



Cisco ASA with Anyconnect VPN and Azure MFA Configuration for LDAP

Published October, 2015

Version 1.0

Azure Multi-Factor Authentication seamlessly integrates with your Cisco® ASA VPN appliance to provide additional security for Cisco AnyConnect® VPN logins and portal access. Multi-factor authentication (MFA) is combined with standard user credentials to increase security for user identity verification.

Azure supports several multi-factor authentication methods for Lightweight Directory Access Protocol (LDAP). Each method is a challenge-response mechanism that occurs after primary authentication with standard user credentials.

- Phone call – users receive a phone call with instructions on how to complete login.
- Text message – users receive an SMS message that contains a verification code. Azure supports two-way messaging for LDAP; users are required to send a verification code by text message reply.
- Mobile app – users receive a push notification from client software installed on a smart device, like a phone or tablet. The Azure Authenticator app is available for Windows Phone, iOS, and Android.

This guide will help you to configure Azure Multi-Factor Authentication (MFA) server and Cisco ASA to use LDAP for AnyConnect VPN authentication.

Overview

The Azure Multi-Factor Authentication server acts as an LDAP server. The Cisco ASA appliance acts as an LDAP client. The LDAP server works as a proxy to forward requests that use multiple authentication factors to a target directory service. The proxy receives a response from the directory, which it sends to the LDAP client. Access is granted only when both the user credentials (primary authentication) and the MFA challenge succeed. See the diagram in Figure 1 for reference.

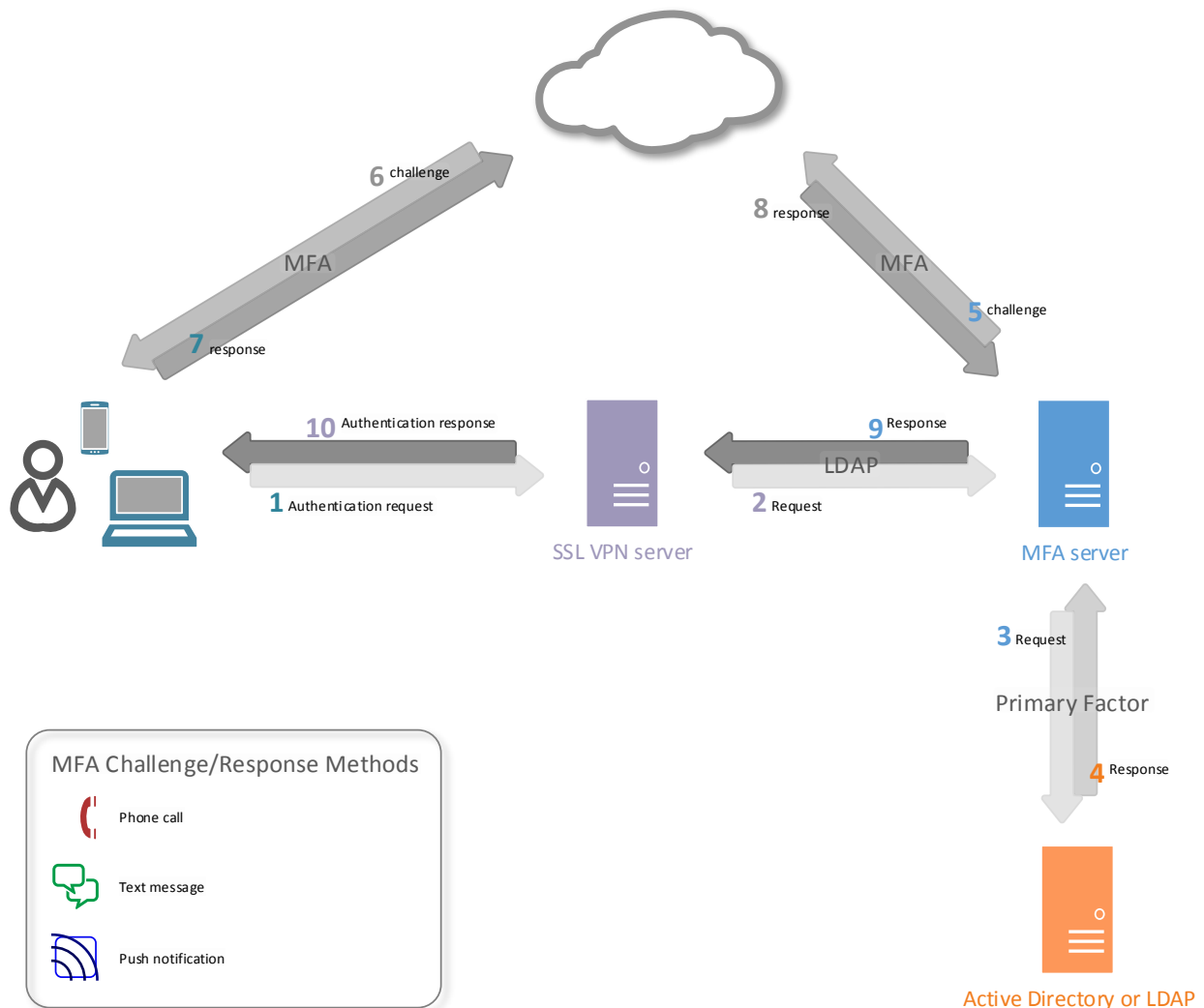


Figure 1

The diagram above represents the logical process flow for MFA. The user experience for MFA is fairly similar to traditional login. See Figure 2 for a description of the workflow.



Figure 2

Guide Usage

The information in this guide explains the configuration common to most deployments. It is important to note two things:

- Every organization is different and may require additional or different configuration.
- Some configuration may have other methods to accomplish the same task than those described.

Information is based on the conditions described in the [Prerequisites](#) and [Components](#) sections. The [Conventions](#) section provides usage information and details about the environment used for this guide.

Prerequisites

The following conditions are required to set up Azure MFA:

- An MFA server installed on a system with either:
 - Windows Server 2003 or higher.
 - Windows Vista or higher, that has Users Portal and Web Service SDK services installed.
- A Cisco ASA appliance with Adaptive Security Device Manager (ASDM) access and default AnyConnect client configuration to use for MFA.
NOTE: Default configuration can be configured by running the AnyConnect VPN wizard from the ASDM console.
- Cisco AnyConnect client software installed on all clients that connect remotely to the network.
- Familiarity with the following technologies:
 - LDAP configuration
 - VPN appliance administration

Deployments offering the mobile app authentication option will also require:

- MFA deployed on systems with Windows Vista or higher require the Mobile App Web service to be installed.
- A user device with the Azure authentication application installed.

Components

The following conditions reflect the assumptions and scope for information described in this guide.

- The Azure MFA server is installed on a domain-joined Windows 2012 R2 server.
- One Azure MFA server will be configured for LDAP.
- One Cisco ASA appliance is configured.

Conventions

Information is based on the following conditions.

- The guide was written using a Cisco ASA 5506 appliance.
- Documentation will refer to the Cisco ASA appliance as the VPN appliance, or just appliance.
- The Azure Multi-Factor Authentication Server is referred to as the MFA server.
- Active Directory (AD) is the directory service used for authentication.
- An SSL certificate will be used to encrypt authentication.
- Users will be imported from AD.

- A default token method will be configured.
- The OATH token method uses verification codes generated by the Azure Authentication app.

NOTE: While Azure MFA includes the option use Personal Identification Numbers (PINs) as an additional factor to the supported authentication methods, that configuration is outside the scope of this guide.

Step 1: Configure Multi-Factor Authentication Server

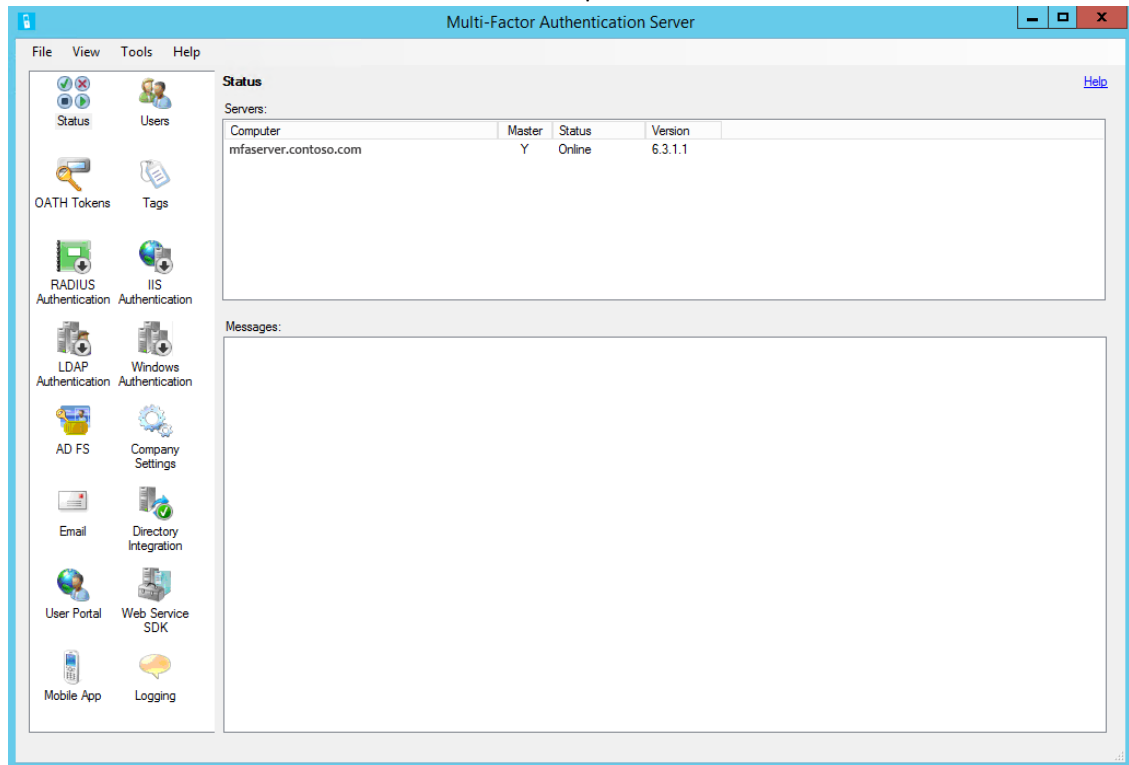
This topic explains how to configure the MFA server and the on-premises resources it requires. First you will log in to the server where MFA is installed. Next you will configure LDAP Authentication. Then you will connect MFA to the directory service, after which you will configure a default authentication method. Finally you will import accounts to the MFA Users group.

Multi-Factor Authentication Server Console

1. Log in to the server where MFA is installed.
2. Open the **Apps** screen.
3. Click the **Multi-Factor Authentication Server** icon:



4. The **Multi-Factor Authentication Server** window opens.

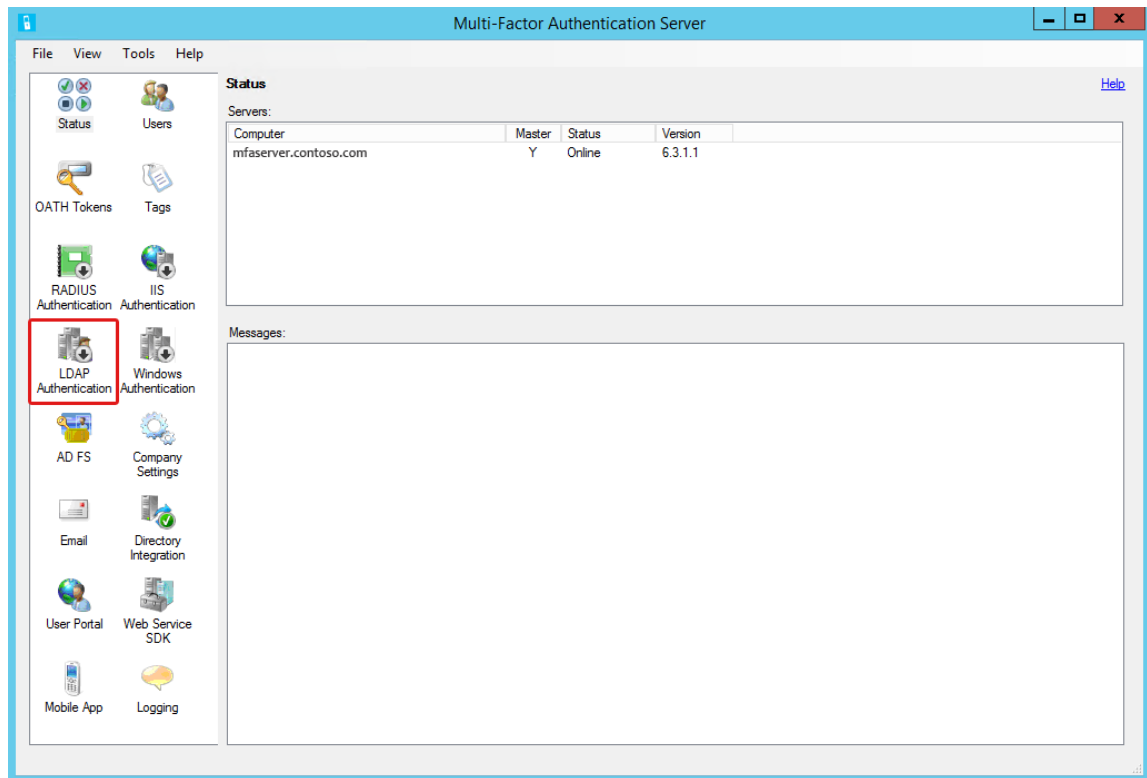


Now you will configure the necessary services.

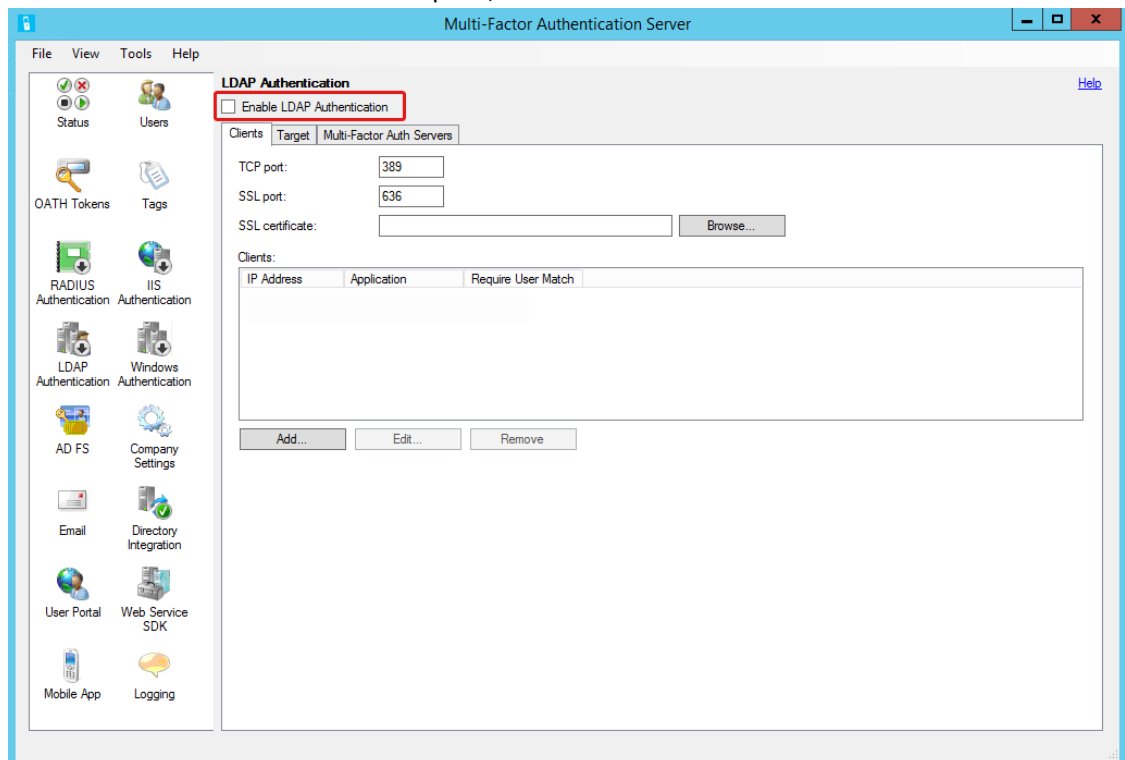
LDAP Authentication

First you will enable LDAP authentication, and then add the VPN appliance as a client.

