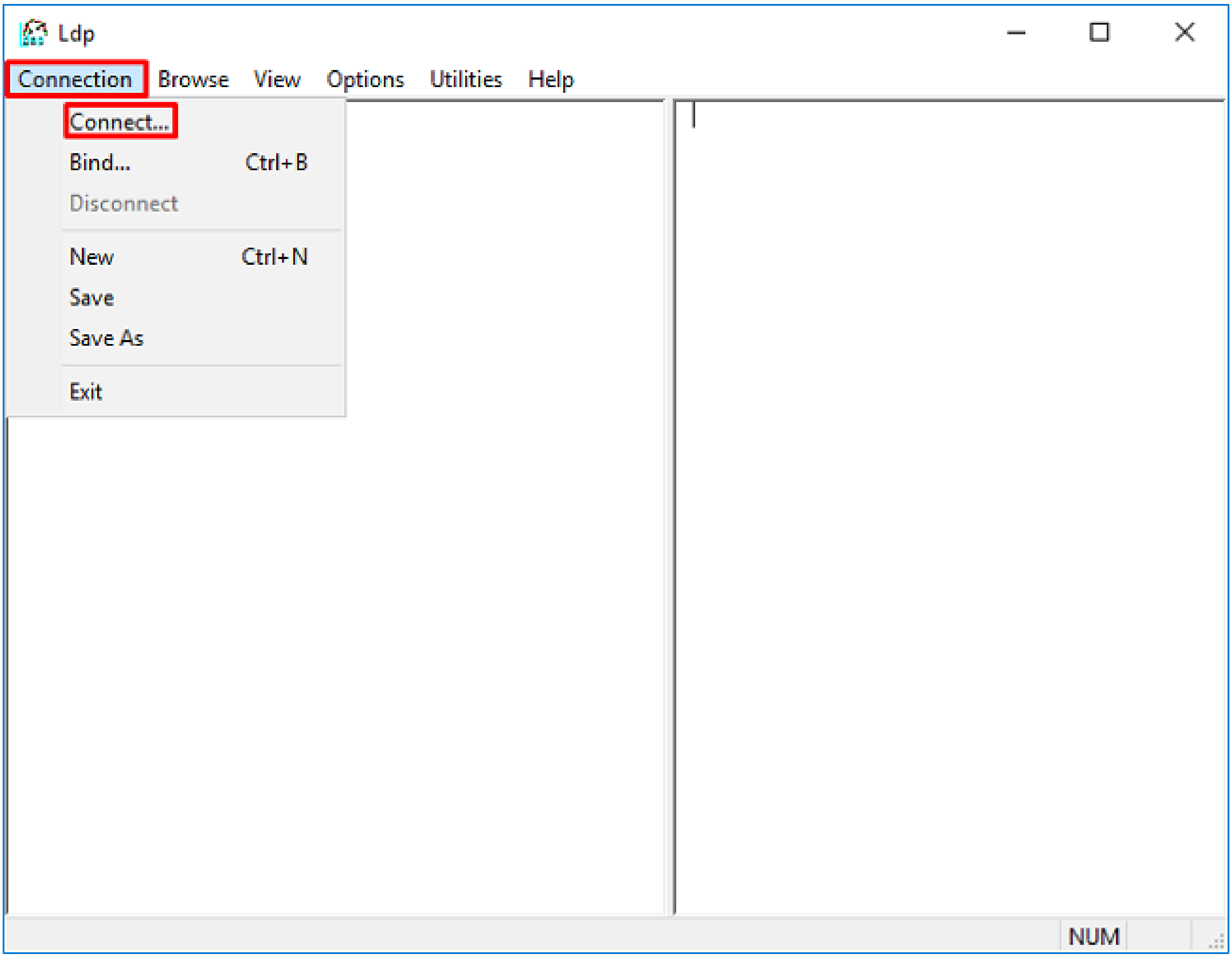
```
[-2147483615] Fiber exit Tx=186 bytes Rx=744 bytes, status=-2
[-2147483615] Session End
```

Potential Solution: Verify that the **Log in DN** and **Log in** password are configured appropriately. This can be verified on the AD server with **ldp.exe**. In order to verify that an account can successfully bind using ldp, go through these steps:

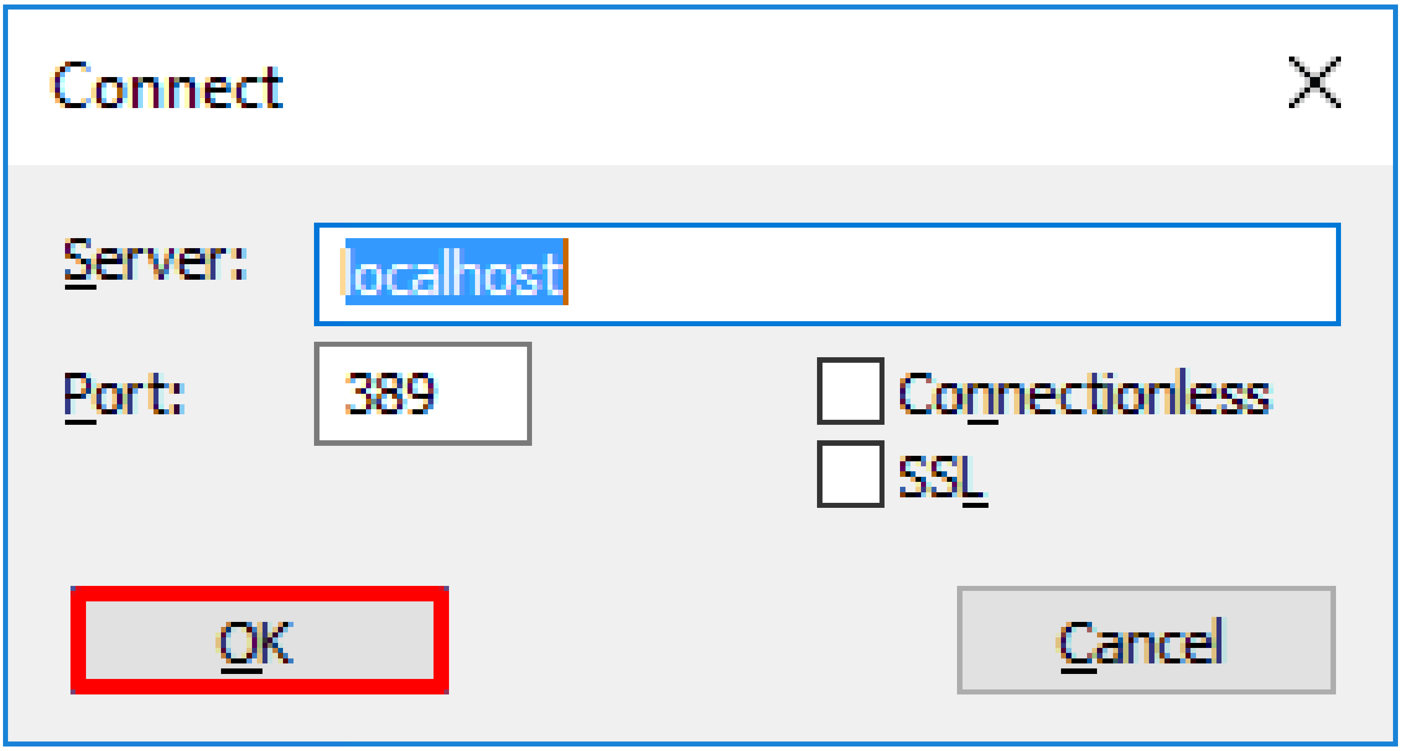
1. On the AD server, press **Win+R** and search for **ldp.exe**


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
ldp.exe
OK
Cancel
Browse...

