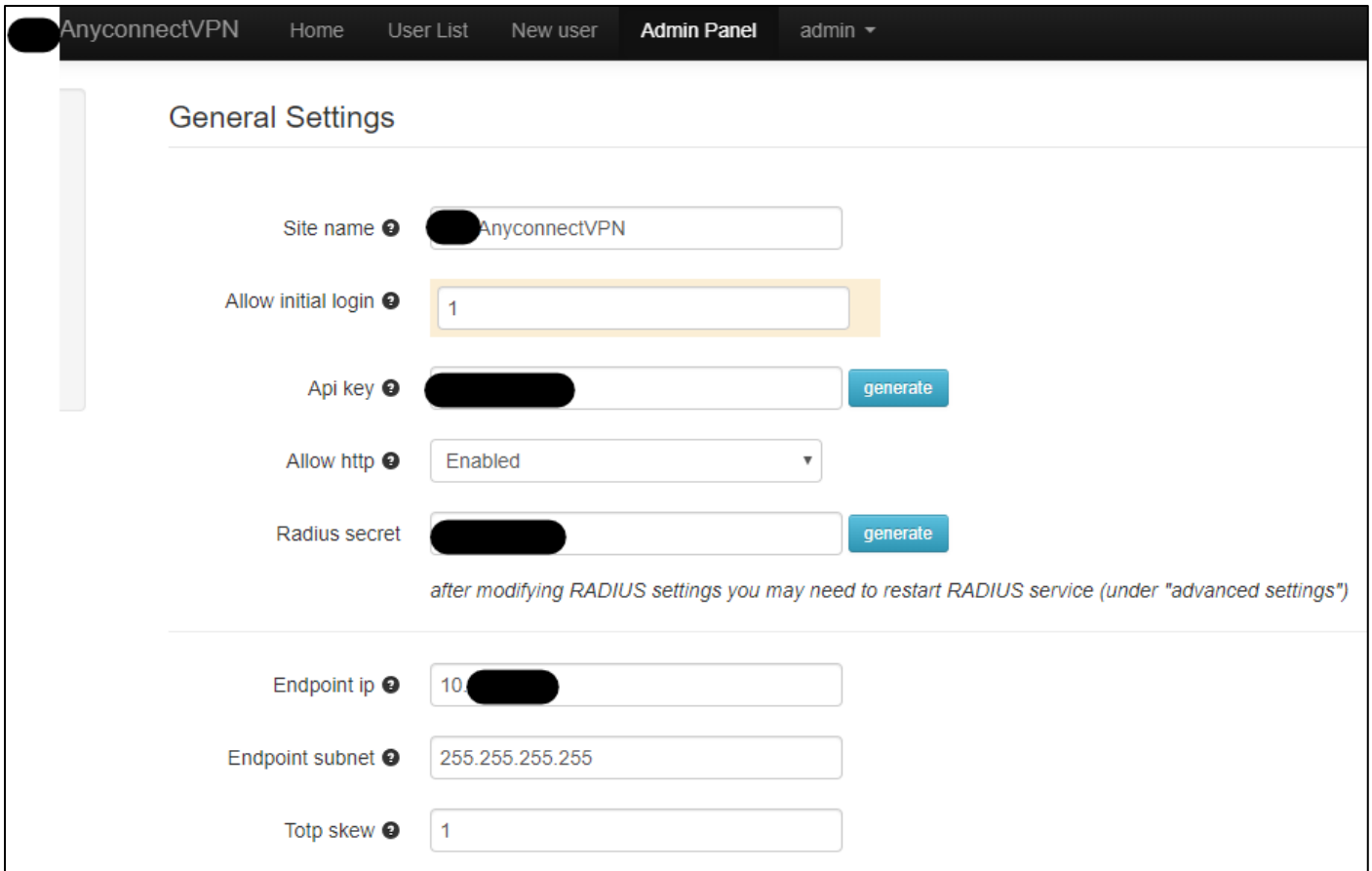


Configuring TOTPRadius and 2FA for Cisco Anyconnect

This guide will document how to configure 2 factor authentication on a Cisco ASA, using Microsoft Active Directory as the first factor and TOTPRadius Server as the second. The configuration is applied through the Cisco Adaptive Security Device Manager (ASDM) configuration tool. The assumption is made that you have a working Anyconnect VPN profile on the ASA, have deployed the TOTP appliance into an appropriate virtual environment and performed basic configuration steps such as setting an IP address and adding the server to DNS, can log in to the Admin Panel using the default username and password, and have tested reachability from the ASA INSIDE interface to the TOTPRadius Server.