1. Click the **LDAP Authentication** icon.

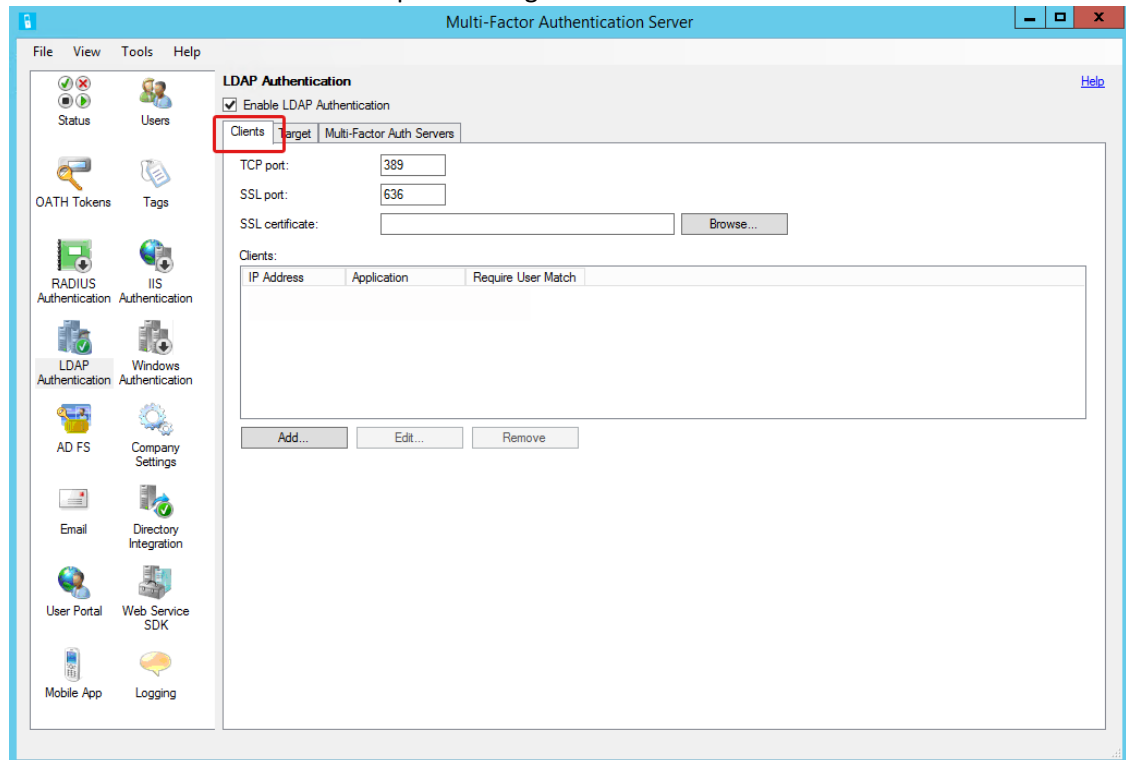


2. When the LDAP Authentication tool opens, select **Enable LDAP Authentication**.

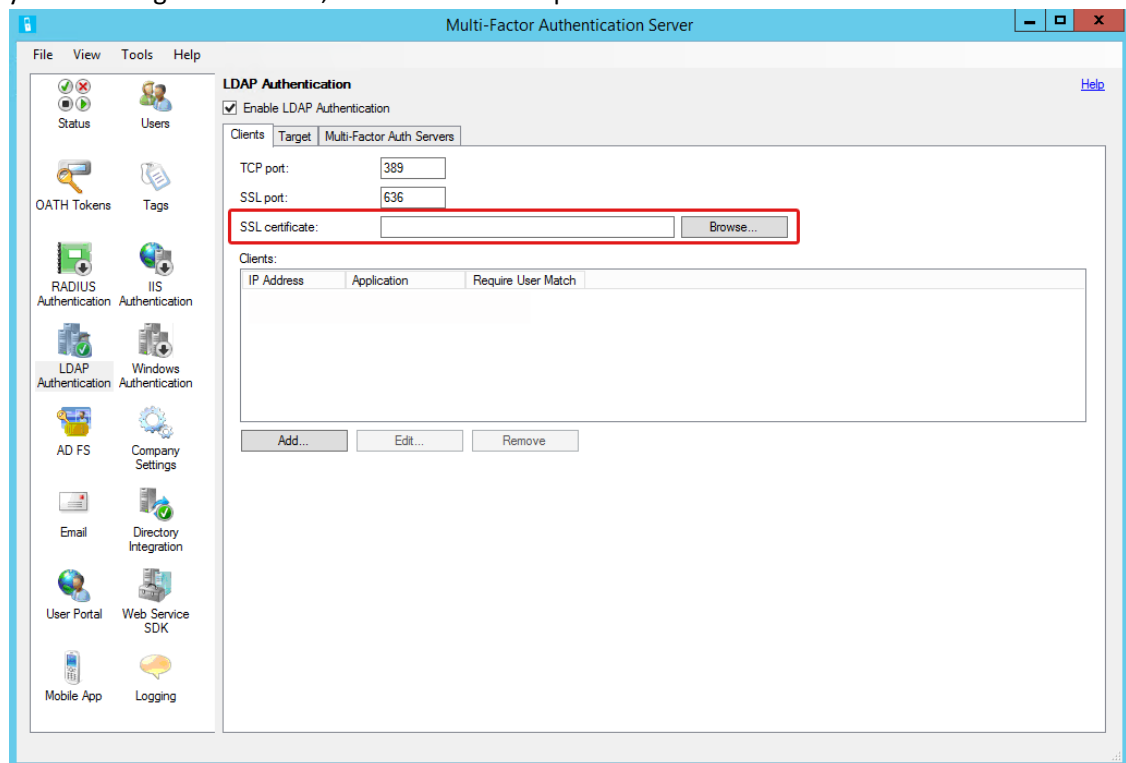


3. Select the **Clients** tab if necessary.

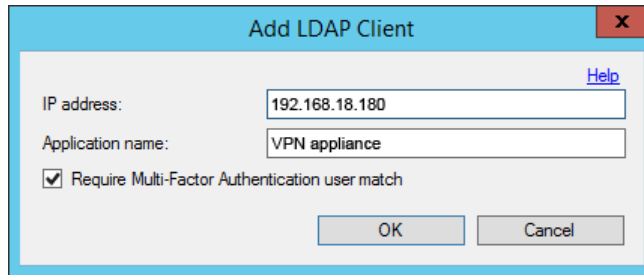
NOTE: Keep track of the port numbers noted for authentication as you will need them for the VPN appliance [configuration](#). Default is 636 when using SSL encryption. Unencrypted authentication is outside the scope for this guide.



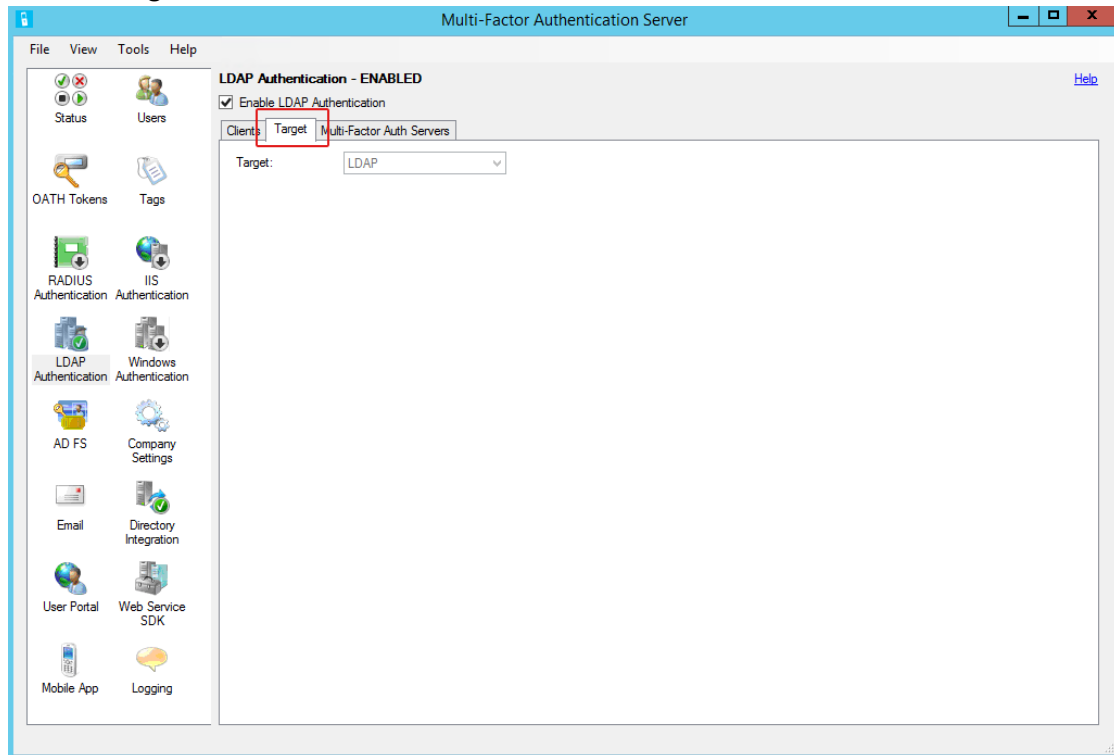
4. If you are using secure LDAP, click **Browse** to import the **SSL certificate**.



5. Click **Add** to open the **Add LDAP Client** dialog box.



6. Complete the following:
 - a. **IP address** – enter the VPN appliance address.
 - b. **Application name** – enter a descriptive name for the VPN appliance.
 - c. **Require Multi-Factor Authentication user match** – select; only users who are included in the MFA [Users](#) list will be granted access.
NOTE: This feature provides better control over remote access. If not enabled (unchecked), then only users who are included in the MFA Users list will need to authenticate with MFA. Other domain users will be able to authenticate without MFA.
7. Select the **Target** tab.



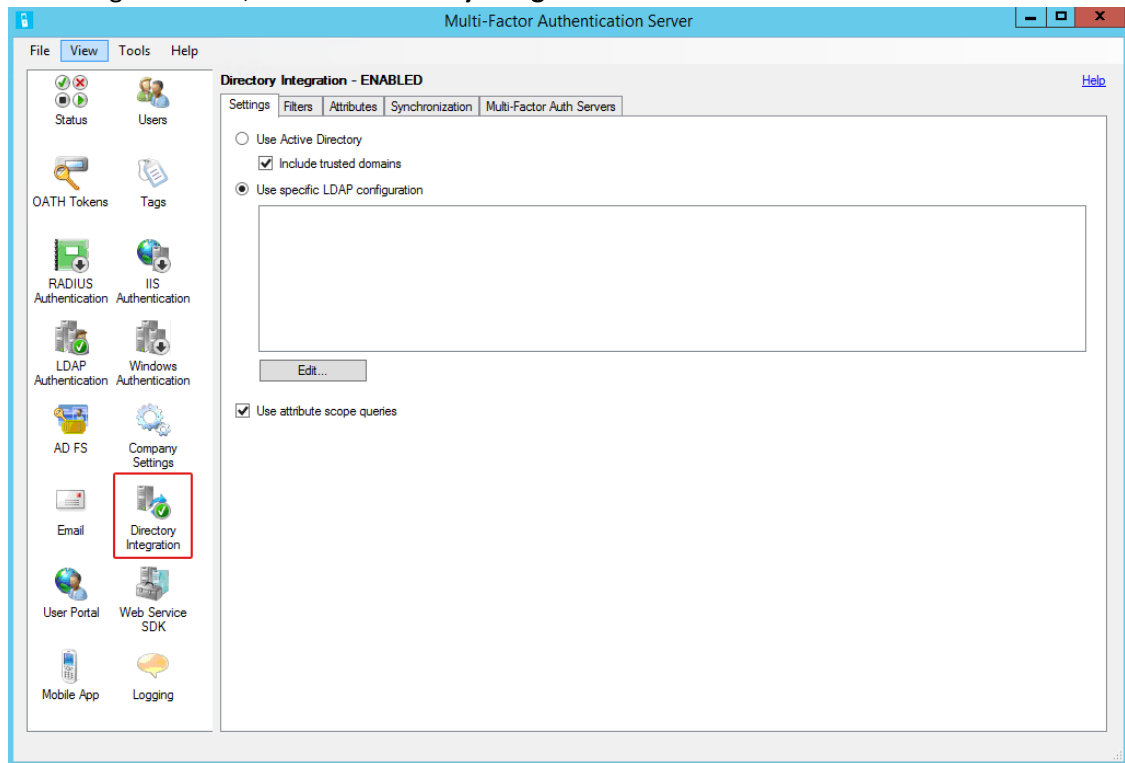
8. Confirm the **Target** field displays **LDAP**.

You have completed configuring LDAP authentication and adding the VPN appliance as an LDAP client. Leave the **Multi-Factor Authentication Server** window open for the next task.

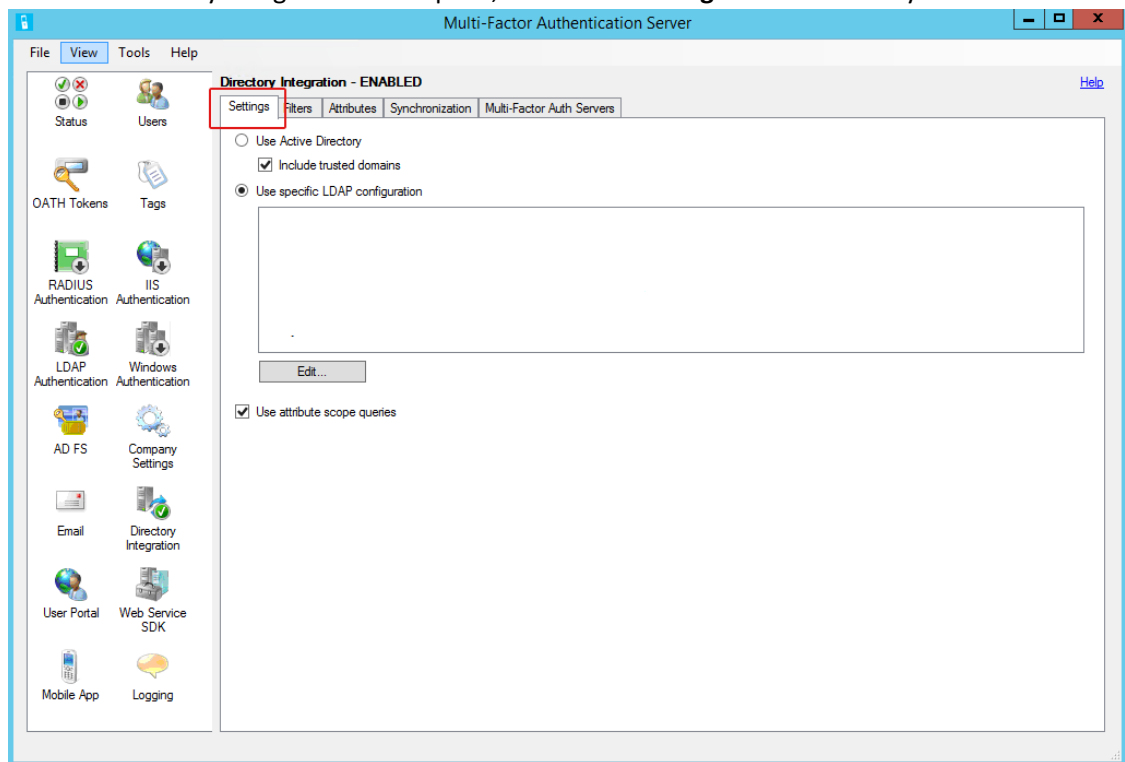
Directory Integration

Now you will connect to the directory service.

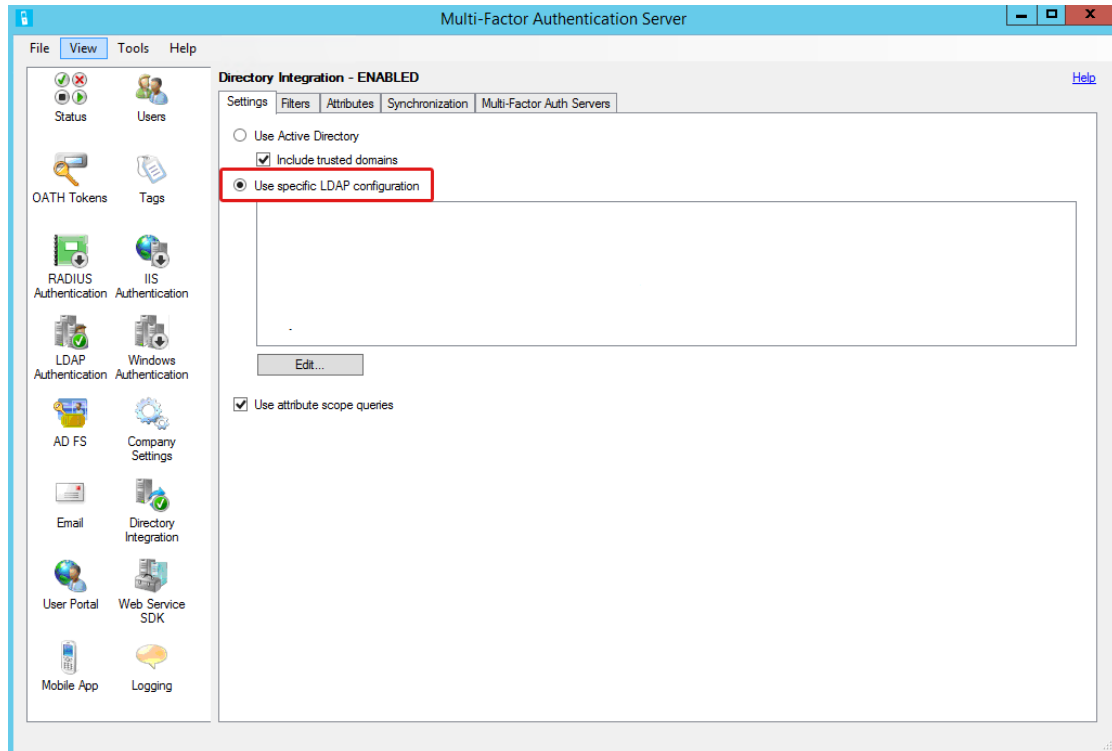
1. In the navigation area, click the **Directory Integration** icon.



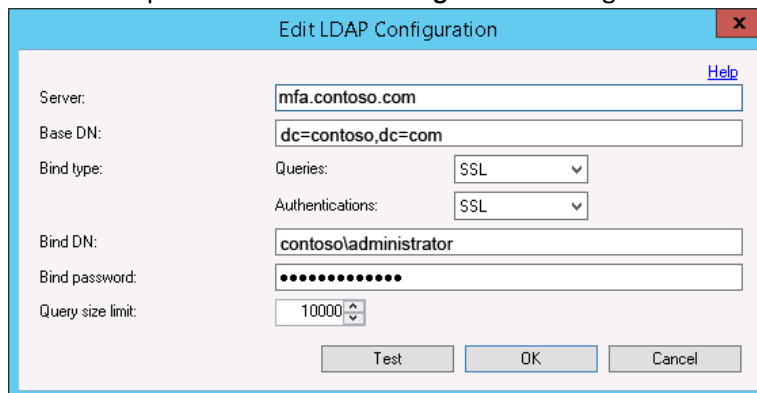
2. When the Directory Integration tool opens, select the **Settings** tab if necessary.



3. Select **Use Specific LDAP configuration**.

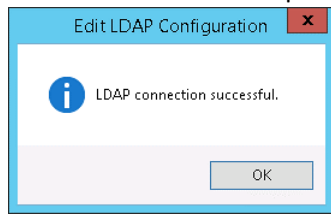


4. Click **Edit** to open the **Edit LDAP Configuration** dialog box.



5. Complete the following:
 - a. **Server** – enter the directory server host name or IP address.
NOTE: An FQDN is required if the **Bind type** below is set to SSL.
 - b. **Base DN** – enter the directory path.
 - c. **Bind type** – select the protocol to use for directory searches and authentication.
NOTE: assigning the correct bind type is essential for security.
 - I. **Queries** – search options are:
 - **Anonymous**
 - **Simple**
 - **SSL**
 - **Windows**
 - II. **Authentication** – authentication options are:
 - **Anonymous**

- **Simple**
 - **SSL**
 - **Windows**
- d. **Bind DN** – only required for the **SSL Bind type**; enter a domain\user account with administrator privileges.
 - e. **Bind Password** – only required for the **SSL Bind type**; enter the password for the account.
 - f. **Query size limit** –specify the maximum number of users a search will return.
6. **Test** – click to confirm that the MFA server is able to successfully connect to the LDAP server.
 7. Once the test completes successfully, click **OK**.
 8. Click **OK** to close the completion prompt.



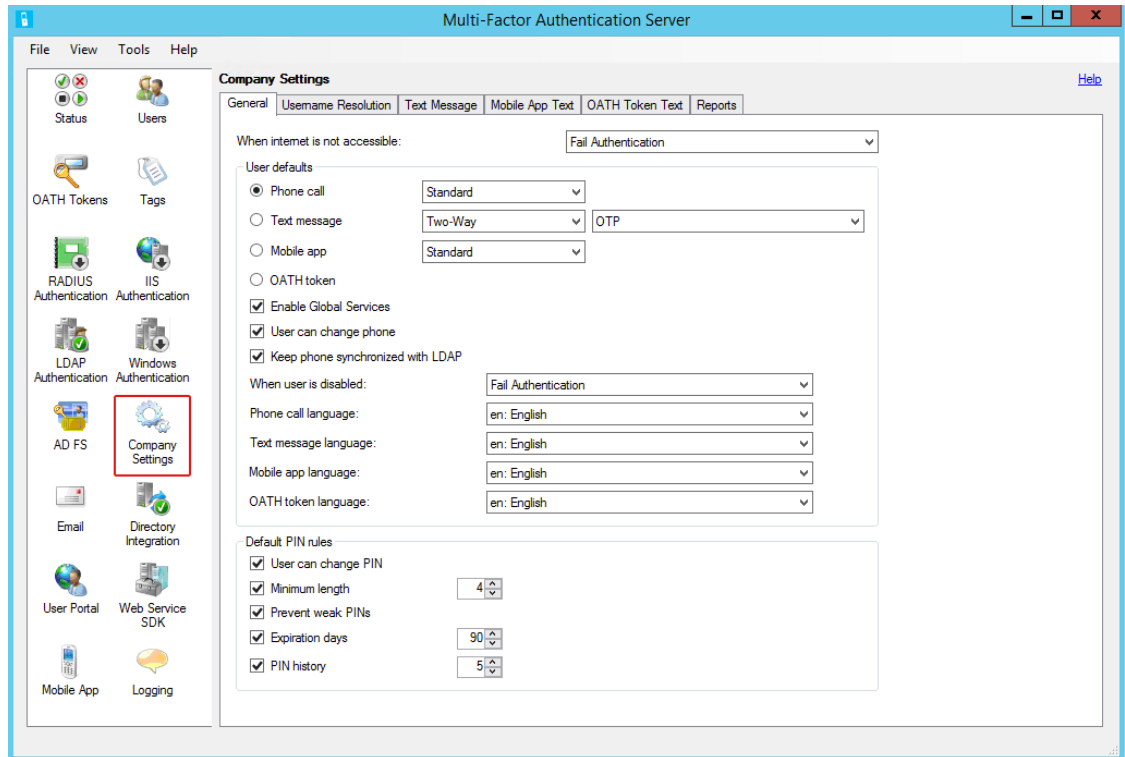
You have completed the MFA server directory service setup. Leave the **Multi-Factor Authentication Server** window open for the next task.