2. Under **Connection**, select **Connect**.



3. Specify **localhost** for server and the appropriate port then click **OK**.



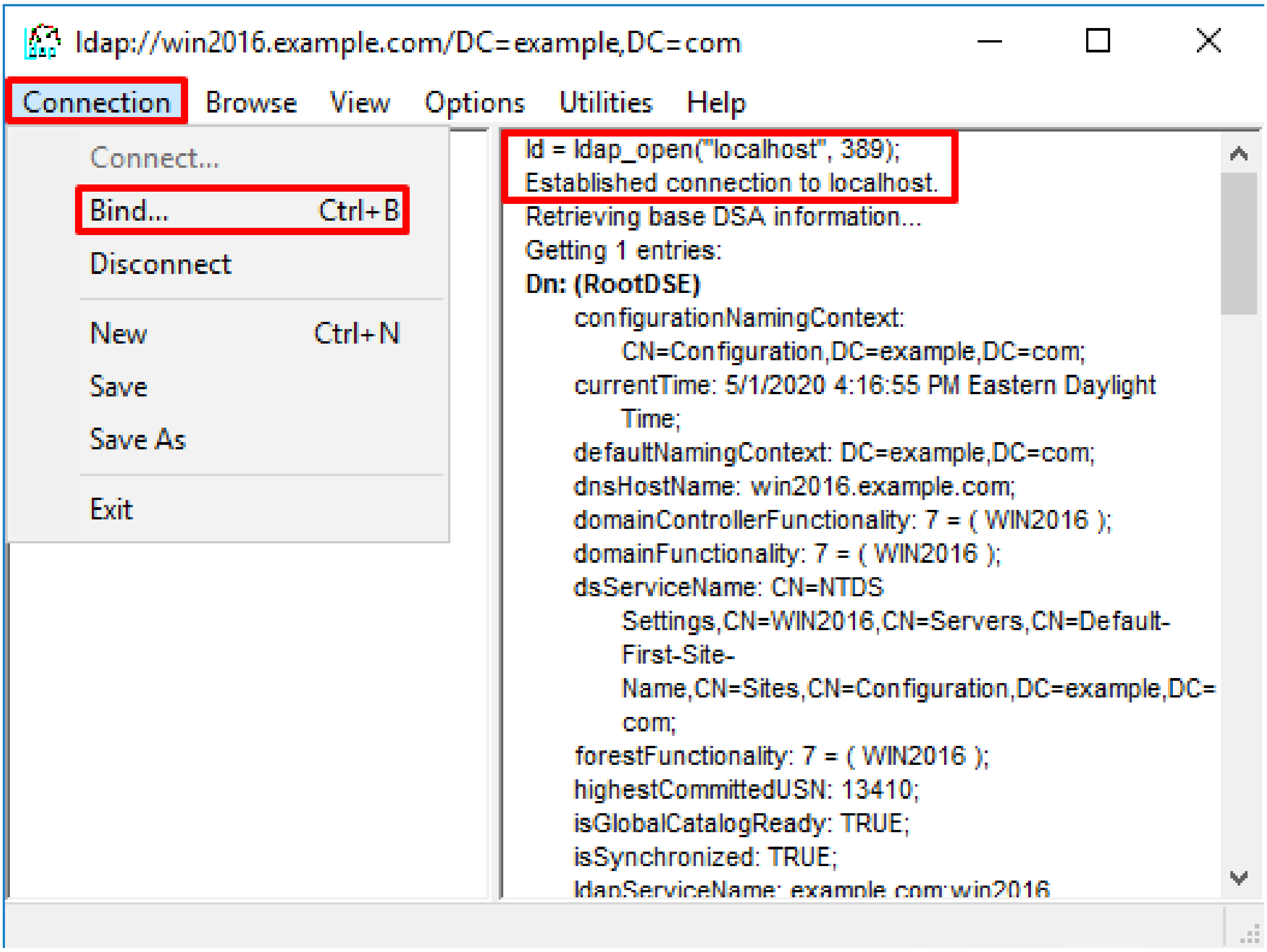
Server: localhost

Port: 389

☐ Connectionless

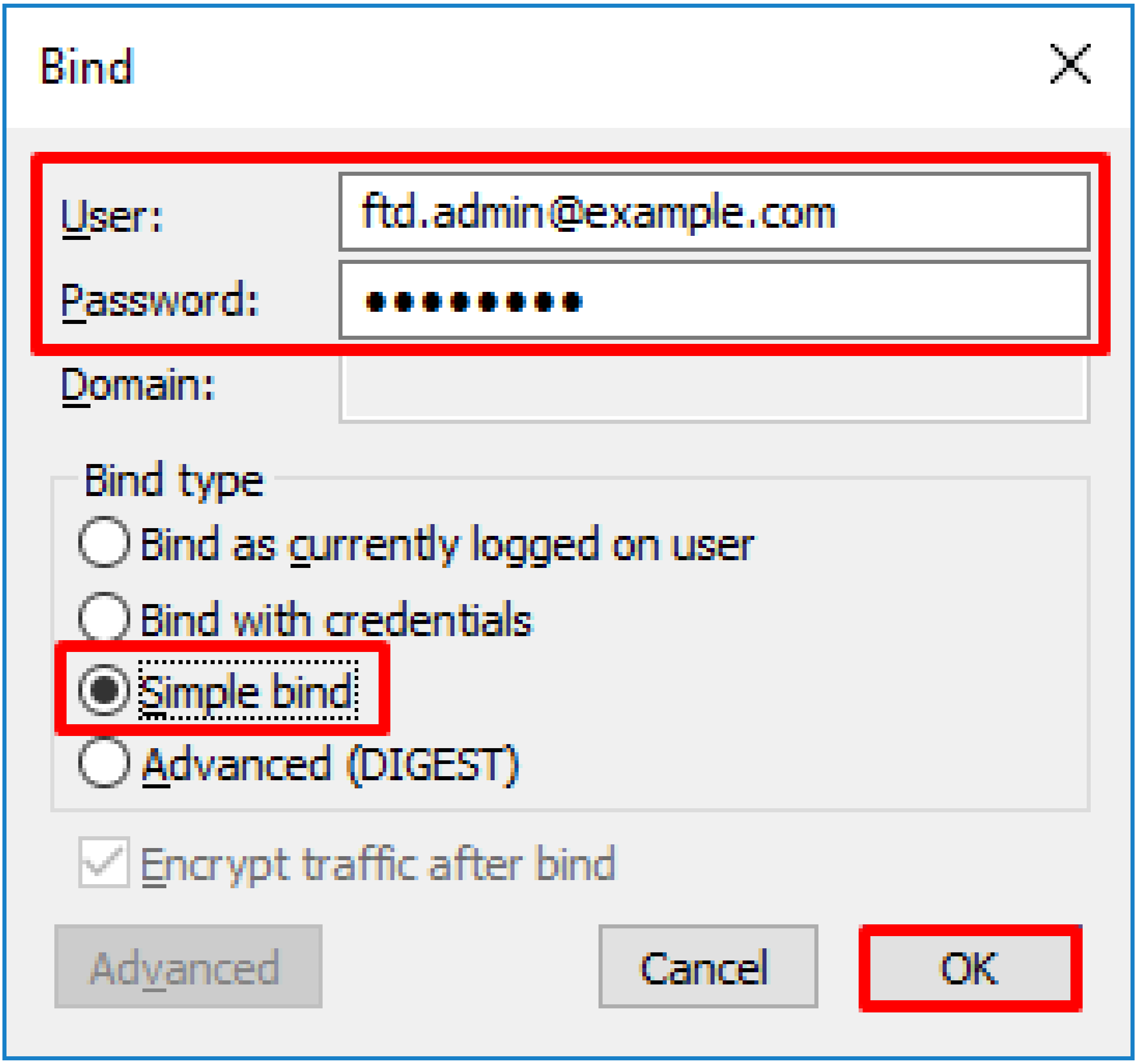
☐ SSL

4. The right column shows text indicating a successful connection. Navigate to **Connection** > **Bind**.



```
ld = ldap_open("localhost", 389);
Established connection to localhost.
Retrieving base DSA information...
Getting 1 entries:
Dn: (RootDSE)
	configurationNamingContext:
		CN=Configuration,DC=example,DC=com;
	currentTime: 5/1/2020 4:16:55 PM Eastern Daylight
		Time;
	defaultNamingContext: DC=example,DC=com;
	dnsHostName: win2016.example.com;