TOTPServer configuration

General Settings



The screenshot shows the 'General Settings' page in the TOTPRadius Admin Panel. The navigation bar at the top includes 'AnyconnectVPN', 'Home', 'User List', 'New user', 'Admin Panel', and 'admin'. The settings are as follows:

- Site name: AnyconnectVPN
- Allow initial login: 1
- Api key: [Redacted] generate
- Allow http: Enabled
- Radius secret: [Redacted] generate

after modifying RADIUS settings you may need to restart RADIUS service (under "advanced settings")

- Endpoint ip: 10.[Redacted]
- Endpoint subnet: 255.255.255.255
- Totp skew: 1

1. Site Name – The name of this installation, will appear in any TOTP app you use. In this instance “mycompanyAnyconnectVPN” was used.
2. Allow Initial Login – must be set to 1 to allow self-service TOTP registration. Otherwise 0.
3. API key – not required for ASA integration
4. Allow HTTP – not required for ASA integration
5. Radius Secret – Make note of this for later, generate a new one if required. Used to secure communication between ASA and TOTPRadius Server.
6. Endpoint IP – the IP address of the INSIDE interface of the Cisco ASA.
7. Endpoint Subnet – 255.255.255.255 to allow only the ASA to authenticate against this server.
8. TOTP Skew – Set to 1 to allow for time sync issues between client and server.

LDAP Settings

LDAP Settings

Ldap [?] Disabled

Enforce 2fa [?] Disabled

Ldap server [?] ldap://[redacted] ldap://[redacted]

Ldap username format [?] %username%@[redacted] test LDAP connection

Ldap search string [?] DC=[redacted] DC=[redacted]

Ldap group restrict [?]

Allow ldap enrollment [?] Enabled users will navigate to http(s)://[redacted] ldap-enroll to enroll

Ldap intro text

TOTPRadius allows users to log in without second factor (e.g. using AD password only) only **once**. If you have not already done so, you can enroll your second factor using this LDAP Enroll web interface. If you have already enrolled, you can close this page.

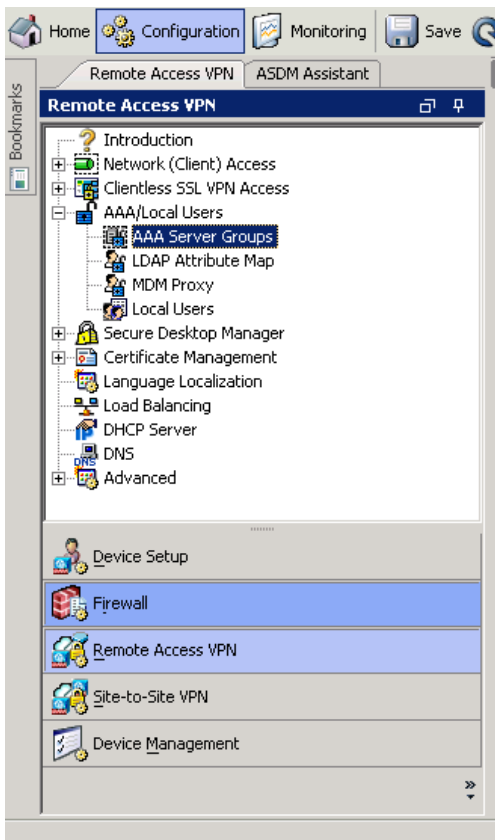
this text will appear on LDAP web enrollment page. HTML is allowed

Ldap admins [?] [redacted]

1. LDAP – Disabled
2. Enforce 2fa – Disabled
3. LDAP Server – IP address/hostname of active directory DC(s). In this instance, 2 DCs in format ldap://Server1IP ldap://Server2IP
4. LDAP Username Format - [%username%@mydomain.com](#)
5. LDAP Search String - DN for LDAP to search, in this instance the DN of the entire domain, DC=MyDomain, DC=COM.
6. LDAP Group Restrict – Leave blank
7. Click Test LDAP Connection button and enter active directory login details into pop-up window. This test should now succeed.
8. Allow LDAP enrolment – Allow users to log into a portal to self-serve the creation of their second factor.
9. LDAP Admins – provide comma separated list of LDAP accounts allowed access to the admin portal – please note, at time of writing this list is case-sensitive.