Default Authentication Method

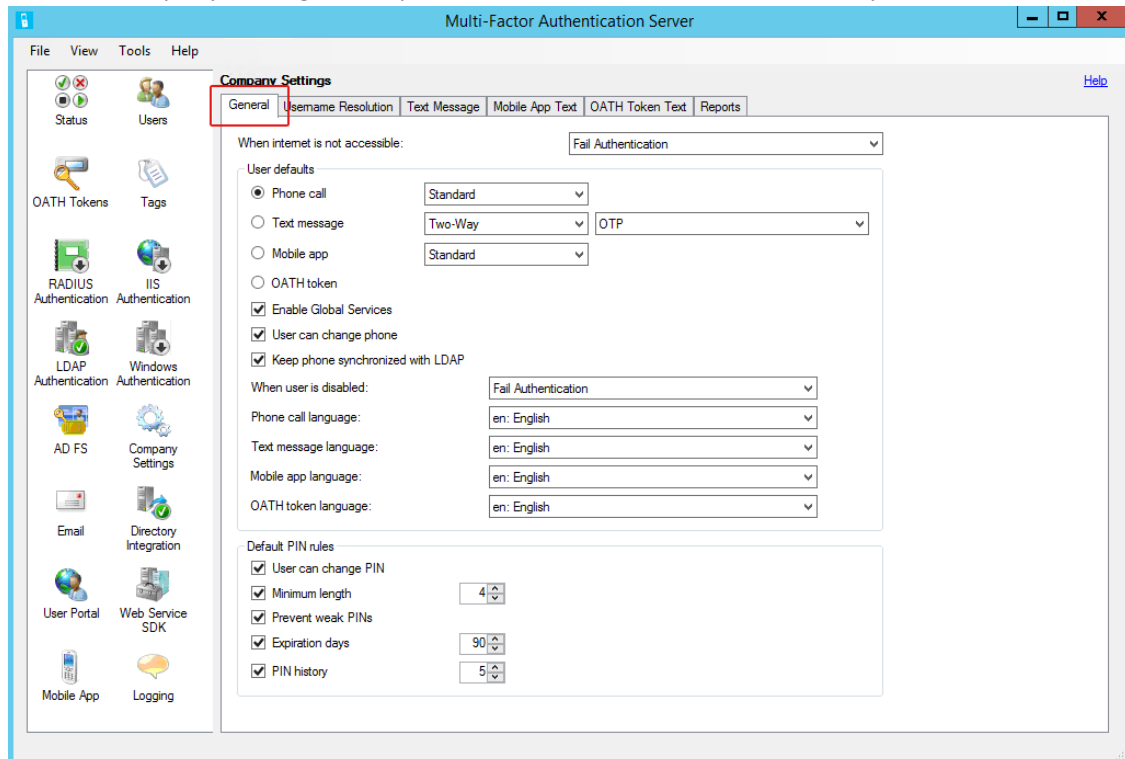
The instructions below explain how to set a default option for the authentication method that will be automatically assigned to MFA user accounts. A default method is required when user are not allowed to change methods. The feature is optional when users are allowed to change their token methods, and may be more convenient if a majority of users need one method.

Configure Company Settings

1. In the navigation area, click the **Company Settings** icon:

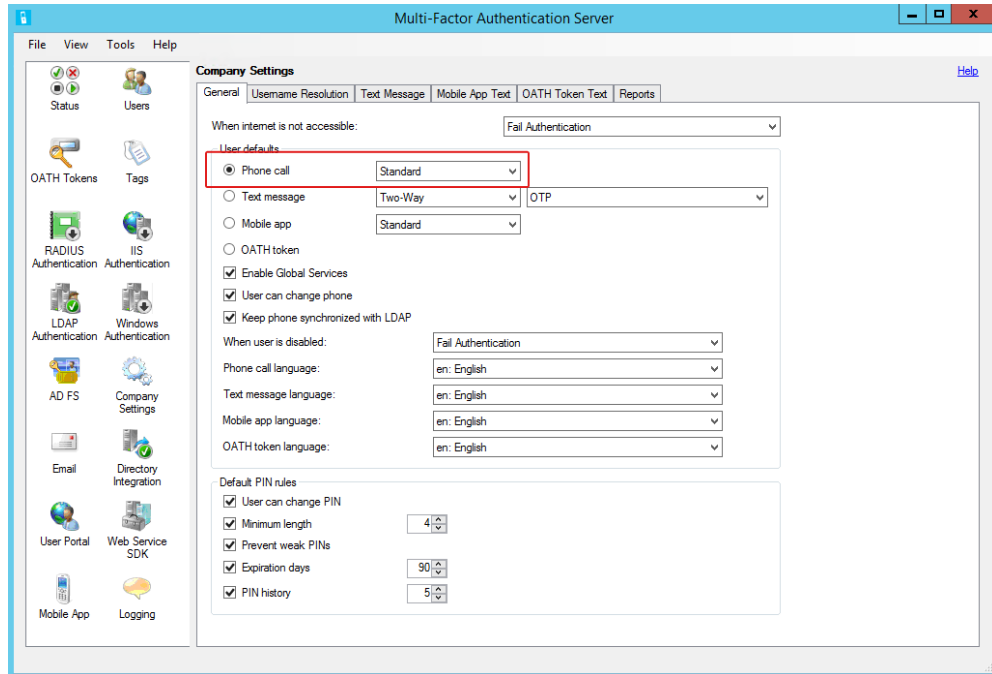


2. When the Company Settings tool opens, select the **General** tab if necessary.

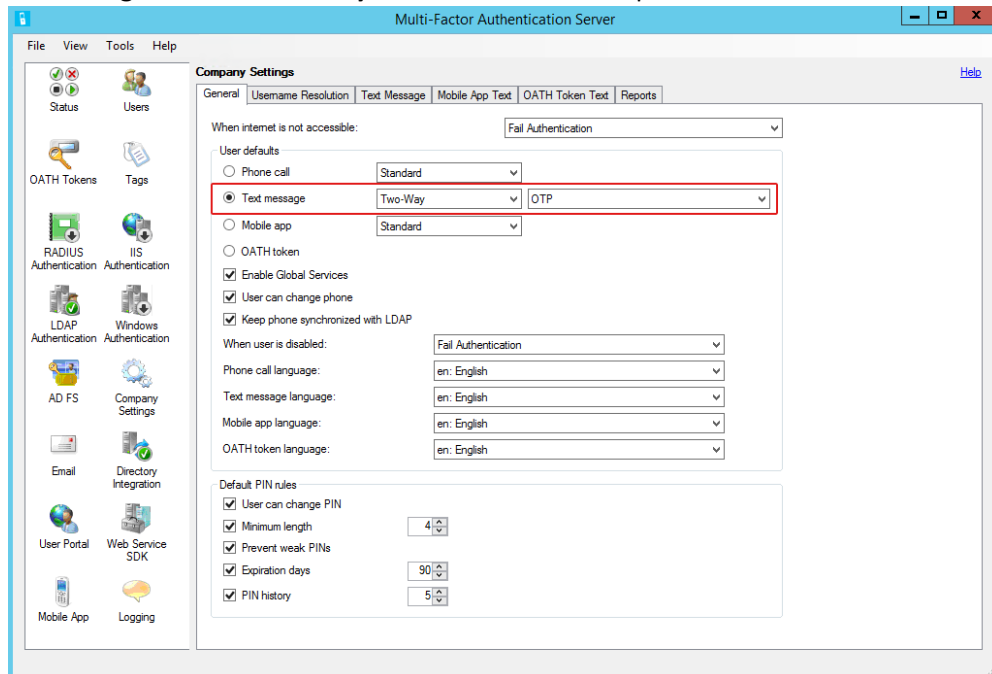


3. Leave default settings except for the following:

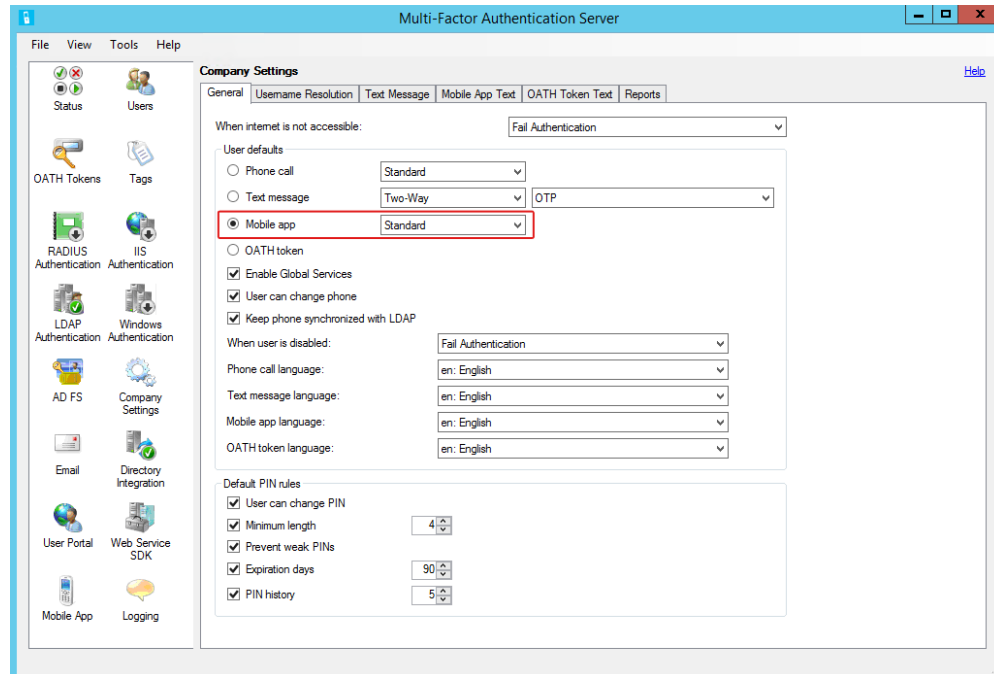
- **User defaults** – select one of the options below:
 - **Phone call** – select **Standard** from the drop menu:



- **Text message** – select **Two-Way** and **OTP** from the drop menus:



- **Mobile app** – select **Standard** from the drop menu:



Note: This option will require users to [register](#) their devices through the Azure authentication app.

This completes the company information setup to designate the default authentication method for LDAP Authentication. Leave the **Multi-Factor Authentication Server** window open for the next task.

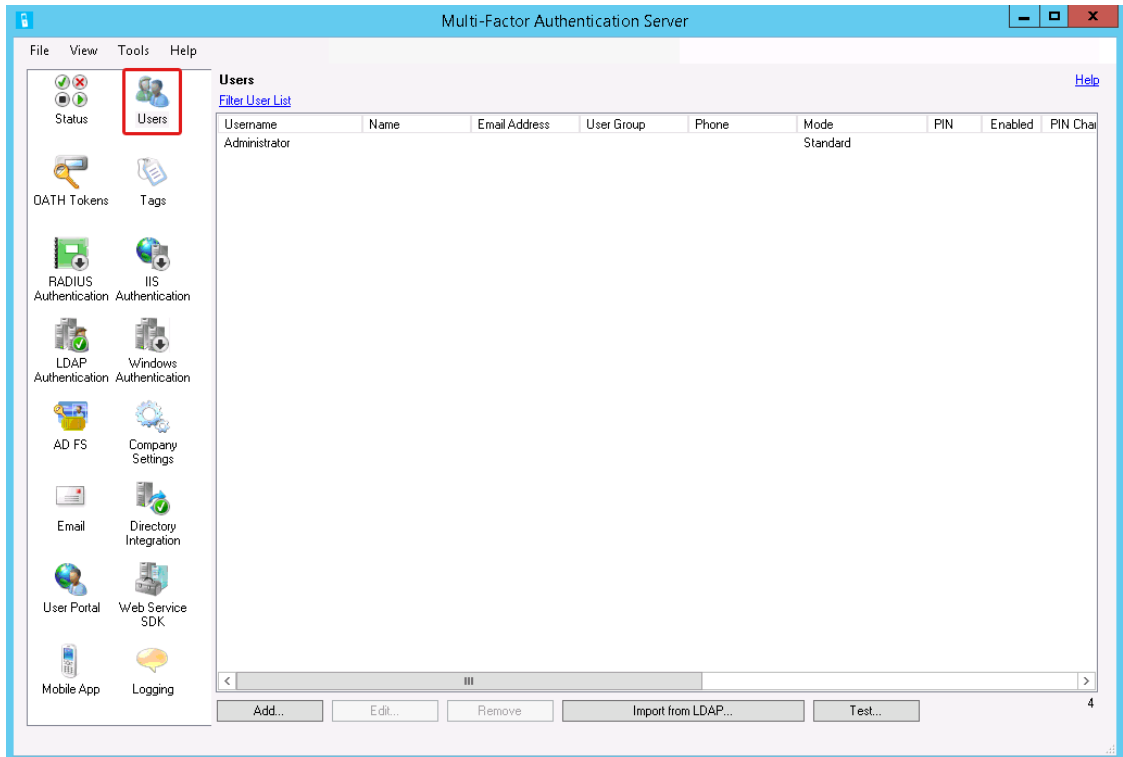
MFA Users

When the VPN appliance was configured as an LDAP client, access was restricted to members of the MFA Users group. This provides more control over remote access, and is a security best practice. Now accounts need to be imported from the directory service. Then, the MFA administrator account needs to be configured so that LDAP requests do not require MFA.

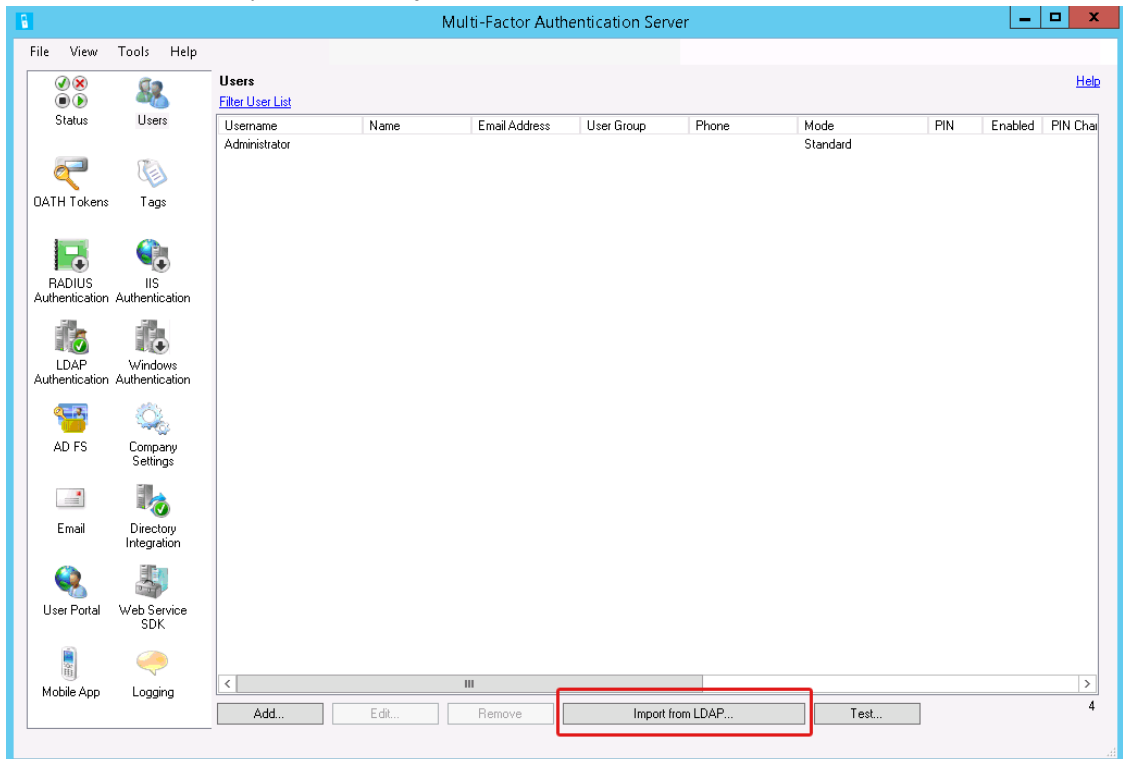
Import User Accounts

These instructions are for on-demand user import.

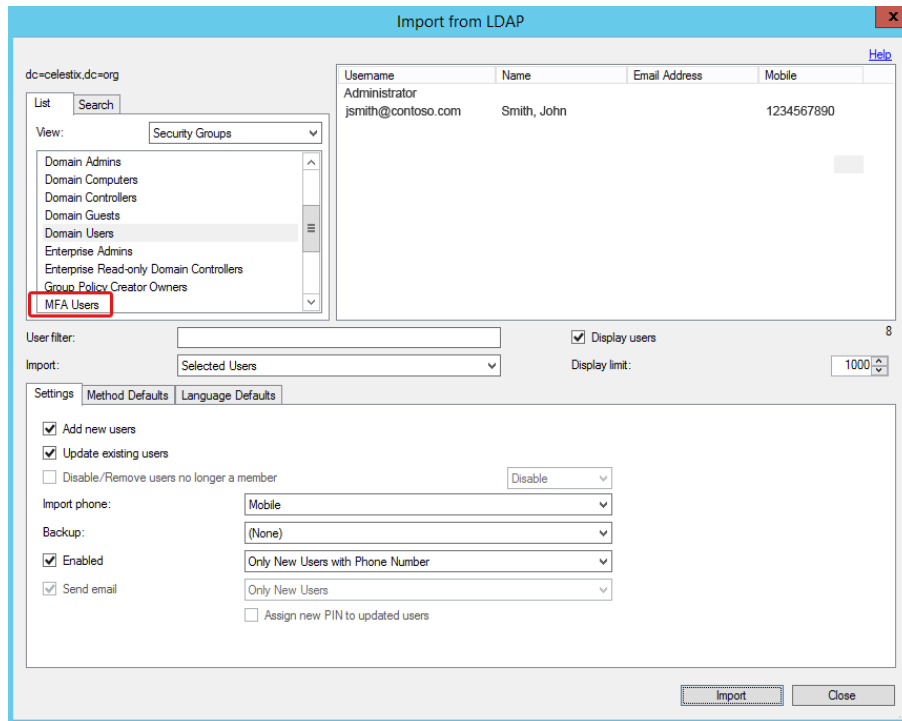
1. In the navigation area, click the **Users** icon.