	domainControllerFunctionality: 7 = ( WIN2016 );
	domainFunctionality: 7 = ( WIN2016 );
	dsServiceName: CN=NTDS
		Settings,CN=WIN2016,CN=Servers,CN=Default-
		First-Site-
		Name,CN=Sites,CN=Configuration,DC=example,DC=
		com;
	forestFunctionality: 7 = ( WIN2016 );
	highestCommittedUSN: 13410;
	isGlobalCatalogReady: TRUE;
	isSynchronized: TRUE;
	ldapServiceName: example.com:win2016
```

5. Select **Simple Bind** then specify the **Directory Account User** and **Password**. Click **OK**.



User: ftd.admin@example.com

Password: ●●●●●●●●●

Domain:

Bind type

○ Bind as currently logged on user

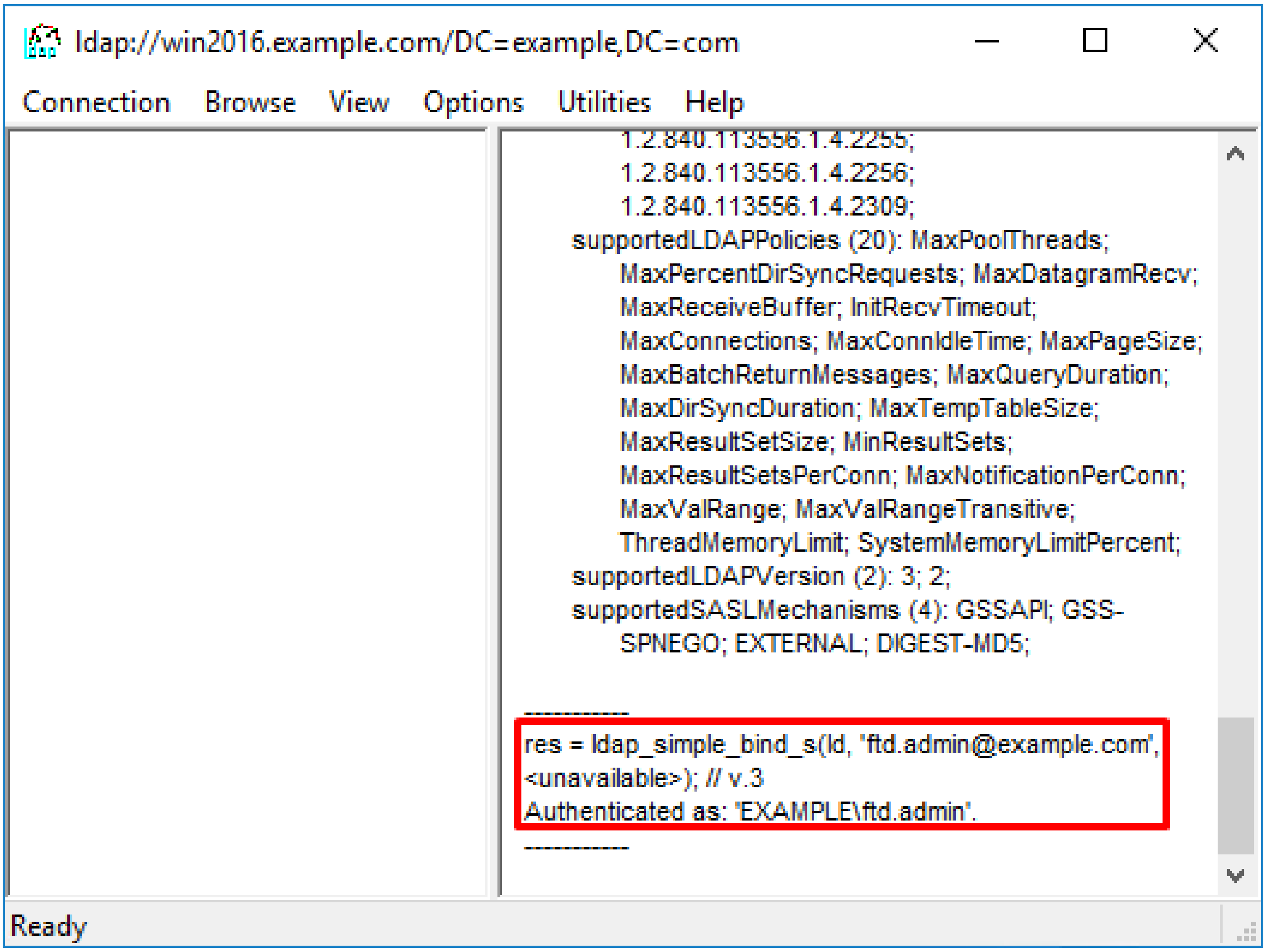
○ Bind with credentials

● Simple bind

○ Advanced (DIGEST)