ASA Configuration

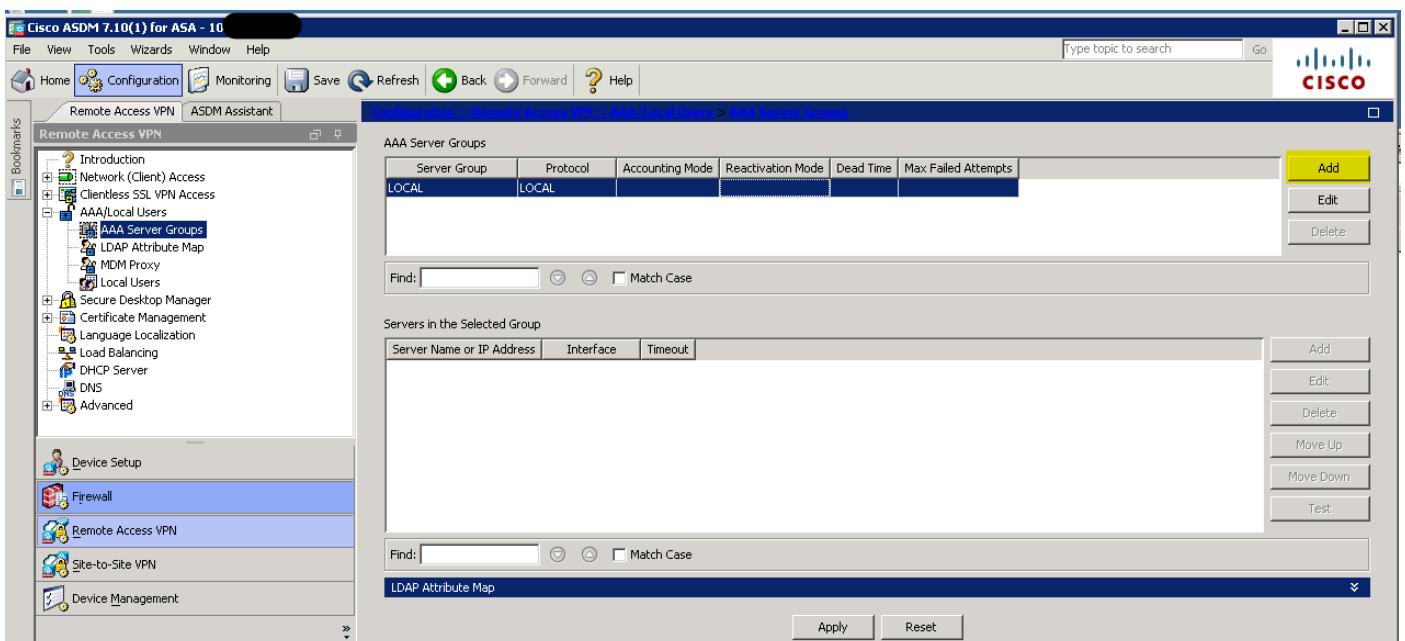
In the ASDM, go to Configuration > Remote Access VPN > AAA/Local Users > AAA server Groups.



We are going to add 2 separate server groups, one LDAP server group to carry out the first authentication against active directory, and a second RADIUS group to authenticate against our TOTPRadius Server instance.

First, we will set up the TOTPRadius Server

Click the Add button next to the AAA Server Groups as highlighted below.



In the popup window that appears, give your server group an appropriate name. The remaining settings can be left at default setting. Hit OK.

AAA Server Group: 2FARADIUS

Protocol: RADIUS

Accounting Mode: Simultaneous Single

Reactivation Mode: Depletion Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

Enable interim accounting update

Update Interval: 24 Hours

Enable Active Directory Agent mode

ISE Policy Enforcement

Enable dynamic authorization

Dynamic Authorization Port: 1700

Use authorization only mode (no common password configuration required)

VPN3K Compatibility Option

OK Cancel Help

Select the newly created server group in the top box, and click the Add button highlighted below to add a new server to this group.

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
2FARAD	RADIUS	Single	Depletion	10	3
LOCAL	LOCAL				
RALDAP	LDAP		Depletion	10	3

Servers in the Selected Group

Server Name or IP Address	Interface	Timeout
---------------------------	-----------	---------

Apply Reset

Device configuration refreshed successfully. tsoadmin 15 20/06/19 13:44:16 UTC

In the pop up window, set the following.

1. Interface Name – the interface facing your TOTPRadius Server, usually INSIDE
2. Server Name or IP Address – the DNS name or IP address of the TOTPRadius Server.
3. Server Authentication Port – Change this to 1812.
4. Server Secret Key – This is the Radius Secret from step 5 of the first part of this document.

Once this is complete, hit OK.

