Citrix NetScaler SSL VPN and Azure MFA Configuration for RADIUS

Published October, 2015

Version 1.0

Azure Multi-Factor Authentication seamlessly integrates with your Citrix NetScaler SSL VPN appliance to provide additional security for VPN logins and VPN 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 the RADIUS protocol. 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 options for RADIUS:
* One-way messaging requires users to enter a sent verification code in a prompt on the login page.
* Two-way messaging requires users to send the 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.
* OATH token – users have a token that generates a verification code which is then entered in a prompt on the portal login page. Azure supports two options:
* Third-party OATH tokens can be imported to the system and synced with user accounts. A common example is a hardware token like a key fob.
* The Azure Authenticator app for smart devices can serve as an OATH token to generate verification codes for Windows Phone, iOS, and Android devices.

This guide will help you to configure Azure MFA server and Citrix NetScaler SSL VPN to use the RADIUS protocol for authentication.

# Overview

The Azure Multi-Factor Authentication server acts as a RADIUS server. The Citrix NetScaler SSL VPN appliance acts a RADIUS client. The RADIUS 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 RADIUS 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

# 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](#parameters_prereq) and [Components](#parameters_components) sections. The [Conventions](#parameters_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 virtual server configured on the NetScaler appliance to use for MFA.
* Familiarity with the following technologies:
* RADIUS configuration
* SSL 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 RADIUS.
* One Citrix NetScaler SSL VPN appliance is configured.

## Conventions

Information is based on the following conditions.

* The guide was written using the Citrix NetScaler VPX virtual appliance.
* Documentation will refer to the Citrix NetScaler appliance as the SSL 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.
* 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

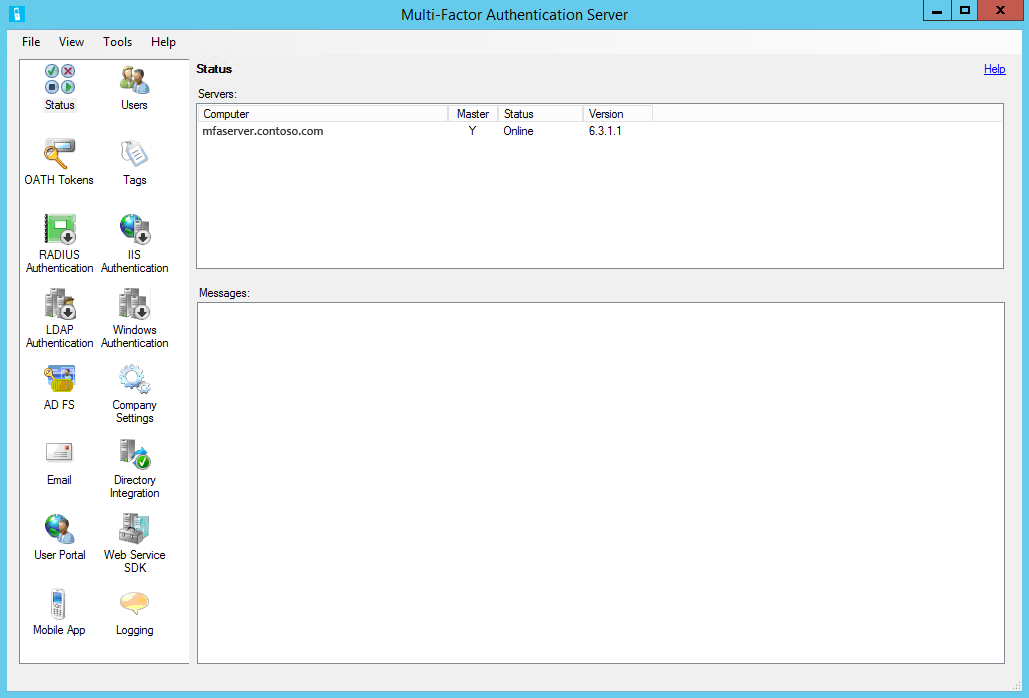
This topic explains how to configure the MFA server and the on-premises resources it requires. First you will log in to the server where MFA is installed. Next you will configure RADIUS Authentication. Then you will connect MFA to the directory service, after which you will configure a default authentication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



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

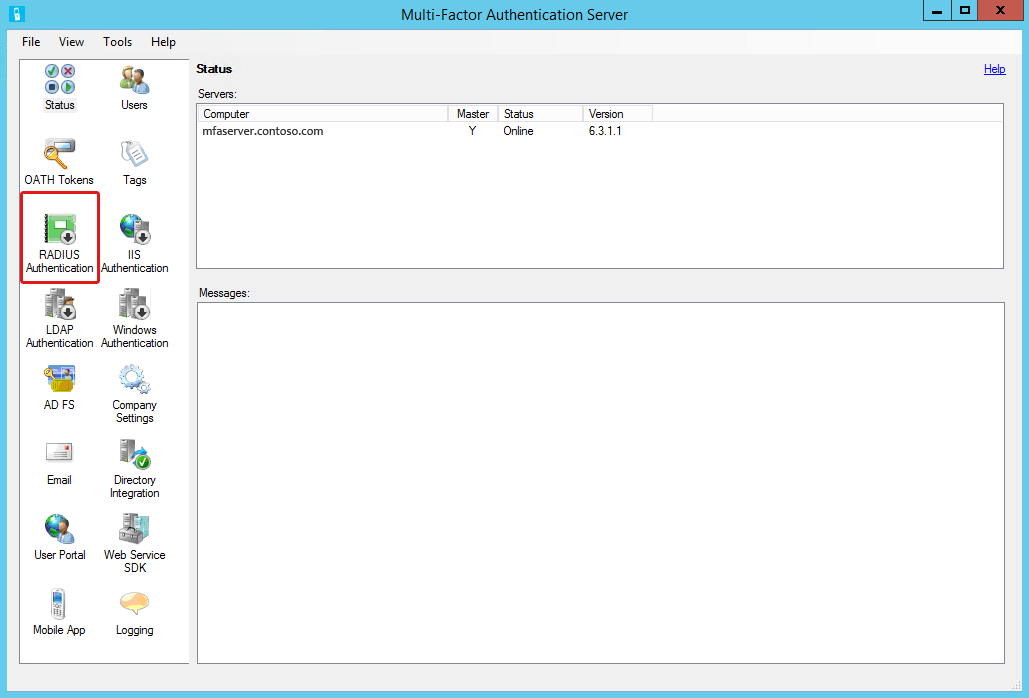


Now you will configure the necessary services.

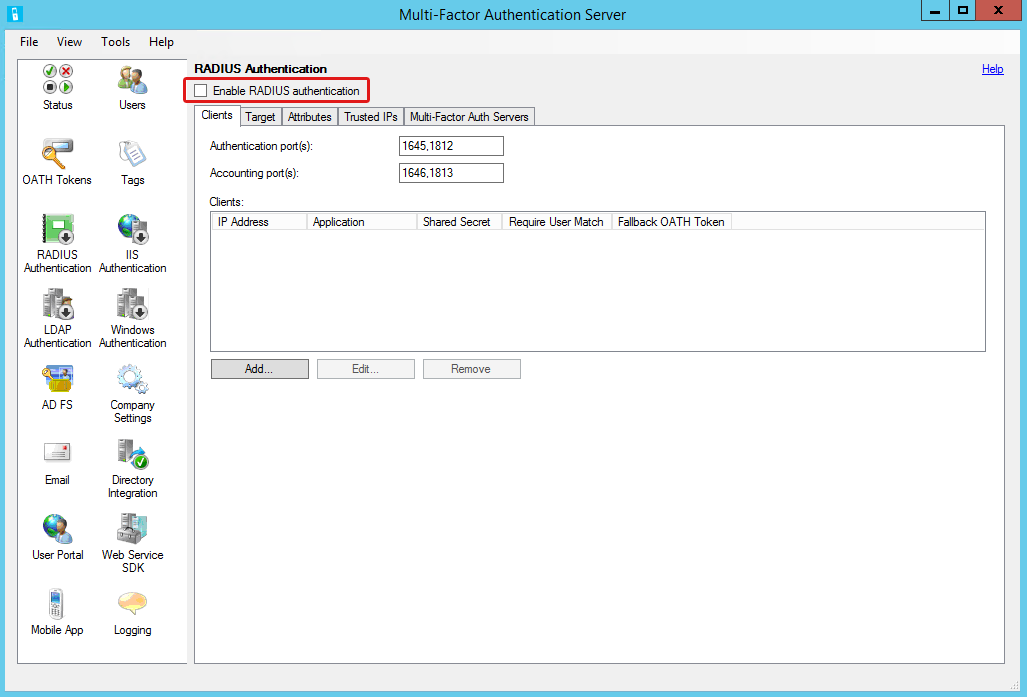
## RADIUS Authentication

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

1. Click the **RADIUS Authentication** icon.

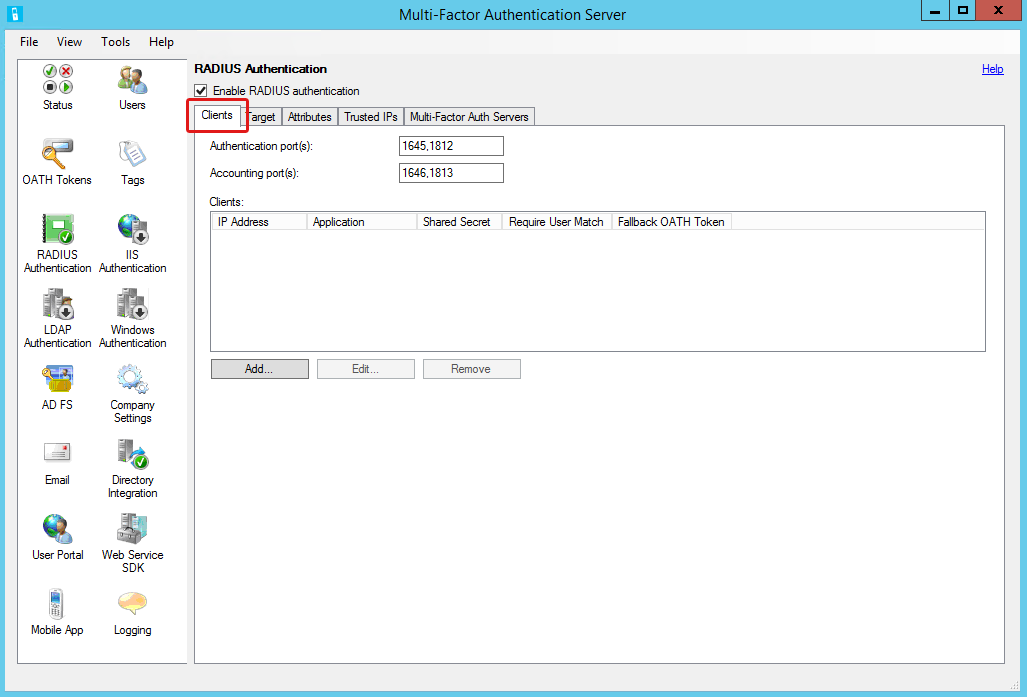


1. When the RADIUS Authentication tool opens, select **Enable RADIUS authentication**.

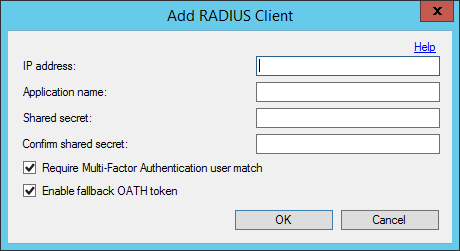


1. Select the **Clients** tab if necessary.

NOTE: Keep track of the port numbers noted for authentication and as you will need them for the SSL VPN appliance [configuration](#configSSLvpn). Authentication defaults are 1645 or 1812.



1. Click **Add** to open the **Add RADIUS Client** dialog box.



1. Complete the following:
2. **IP address** – enter the SSL VPN server address.
3. **Application name** – enter a descriptive name for the SSL VPN server.
4. **Shared secret** – create passphrase to secure the RADIUS communication.

NOTE: The shared secret will be configured on both the MFA server and SSL/VPN server, so keep track of it.

1. **Require Multi-Factor Authentication user match** – select; only users who are included in the MFA [Users](#mfaUsersTool) 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.

