SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com

Cisco SA Integration Guide (ASA)

SecurAccess Integration Guide

Version 2.0 – 25/04/18

Cisco ASA Integration Guide (ASA)

Contents

1.1 Solution Summary

SecurEnvoy's SecurAccess MFA solution integrates with Cisco's Adaptive Security Appliance (ASA) through the use of AAA Server for authorisation and Dynamic Access Policies for LDAP group membership and access control.

1.2 Guide Usage

The information in this guide describes the configuration required for integration with SecurEnvoy and 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.

1.3 Prerequisites

The following conditions are required to set up SecurEnvoy's MFA Solution:

- A SecurAccess MFA server installed, configured and working on a system with:
  - Windows Server 2003 or higher.

  Note: Please see SecurEnvoy's SecurAccess deployment guide on how to setup MFA server solution.
- A Cisco ASA appliance – version 8.3 and above, 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 unless the Clientless solution will be used.
- Familiarity with the following technologies:
  - RADIUS configuration
  - Cisco ASA VPN appliance administration

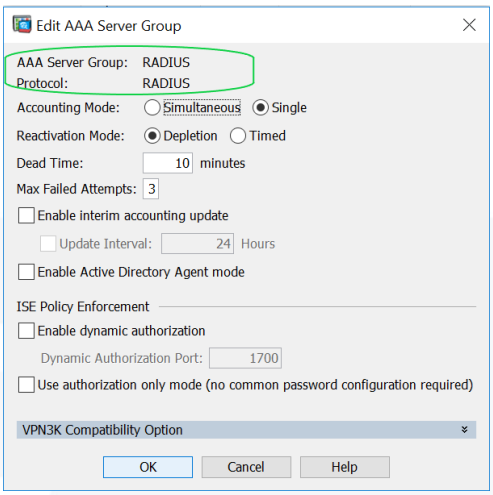
1.4 Authentication

The following section describes the steps required to configure the Cisco ASA to authenticate users via RADIUS and assign security policies to users based on their LDAP groups.

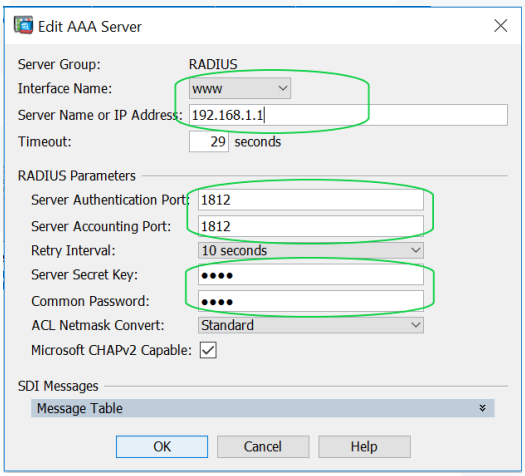
1.41 Setup RADIUS Connection

Navigate to Configuration\Remote Access VPN\AAA/Local Users\AAA Server Groups and select add, to configure a new Server.

- Configure a AAA Server Group Name e.g. RADIUS and select the protocol RADIUS from the drop-down list, selecting OK to finish.

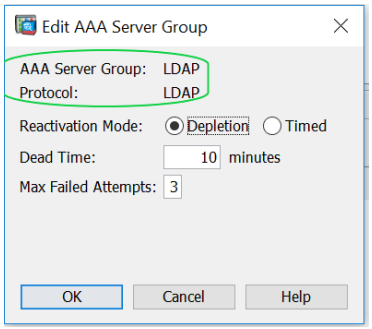


- Highlight the newly created Server group and click Add to define a new RADIUS server.
- Select the Interface Name (Usually the Cisco ASA interface that is closest to the RADIUS Server, which is the SecurEnvoy Server in this case).
- Fill in the Server Name (if using DNS or the IP address of the SecurEnvoy Server)
- Change the Server Authentication and Accounting port to 1812
- Enter in the Server Secret Key and Common Password that was configured and matches the key configured when RADIUS was setup on SecurEnvoy SecurAccess Server.
- Click OK to continue