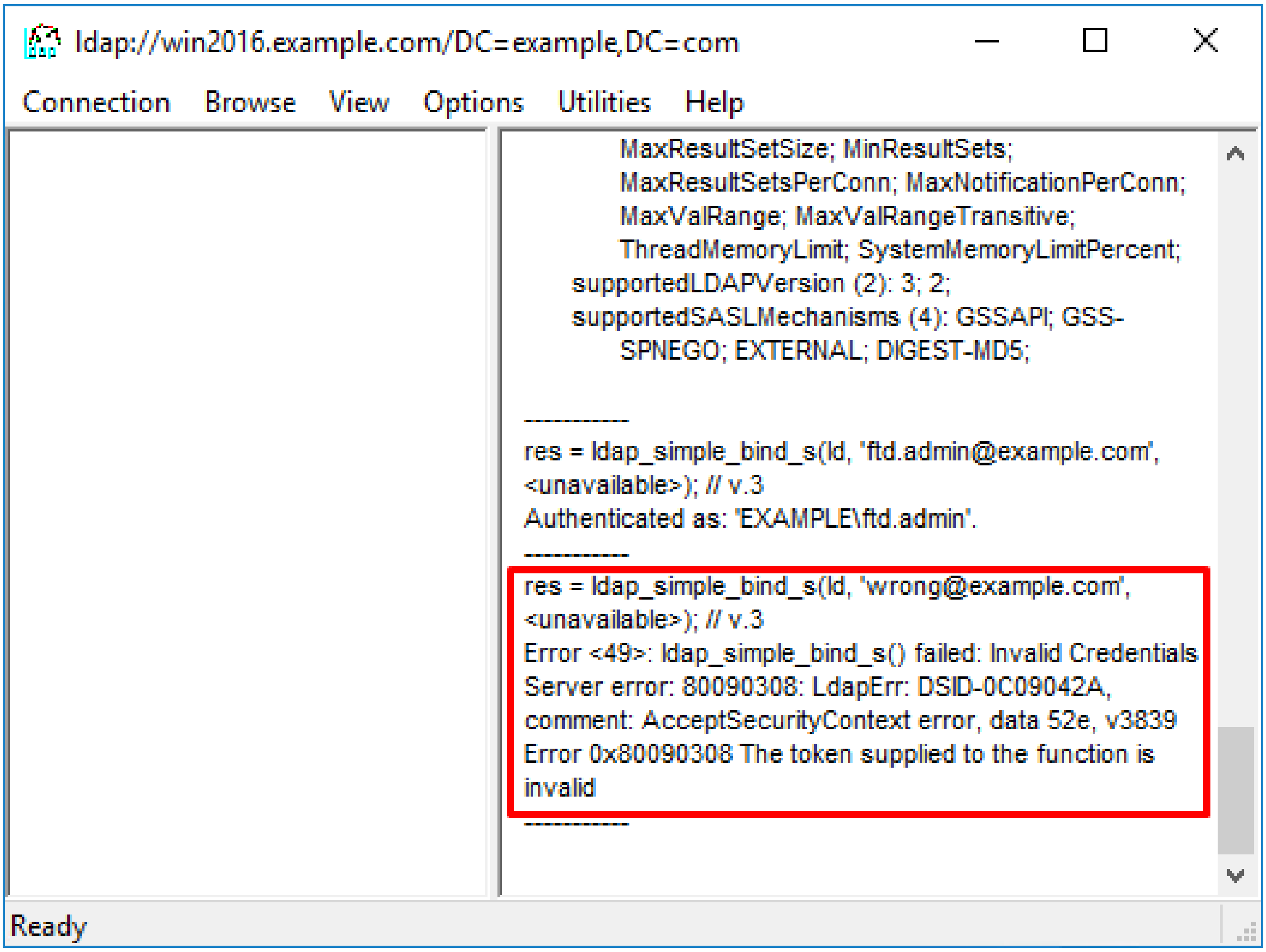
☑ Encrypt traffic after bind

With a successful bind, ldp shows Authenticated as: **DOMAIN\username**



```
            1.2.840.113556.1.4.2255;
            1.2.840.113556.1.4.2256;
            1.2.840.113556.1.4.2309;
        supportedLDAPPolicies (20): MaxPoolThreads;
            MaxPercentDirSyncRequests; MaxDatagramRecv;
            MaxReceiveBuffer; InitRecvTimeout;
            MaxConnections; MaxConnIdleTime; MaxPageSize;
            MaxBatchReturnMessages; MaxQueryDuration;
            MaxDirSyncDuration; MaxTempTableSize;
            MaxResultSetSize; MinResultSets;
            MaxResultSetsPerConn; MaxNotificationPerConn;
            MaxValRange; MaxValRangeTransitive;
            ThreadMemoryLimit; SystemMemoryLimitPercent;
        supportedLDAPVersion (2): 3; 2;
        supportedSASLMechanisms (4): GSSAPI; GSS-
            SPNEGO; EXTERNAL; DIGEST-MD5;

-----------
res = ldap_simple_bind_s(ld, 'ftd.admin@example.com',
<unavailable>); // v.3
Authenticated as: 'EXAMPLE\ftd.admin'.
-----------
```

An attempt to bind with an invalid username or password results in a failure such as the two seen here.


ldap://win2016.example.com/DC=example,DC=com
Connection Browse View Options Utilities Help
Ready

```
        MaxResultSetSize; MinResultSets;
        MaxResultSetsPerConn; MaxNotificationPerConn;
        MaxValRange; MaxValRangeTransitive;
        ThreadMemoryLimit; SystemMemoryLimitPercent;
    supportedLDAPVersion (2): 3; 2;
    supportedSASLMechanisms (4): GSSAPI; GSS-
        SPNEGO; EXTERNAL; DIGEST-MD5;

-----------
res = ldap_simple_bind_s(ld, 'ftd.admin@example.com',
<unavailable>); // v.3
Authenticated as: 'EXAMPLE\ftd.admin'.
-----------
res = ldap_simple_bind_s(ld, 'wrong@example.com',
<unavailable>); // v.3
Error <49>: ldap_simple_bind_s() failed: Invalid Credentials
Server error: 80090308: LdapErr: DSID-0C09042A,
comment: AcceptSecurityContext error, data 52e, v3839
Error 0x80090308 The token supplied to the function is
invalid
-----------
```