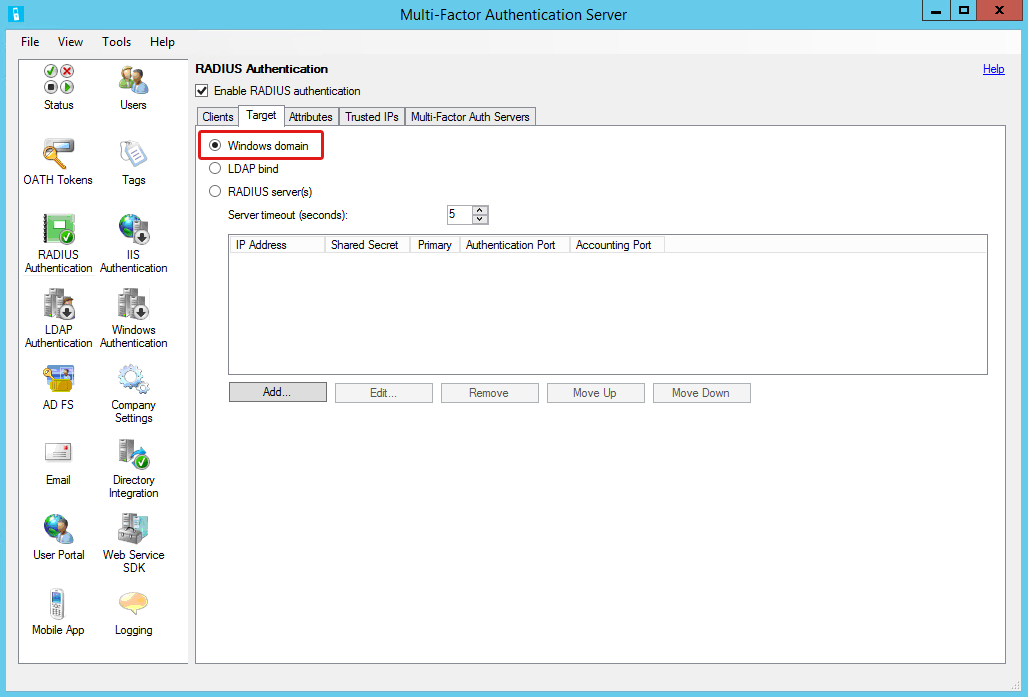
1. **Enable fallback OATH token** – select to provide an alternate method of authentication in the event the default method times out.

NOTE: This feature only applies when OATH token is not the method assigned to a user account. When invoked, the user will be prompted to authenticate with a hardware token if one is registered for the user account.

1. Select the **Target** tab.



1. Select **Windows Domain**; this will configure the MFA server to use AD for primary authentication.

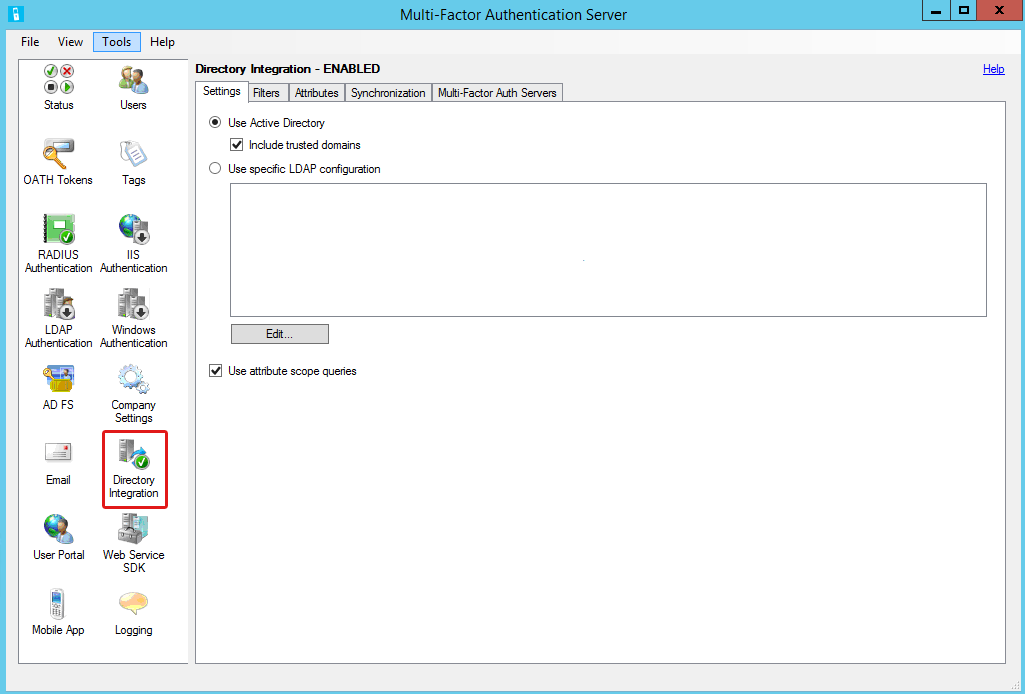


You have completed configuring RADIUS authentication and adding the SSL VPN server as a RADIUS client. Leave the **Multi-Factor Authentication Server** window open for the next task.

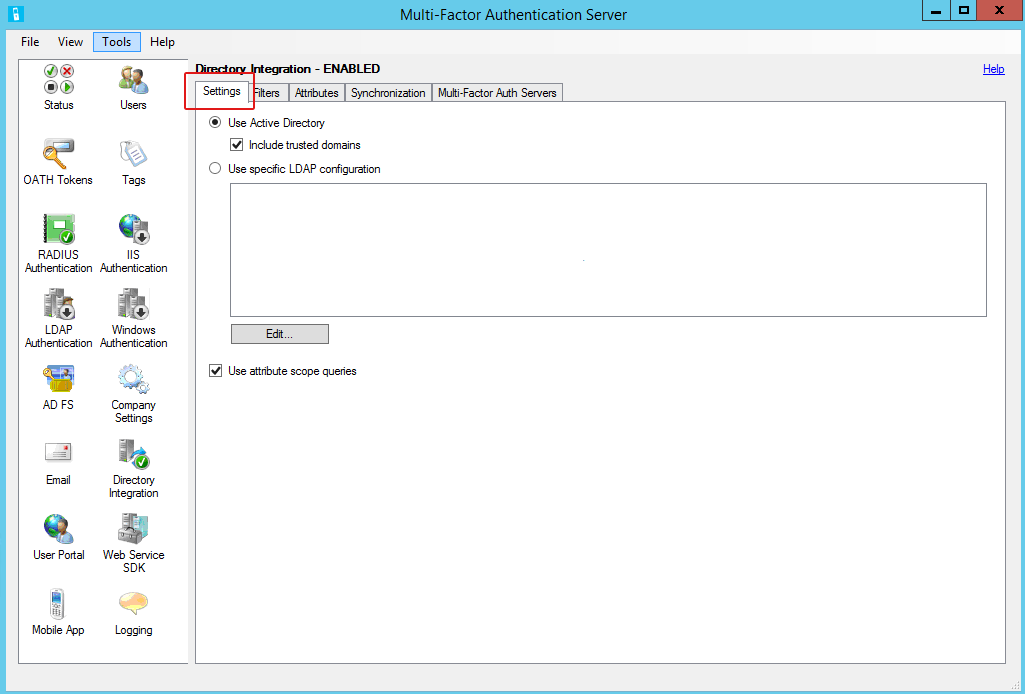
## Directory Integration

Now you will connect to the directory service.

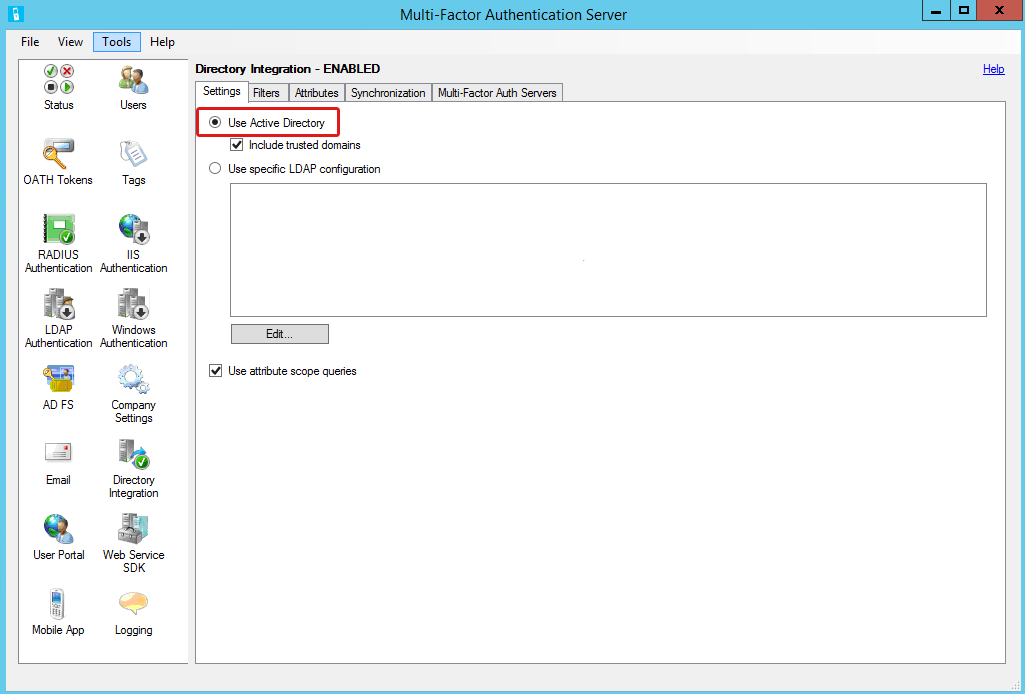
1. In the navigation area, click the **Directory Integration** icon.



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



1. Select **Use Active Directory**.



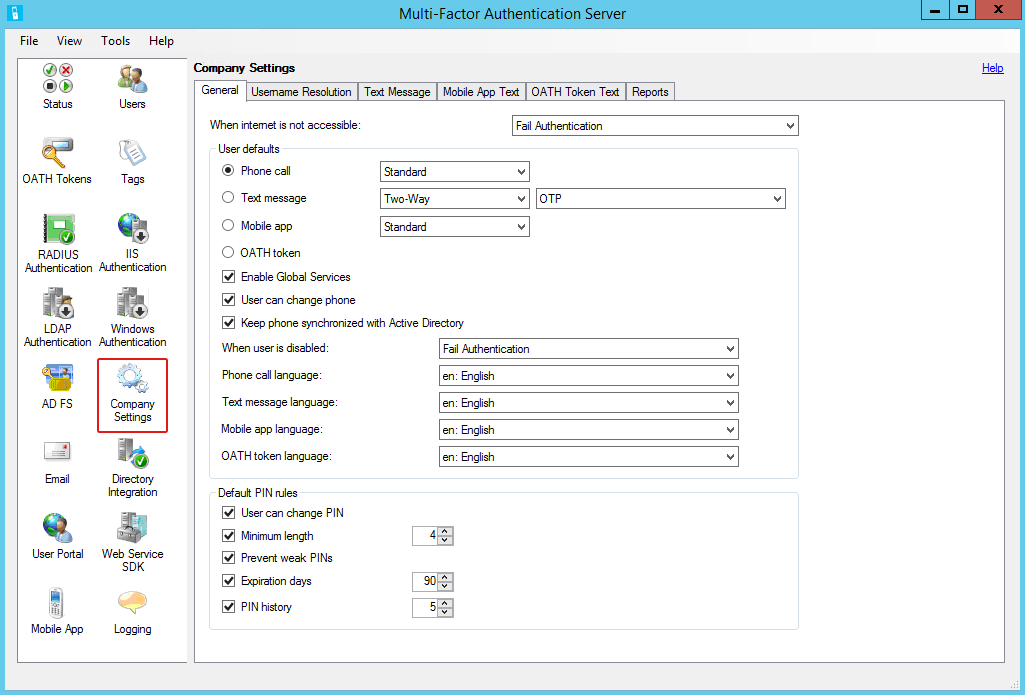
You have completed the MFA server directory service setup. Leave the **Multi-Factor Authentication Server** window open for the next task.