Server Group: 2FARAD

Interface Name: INSIDE

Server Name or IP Address: [REDACTED]

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1812

Server Accounting Port: 1646

Retry Interval: 10 seconds

Server Secret Key: *****

Common Password: [REDACTED]

ACL Netmask Convert: Standard

Microsoft CHAPv2 Capable:

SDI Messages

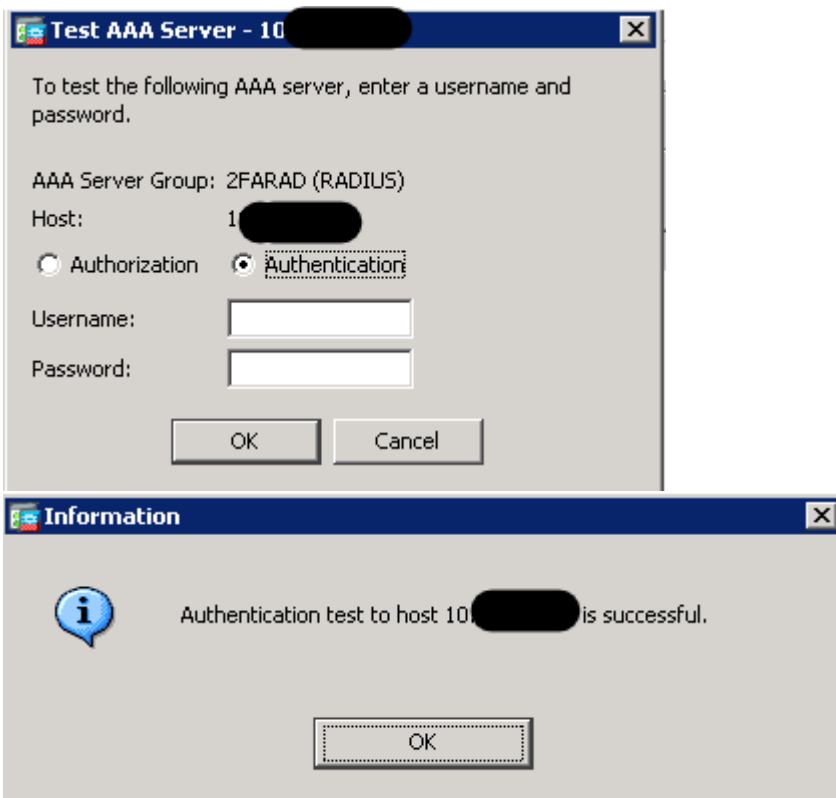
Message Name	Message Text
ready-for-sys-pin	ACCEPT A SYSTEM GENERATED PIN
next-code	Enter Next PASSCODE
next-code-and-reauth	new PIN with the next card code
new-pin-req	Enter your new Alpha-Numerical ...
new-pin-sup	Please remember your new PIN
new-pin-reenter	Reenter PIN:
new-pin-sys-ok	New PIN Accepted
new-pin-meth	Do you want to enter your own pin

(Double-click in a text cell to make changes.)