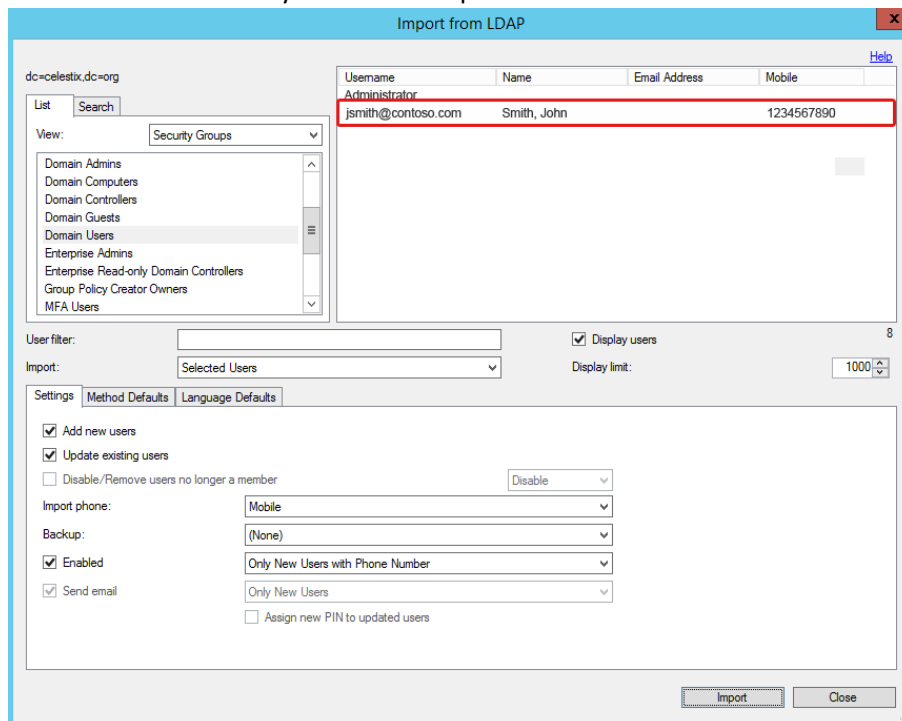
2. When the Users tool opens, Click **Import from LDAP**.



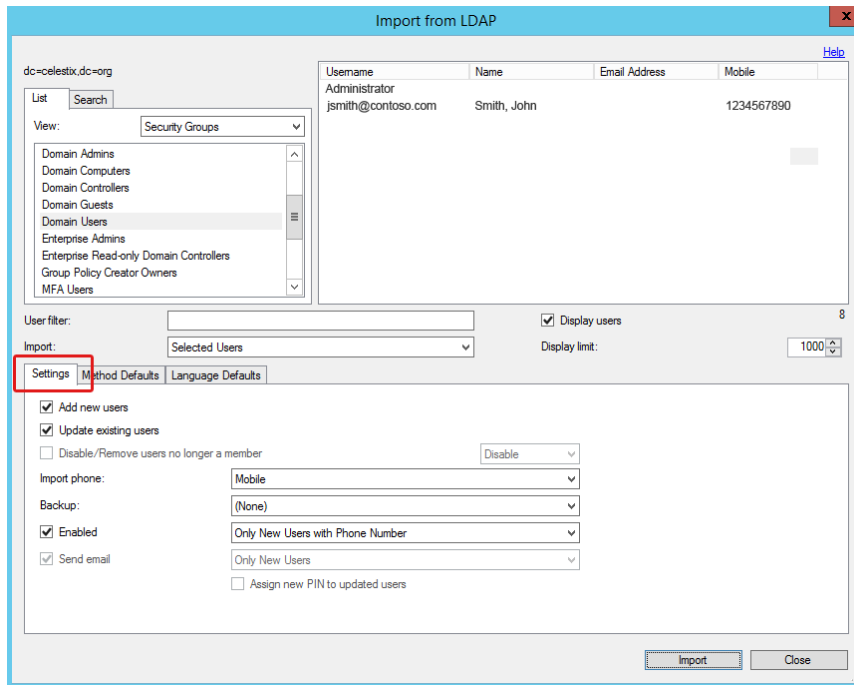
3. On the import screen, select a user group.



4. Select the user accounts you want to import.

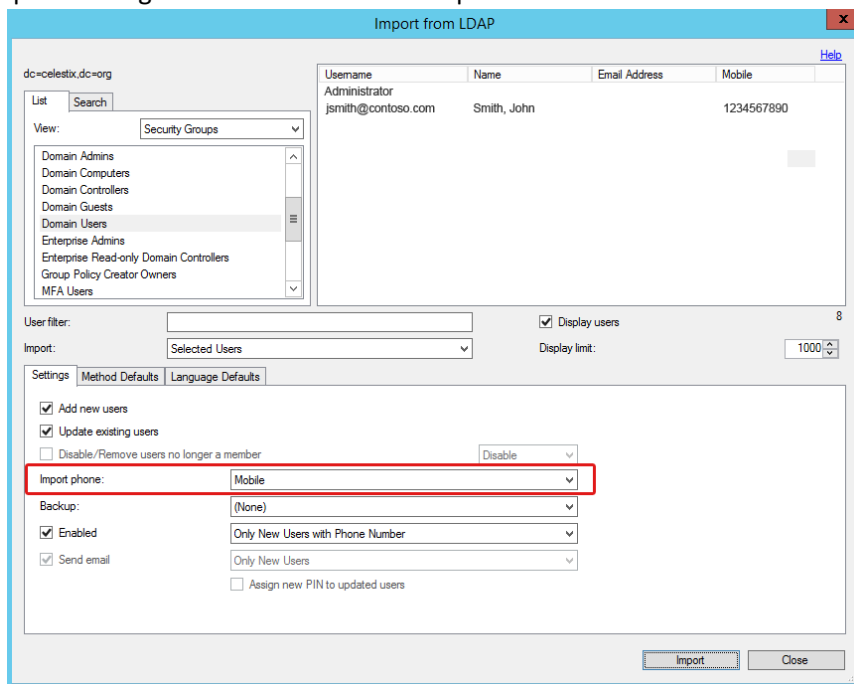


5. Leave the default settings except for the following:
 a. Select the **Settings** tab if necessary.

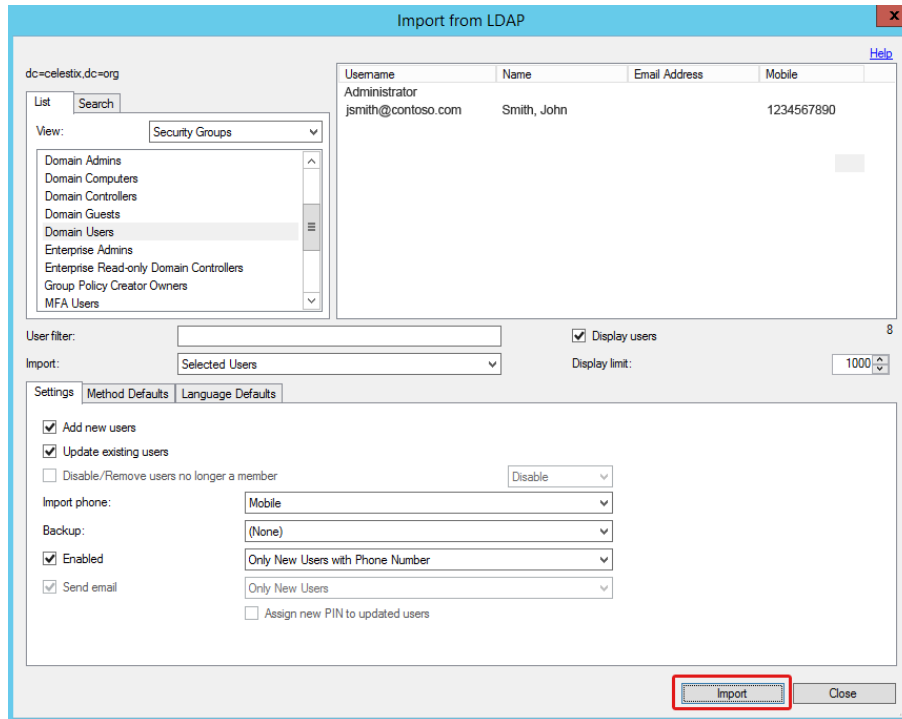


b. In the **Import Phone** drop menu, select **Mobile**.

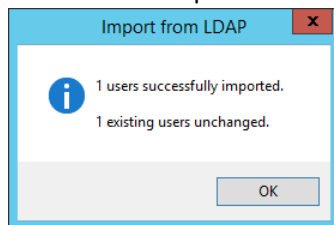
NOTE: For purposes of this guide we are designating the Mobile attribute for the phone import setting. It is the most common option used for MFA.



6. Click the **Import** button.



7. Click **OK** in the import success dialog box.



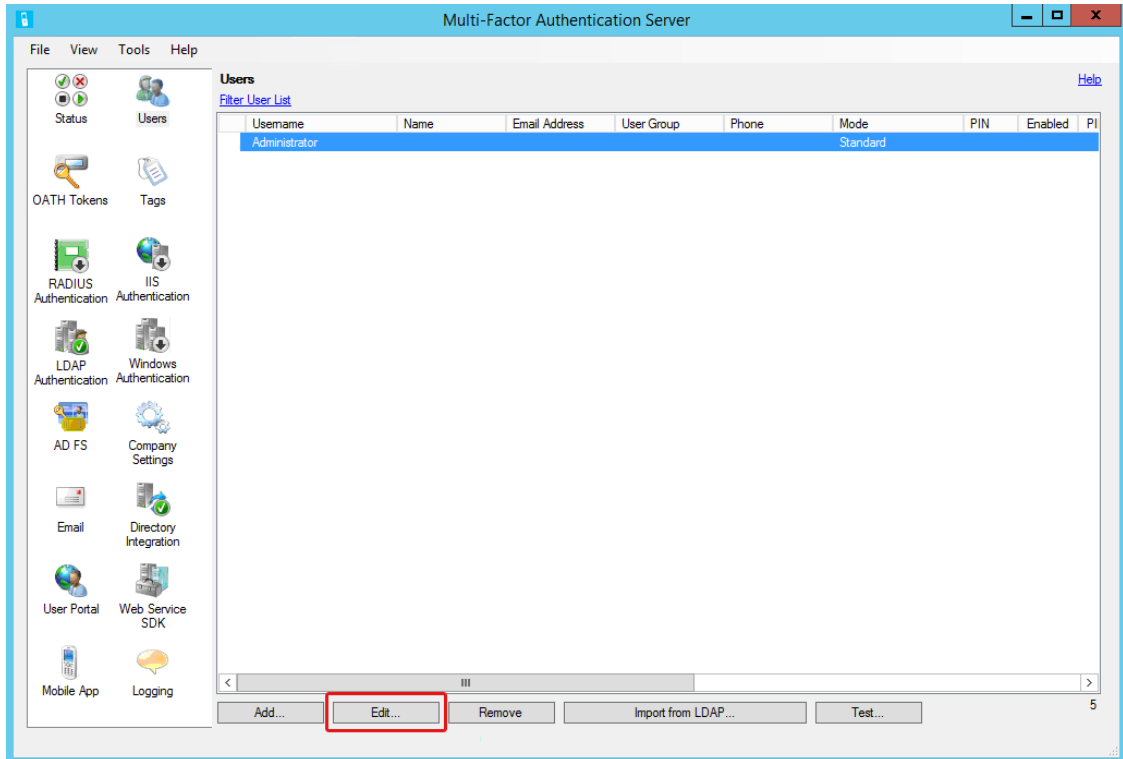
8. Click the **Close** button on the import screen to return to the Users pane.

Leave the Users tool open for the next task.

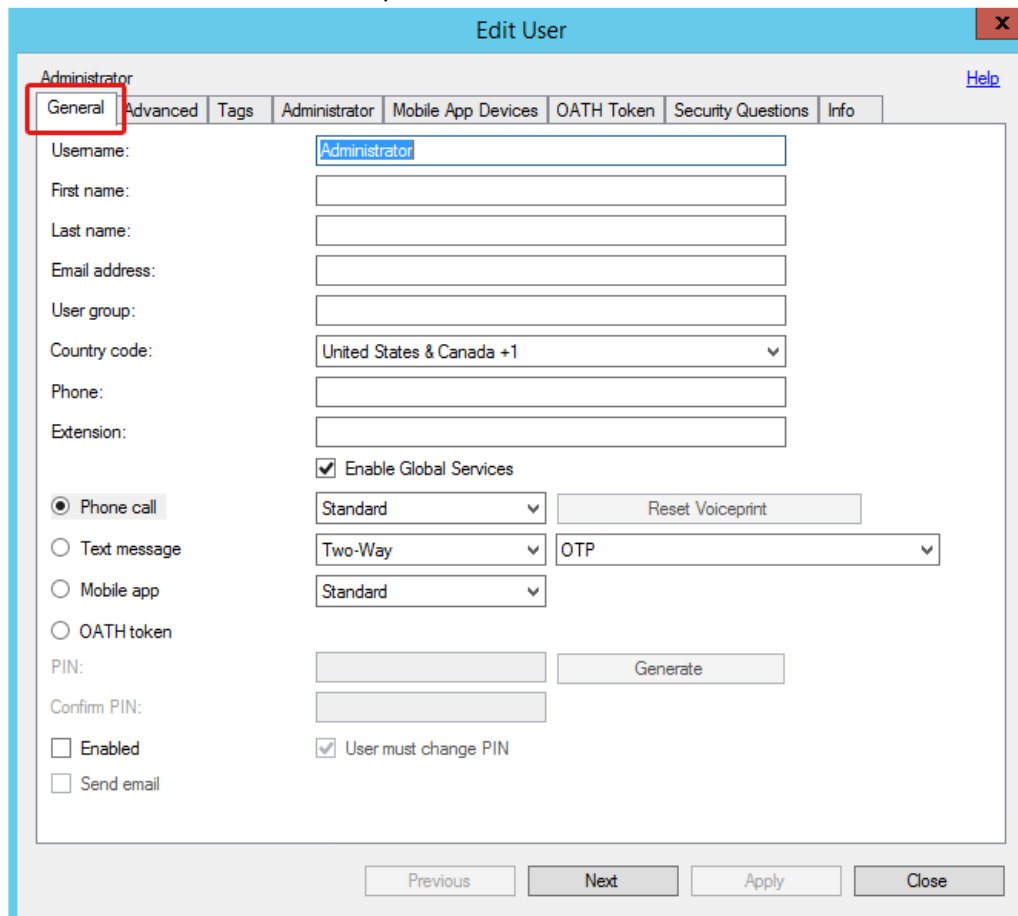
Administrator Account

The following instructions explain how to configure the MFA administrator account to facilitate LDAP requests without needing to negotiate multi-factor authentication requests. This provides the best balance between security and functionality when the administrator account is used for LDAP requests.

1. Select the **Administrator** account.
2. Click Edit.



3. Select the **General** tab if necessary.



4. Clear the **Enabled** checkbox.

The screenshot shows the 'Edit User' dialog box for the 'Administrator' user. The 'General' tab is selected, and the 'Enabled' checkbox is highlighted with a red box. The dialog box contains the following fields and options:

- Administrator** (Title)
- Help** (Link)
- General** (Selected tab) | **Advanced** | **Tags** | **Administrator** | **Mobile App Devices** | **OATH Token** | **Security Questions** | **Info**
- Username:** Administrator
- First name:** (Empty)
- Last name:** (Empty)
- Email address:** (Empty)
- User group:** (Empty)
- Country code:** United States & Canada +1
- Phone:** (Empty)
- Extension:** (Empty)
- Enable Global Services**
- Phone call** | Standard | Reset Voiceprint
- Text message** | Two-Way | OTP
- Mobile app** | Standard
- OATH token**
- PIN:** (Empty) | Generate
- Confirm PIN:** (Empty)
- Enabled** (Highlighted with a red box)
- Send email**
- User must change PIN**
- Previous** | **Next** | **Apply** | **Close**

5. Select the **Advanced** tab.

The screenshot shows the 'Edit User' dialog box with the 'Advanced' tab selected. The 'Advanced' tab is highlighted with a red box. The form contains the following settings:

- Backup phone:**
 - Country code: United States & Canada +1
 - Phone: [Empty text box]
 - Extension: [Empty text box]
- User can change phone
- Keep phone synchronized
- When user is disabled: Succeed Authentication
- Phone call language: en: English
- Text message language: en: English
- Mobile app language: en: English
- OATH token language: en: English
- Override PIN rules
- PIN Rules:**
 - User can change PIN
 - Minimum length: 4
 - Prevent weak PINs
 - Expiration days: 90
 - PIN history: 5
- Account used for LDAP Authentication password changes

At the bottom of the dialog, there are buttons for 'Previous', 'Next', 'Apply', and 'Close'.

6. Leave the default settings, except for the following:
 - a. **When user is disabled** – select Succeed Authentication.
 - b. **Account is used for LDAP Authentication password changes** – select to allow end users to change their own passwords.

The screenshot shows the 'Edit User' dialog box with the following configuration:

- Administrator
- General | **Advanced** | Tags | Administrator | Mobile App Devices | OATH Token | Security Questions | Info
- Backup phone: Country code: United States & Canada +1
- Phone: [Empty field]
- Extension: [Empty field]
- User can change phone
- Keep phone synchronized
- When user is disabled: Succeed Authentication
- Phone call language: en: English
- Text message language: en: English
- Mobile app language: en: English
- OATH token language: en: English
- Override PIN rules
- PIN Rules:
 - User can change PIN
 - Minimum length: 4
 - Prevent weak PINs
 - Expiration days: 90
 - PIN history: 5
- Account used for LDAP Authentication password changes
- Buttons: Previous, Next, Apply, Close

7. Click **Apply**.
8. Click **Close**.

You have completed MFA server configuration.

Step 2: Configure the VPN Appliance

Now that the authentication process has been configured to use multiple factors, you need to configure the VPN appliance to connect to the LDAP server.

ASDM Console

Configure an authentication server on the VPN appliance that will send LDAP authentication requests to the Azure MFA server.

First you will configure a server group for the MFA LDAP server. Next you need a connection profile for AnyConnect to access the LDAP server. Then you will create a profile to set a custom timeout value to ensure that AnyConnect VPN clients have enough time to log in using MFA.

Create AAA Server Group

1. Log in to the Cisco ASDM console for the VPN appliance.

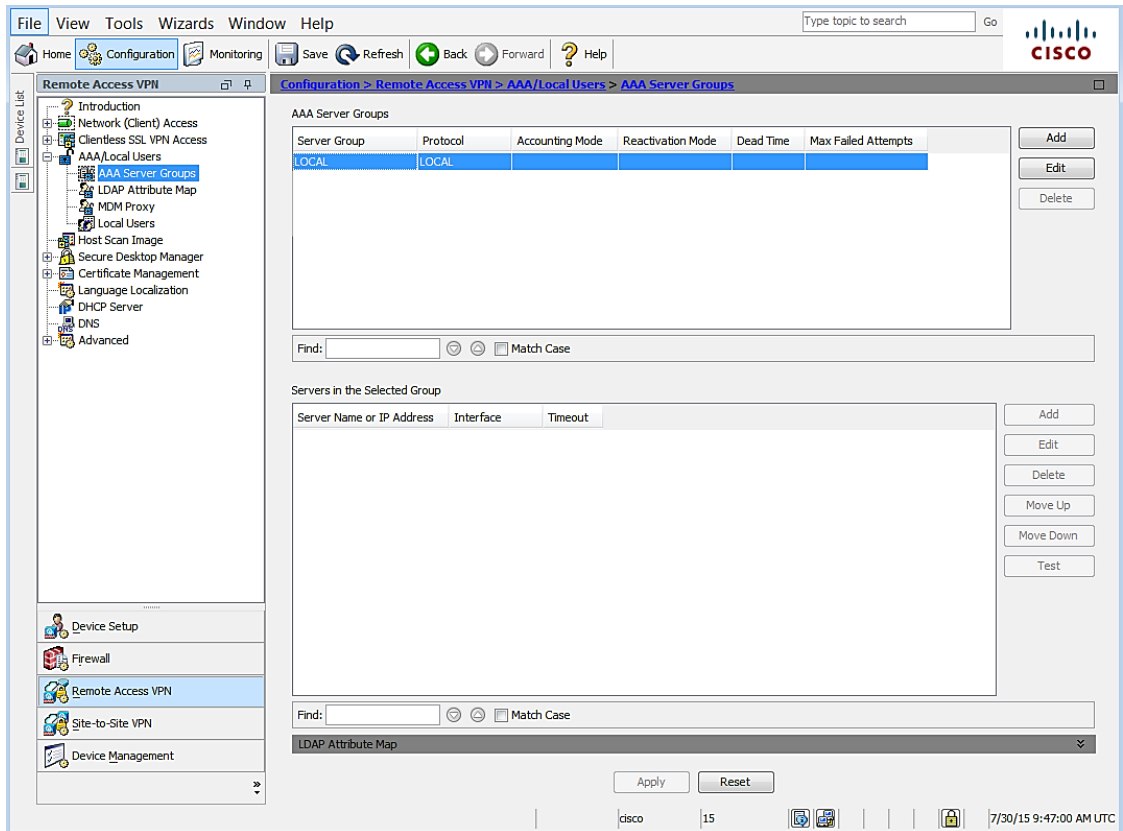
The screenshot displays the Cisco ASDM 7.4 for ASA console interface for the device 192.168.20.100. The main content area is divided into several sections:

- Device Information:** Host Name: ciscoasa, ASA Version: 9.3(3)2, ASDM Version: 7.4(2), Firewall Mode: Routed, Environment Status: OK, Device Uptime: 0d 1h 42m 13s, Device Type: ASA 5506, Context Mode: Single, Total Flash: 8192 MB.
- Interface Status:** A table showing interface status for 'inside' and 'outside'.
- VPN Sessions:** IPsec: 0, Clientless SSL VPN: 0, AnyConnect Client: 0.
- System Resources Status:** Total Memory Usage, Total CPU Usage, Core Usage.
- Traffic Status:** Connections Per Second Usage and 'outside' Interface Traffic Usage (Kbps).