## Default Authentication Method

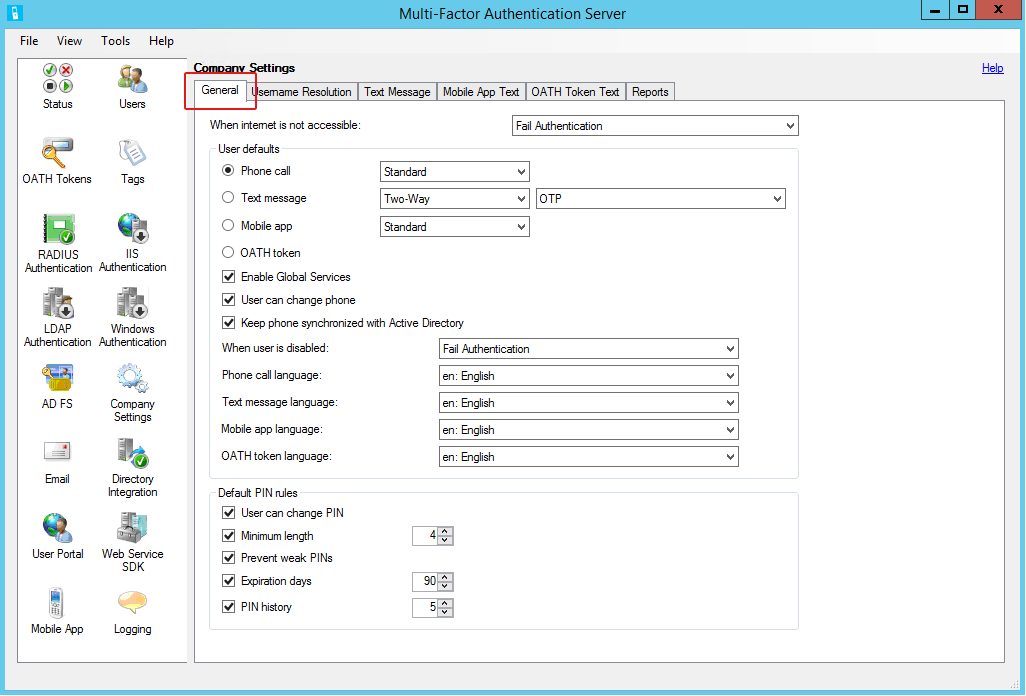
The instructions below explain how to set a default option for the authentication method that will be automatically assigned to MFA user accounts. A default method is required when user are not allowed to change methods. The feature is optional when users are allowed to change their token methods, and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

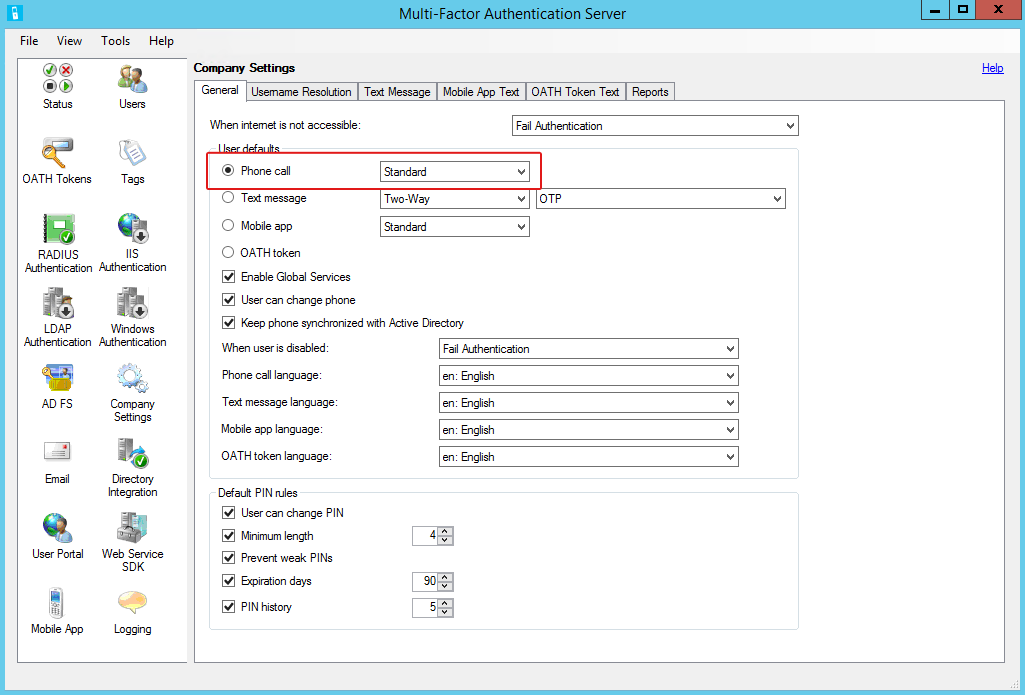


1. When the Company Settings tool opens, select the **General** tab if necessary.

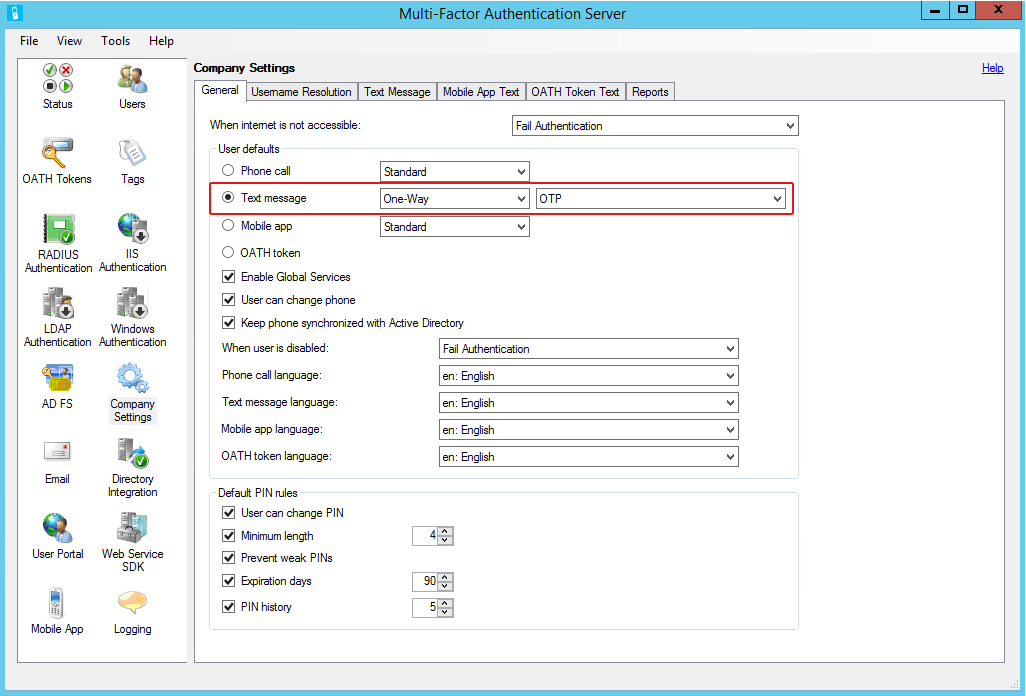


1. Leave default settings except for the following:

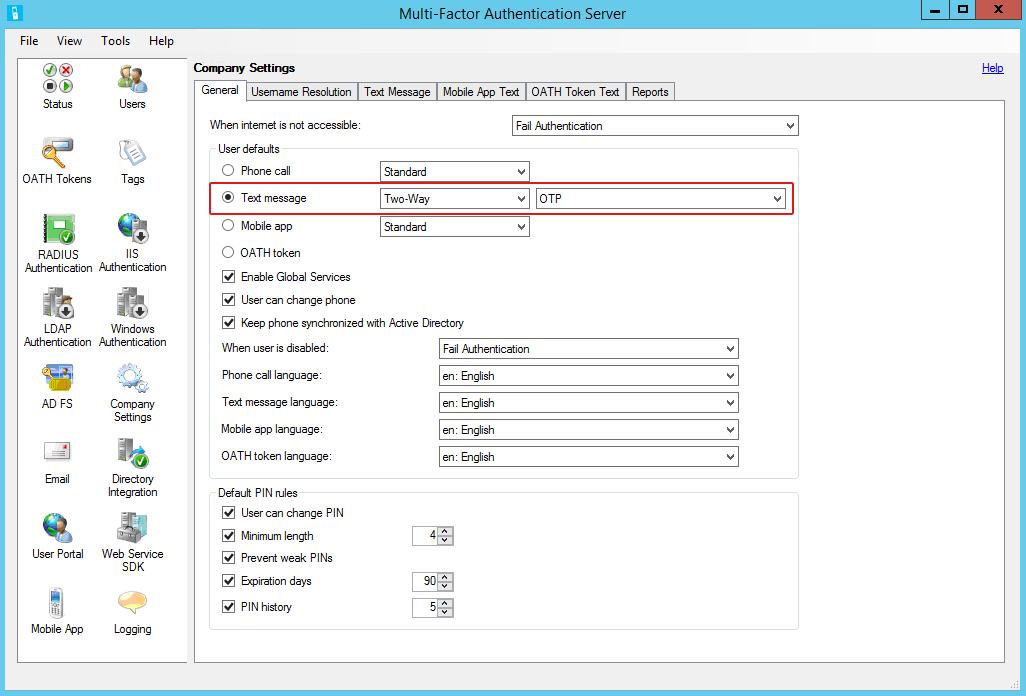
* **User defaults** – select one of the options below:
* **Phone call** – select **Standard** from the drop menu:



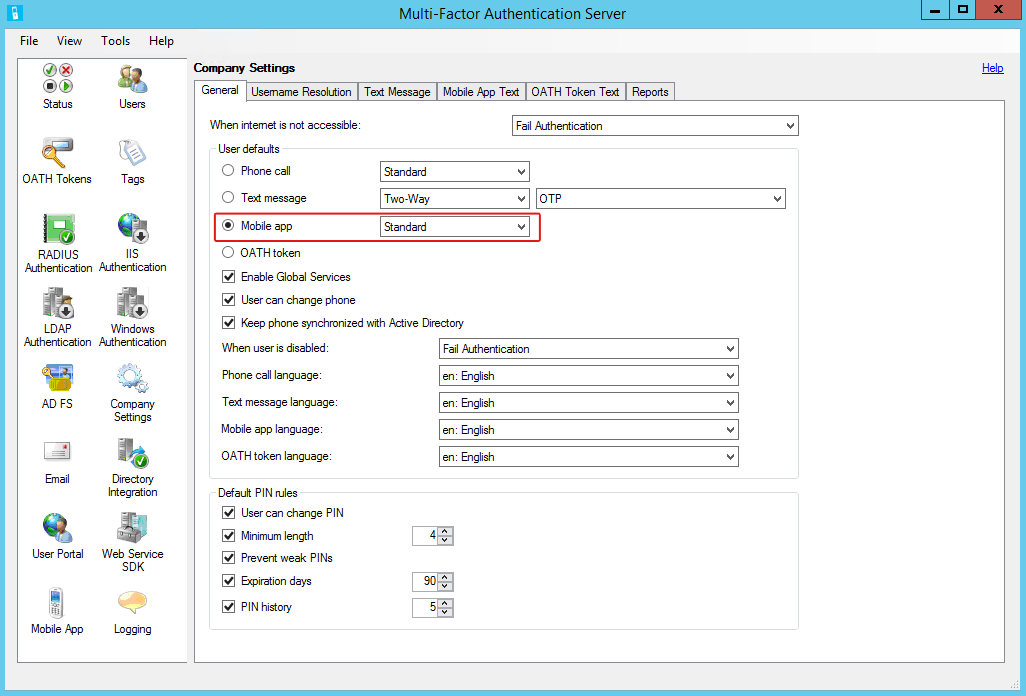
* **Text message** – configure one of the following:
* **One-Way** and **OTP** from the drop menus:



* **Two-Way** and **OTP** from the drop menus:



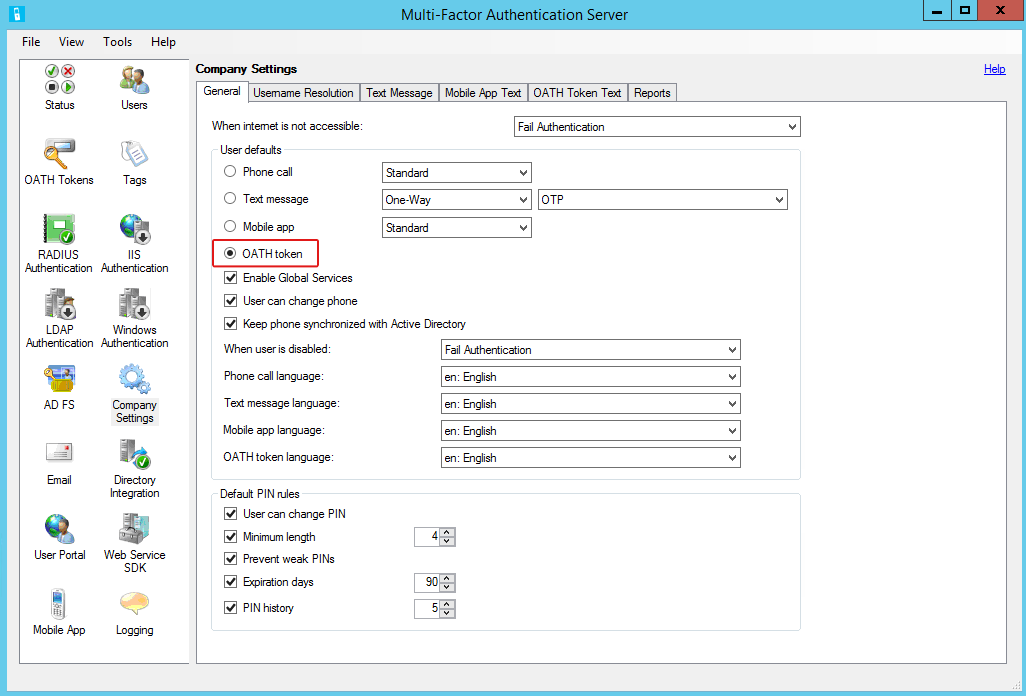
* **Mobile app** – select **Standard** from the drop menu:



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

* **OATH token**

NOTE: This guide provides information about using the OATH token method through the Azure Authenticator app. While third-party tokens can be imported through the Multi-Factor Authentication **OATH Tokens** feature, that function is outside the scope of this this guide.