LDAP Server Unable to Find the Username

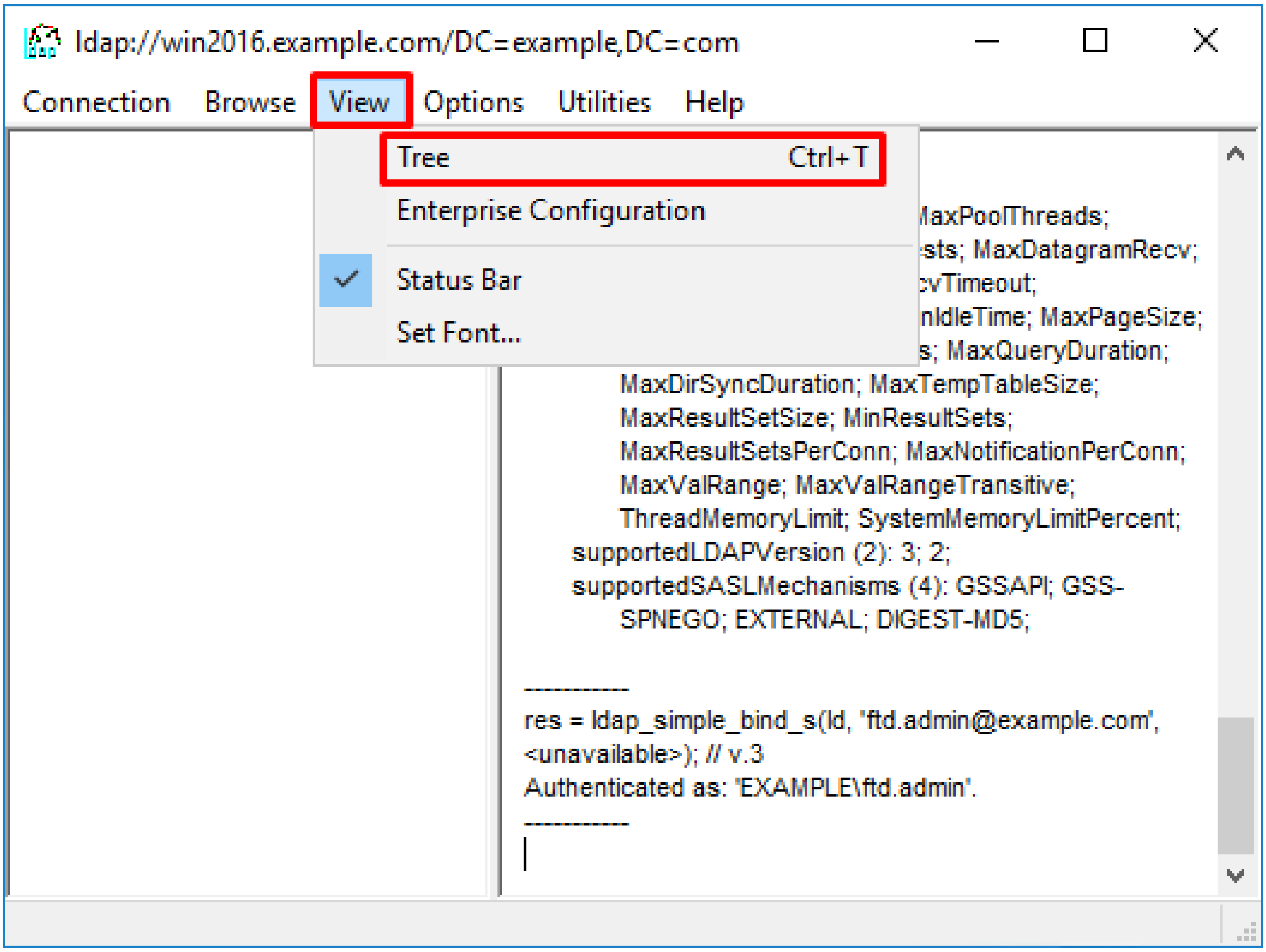
<#root>

```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] supportedLDAPVersion: value = 3
[-2147483612] supportedLDAPVersion: value = 2
[-2147483612] LDAP server 192.168.1.1 is Active directory
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] LDAP Search:
        Base DN = [dc=example,dc=com]
        Filter  = [samaccountname=it.admi]
        Scope   = [SUBTREE]
[-2147483612]

Search result parsing returned failure status

[-2147483612] Talking to Active Directory server 192.168.1.1
[-2147483612] Reading password policy for it.admi, dn:
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] Fiber exit Tx=456 bytes Rx=1082 bytes, status=-1
```

```
[-2147483612] Session End
```

Potential Solution: Verify that AD can find the user with the search done by the FTD. This can be done with **ldp.exe** as well.

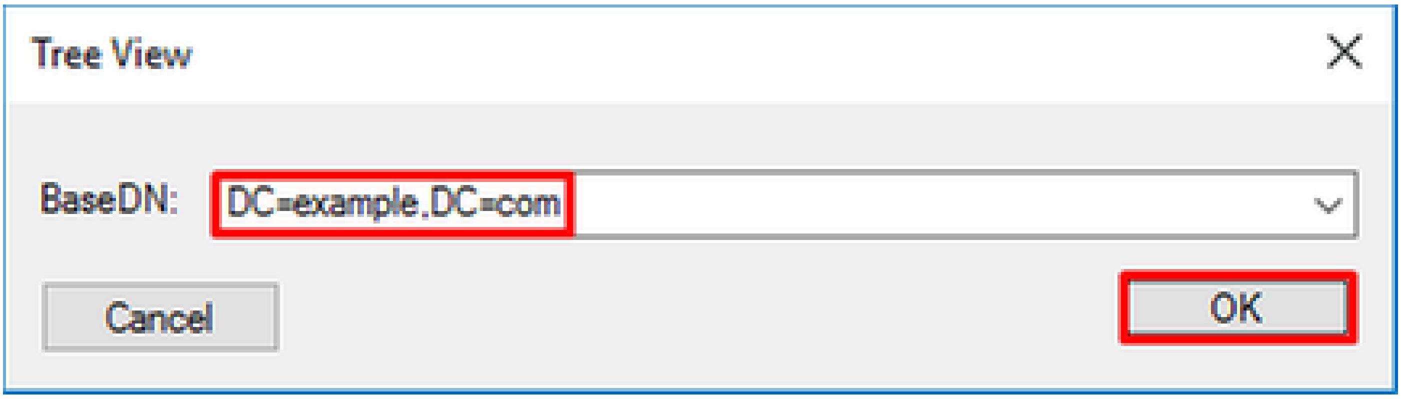
1. After successfully binding as seen above, navigate to **View** > **Tree**.



ldap://win2016.example.com/DC=example,DC=com

```
MaxPoolThreads;
sts; MaxDatagramRecv;
cvTimeout;
nIdleTime; MaxPageSize;
s; MaxQueryDuration;
      MaxDirSyncDuration; MaxTempTableSize;
      MaxResultSetSize; MinResultSets;
      MaxResultSetsPerConn; MaxNotificationPerConn;
      MaxValRange; MaxValRangeTransitive;
      ThreadMemoryLimit; SystemMemoryLimitPercent;
   supportedLDAPVersion (2): 3; 2;
   supportedSASLMechanisms (4): GSSAPI; GSS-
      SPNEGO; EXTERNAL; DIGEST-MD5;

-----------
res = ldap_simple_bind_s(ld, 'ftd.admin@example.com',
<unavailable>); // v.3
Authenticated as: 'EXAMPLE\ftd.admin'.
-----------
```