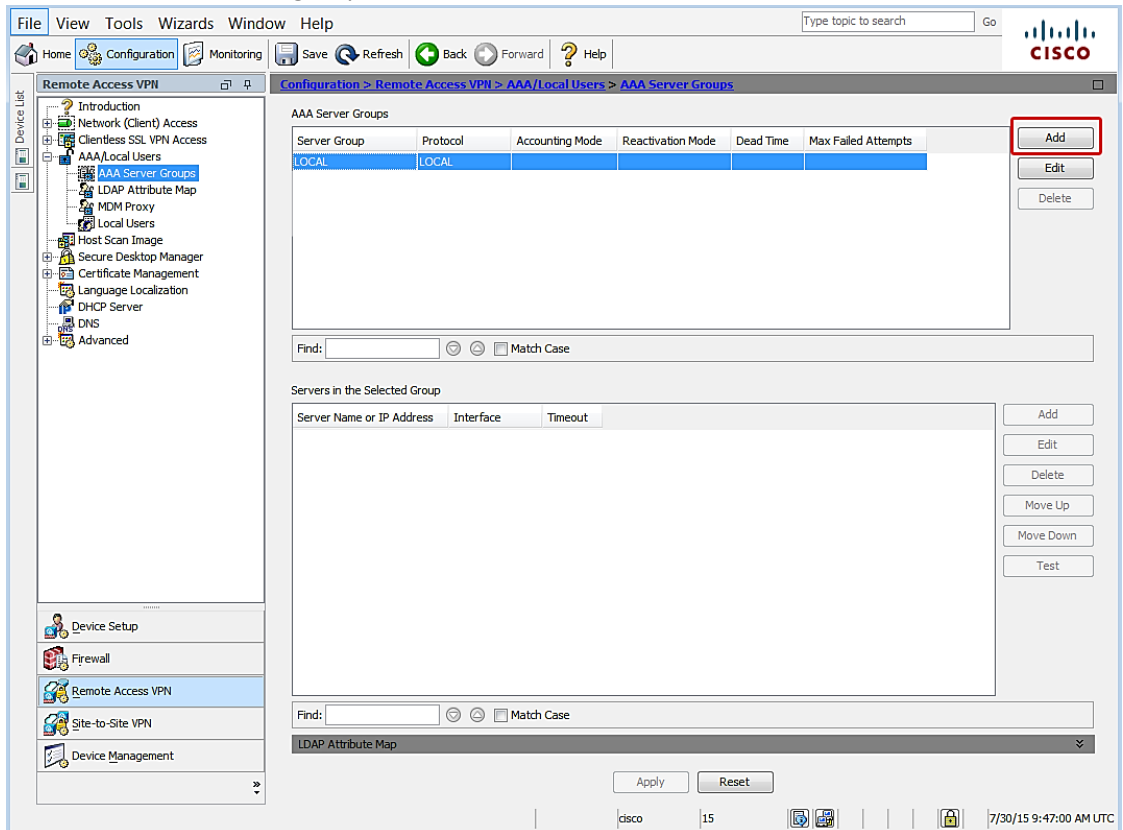
Interface	IP Address/Mask	Line	Link	Kbps
inside	192.168.20.100/20	up	up	11
outside	172.16.1.1/24	down	down	0

The 'outside' Interface Traffic Usage (Kbps) chart shows 'Interface is down.' The status bar at the bottom indicates the time is 7/29/15 11:44:50 AM UTC.

2. Navigate to **Configuration | Remote Access VPN | AAA/Local users | AAA server groups.**



3. Click **Add** to create a new group.



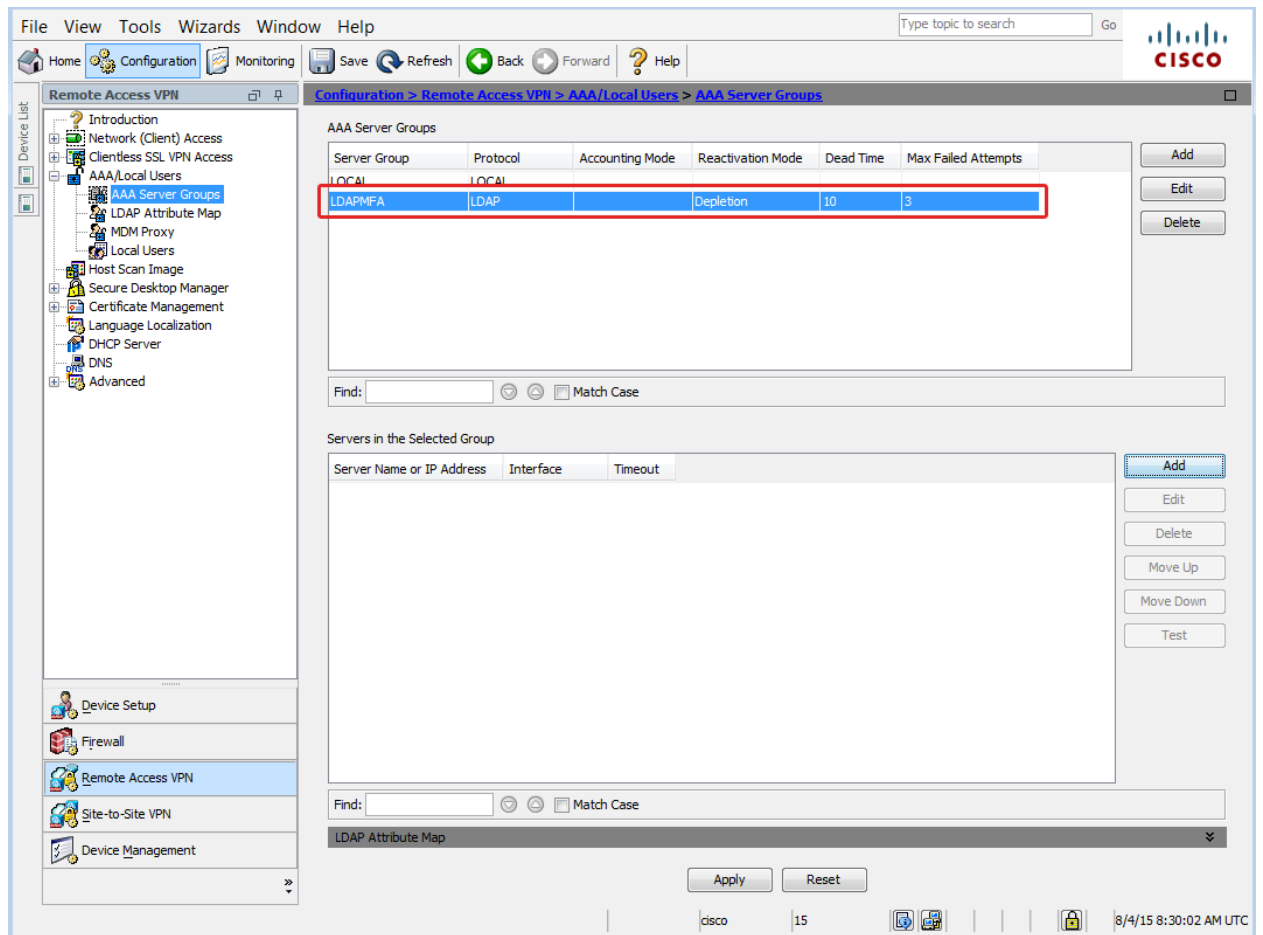
4. The Add a new AAA Server Group dialog opens.

The screenshot shows a dialog box titled "Add AAA Server Group". It contains the following fields and controls:

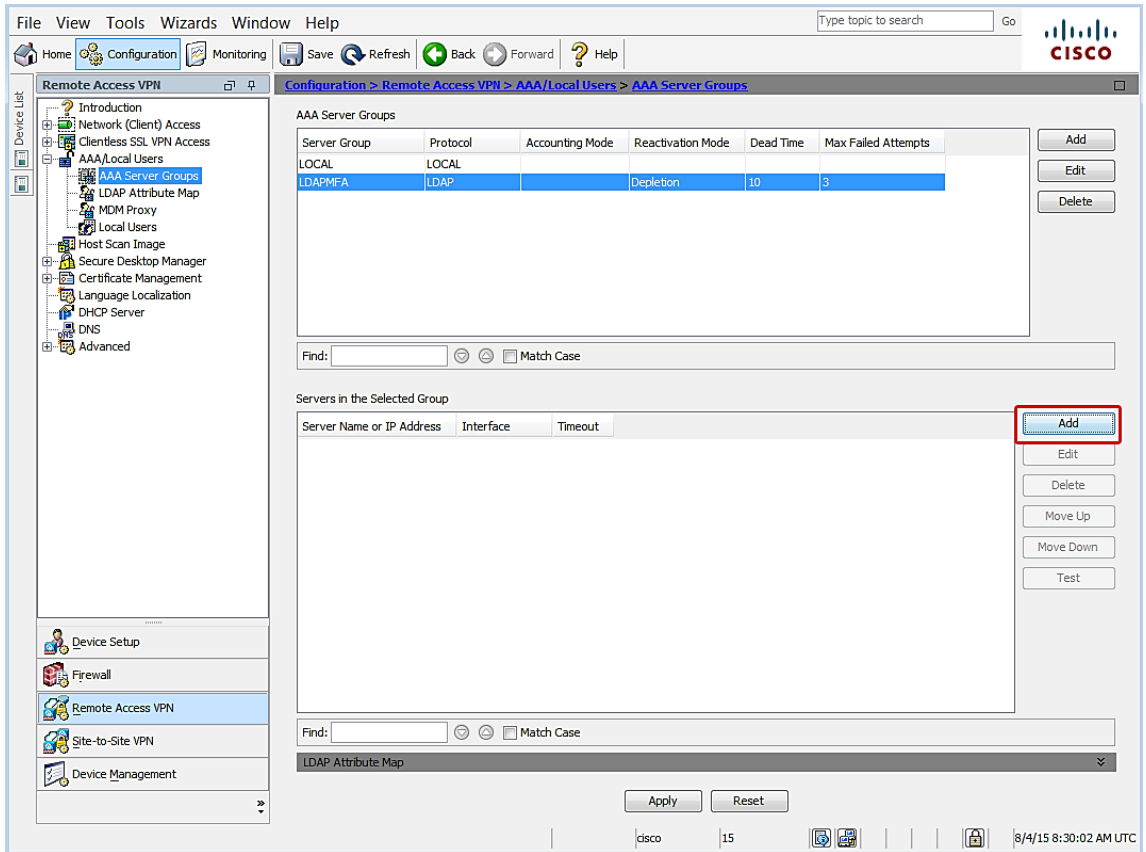
- AAA Server Group:** An empty text input field.
- Protocol:** A dropdown menu currently set to "LDAP".
- Reactivation Mode:** Two radio buttons, "Depletion" (selected) and "Timed".
- Dead Time:** A text input field containing "10" followed by the label "minutes".
- Max Failed Attempts:** A text input field containing "3".

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

5. Leave the default settings except for the following:
 - a. **AAA Server Group** – specify a name to identify the group for the MFA server.
 - b. **Protocol** – select **LDAP**.
 - c. Click **OK**.
6. In the **AAA Server Groups** list, select the server group you just created.



7. In the **Servers in the Selected Group** pane, click **Add**.



8. The Add AAA Server dialog opens.

9. Leave the default settings except for the following:
 - a. **Interface Name** – select the interface that will handle communication with the MFA Server.
 - b. **Server Name or IP Address** – specify the name or the IP address of the MFA server.
 - c. **Timeout (seconds)** – it is important to set a sufficient length of time for users to authenticate. 60 seconds is a common duration, but may need to be adjusted. For example, large organizations may need more time to accommodate a higher volume of requests.
 - d. **Server port** – enter the port number used for authentication communication on the MFA Server. Default is 636 when using SSL encryption.
 - e. **Server Type** – select the LDAP server type. In this example we are using Active Directory, and will select **Microsoft**.
 - f. **Base DN** – specify where the authentication server should begin searching for user entries.
 - g. **Scope** – specify the extent of the search in the LDAP hierarchy that the server should query.
 - h. **Naming Attribute** – enter unique naming attribute that identifies an entry on the target LDAP server. For example, sAMAccountName or userPrincipalName.
 - i. **Login DN** – enter a domain administrator account DN that has rights to search or lookup users in the target LDAP server.
 - j. **Login Password** – enter the administrator password.
 - k. **LDAP Attribute Map** – leave this set to the default, unless your directory has customized attributes.

- I. **LDAP Parameters for group search** – specify whether a group should be extracted from the LDAP server.

NOTE: If there are a large number of groups to query, the [timeout](#) setting may require a higher value.

- m. Click **OK**.

10. Click **APPLY** to save the configuration.

The screenshot shows the Cisco Configuration Assistant interface. The left pane displays the configuration tree with 'Remote Access VPN' expanded to 'AAA Server Groups'. The main pane shows the configuration for the 'LDAPMFA' group. The 'Servers in the Selected Group' table is as follows:

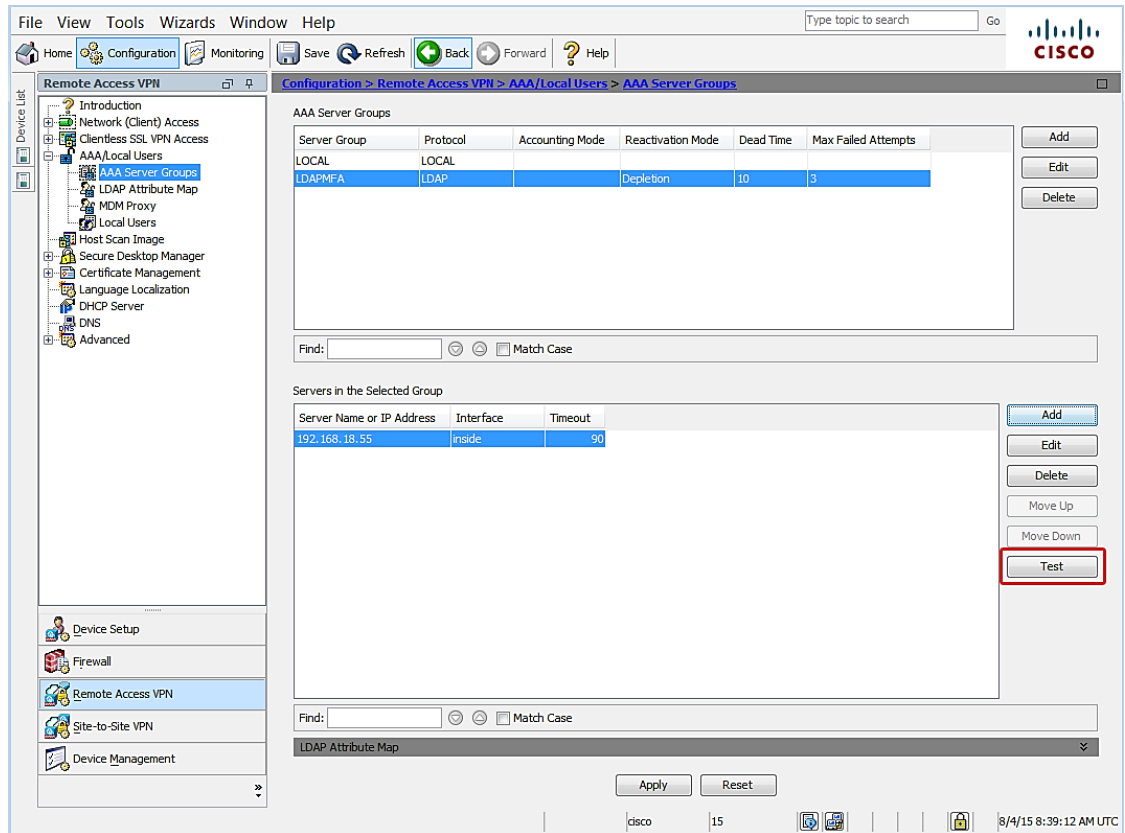
Server Name or IP Address	Interface	Timeout
192.168.18.55	inside	90

The 'Apply' button at the bottom right is highlighted with a red box. The status bar at the bottom shows 'cisco | 15' and the date '8/4/15 8:39:12 AM L'.

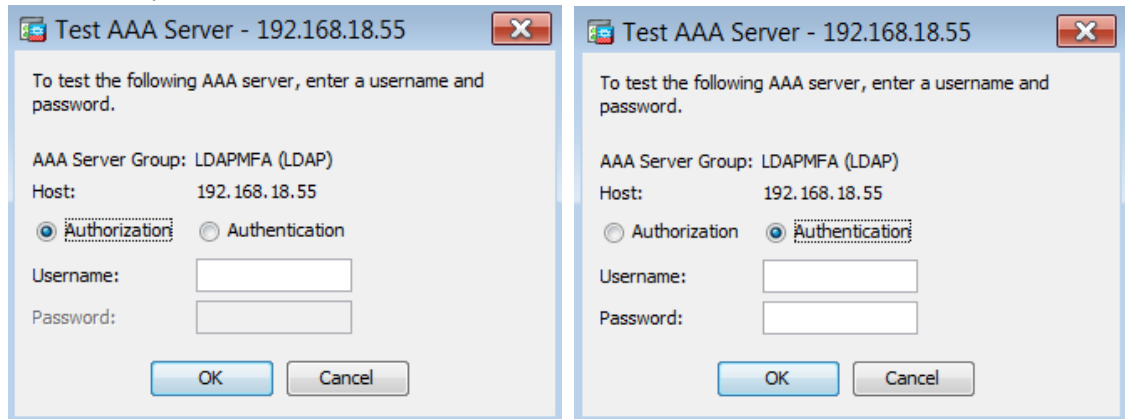
Test Configuration

You can test the connection to MFA server to confirm that the connection is correctly configured.