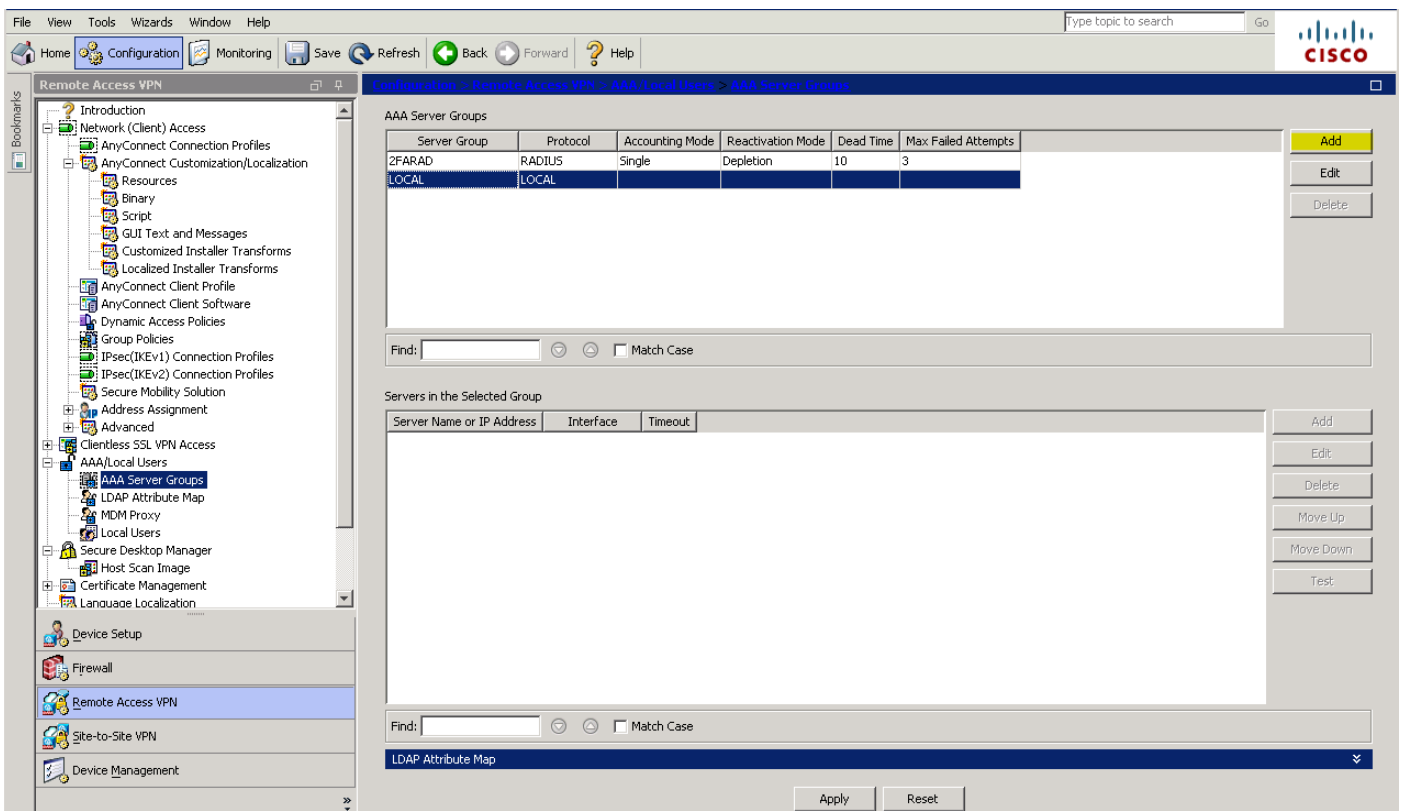
Restore default message texts

OK Cancel Help

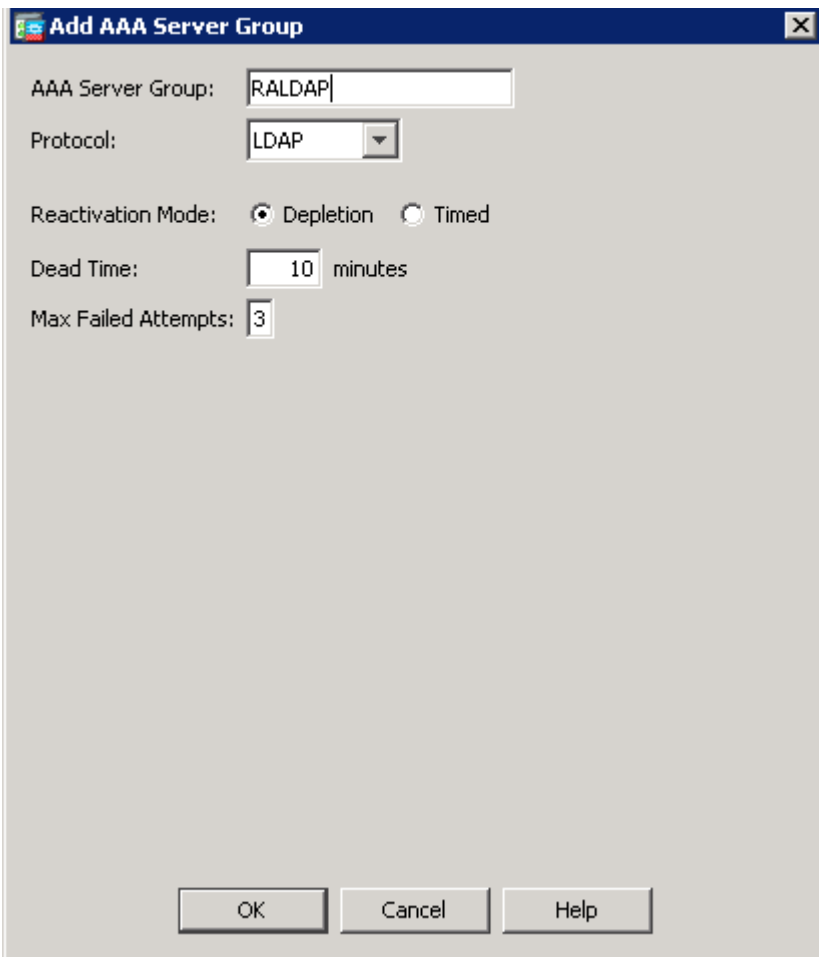
So long as you have at least one user enrolled in TOTPRadius Server, you should then be able to hit the Test button to the right of the screen and the below window will appear. Select Authentication, and enter the windows domain username of an enrolled user, and the current TOTP code for that user. This test should come back successfully.