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

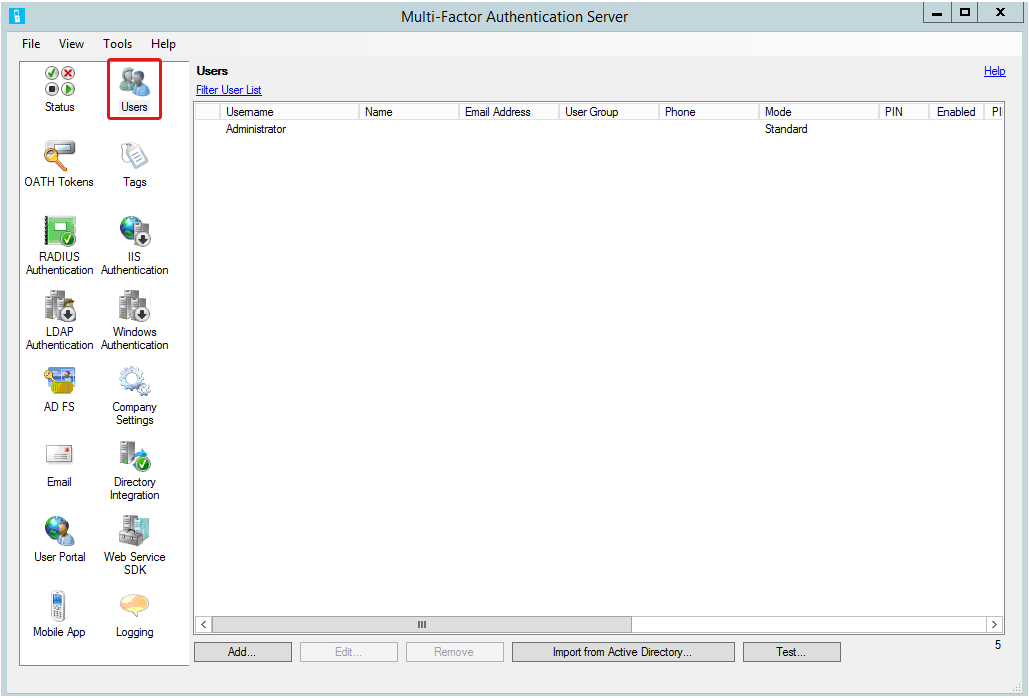
## MFA Users

When the SSL VPN appliance was configured as a RADIUS 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.

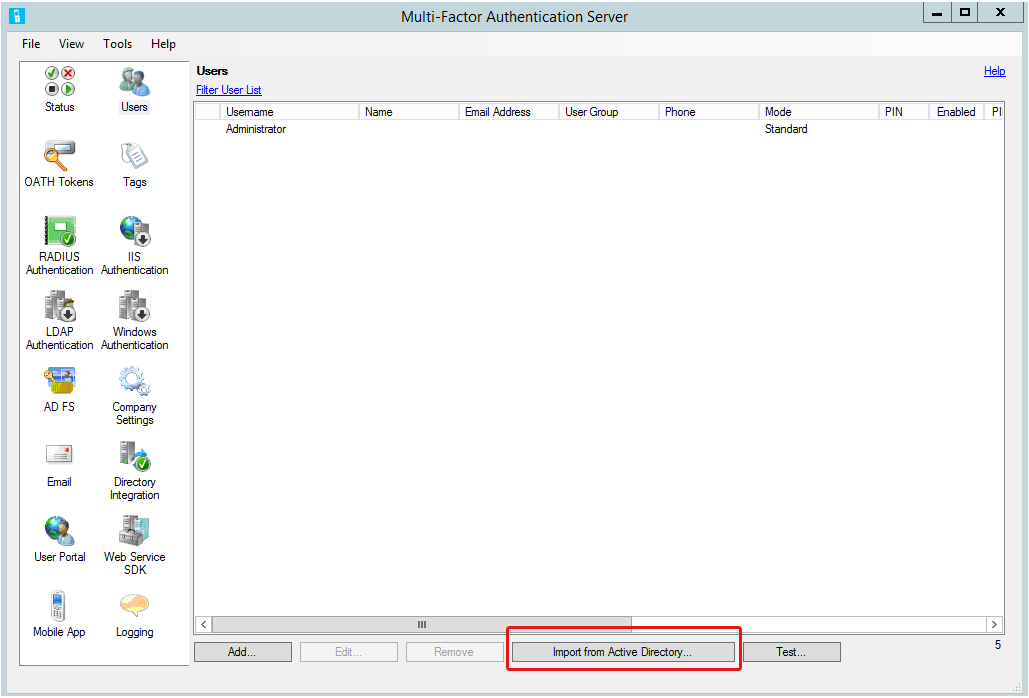
### Import User Accounts

Theses instructions are for on-demand user import.

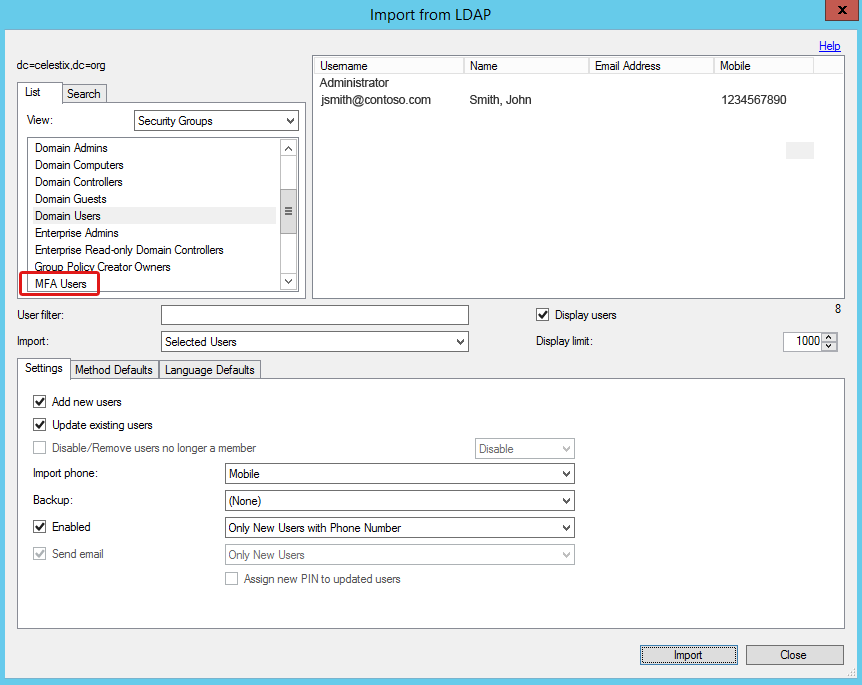
1. In the navigation area, click the **Users** icon.



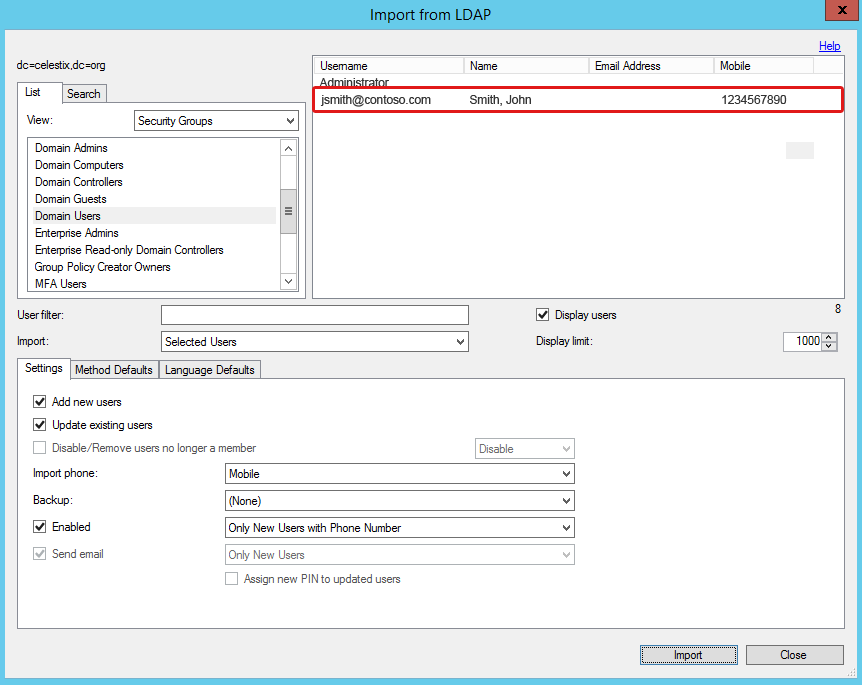
1. When the Users tool opens, Click **Import from Active Directory**.



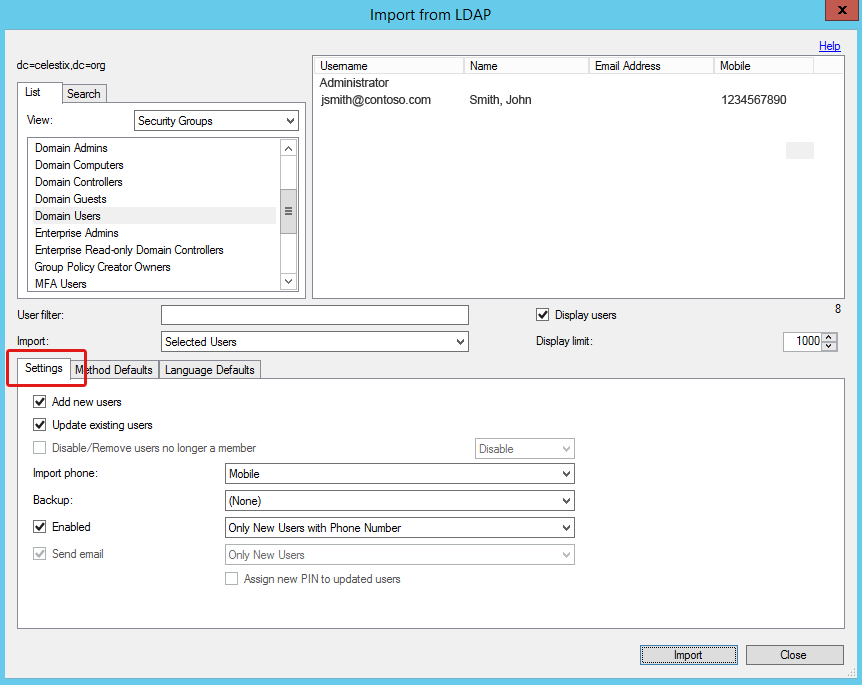
1. On the import screen, select a user group.