1. Make sure the LDAP server you created is still selected.
2. Click the **Test** button to open the test tool.



3. Select a test option:

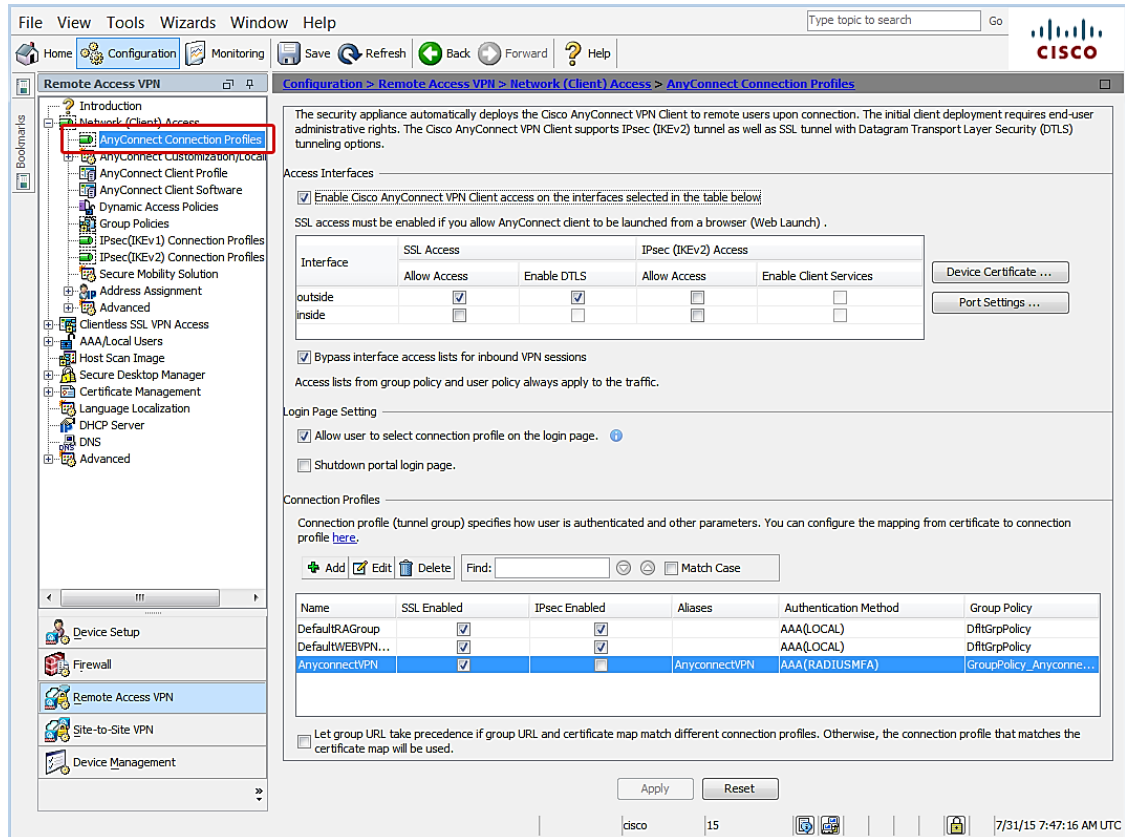


4. Enter credentials for an account that is configured for Azure MFA.

5. Click **OK** and wait for test results to post.

Enable Connection Profile

1. Navigate **Remote Access VPN | Network (Client) Access | AnyConnect Connection Profiles**.



2. Leave default settings, except for the following:
 - a. **Enable Cisco AnyConnect VPN Client access on the interfaces selected in table below** – confirm checkbox is selected.

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

Allow user to select connection profile on the login page. ⓘ

Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Find:

 Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultTRAGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPN...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
AnyconnectVPN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AnyconnectVPN	AAA(RADIUSMFA)	GroupPolicy_Anyconne...

Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

b. Select the appropriate SSL interface access option.

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

Allow user to select connection profile on the login page. ⓘ

Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

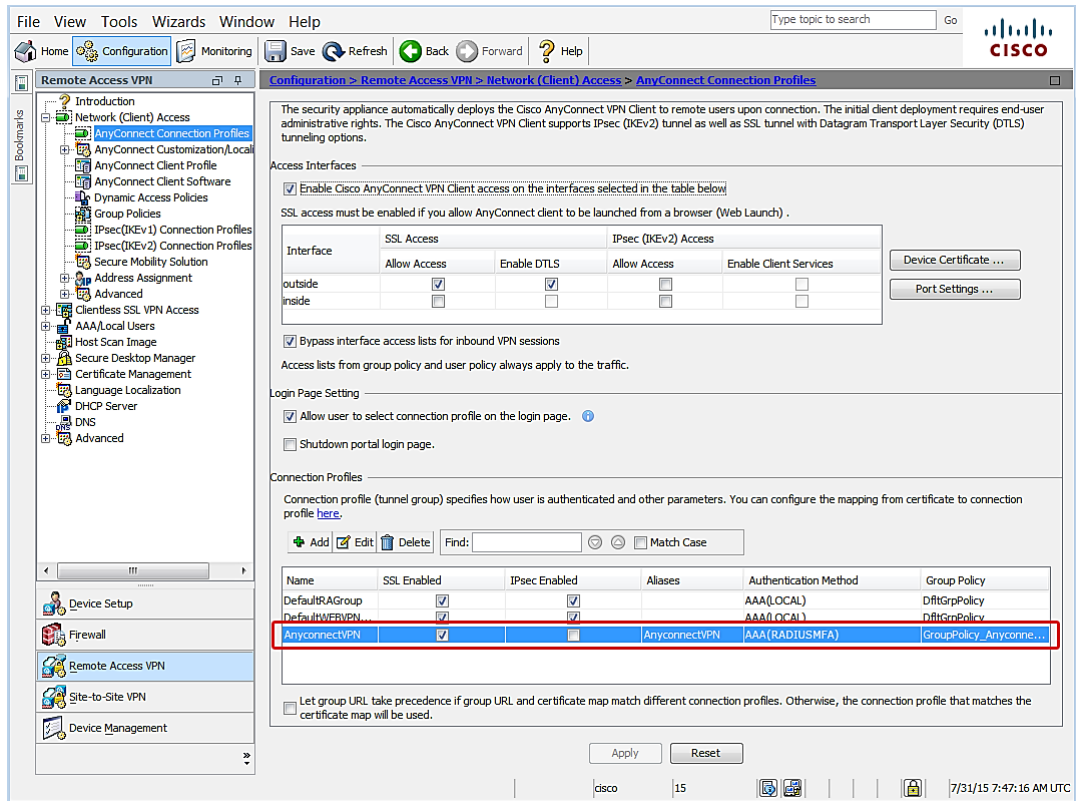
Find:

 Match Case

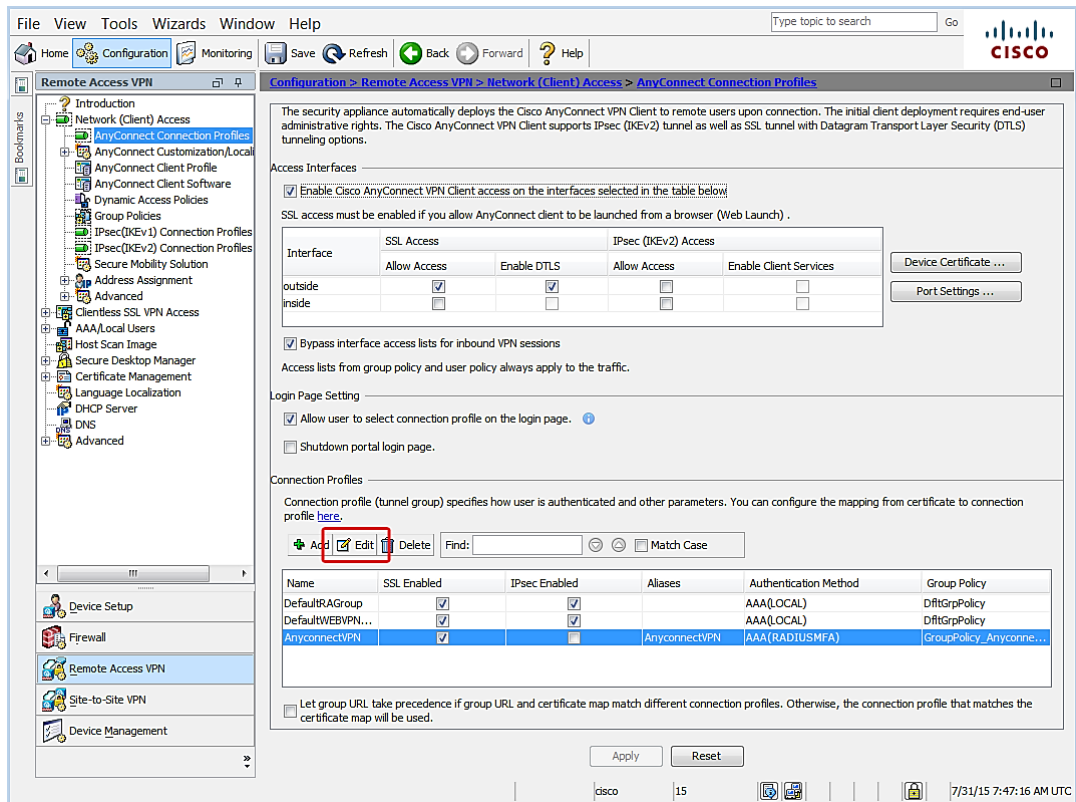
Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultTRAGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPN...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
AnyconnectVPN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AnyconnectVPN	AAA(RADIUSMFA)	GroupPolicy_Anyconne...

Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

c. Connection Profiles – select the AnyConnect VPN profile.



d. Click Edit.



e. The Edit AnyConnect Connection Profile window opens.

Edit AnyConnect Connection Profile: AnyconnectVPN

Basic | **Advanced**

Name: AnyconnectVPN
Aliases: AnyconnectVPN

Authentication

Method: AAA Certificate Both

AAA Server Group: LDAPMFA Manage...

Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

None DHCP Link DHCP Subnet

Client Address Pools: VPN_Pool Select...

Client IPv6 Address Pools: Select...

Default Group Policy

Group Policy: GroupPolicy_AnyconnectVPN Manage...

(Following field is an attribute of the group policy selected above.)

Enable SSL VPN client protocol

Enable IPsec(IKEv2) client protocol

DNS Servers: 192.168.31.4

WINS Servers:

Domain Name: example.com

Find: Next Previous

OK Cancel Help

f. Navigate to **Authentication | Method**.

Edit AnyConnect Connection Profile: AnyconnectVPN

Basic
Advanced

Name: AnyconnectVPN
Aliases: AnyconnectVPN

Authentication

Method: AAA Certificate Both

AAA Server Group: LDAPMFA Manage...

Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

None DHCP Link DHCP Subnet

Client Address Pools: VPN_Pool Select...

Client IPv6 Address Pools: Select...

Default Group Policy

Group Policy: GroupPolicy_AnyconnectVPN Manage...

(Following field is an attribute of the group policy selected above.)

Enable SSL VPN client protocol

Enable IPsec(IKEv2) client protocol

DNS Servers: 192.168.31.4

WINS Servers:

Domain Name: example.com

Find: Next Previous

OK Cancel Help

- g. Confirm the following:
 - i. **Method** – make sure **AAA** is selected.
 - ii. **AAA Server Group** – make sure the group created for the MFA server is selected.
- h. Click **OK**.
- i. Click **Apply** to save the configuration.

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

Access Interfaces

Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Bypass interface access lists for inbound VPN sessions

Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

Allow user to select connection profile on the login page.

Shutdown portal login page.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Add Edit Delete Find: Match Case

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPN...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
AnyconnectVPN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AnyconnectVPN	AAA(RADIUSMFA)	GroupPolicy_Anyconne...

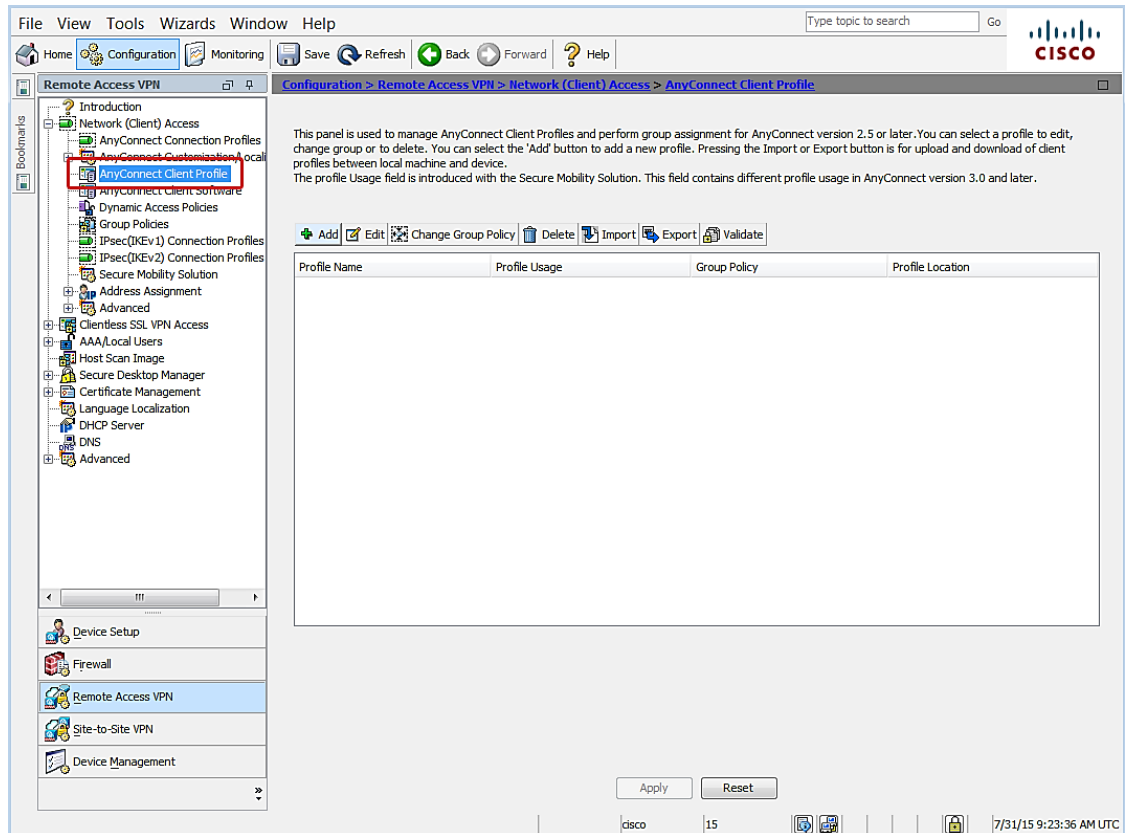
Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

Apply Reset

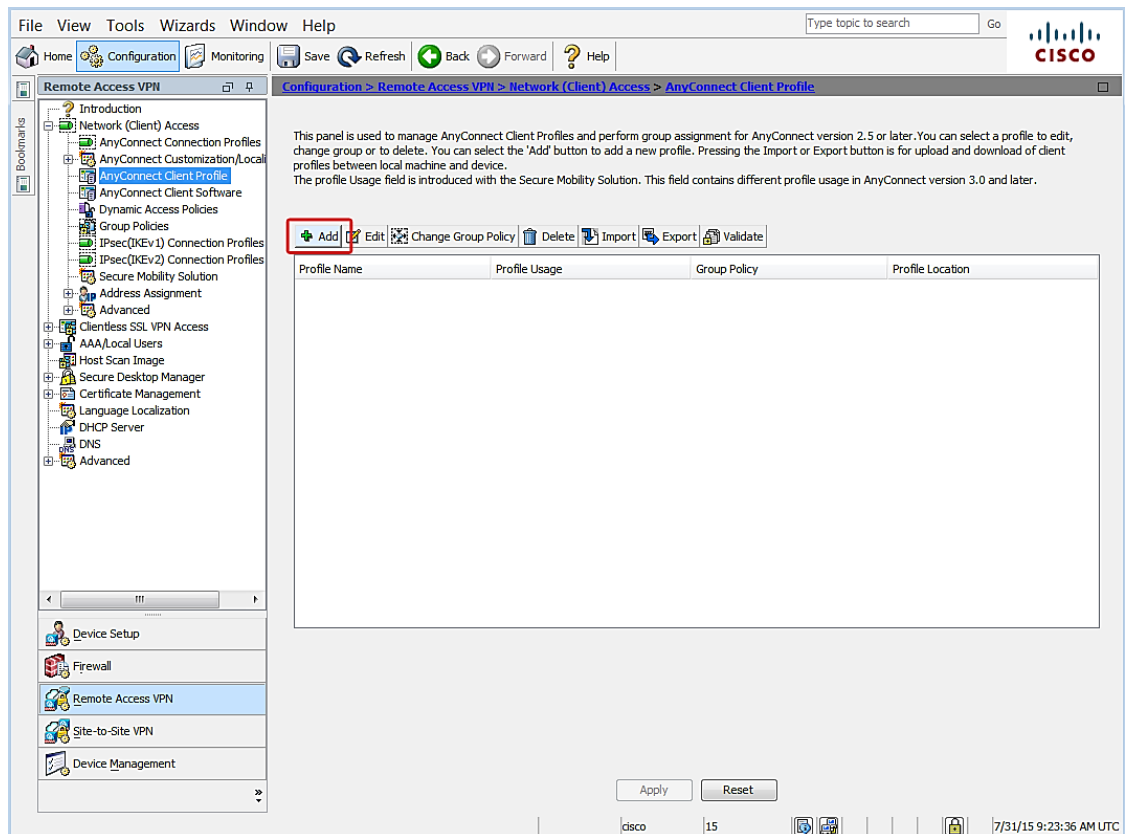
disco 15 7/31/15 7:47:16 AM UTC

Configure Timeout

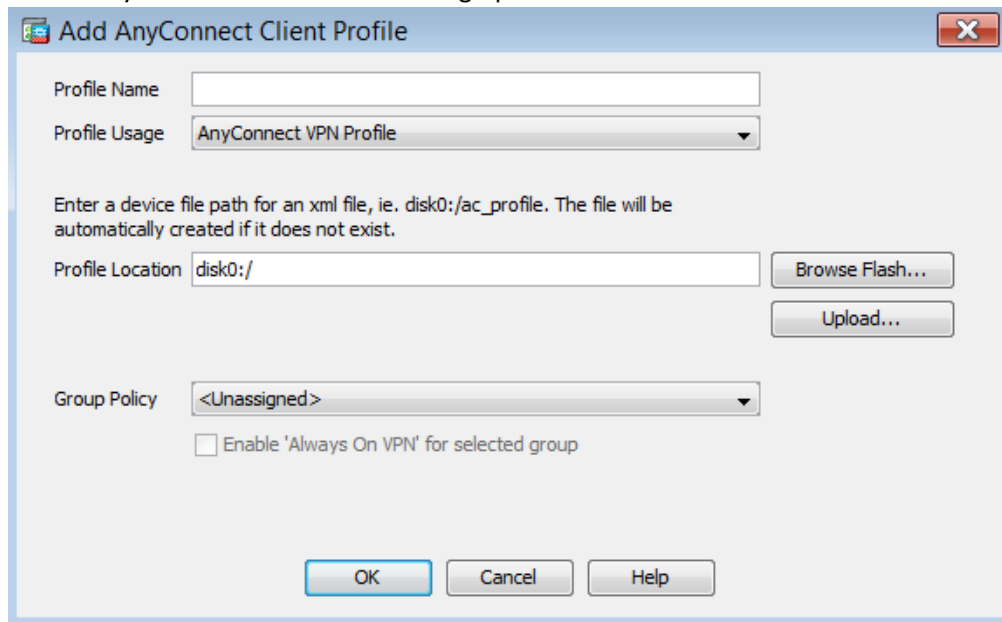
1. Navigate to **Remote Access VPN | Network (Client) Access | AnyConnect Client Profile.**



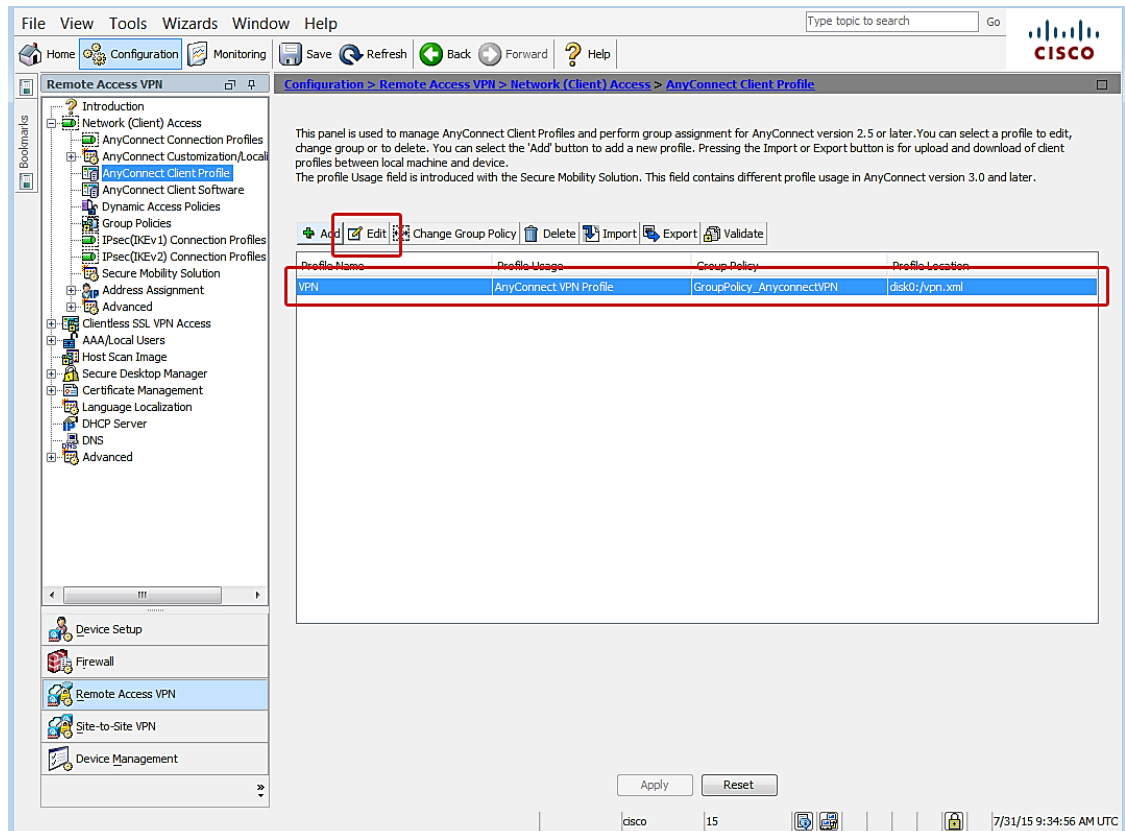
2. Click Add.