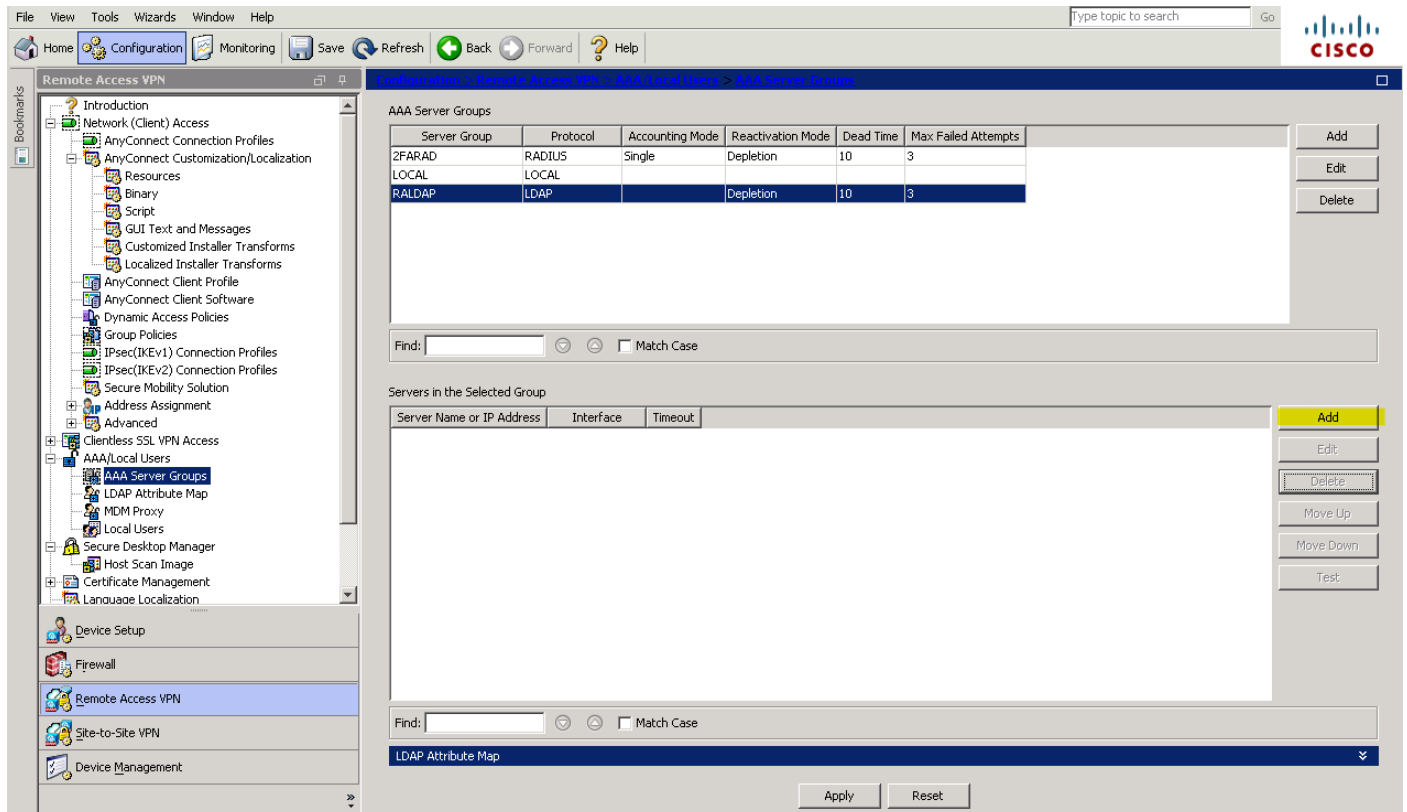
We are now going to add a second AAA server group to the ASA. Once again, select the Add button beside the top block, as below.



In the next windows, give the server group an appropriate name and select protocol LDAP, then hit OK.