1. Select the user accounts you want to import.

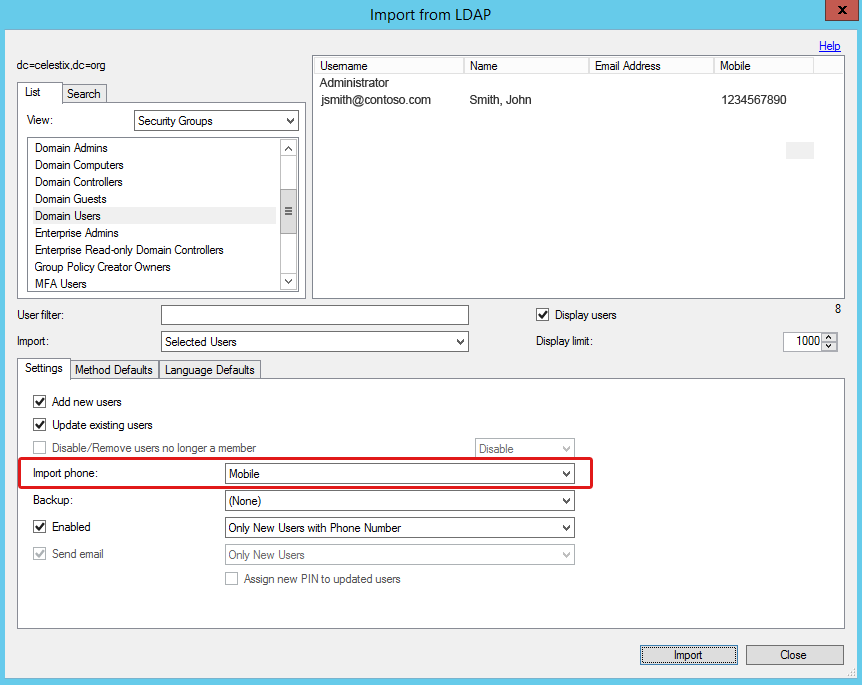


1. Leave the default settings except for the following:
2. Select the **Settings** tab if necessary.

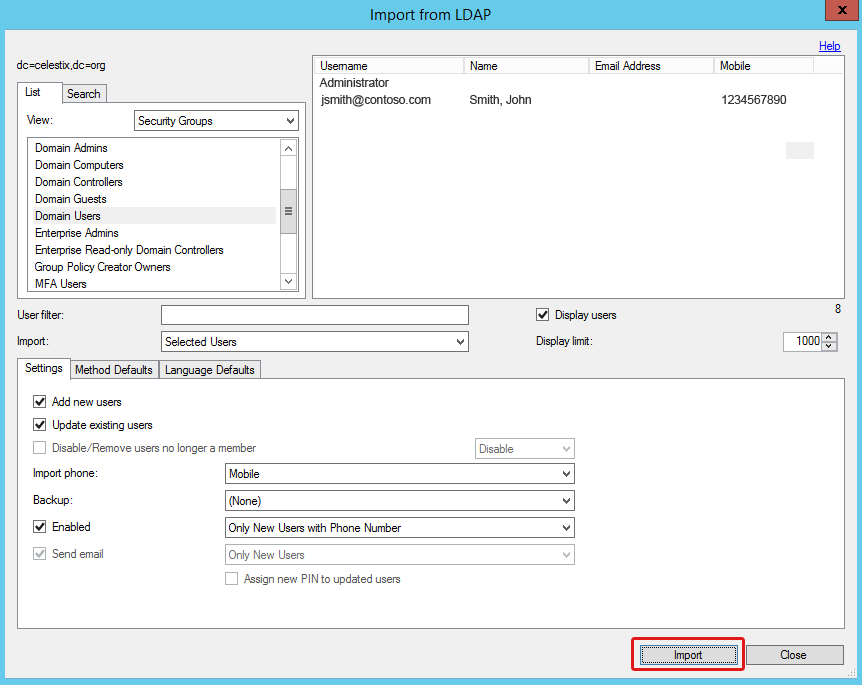


1. In the **Import Phone** drop menu, select **Mobile**.

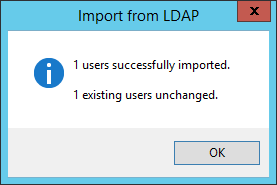
NOTE: For purposes of this guide we are designating the Mobile attribute for the phone import setting. It is the most common option used for MFA.



1. Click the **Import** button.



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



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

You have completed MFA server configuration.

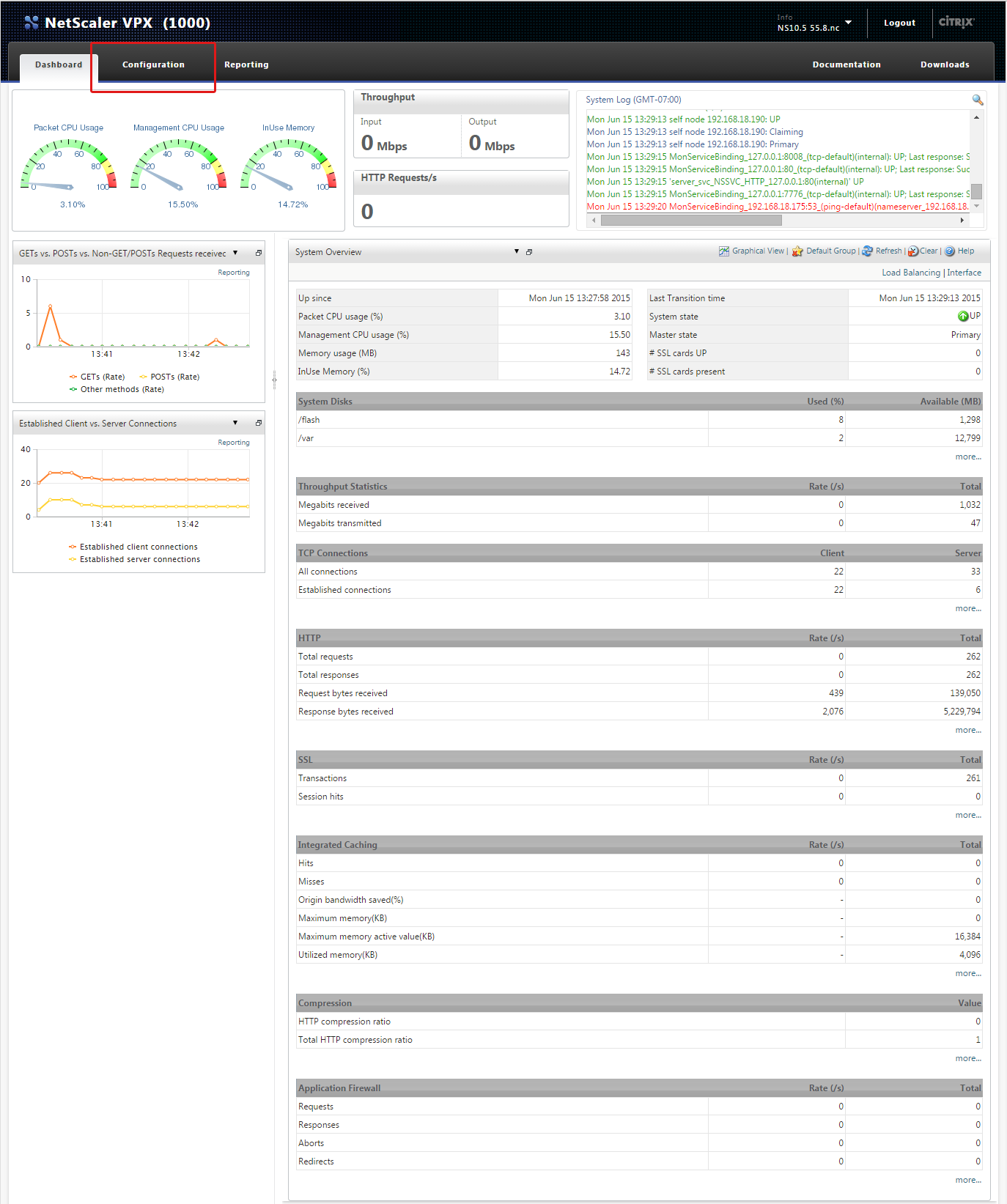
# Step 2: Configure the SSL VPN Appliance

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

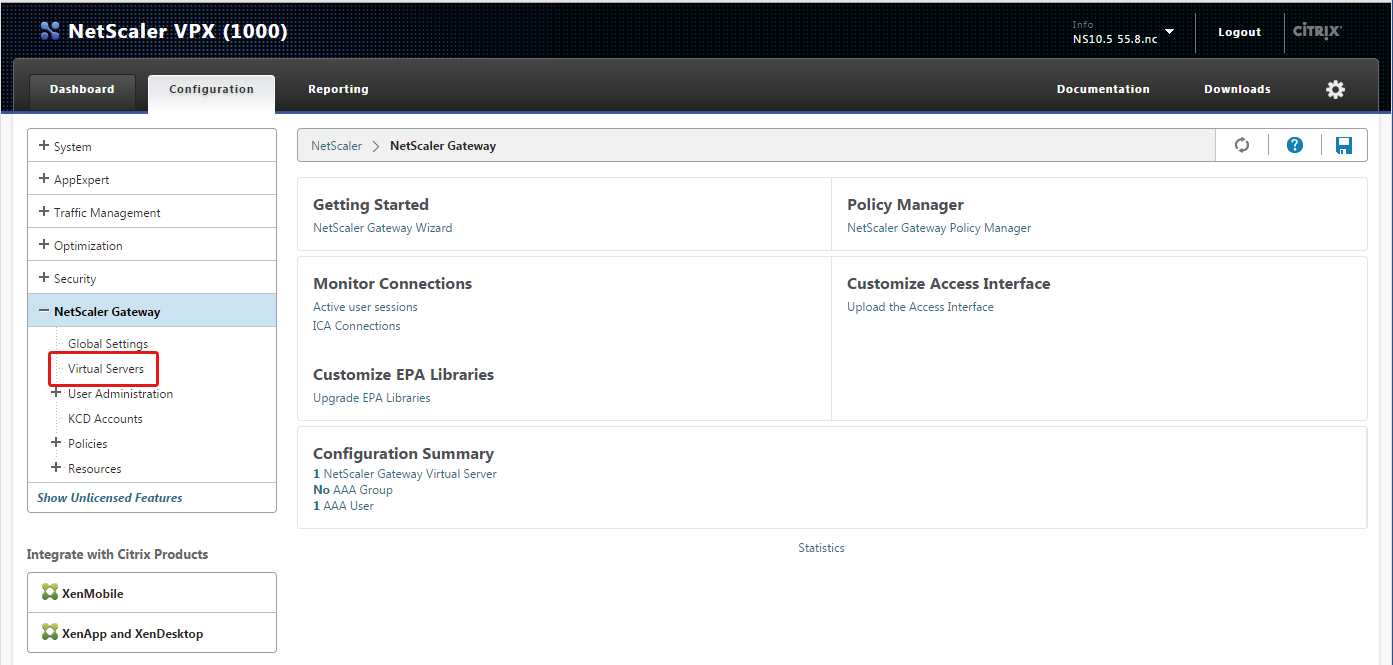
## RADIUS

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

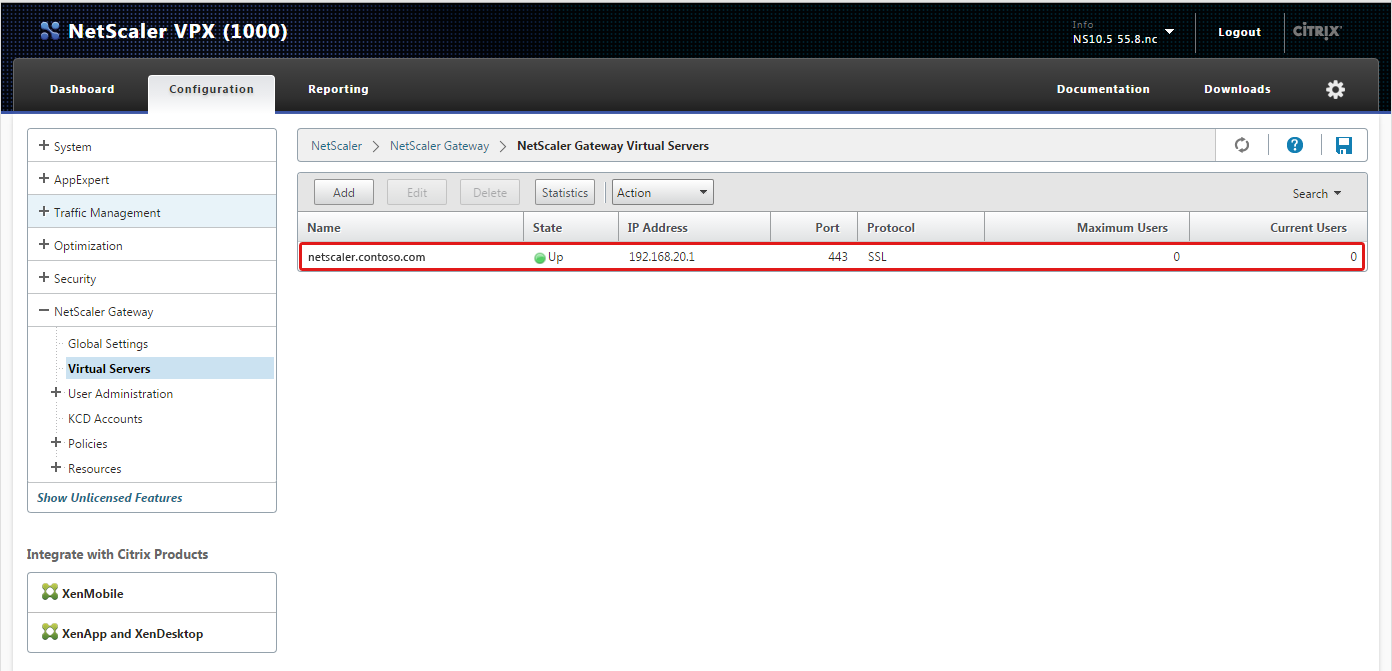
1. Login to the administration interface for the SSL VPN appliance.
2. On the dashboard, click the **Configurations** tab.