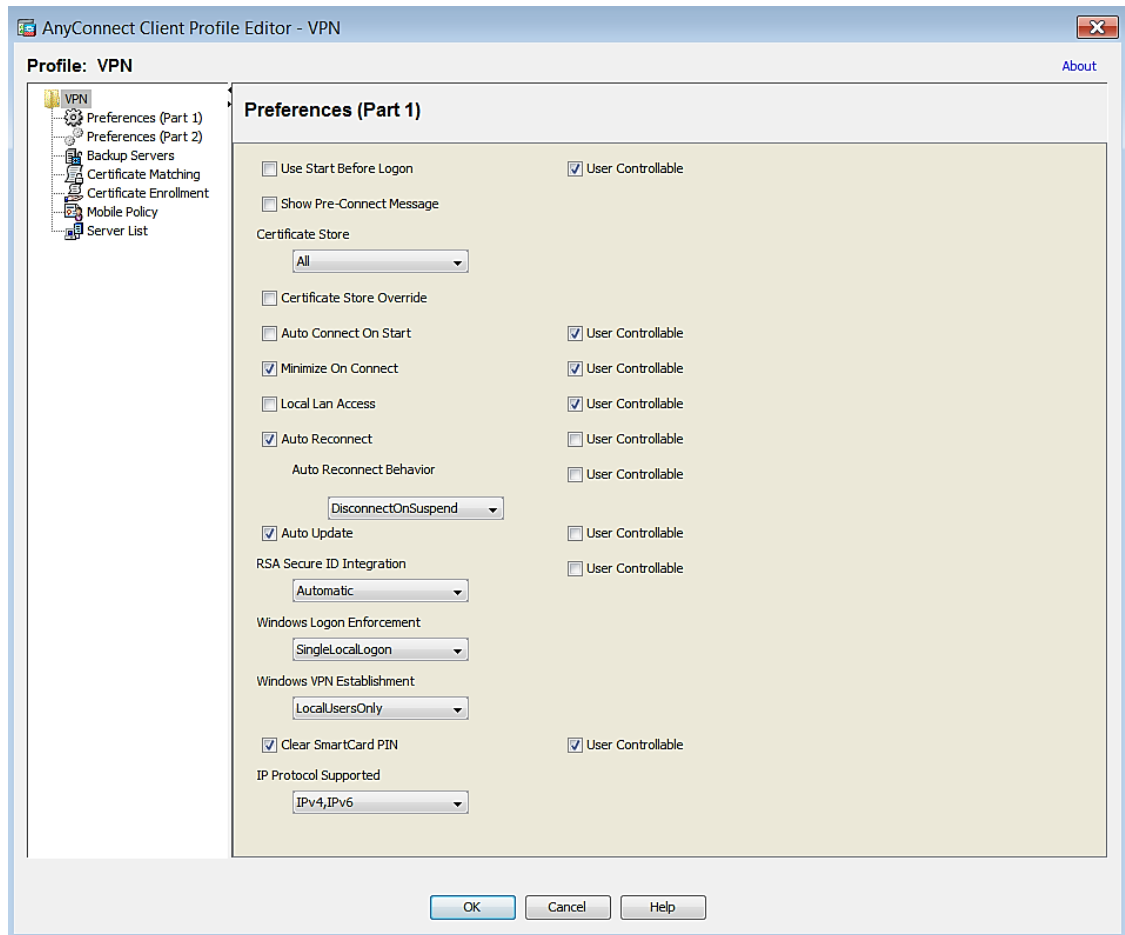
- The Add AnyConnect Client Profile dialog opens.



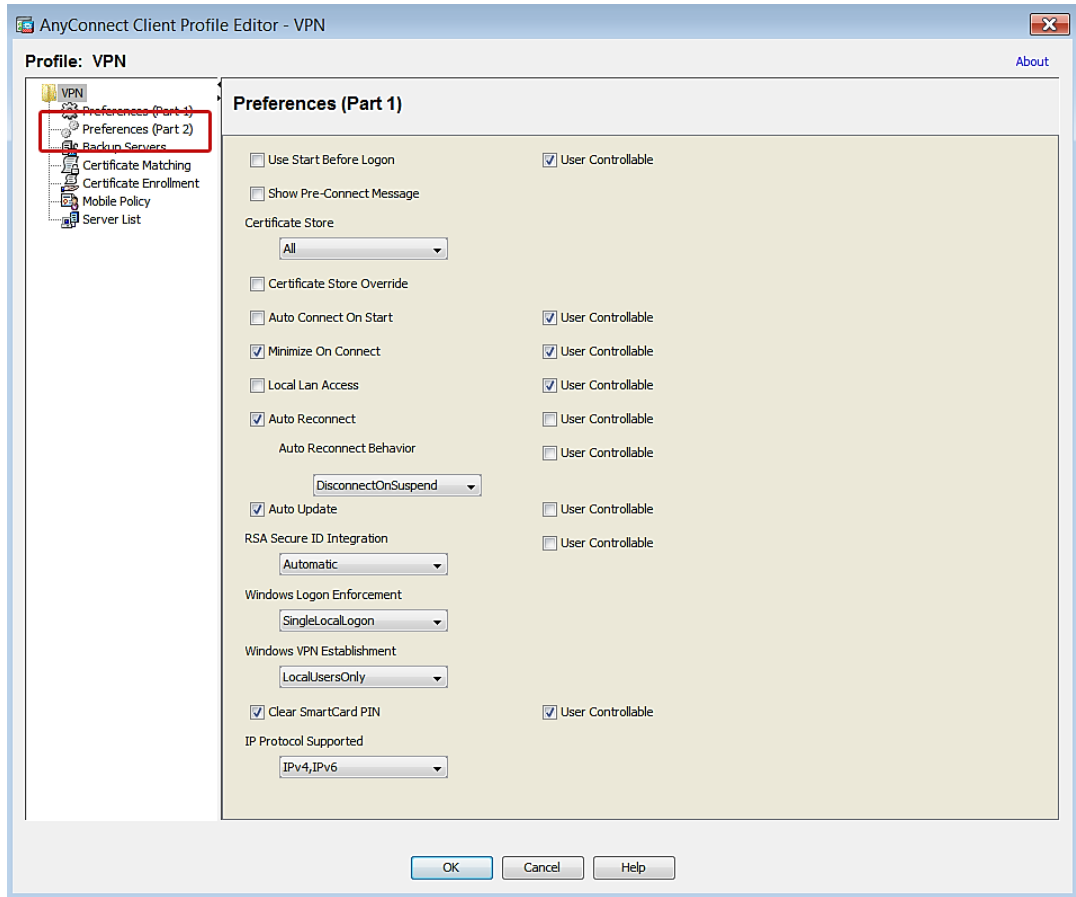
- Leave the default settings, except for the following:
 - Profile Name** – enter a descriptive name for the new VPN profile.
 - Click **OK**.
- Select the VPN Profile that was created and click **Edit**.



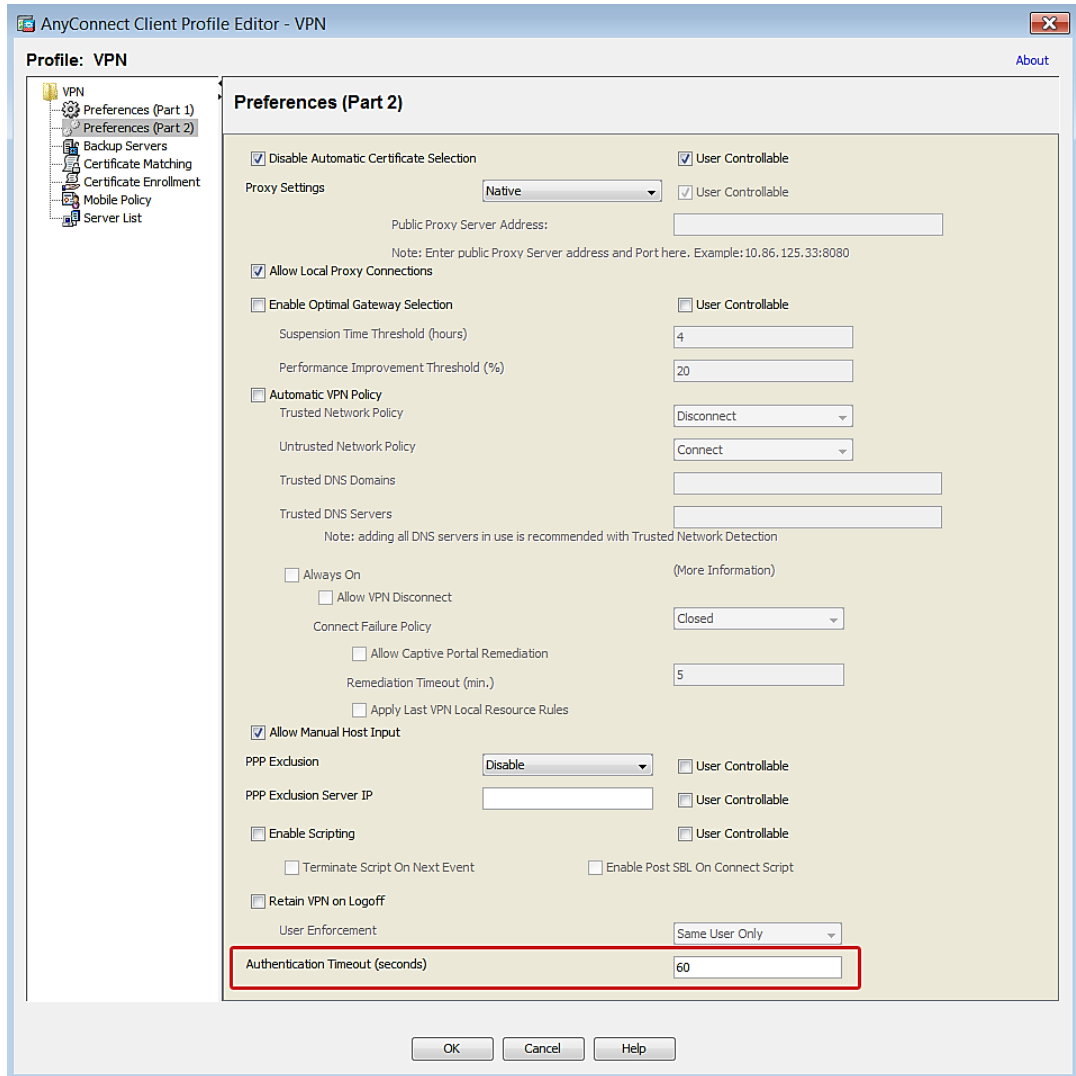
- The AnyConnect Client Profile Editor opens.



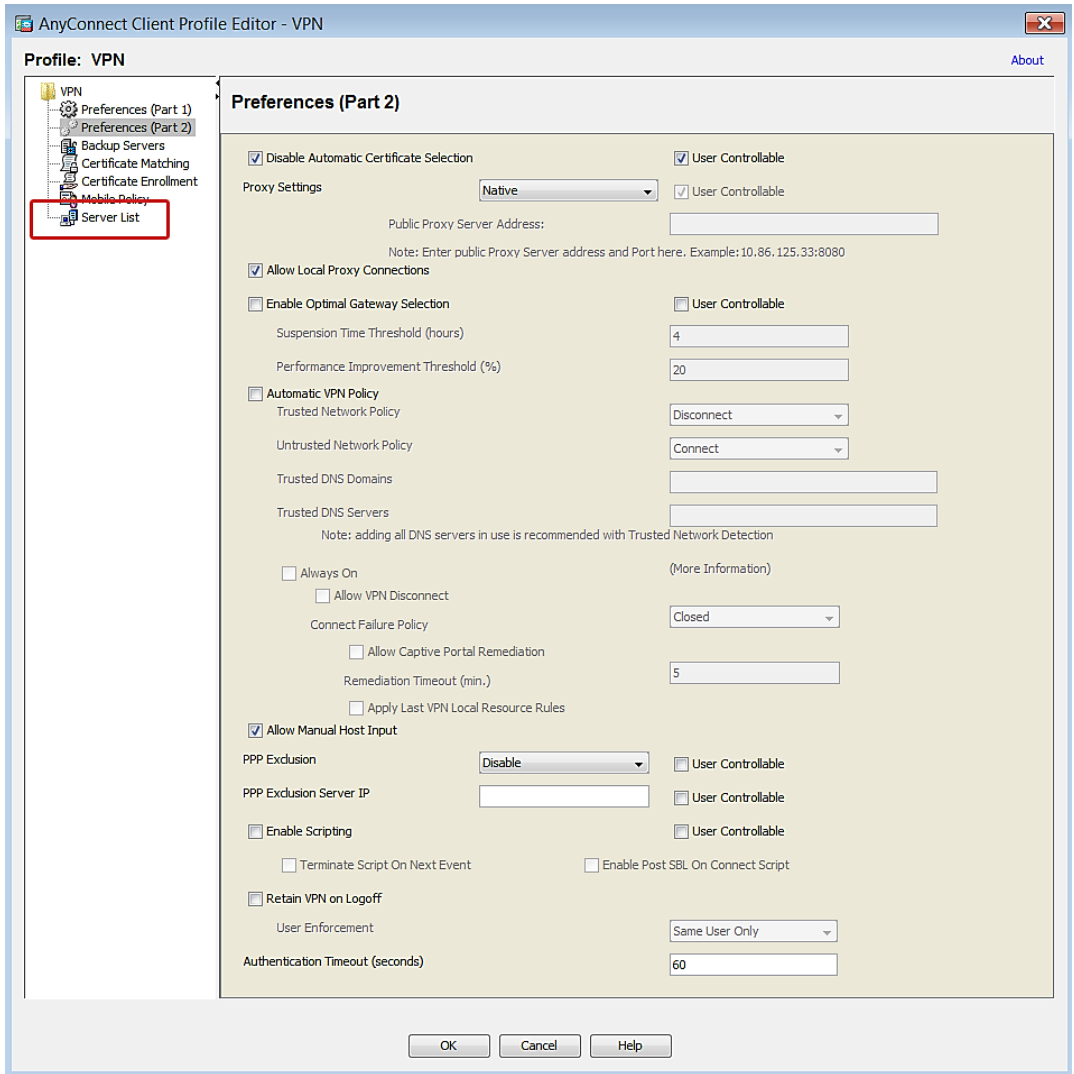
7. Leave default settings except for the following:
 - a. Click **Preferences (Part 2)**.



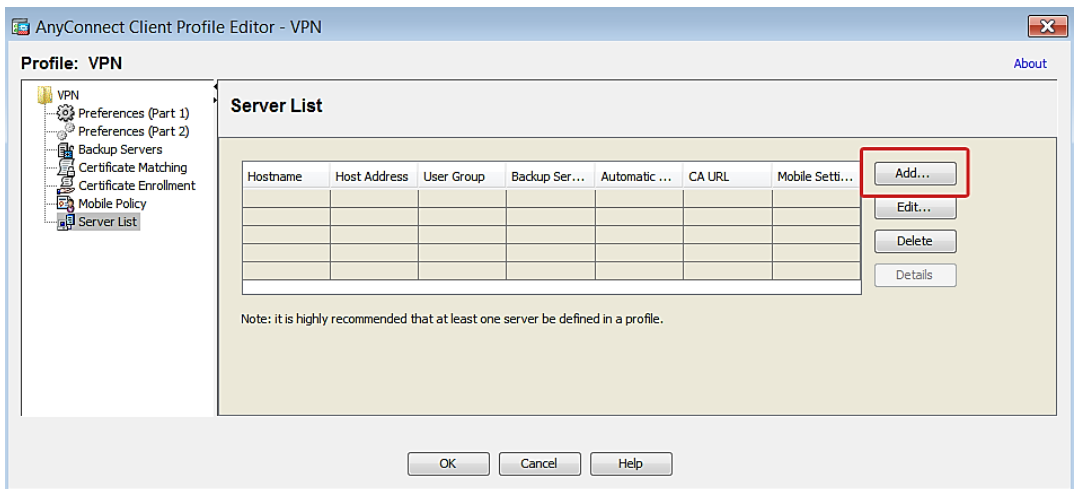
b. Navigate to **Authentication Timeout (seconds)**.



- c. Change the value to **60** seconds. Large organizations may require a longer duration.
- d. Click **Server List**.



e. Click **Add**.



f. Add the Cisco ASA **Host Display Name** and the **FQDN/IP Address** to the profile.

Server List Entry

Host Display Name (required)

FQDN or IP Address / User Group

Group URL

Additional mobile-only settings Edit...

Backup Server List

Host Address Add Move Up Move Down Delete

Load Balancing Server List

Always On is disabled. Load Balancing Fields have been disabled.

Host Address Add Delete

Primary Protocol ASA gateway SSL Auth Method During IKE Negotiation EAP-AnyCon... IKE Identity (IOS gateway only)

Automatic SCEP Host CA URL Prompt For Challenge Password CA Thumbprint

OK Cancel

- g. Click **OK**.
- h. Click **OK** to save configuration changes to the VPN profile.