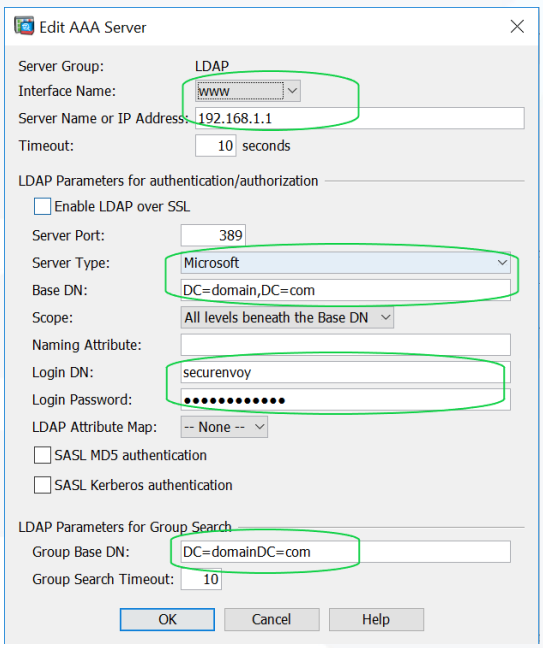


1.41 Setup LDAP Connection

- Navigate to Configuration\Remote Access VPN\AAA/Local Users\AAA Server Groups and select add, to configure a new Server.
- Configure a AAA Server Group Name e.g. LDAP and select the protocol LDAP from the drop-down list, selecting OK to finish.



- Highlight the newly created Server group and click Add in the Servers in the selected group section.
- Select the Interface Name (Usually the Cisco ASA interface that is closest to the LDAP Server, which is the Domain Controller in this case).
- Fill in the Server Name (if using DNS or the IP address of the Primary Domain Controller)
- Select the Server Type from the drop-down list (Dependent on your type of LDAP Server)
- Enter the Base DN: of your domain in the format DC=your-domain-name,DC=com
- Enter in an account username and password that has read access to the domain controller under the section Login DN: and Login Password
- Complete the Group Base DN: of your domain in the format DC=your-domain-name,DC=com
- Click OK to continue

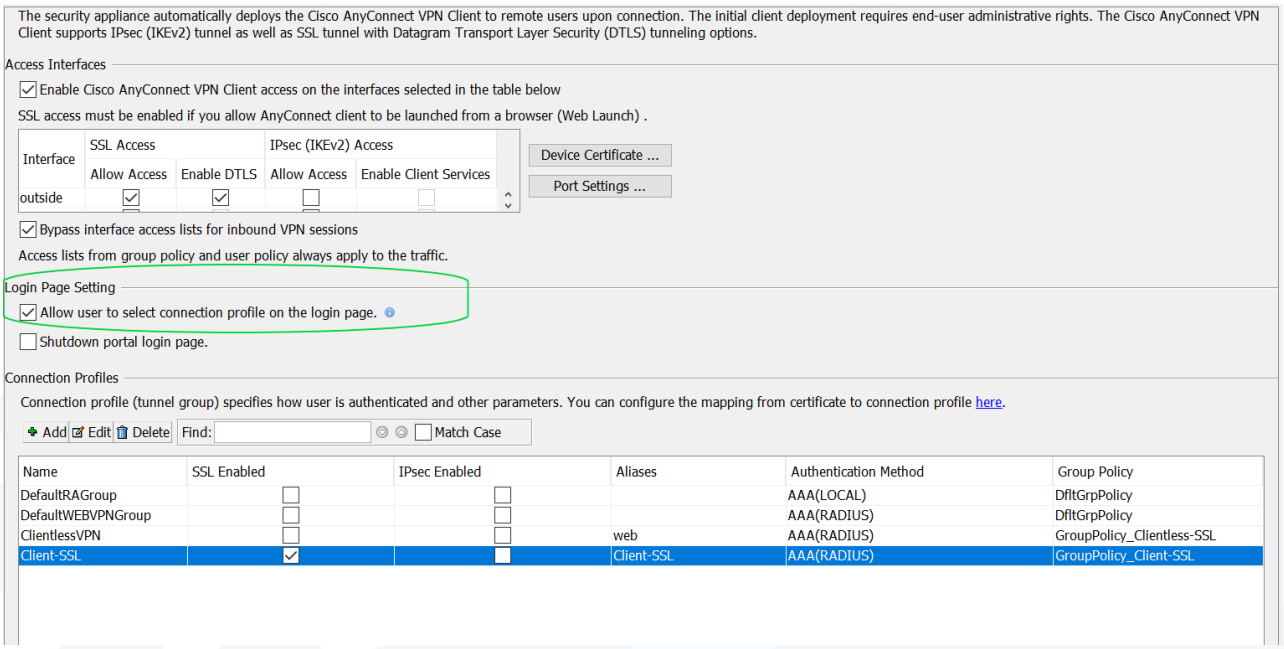


1.5 Cisco AnyConnect VPN (Client)

The following section describes steps required to configure the Cisco AnyConnect SSL VPN client to authenticate with SecurEnvoy's MFA solution, using LDAP groups to define the Cisco ASA security policy that will be assigned to the user.