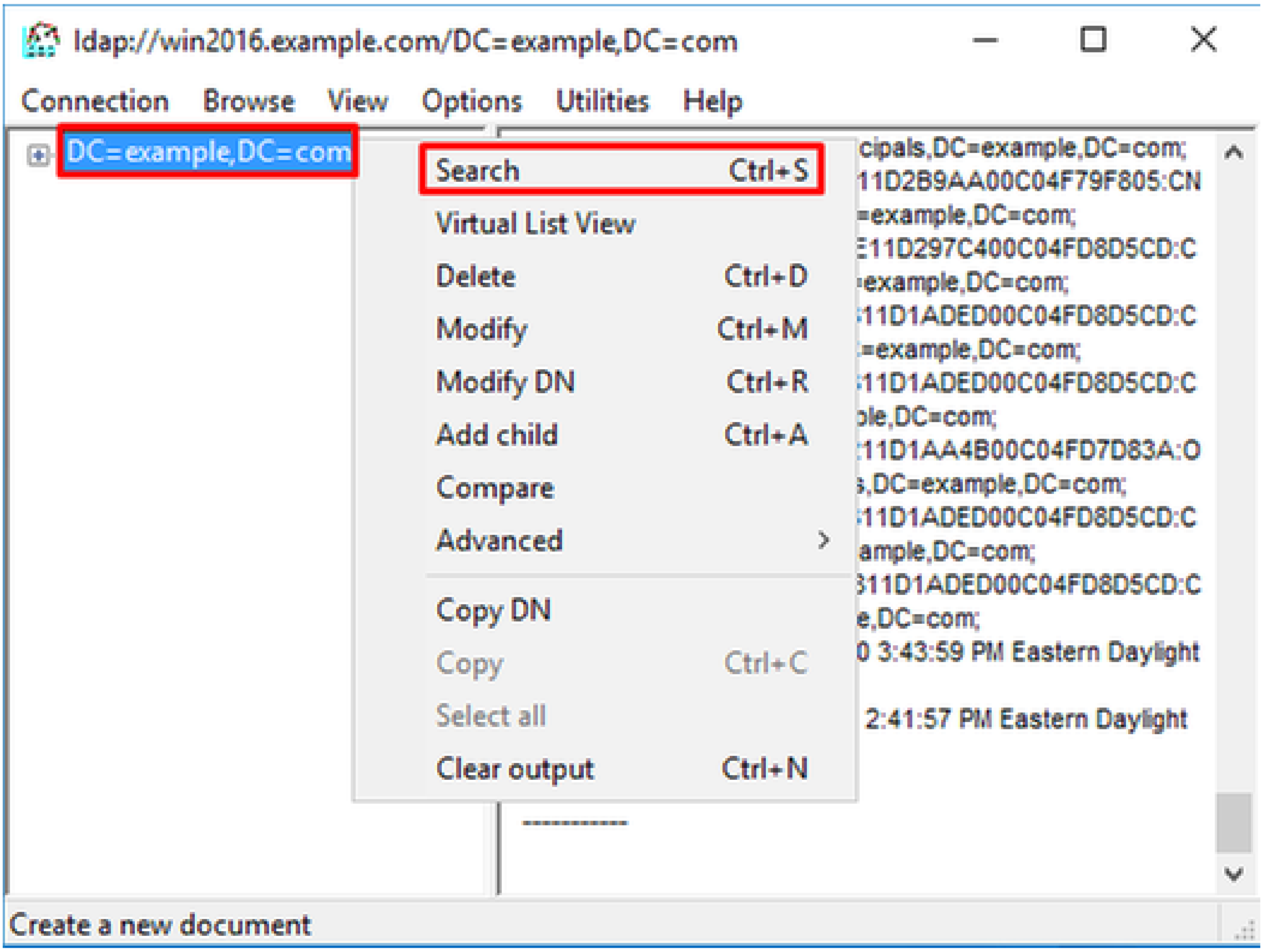
2. Specify the **Base DN** configured on the FTD then click **OK**



Tree View

BaseDN: DC=example,DC=com

3. Right-click the Base DN then click **Search**.

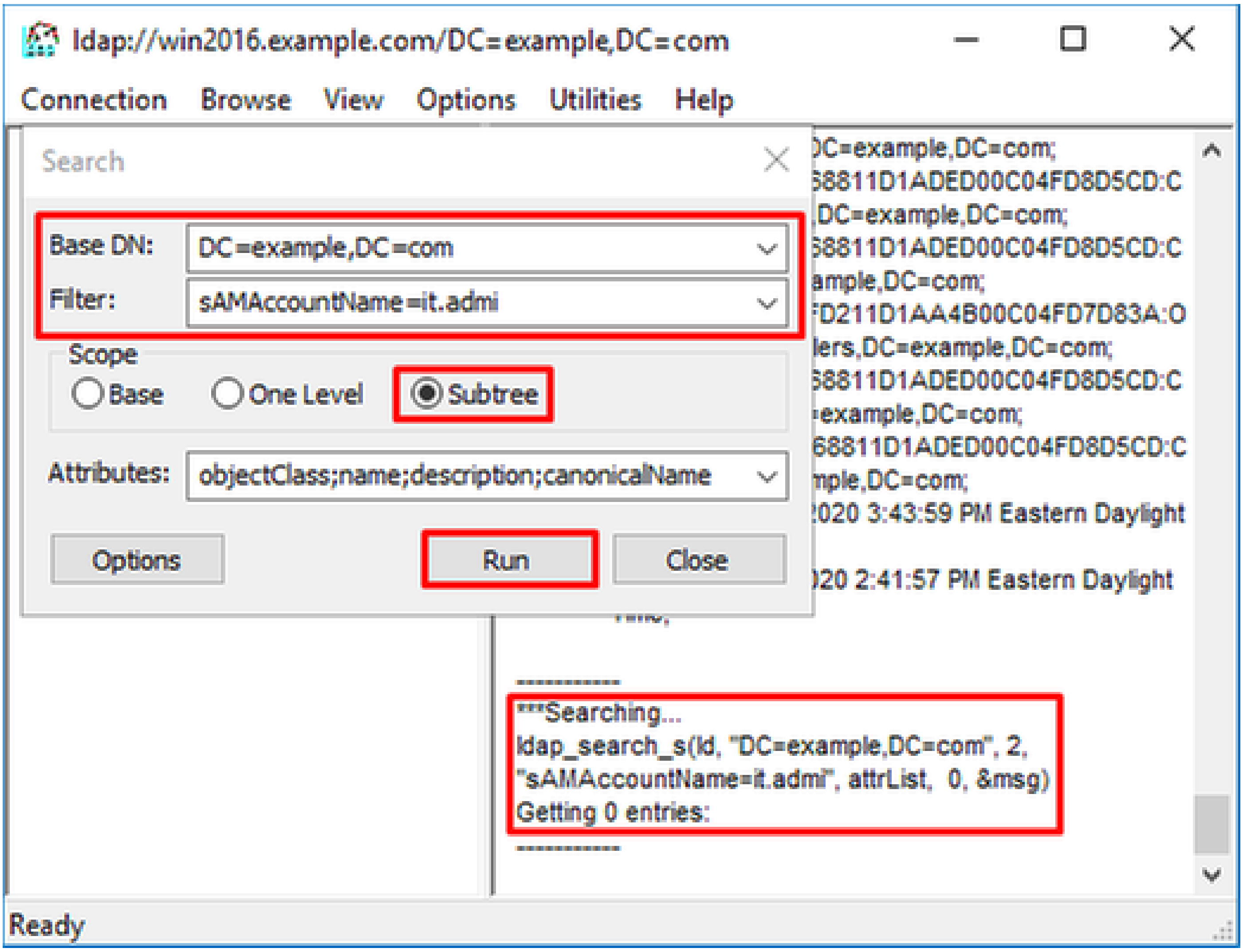


```
cipals,DC=example,DC=com;
11D2B9AA00C04F79F805:CN
=example,DC=com;
E11D297C400C04FD8D5CD:C
example,DC=com;
11D1ADED00C04FD8D5CD:C
=example,DC=com;
11D1ADED00C04FD8D5CD:C
ple,DC=com;
11D1AA4B00C04FD7D83A:O
,DC=example,DC=com;
11D1ADED00C04FD8D5CD:C
ample,DC=com;
311D1ADED00C04FD8D5CD:C
e,DC=com;
0 3:43:59 PM Eastern Daylight

 2:41:57 PM Eastern Daylight
-----------
```

