Configuring MFA Using Cisco ISE and Microsoft Azure MFA

Objective

MFA (Multi-Factor Authentication) is used to verify a user's identity with two or more pieces of evidence to prove their identity. The objective here was to set up MFA access to a network device such as a Cisco router, switch as well as the Cisco Anyconnect. Previously our MFA for the Anyconnect was setup as the secondary authentication on the Cisco ASA.

This article explains how to use the Microsoft Azure MFA server with Cisco ISE to preform MFA on network devices and Anyconnect.

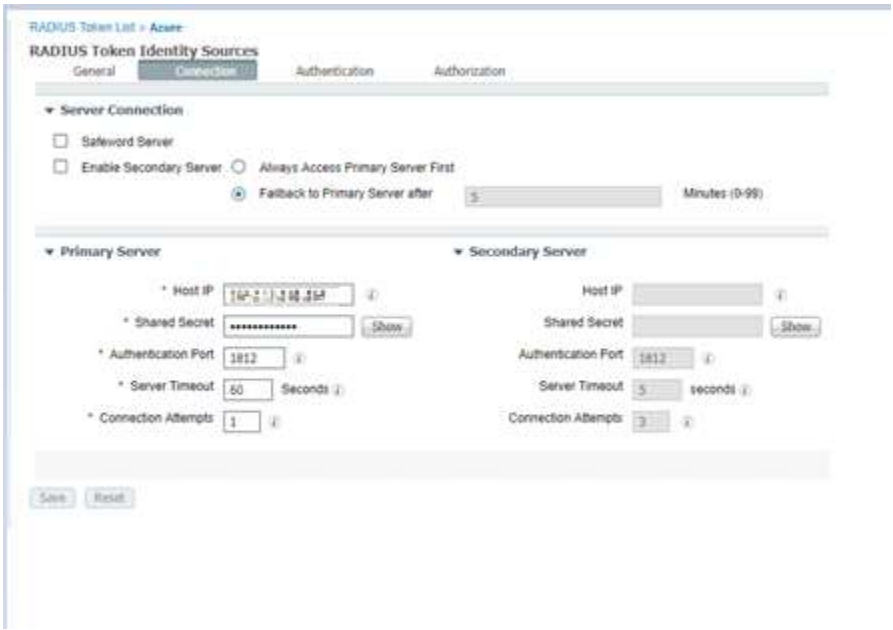
Applicable Devices

Cisco ISE 2.2
Microsoft Azure MFA
Cisco switch

The following steps are taken place after a successful installation of a Microsoft MFA server and Cisco ISE appliance and integrated with Active Directory.

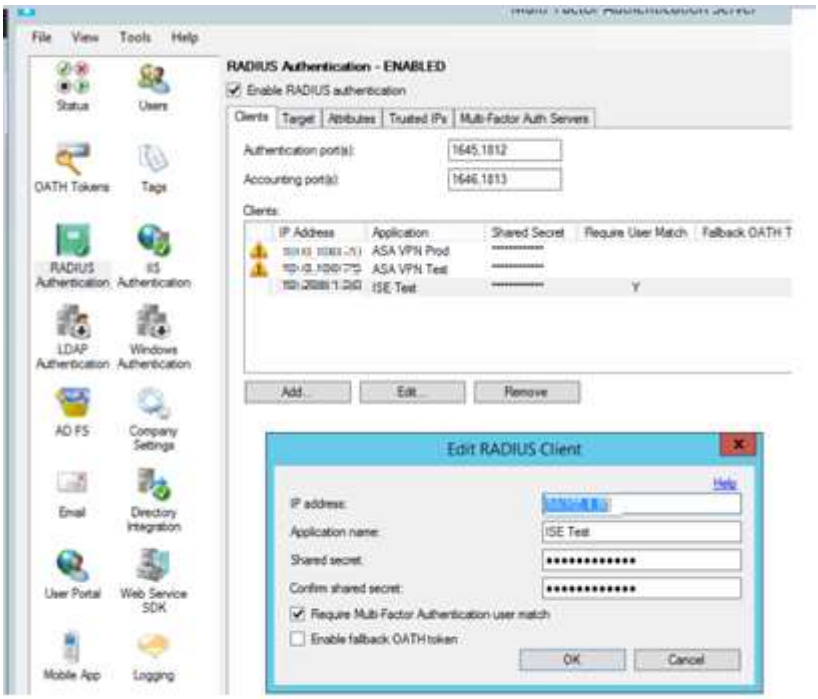
Step-by-Step Procedure

Step 1. In cisco ISE navigate to Administration>External Identity Sources. Add the Azure MFA server to as a RADIUS Token. Enter IP address and shared secret. Set authentication port to 1812 and server timeout to 60 seconds. Save