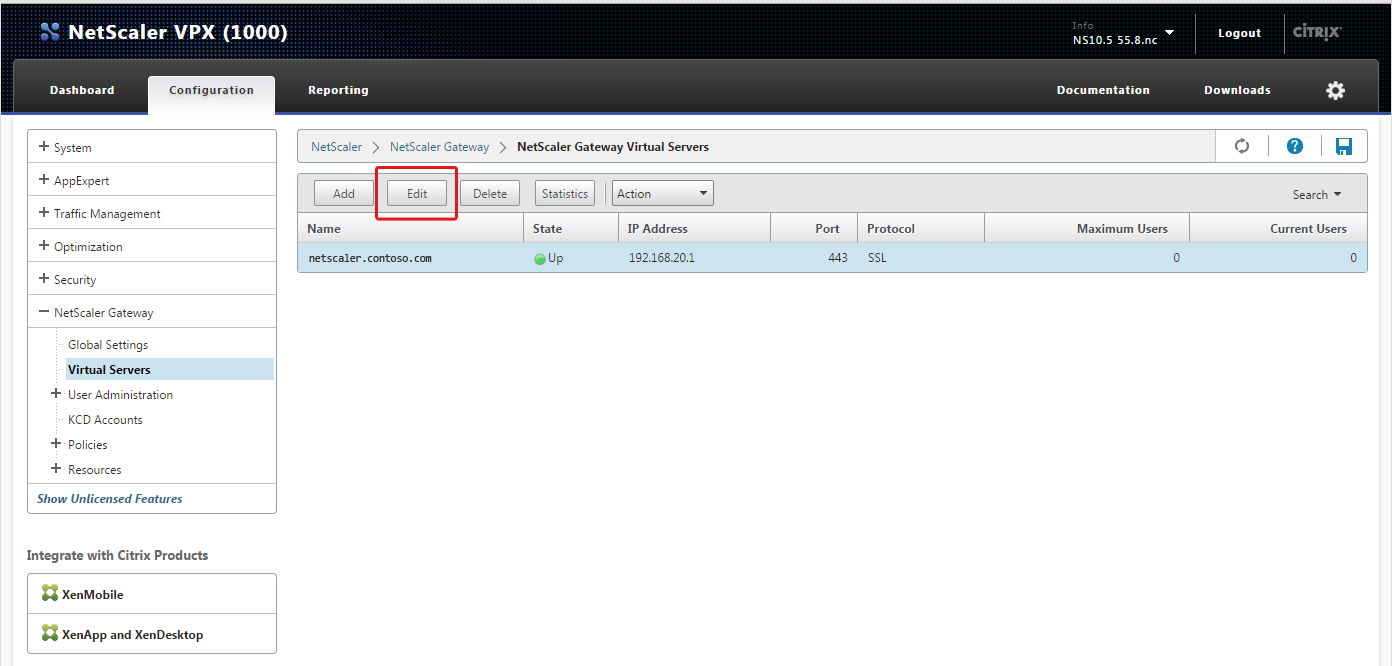
1. Navigate to **NetScaler Gateway**|**Virtual Servers**.



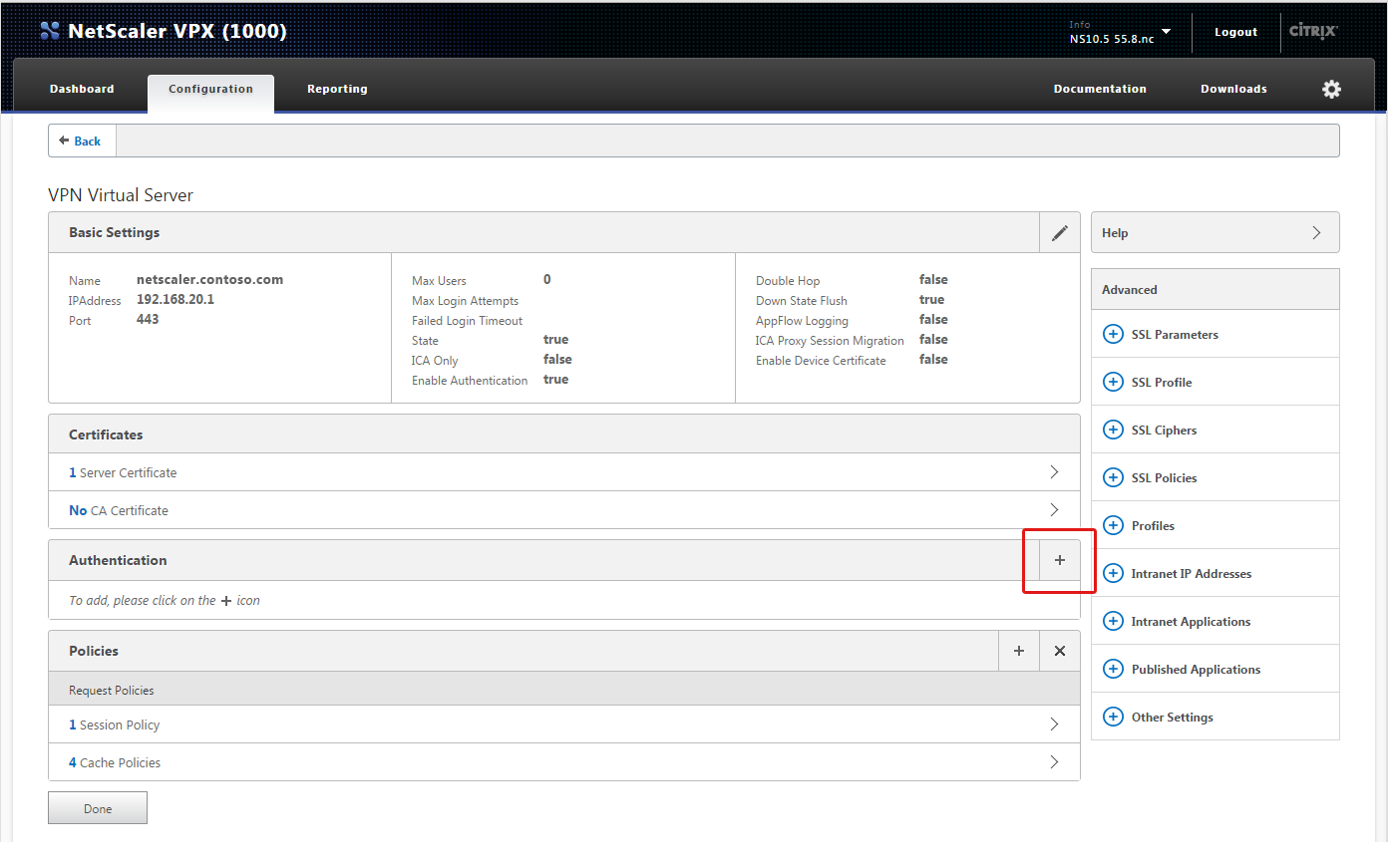
1. Select the virtual server that will be used for MFA.



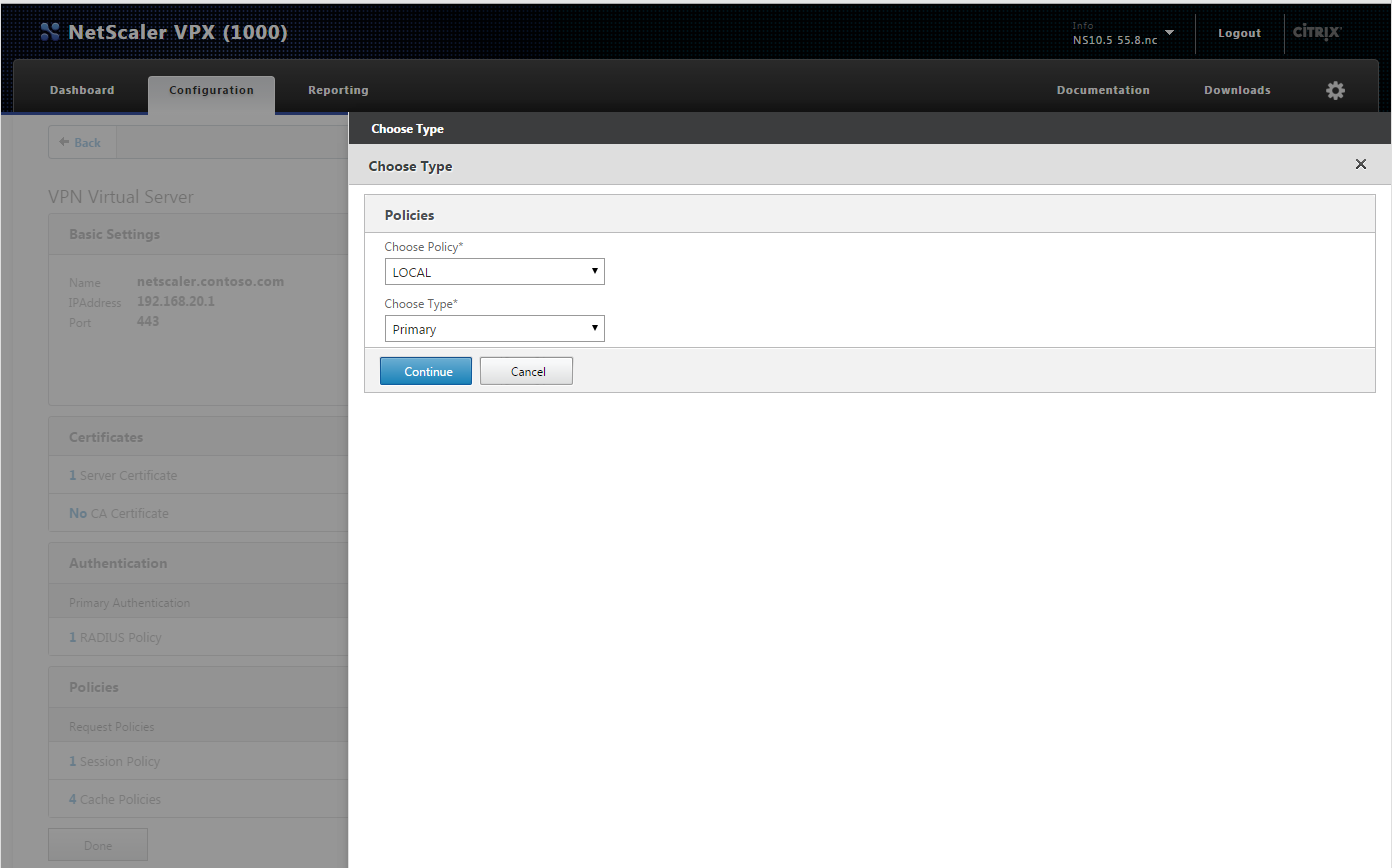
1. Click **Edit**.