4. Specify the same **Base DN**, **Filter**, and **Scope** values as seen in the debugs.

In this example, these are:

- Base DN: dc=example,dc=com
- Filter: samaccountname=it.admi
- Scope:SUBTREE



Base DN: DC=example,DC=com

Filter: sAMAccountName=it.admi

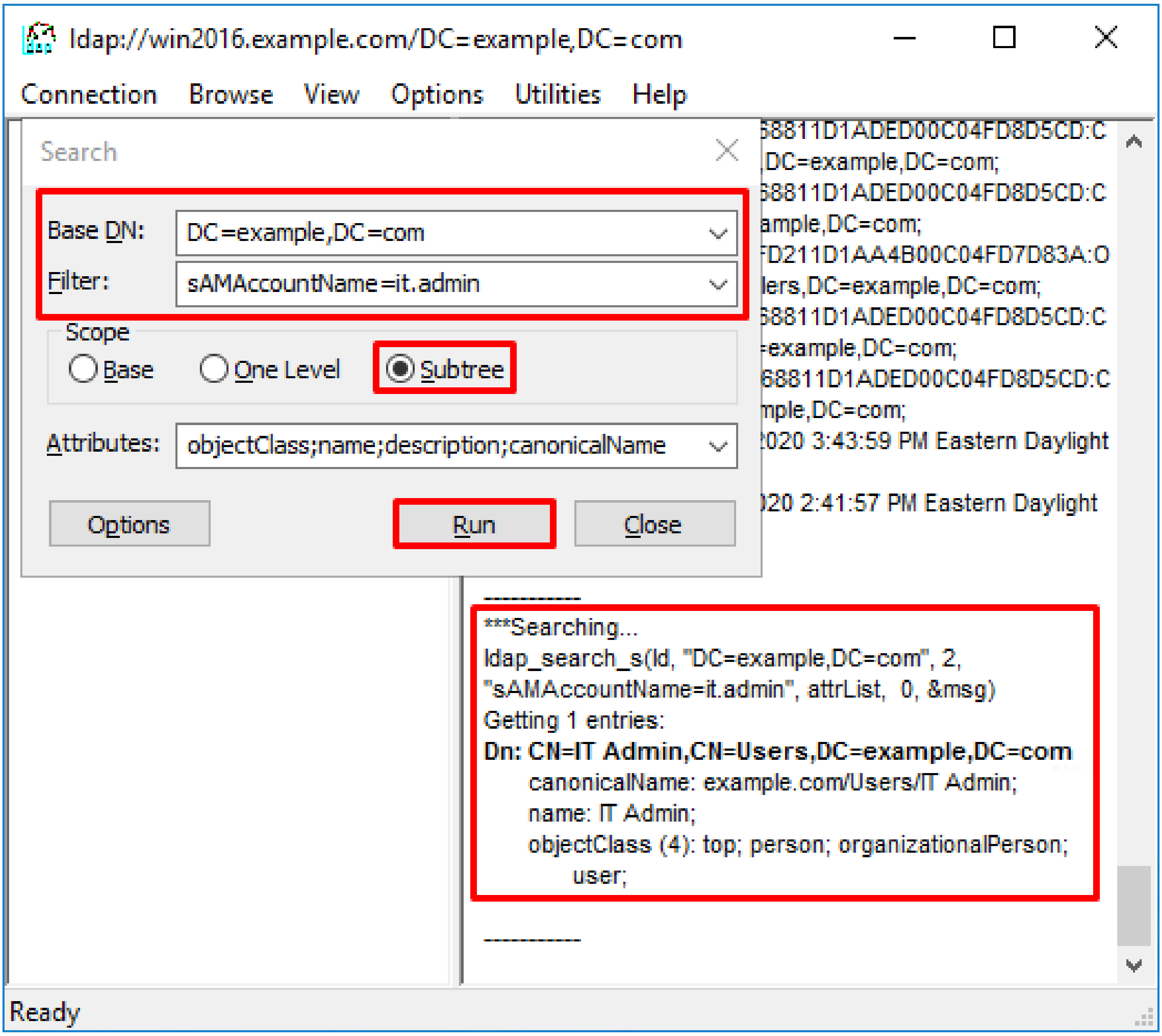
Scope: ○ Base ○ One Level ● Subtree

Attributes: objectClass;name;description;canonicalName

```
)C=example,DC=com;
68811D1ADED00C04FD8D5CD:C
,DC=example,DC=com;
68811D1ADED00C04FD8D5CD:C
ample,DC=com;
FD211D1AA4B00C04FD7D83A:O
lers,DC=example,DC=com;
68811D1ADED00C04FD8D5CD:C
example,DC=com;
68811D1ADED00C04FD8D5CD:C
mple,DC=com;
020 3:43:59 PM Eastern Daylight

020 2:41:57 PM Eastern Daylight
Time;

-----------
***Searching...
ldap_search_s(ld, "DC=example,DC=com", 2, "sAMAccountName=it.admi", attrList,  0, &msg)
Getting 0 entries:
-----------
```

ldp finds 0 entries because there is no user account with the **sAMAccountname it.admi** under the Base DN dc=example,dc=com.

Another attempt with the correct **sAMAccountname it.admin** shows a different result. ldp finds 1 entry under the Base DN dc=example,dc=com and prints that user DN.



Base DN: DC=example,DC=com

Filter: sAMAccountName=it.admin

Scope: ○ Base ○ One Level ● Subtree

Attributes: objectClass;name;description;canonicalName

```
58811D1ADED00C04FD8D5CD:C
,DC=example,DC=com;
58811D1ADED00C04FD8D5CD:C
ample,DC=com;
FD211D1AA4B00C04FD7D83A:O
lers,DC=example,DC=com;
58811D1ADED00C04FD8D5CD:C
=example,DC=com;
68811D1ADED00C04FD8D5CD:C
mple,DC=com;
2020 3:43:59 PM Eastern Daylight

020 2:41:57 PM Eastern Daylight
```

```
-----------
***Searching...
ldap_search_s(ld, "DC=example,DC=com", 2, "sAMAccountName=it.admin", attrList,  0, &msg)
Getting 1 entries:
Dn: CN=IT Admin,CN=Users,DC=example,DC=com
      canonicalName: example.com/Users/IT Admin;
      name: IT Admin;
      objectClass (4): top; person; organizationalPerson;
            user;

-----------
```

Incorrect Password for the Username

<#root>

```
[-2147483613] Session Start
[-2147483613] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483613] Fiber started
[-2147483613] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483613] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483613] supportedLDAPVersion: value = 3
[-2147483613] supportedLDAPVersion: value = 2
[-2147483613] LDAP server 192.168.1.1 is Active directory
[-2147483613] Binding as ftd.admin@example.com
[-2147483613] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483613] LDAP Search:
        Base DN = [dc=example,dc=com]
        Filter  = [samaccountname=it.admin]
        Scope   = [SUBTREE]
[-2147483613] User DN = [CN=IT Admin,CN=Users,DC=example,DC=com]
[-2147483613] Talking to Active Directory server 192.168.1.1
```

```
[-2147483613] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[-2147483613] Read bad password count 0
[-2147483613] Binding as it.admin
[-2147483613] Performing Simple authentication for it.admin to 192.168.1.1
[-2147483613]

Simple authentication for it.admin returned code (49) Invalid credentials

[-2147483613] Message (it.admin): 80090308: LdapErr: DSID-0C09042A, comment: AcceptSecurityContext erro
[-2147483613]

Invalid password for it.admin

[-2147483613] Fiber exit Tx=514 bytes Rx=2764 bytes, status=-1
[-2147483613] Session End
```

Potential Solution: Verify that the user password is configured appropriately and that it is not expired. Similar to the Log in DN, the FTD does a bind against AD with the user credentials.