AnyConnect Client Profile Editor - VPN

Profile: VPN About

VPN

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Server List

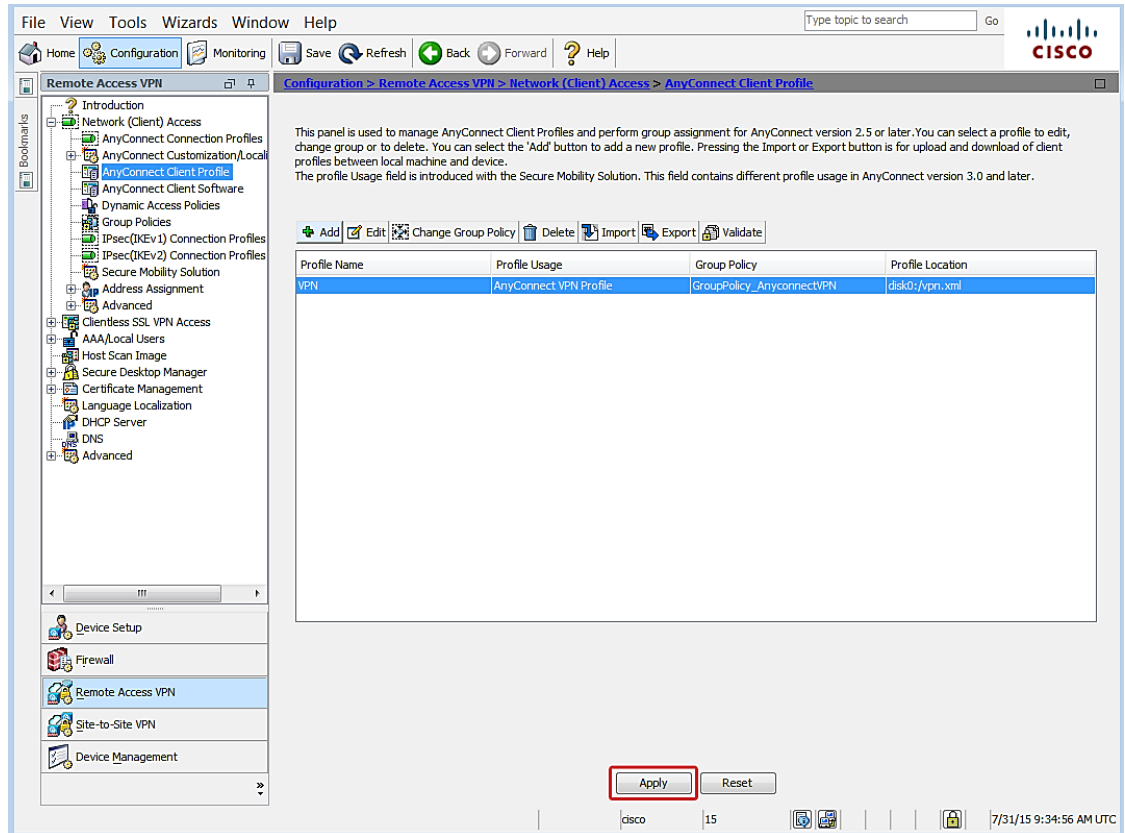
Hostname	Host Address	User Group	Backup Ser...	Automatic ...	CA URL	Mobile Setti...
discoasa	172.16.1.1		-- Inherited --			

Add... Edit... Delete Details

Note: it is highly recommended that at least one server be defined in a profile.

OK Cancel Help

- 8. Click **Apply** to save the configuration.



IMPORTANT: The AnyConnect Client Profile you just created must be installed on every device that will use MFA authentication to avoid timeout issues during the login process. One way to accomplish this would be to require clients to connect to the AnyConnect portal and then push the profile automatically.

You have completed VPN appliance setup.

Step 3: Test Authentication

The topics below are provided to help test authentication with the setup you just completed. Login instructions are provided for each of the authentication methods. Device registration instructions are included for deployments that use the mobile app authentication method; if you aren't going to use mobile app, then skip straight to the [Login](#) section.

Device Registration for Azure Authenticator Users

This step only applies when the mobile app authentication method is used.

The following instructions explain how to activate a user device through the MFA server Users Portal. Please note the following requirements prior to getting started.

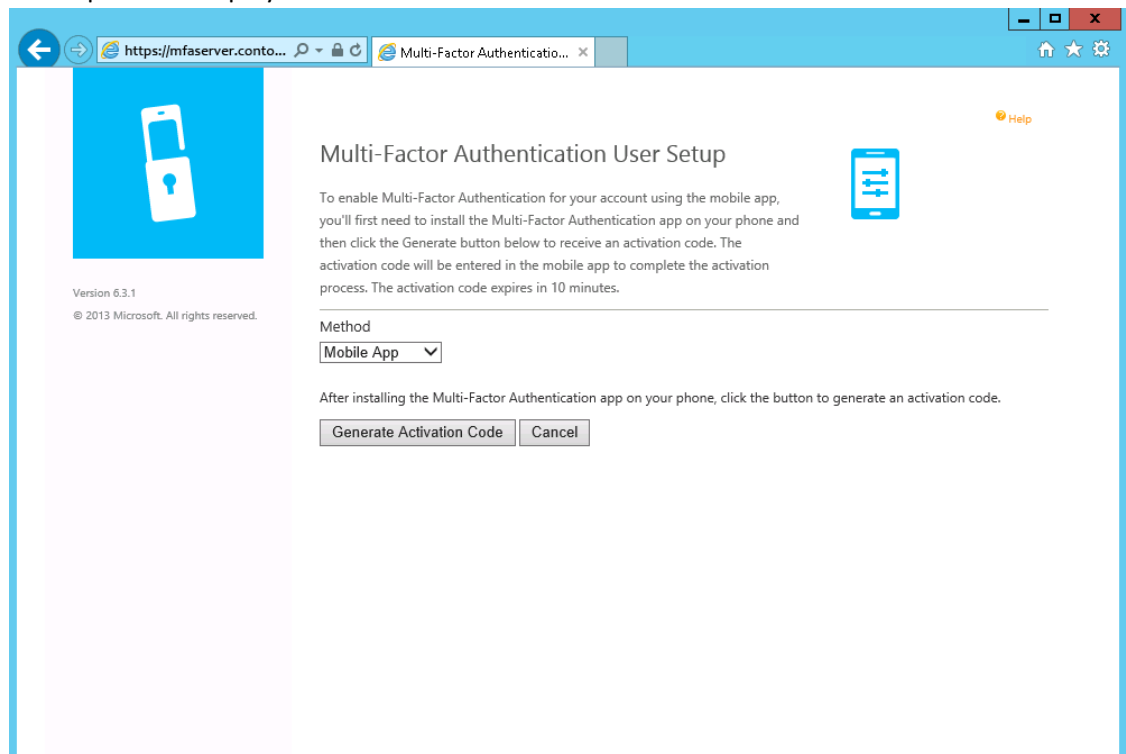
Requirements

- A device with the Azure Authenticator mobile application installed. The application can be downloaded from the platform store for the following devices:
 - Windows Phone
 - Android
 - iOS
- The Azure Users Portal address.
- A computer to access the Users Portal.
- User credentials

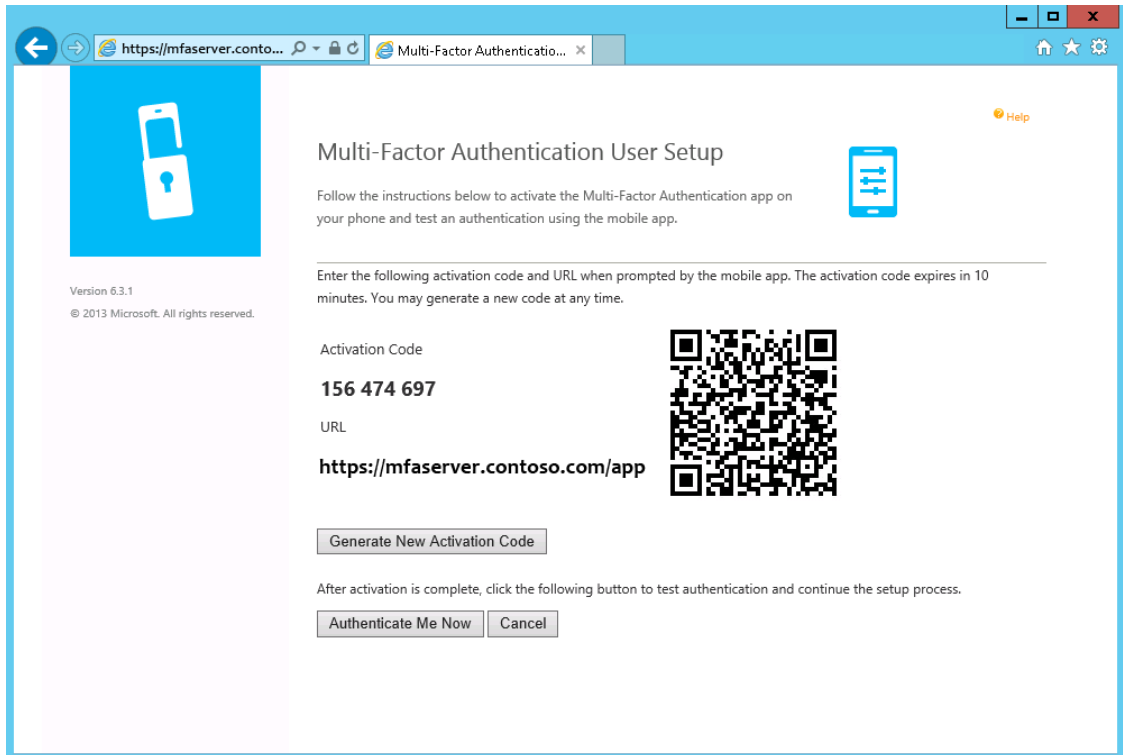
Activate Device

NOTE: Information provided below is current as of the publication date, but is subject to change without notice.

1. Log in to the Azure user portal from a computer.
2. The setup screen displays.

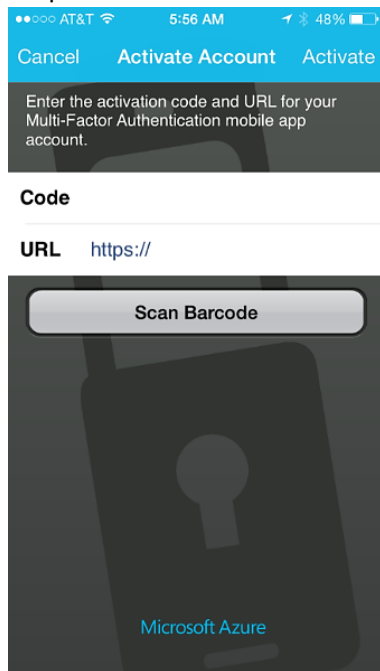


3. Click **Generate Activation Code**.
4. Activation code options will display.



5. Open the mobile authentication app on the user device.

Example:



6. There are two options:
 - Enter the Activation Code and URL displayed on the Users Portal screen on the device activation screen.
 - Use the device to scan the barcode displayed on Users Portal screen.

You have completed device activation.

Login

Now you are ready to test MFA authentication. Please note the requirements listed below before you start.

General Requirements

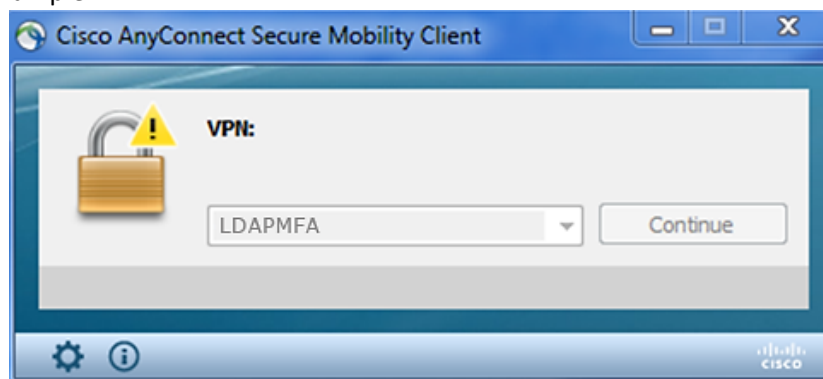
- The Cisco AnyConnect VPN Client Profile installed on the device that will access the network
- The IP address or hostname for AnyConnect VPN access
- User credentials

Phone Call

Required: A phone with the number listed in the AD user account **Mobile** phone attribute.

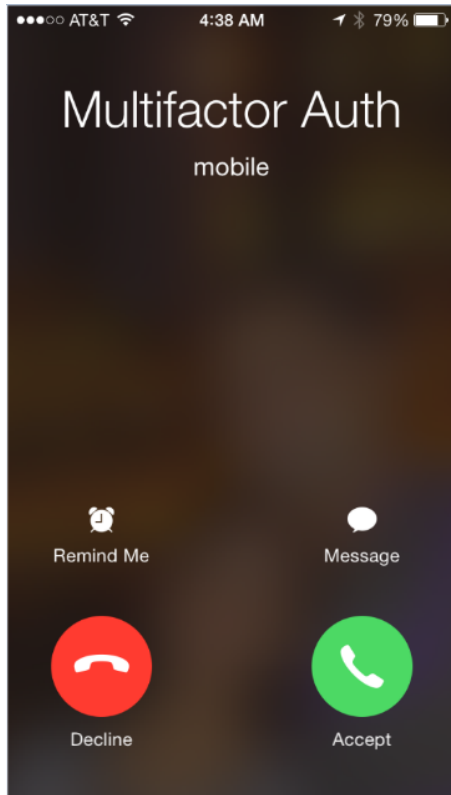
1. On a computer, launch the AnyConnect client and connect to the network.

Example:



2. Enter user credentials.
 3. Check the phone for a call.
- NOTE: The call originates in the cloud from the Azure MFA application.

Example:



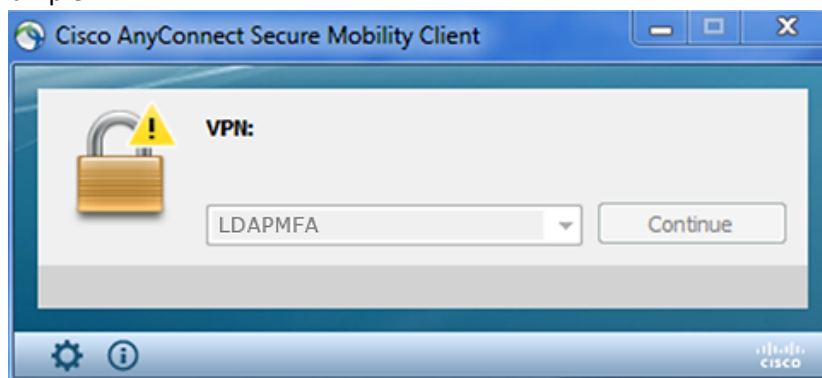
4. The phone call will provide instructions to complete authentication.

Text Message

Required: An SMS-capable phone with the number listed in the user account **Mobile** phone attribute

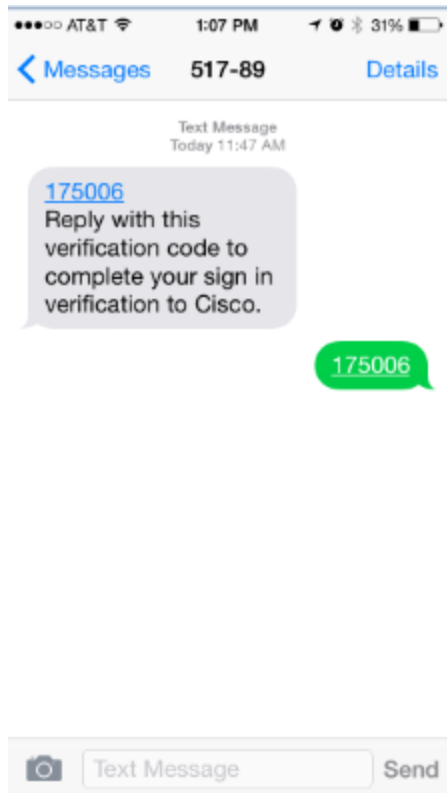
1. On a computer, launch the AnyConnect client and connect to the network.

Example:



2. Enter user credentials.
3. Check the phone for a text message with the verification code.

Example:



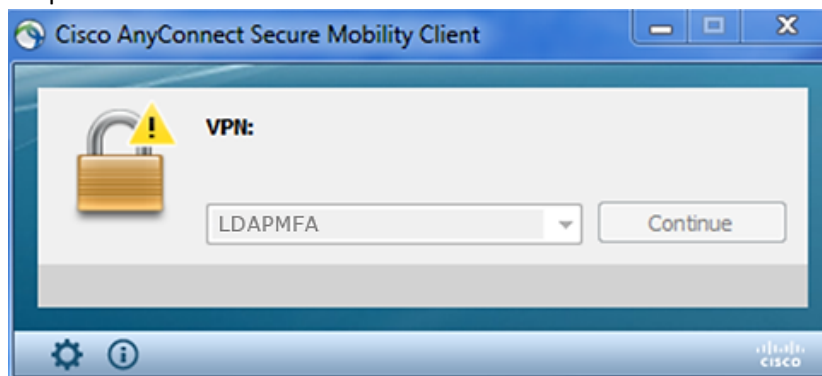
4. Reply to the text message with the same verification code.

Mobile App

Required: A device with the Azure Authenticator app activated.

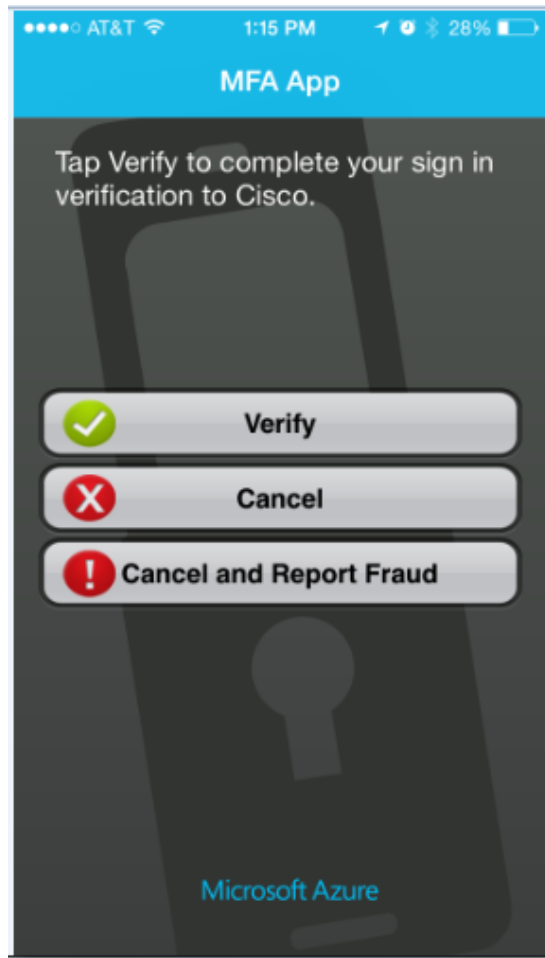
1. On a computer, launch the AnyConnect client and connect to the network.

Example:



2. Enter user credentials.
3. Check the device with Azure Authenticator for a prompt.

Example



4. Click **Verify**.
5. The authentication application will communicate with the MFA server to complete authentication.

Successful authentication for the VPN connection is indicated by the client. Example:



This completes the setup and testing for Azure Multi-Factor Authentication using the LDAP protocol in a Cisco ASA/AnyConnect VPN appliance deployment.