1.5.1 VPN Wizard

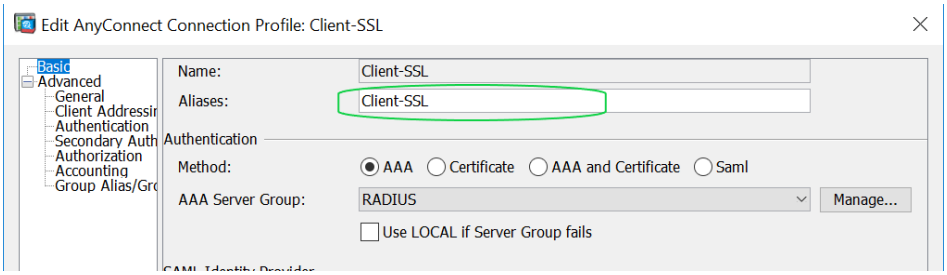
- Run the Cisco AnyConnect VPN Wizard from the Cisco ASDM and give it a meaningful Connection Profile name e.g. Client-SSL
- Navigate to Wizards\VPN Wizards\AnyConnect VPN Wizard…. From the Cisco ASDM tool bar.
- *Note: Select the previously configured group RADIUS when the wizard asks for Authentication methods.*
- On completion of all steps in the Wizard, navigate to the Remote Access VPN connections section. Configuration\Remote Access VPN\Network (Client) Access\AnyConnect Connection Profiles
- From the Network (Client) Access home page, make sure "Allow user to select connection profile on the login page" is selected.



1.5.2 Aliases

On completion of the Wizard, we will need to create an alias for the newly created Client-SSL profile.

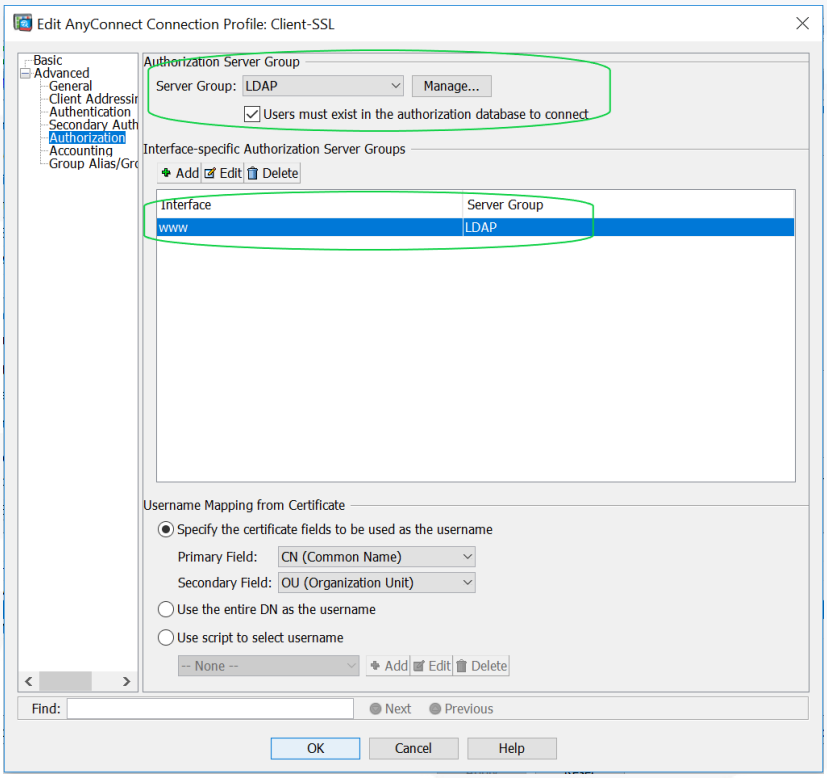
- Highlight and edit the newly created Client-SSL Profile
- Create a meaningful name under the Aliases section



1.5.3 Authorisation

The following section will configure the ASA to check the user logging in, is present in the LDAP directory before allowing access.

- Whilst editing the Connection Profile, select the Advanced\Authorization section
- Select from the list, the previously created LDAP Group and select Users must exist in the authorisation database to connect
- Click OK to continue



1.5.4 Group Policy

As best practice it is advisable to create a Group Policy for the newly created AnyConnect SSL Client VPN.