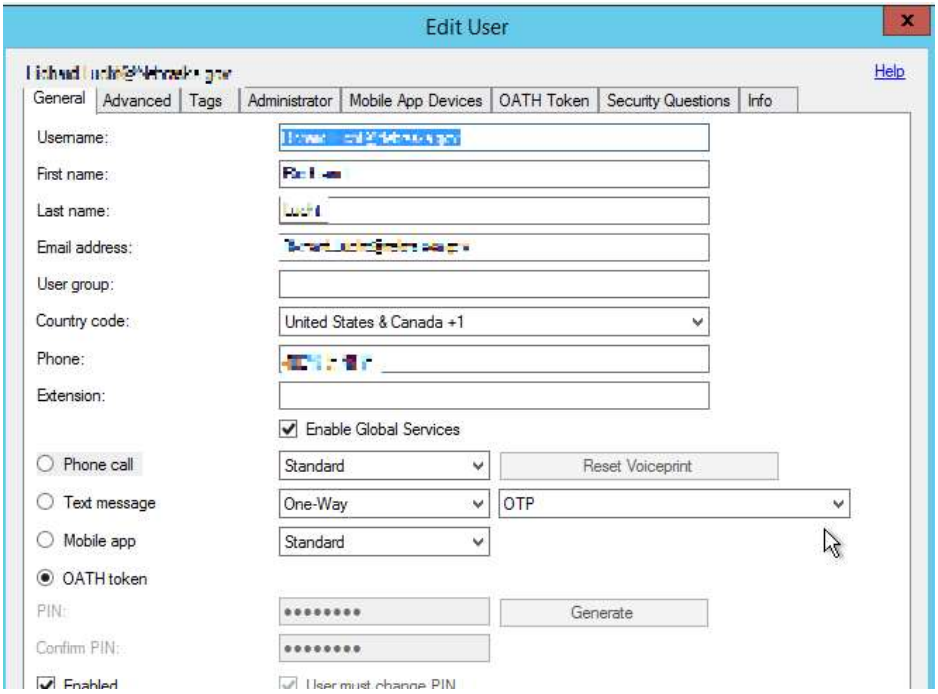
Richard Lucht
Jan 12, 2018

Step 2. In Microsoft Azure MFA add the IP address of the ISE appliance along with the shared secret to the Client list.



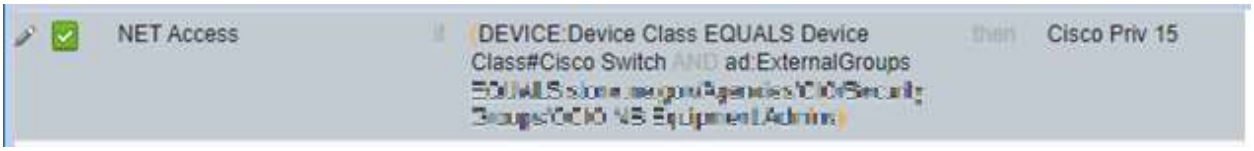
Step 3. Add users to MFA and give them option to use push notification or Token through a mobile app.

Richard Lucht
Jan 12, 2018



Step 4. Navigate to the Policy> Policy Set> and create your Authentication Policy Using the Azure MFA as your identity store.

Step 5. Configure the authorization policy using your user's active directory group and permissions



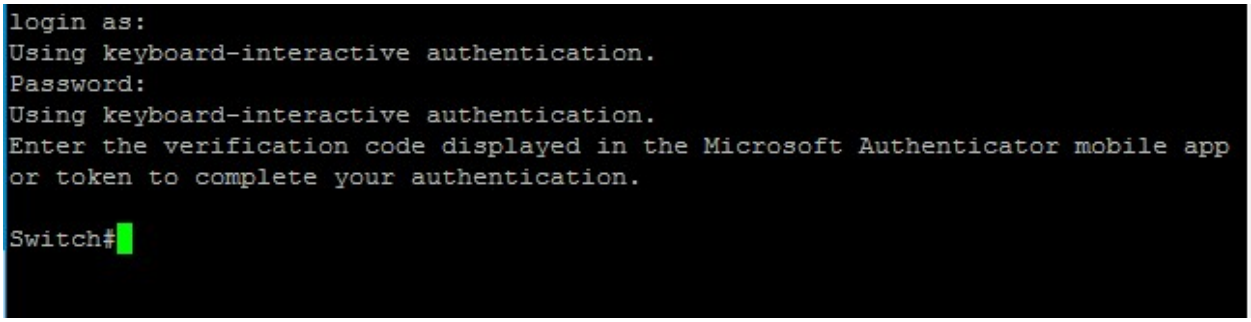
Step 6. Cisco switch configuration for Radius authentication through ISE. No additional configurations are needed if the switch already uses ISE for Radius authentication.

```
aaa authentication login default group ISE_SERVERS local
aaa authentication dot1x default group ISE_SERVERS
aaa authorization exec default group ISE_SERVERS local
aaa authorization network default group ISE_SERVERS
```

```
radius server ISE1
 address ipv4 [redacted] auth-port 1645 acct-port 1646
 timeout 10
 retransmit 0
 key
```

Step 7. Test login using Token on the Authenticator mobile app, results are same with push notification.

Richard Lucht
Jan 12, 2018



Results from further testing, using Azure as the Identity in the Authentication Policy we found that all Cisco devices we tested the Token prompted with the same message. We tested a Cisco router, a switch and an ASA. Also on our VPN Authentication policy after connecting to the Anyconnect we were prompted the same message when using the Token. Using the push notification we were prompted on our mobile device with a “Deny” or “Approve”. We also tested non-cisco devices, we could not get the prompt to come up but the push notification worked.

Richard Lucht
Jan 12, 2018