Select the newly created server group and click Add to add a server to this group.



In the windows that pops up set

1. Interface name – select the interface facing your Active Directory DC
2. Server name or IP Address - The IP or FQDN of your DC
3. Server Type – Microsoft
4. Base DN – DN for LDAP to search, in this instance the DN of the entire domain, DC=MyDomain, DC=COM.
5. Scope – All levels beneath the Base DN.
6. Naming Attribute – samaccountname
7. Login DN – the DN of an account with appropriate permission to query active directory.
8. Login Password – the password of the above account.

Edit AAA Server

Server Group: RALDAP

Interface Name: INSIDE

Server Name or IP Address: 10...

Timeout: 10 seconds

LDAP Parameters for authentication/authorization

Enable LDAP over SSL

Server Port: 389

Server Type: Microsoft

Base DN: DC=..., DC=...

Scope: All levels beneath the Base DN

Naming Attribute: samaccountname

Login DN: CN=..., OU=..., OU=..., DC=..., DC=...

Login Password: *****

LDAP Attribute Map: -- None --

SASL MD5 authentication

SASL Kerberos authentication

LDAP Parameters for Group Search

Group Base DN:

Group Search Timeout: 10

OK Cancel Help

You should now have 2 separate server groups set up. We now need to add these to your Anyconnect Connection Profile. In ASDM, browse to Configuration > Remote Access VPN > Anyconnect Connection profile. Select your VPN Connection Profile in the Connection Profiles block at the bottom of this screen and click Edit, as highlighted below.

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
INSIDE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
OUTSIDE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" 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
DefaultRAGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPNGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
VPNUsersZFA	<input checked="" type="checkbox"/>	<input type="checkbox"/>		AAA(RALDAP)	NOACCESS

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.

In the Basic section of the window that pops up, where highlighted below select the AAA Server Group you created to perform LDAP authentication against your AD DC.

Edit AnyConnect Connection Profile: VPNUsers2FA

Basic
Advanced

Name: VPNUsers2FA
Aliases: [Redacted]

Authentication
Method: AAA
AAA Server Group: RALDAP [Manage...]
 Use LOCAL if Server Group fails

SAML Identity Provider
SAML Server : --- None --- [Manage...]

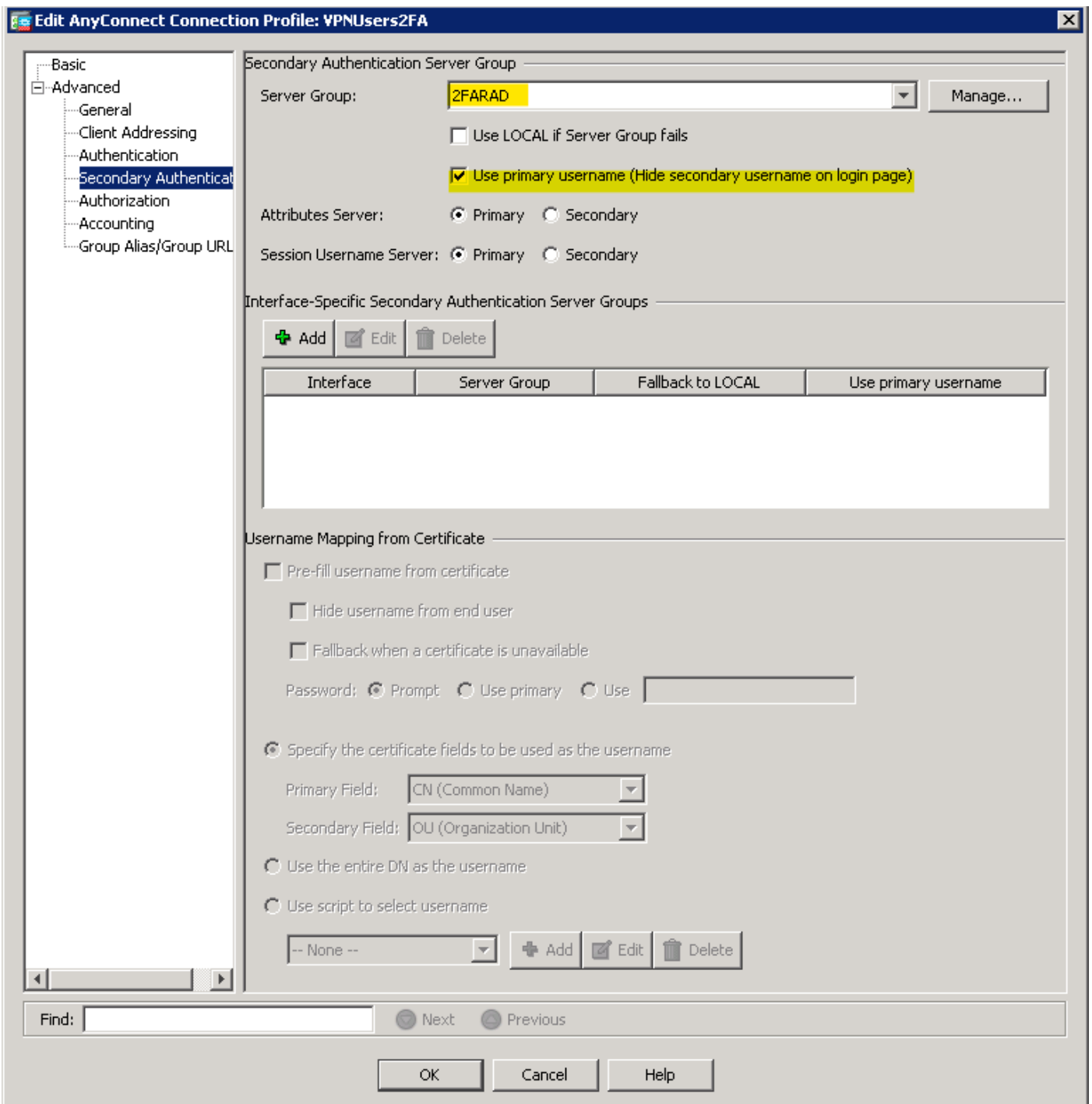
Client Address Assignment
DHCP Servers: [Redacted]
 None DHCP Link DHCP Subnet
Client Address Pools: [Redacted] [Select...]
Client IPv6 Address Pools: [Redacted] [Select...]