This bind can also be done in ldp to verify that the AD is able to recognize the same username and password credentials. The steps in ldp are shown in the section **Binding Login DN and/or password incorrect**.

Additionally, the Microsoft server **Event Viewer** logs can be reviewed for a potential failure reason.

Test AAA

The test **aaa-server** command can be used to simulate an authentication attempt from the FTD with a specific username and password. This can be used to test for connection or authentication failures. The command is **_t_est aaa-server authentication [AAA-server] host [AD IP/hostname]**.

<#root>

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
 realm-id 7
aaa-server

LAB-AD

 host

win2016.example.com

 server-port 389
 ldap-base-dn DC=example,DC=com
 ldap-scope subtree
 ldap-login-password *****
 ldap-login-dn ftd.admin@example.com
 server-type auto-detect

> test aaa-server authentication

LAB-AD

 host

win2016.example.com

Username: it.admin
Password: ********
```

```
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful
```

Packet Captures

Packet captures can be used to verify reachability to the AD server. If LDAP packets leave the FTD, but there is no response, this could indicate a routing issue.

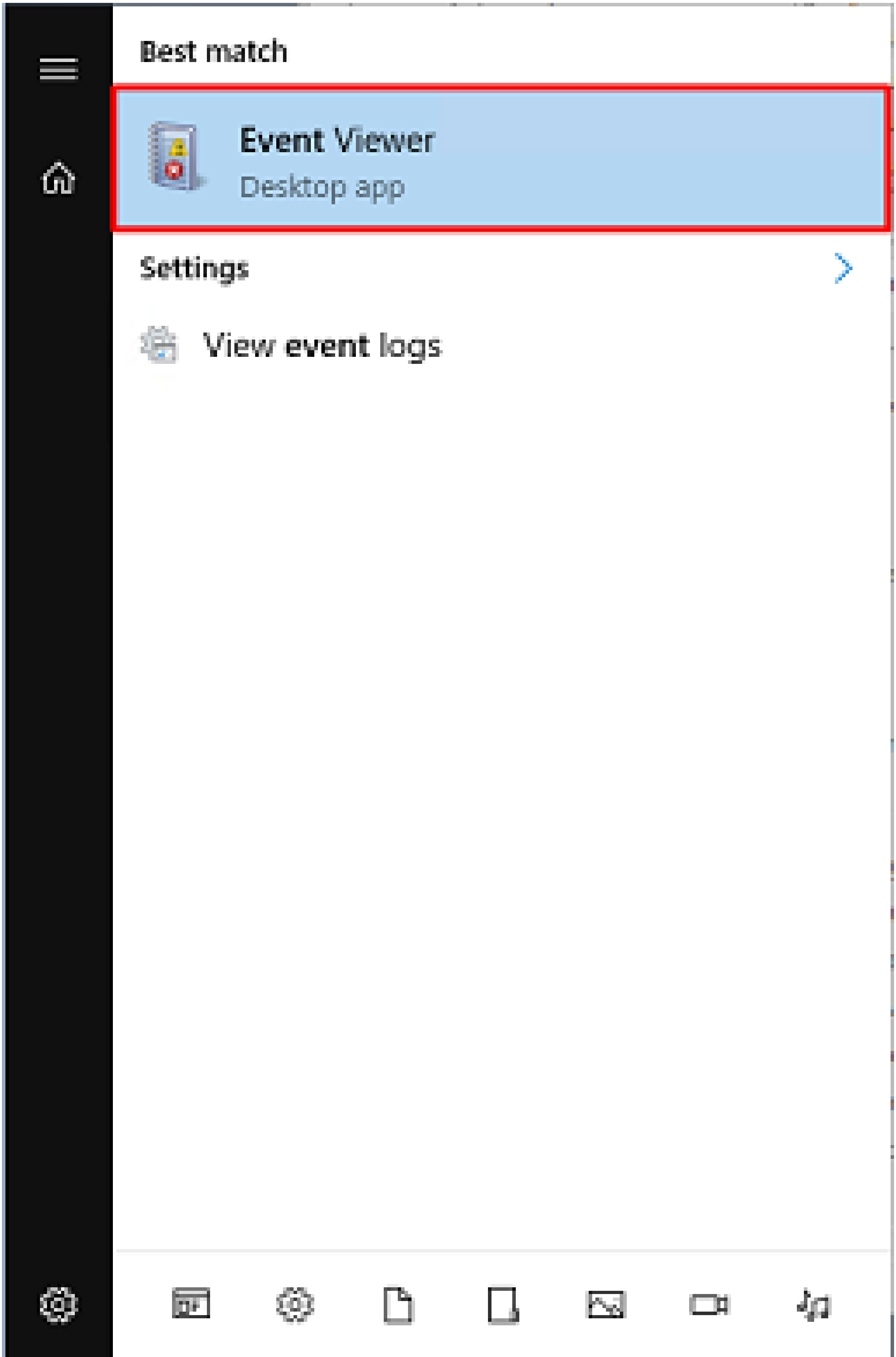
Capture shows the bidirectional LDAP traffic.

```
> show route 192.168.1.1

Routing entry for 192.168.1.0 255.255.255.0
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via inside
      Route metric is 0, traffic share count is 1

> capture AD interface inside match tcp any host 192.168.1.1 eq 389

> show capture
capture AD type raw-data interface inside [Capturing - 0 bytes]
  match tcp any host 192.168.1.1 eq ldap

> test aaa-server authentication LAB-AD host win2016.example.com username it.admin password ******
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful

> show capture
capture AD type raw-data interface inside [Capturing - 10905 bytes]
  match tcp any host 192.168.1.1 eq ldap

> show capture AD

54 packets captured

   1: 23:02:16.770712       192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win 32768
   2: 23:02:16.772009       192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack 36819128
   3: 23:02:16.772039       192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768 <nop,nop,ti
   4: 23:02:16.772482       192.168.1.17.61960 > 192.168.1.1.389: P 3681912835:3681912980(145) ack 4915
   5: 23:02:16.772924       192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack 368191
   6: 23:02:16.772955       192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768 <nop,nop,ti
   7: 23:02:16.773428       192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44) ack 49152
   8: 23:02:16.775030       192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack 3681913
   9: 23:02:16.775075       192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768 <nop,nop,ti
[...]
54 packets shown
```

Windows Server Event Viewer Logs

The **Event Viewer** logs on the AD server can provide more detailed information as to why a failure occurred.

1. Search for and open **Event Viewer**.


Best match
Event Viewer
Desktop app
Settings
View event logs