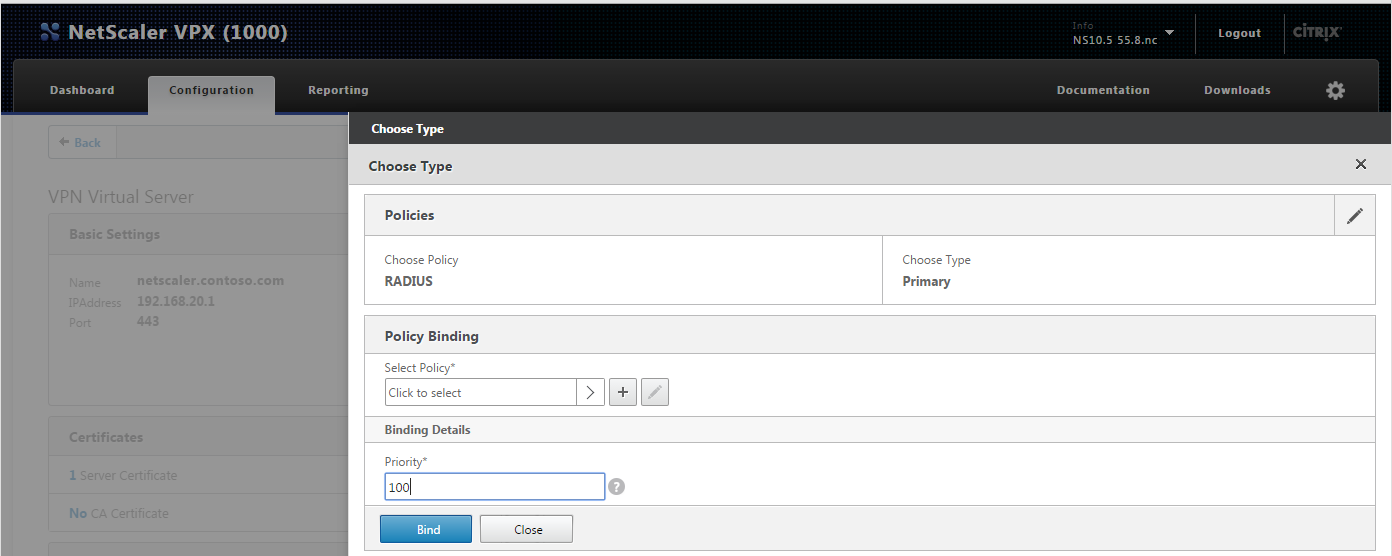
1. On the VPN Virtual Server page, navigate to **Authentication** and click the **+** symbol.



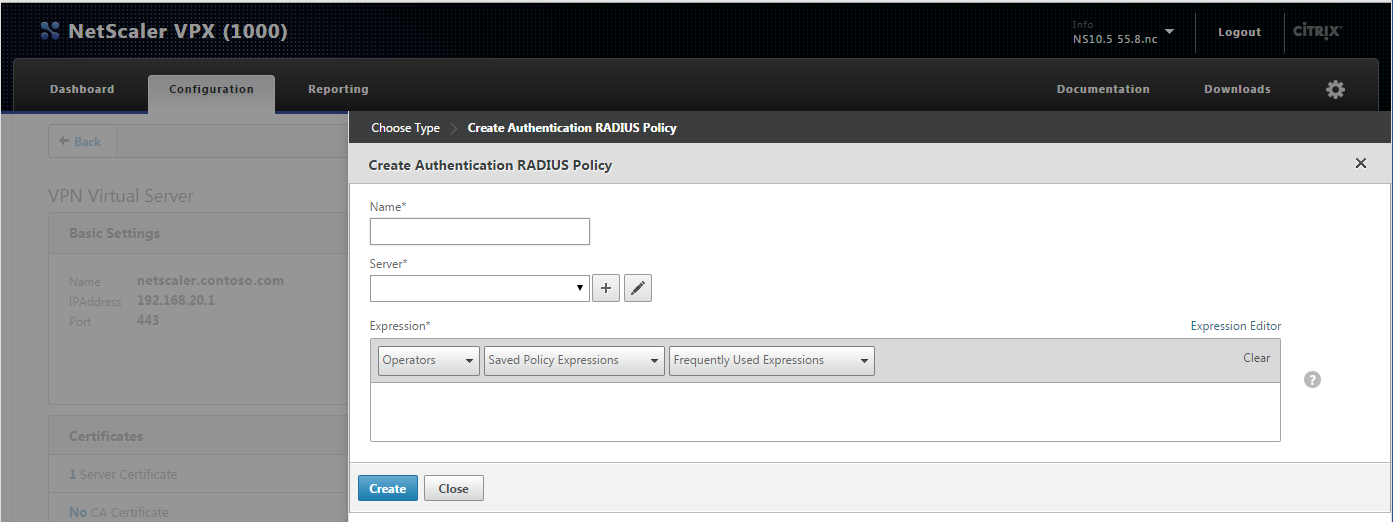
1. The pane to add a new policy opens.



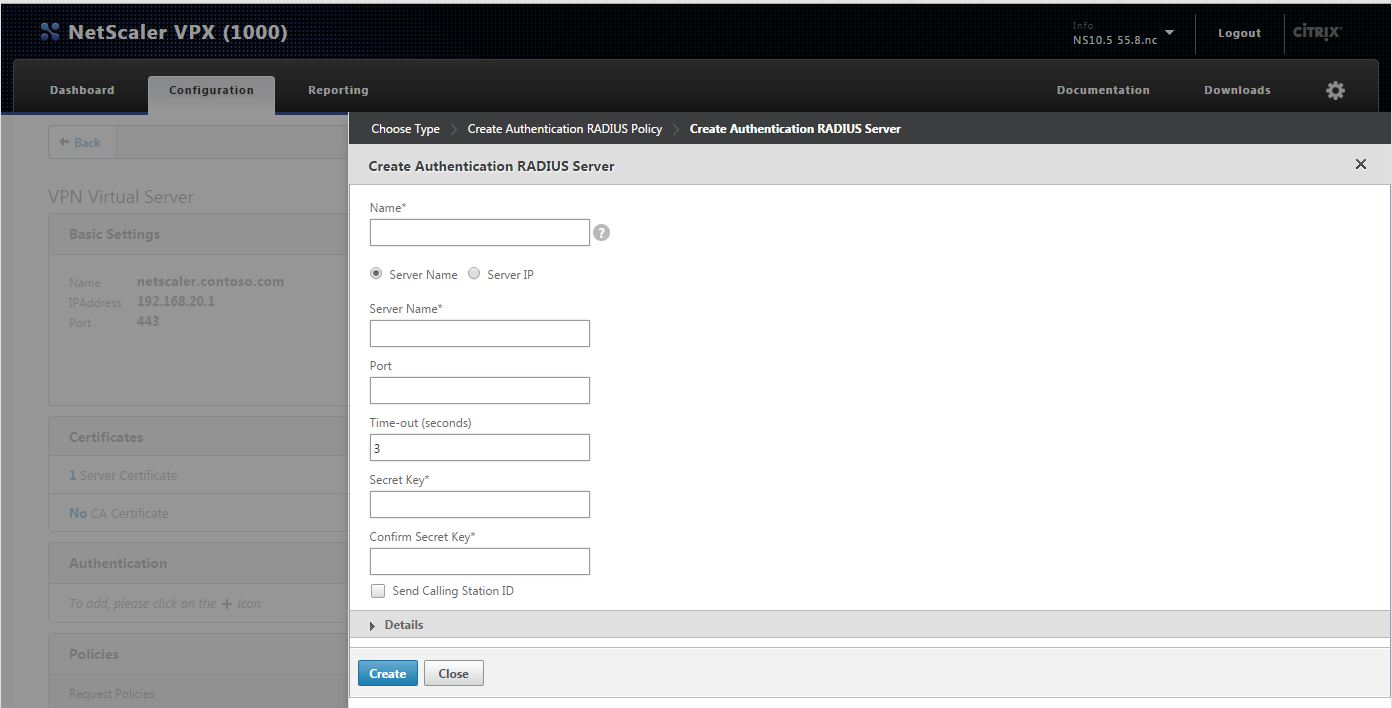
1. Complete the following in the Policies pane:
2. **Choose Policy** – select **RADIUS**.
3. **Choose Type** – select **Primary**.
4. **Continue** – click to add RADIUS policy.
5. On the Policy Binding panel, complete the following:



1. **Priority** – enter 100.
2. **Select Policy** – click the **+** symbol to add a new policy binding.
3. The Create Authentication RADIUS Policy pane opens.



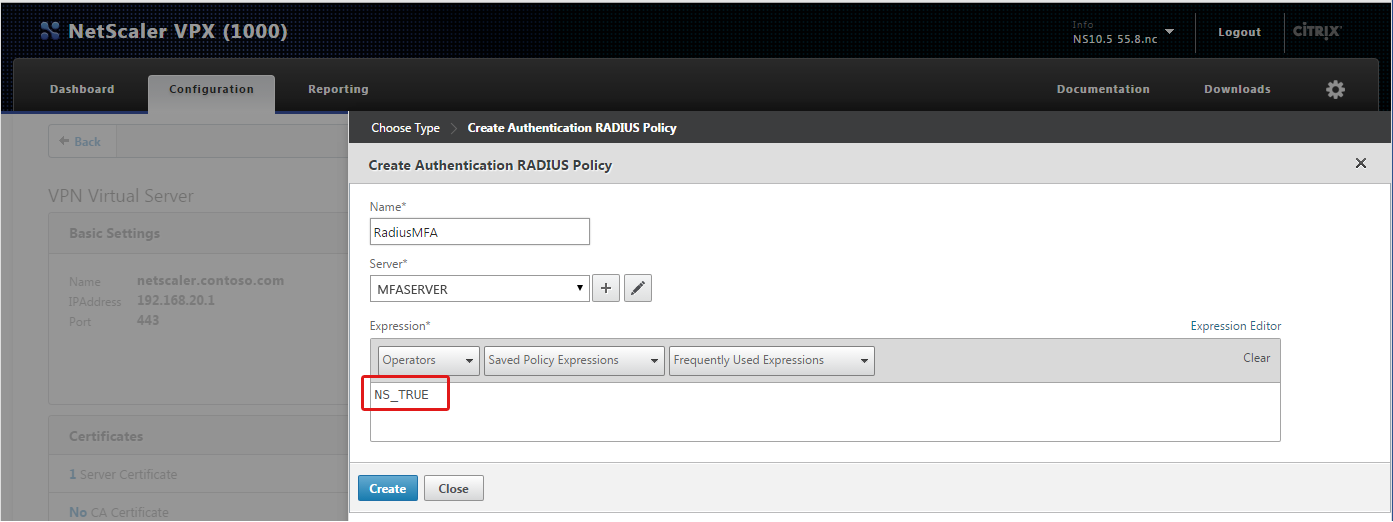
1. Complete the following:
2. **Name** – enter a descriptive name for the new RADIUS policy.
3. **Server** – click the **+** symbol to add a new RADIUS server.
4. On the Create Authentication RADIUS Server screen, complete the following:



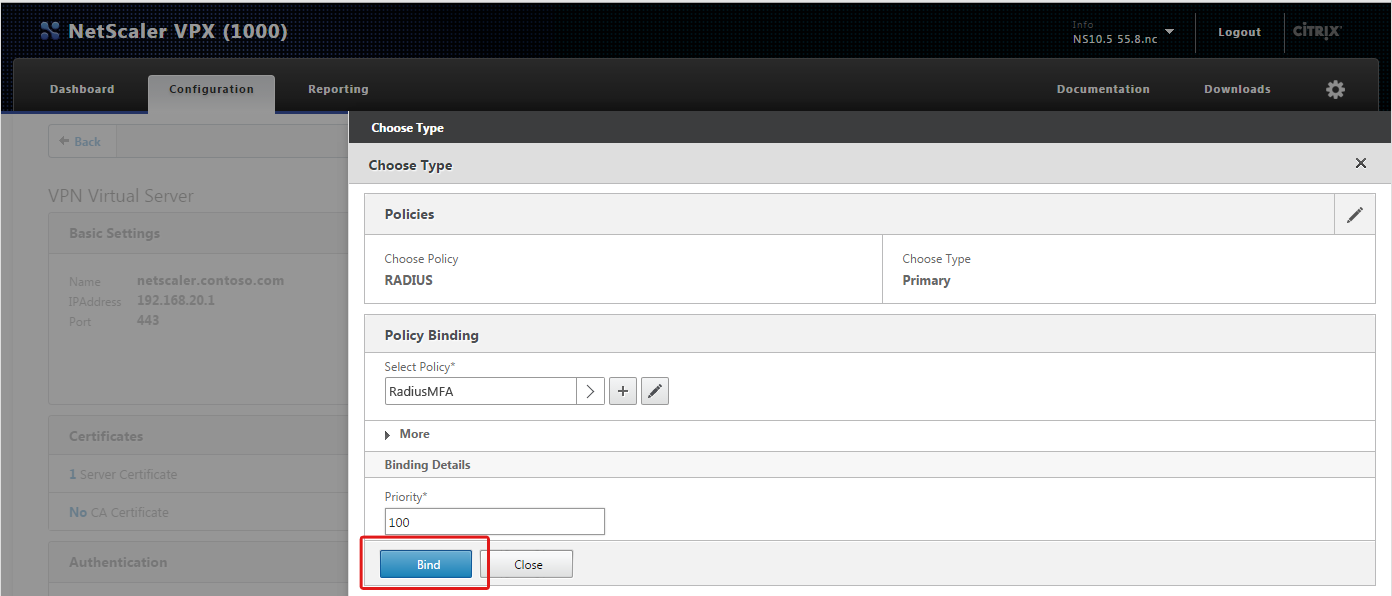
1. **Name** – enter a friendly name to identify the Azure MFA server as the RADIUS server.
2. Select an option to use for connecting to the MFA server:

* **Server Name** – select to designate the MFA server’s computer name in the **Server Name** field below.
* **Server IP** – select to designate the MFA server’s **IP Address** in the field below.