Default Group Policy
Group Policy: [Redacted] [Manage...]
(Following fields are linked to attribute of the group policy selected above.)
 Enable SSL VPN client protocol
 Enable IPsec(IKEv2) client protocol
DNS Servers: [Redacted]
WINS Servers: [Redacted]
Domain Name: [Redacted]

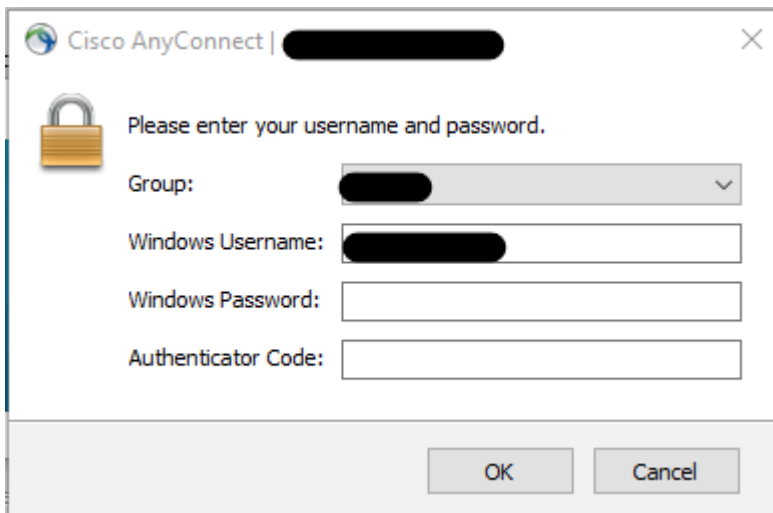
Find: [Redacted] [Next] [Previous]

OK Cancel Help

Now navigate to Advanced > Secondary Authentication. Set the server group to the AAA Server you created to authenticate against TOTPRadius Server. Be sure to also tick Use Primary Username, this will ensure users are presented with a single username field, one password field for their AD password and a second password field for their TOTP code.



Once applied to the ASA, Anyconnect connection attempts should present a password window similar to the below.



Optional

It is possible to customise the text fields presented to users by the Anyconnect client, e.g. to display the “Password” label to show as “Windows Password” as in the above screenshot. This is controlled in Configuration > Remote Access VPN > Anyconnect Customization/Localization > GUI Text and Messages. Edit an existing translation table or add a new one. Within the text of the window that pops up, find the line with msgid “Password” and change the corresponding msgstr to “Authenticator Code” or similar suitable description. Due to the volume of text here, you may find it easier to copy this text to a text editor, use CTRL+F to find and the msgid and make the changes, and then copy/paste it back into ASDM.