1. **Port** – enter the port number used for authentication communication on the MFA Server. Defaults are 1812 or 1645.
2. **Time-out (seconds)** – it is important to set a sufficient length of time for users to authenticate. 30 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.
3. **Secret Key** – enter the security passphrase created to encrypt communication between MFA and the NetScaler VPX.
4. **Confirm Secret Key** – confirm the same key passphrase.
5. Click **Create** to save server configuration and return to the Create Authentication RADIUS Policy pane.
6. **Expression** – enter **NS\_TRUE**. This is required to enable and authenticate all devices through the new policy.



1. Click **Create** to save the policy configuration.
2. Click **Bind** to append the RADIUS policy configuration.



You have completed SSL 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 method for the push notification or OATH token options. If you aren’t going to use mobile app, then skip straight to the [Login](#testAuth_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.

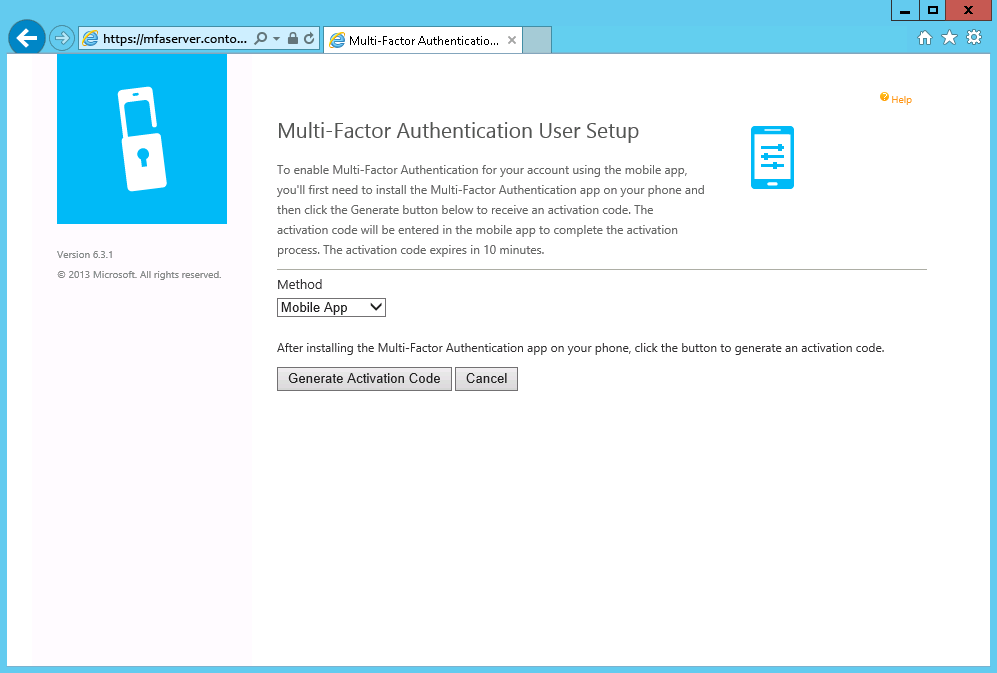
### Requirements

* 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

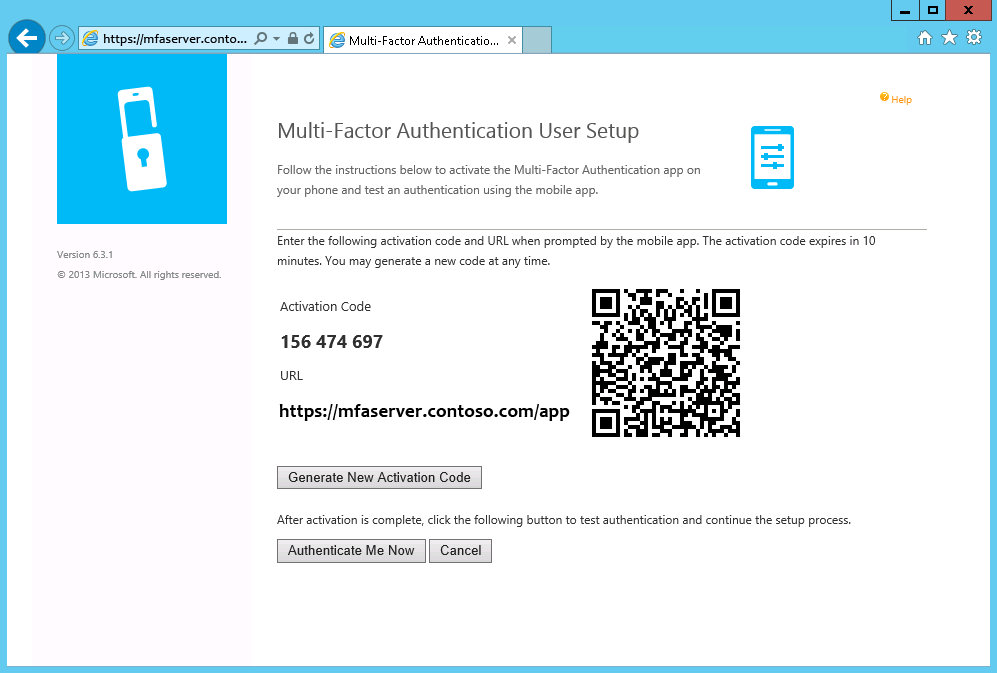
### Activate Device

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.

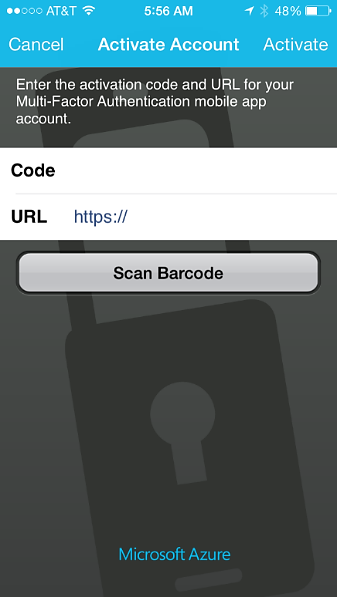


1. Click **Generate Activation Code**.
2. Activation code options will display.



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

Example:



1. 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

* A computer to access the login screen.
* The SSL VPN appliance URL for network sign in.
* User credentials

### Phone Call

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

1. On a computer, open the login page in a web browser.
2. Enter user credentials.
3. Check the phone for a call.

NOTE: The call originates in the cloud from the Azure MFA application.

Example:



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

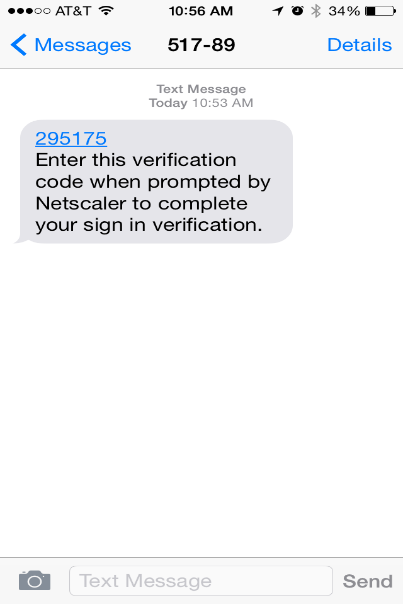
### Text Message

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

#### One-Way Text Message

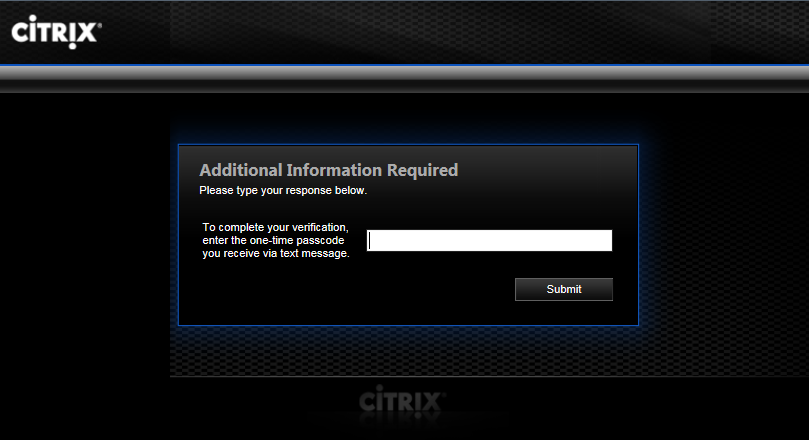
1. On a computer, open the login page in a web browser.
2. Enter user credentials.
3. Retrieve the verification code from the text message.

Example:



1. Enter the verification code on the login page response prompt.

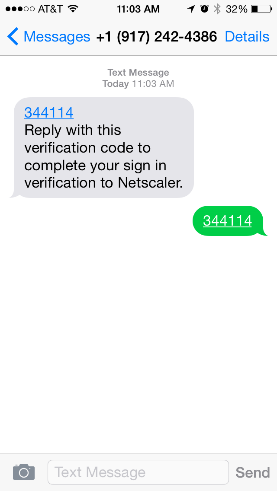
Example:



#### Two-Way Text Message

1. On a computer, open the login page in a web browser.
2. Enter user credentials.
3. Check the phone for a text message with the verification code.

Example:



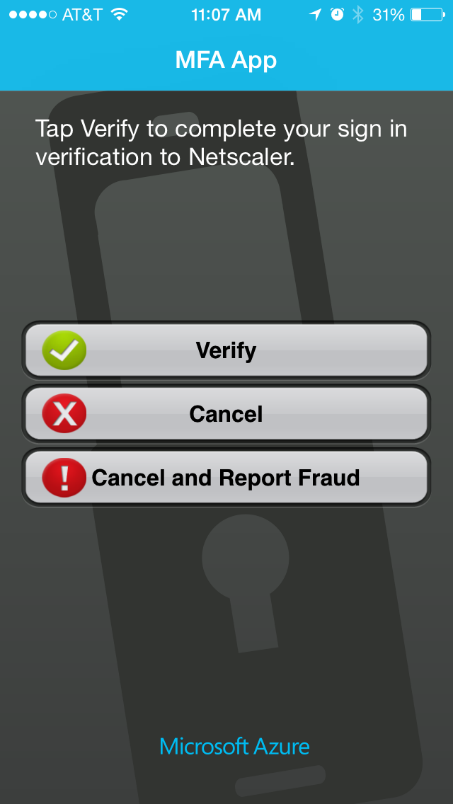
1. Reply to the text message with the same verification code.

### Mobile App

Required: A device with the Azure Authenticator app activated.

1. On a computer, open the login page in a web browser.
2. Enter user credentials.
3. Check the device with Azure Authenticator for a prompt.

Example:



1. Click **Verify**.
2. The authentication application will communicate with the MFA server to complete authentication.

### Oath Token

Required: A device with the Azure Authenticator app activated.

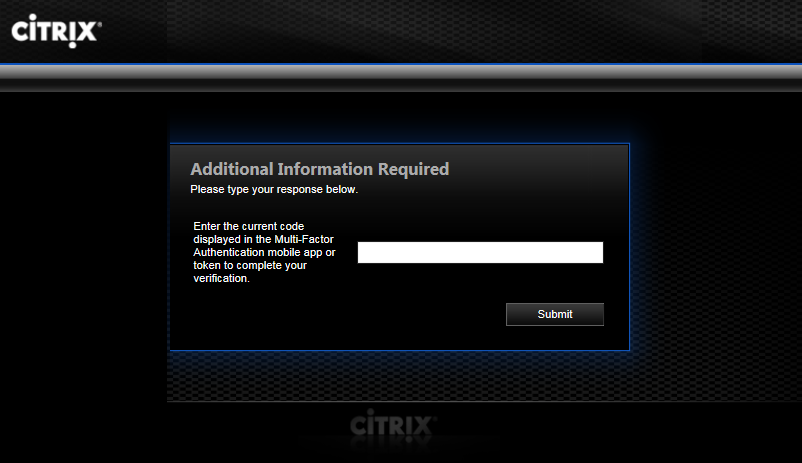
1. On a computer, open the login page in a web browser.
2. Enter user credentials.
3. On the mobile device, open the Azure Authenticator app.
4. Retrieve a verification code from the app.

Example:



1. Enter the verification code on the login page response prompt.

Example:



Successful authentication will grant access through the browser session.

This completes the setup and testing for Azure Multi-Factor Authentication using the RADIUS protocol in a Citrix NetScaler SSL VPN appliance deployment.