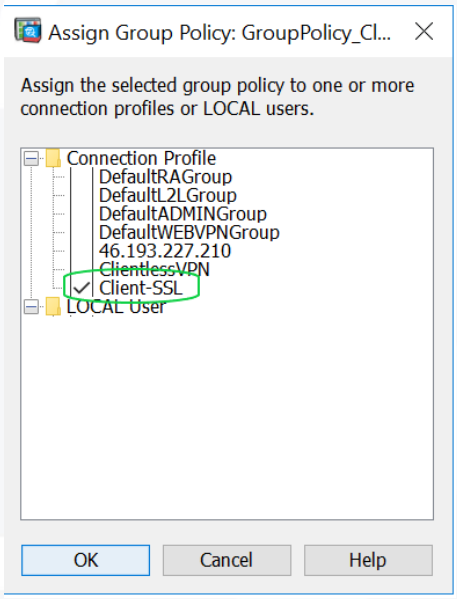
- Navigate to Configuration\Remote Access VPN\Network (Client) Access\Group Policies
- Click Add (Select Internal Group Policy if asked) and provide a meaningful name e.g. GroupPolicy_Client-SSL
- Untick the Inherit checkbox next to Tunnelling Protocols and uncheck all except SSL VPN Client

If it is required for the client to have local internet breakout additional to the VPN tunnel, then this can be configured under Split Tunnelling in the Advanced section of the Group Policy.

- On completion of the above configuration, select OK to proceed

We now need to assign the Group Policy to the Connection Profile created following the run of the VPN Wizard.

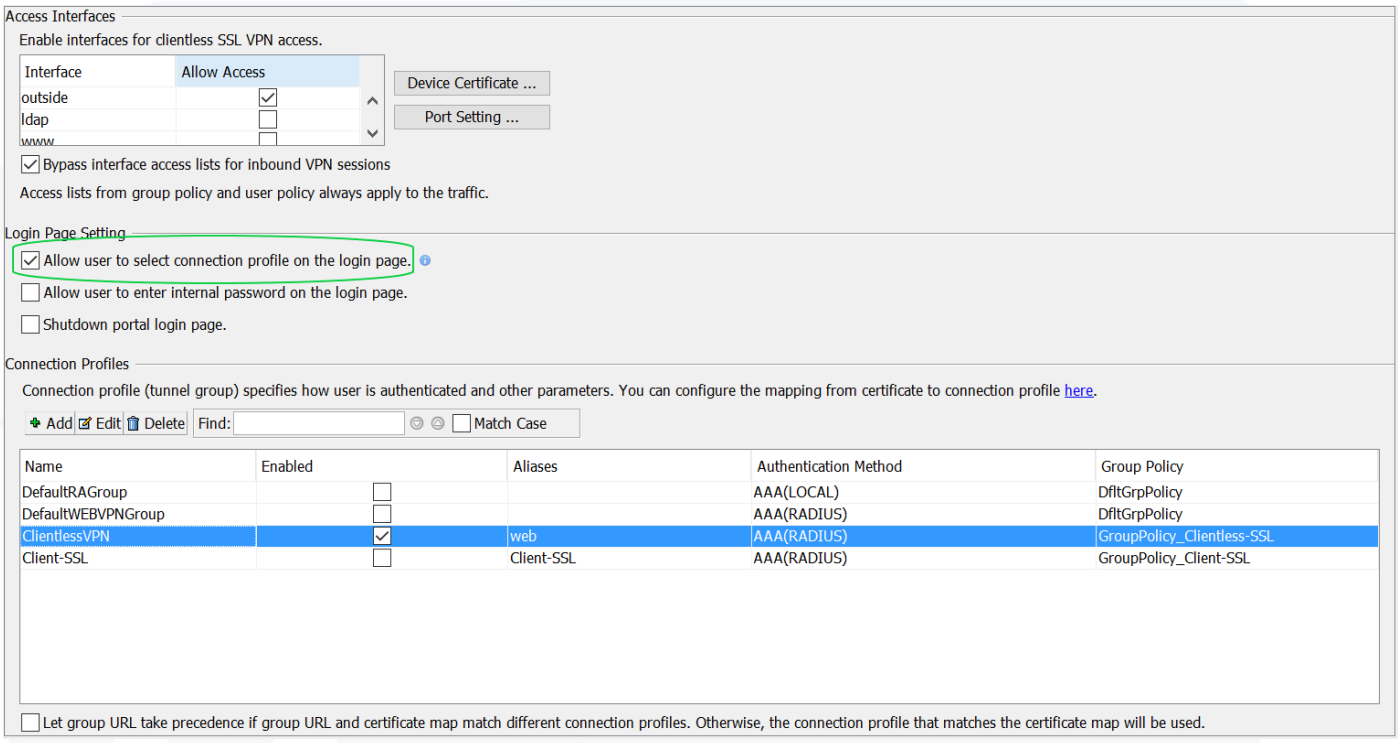
- Highlight the newly created GroupPolicy_Client-SSL and click Assign
- Tick the box next to the Connection Profile created earlier e.g. Client-SSL



1.6 Cisco Clientless SSL VPN Access

1.6.1 VPN Wizard

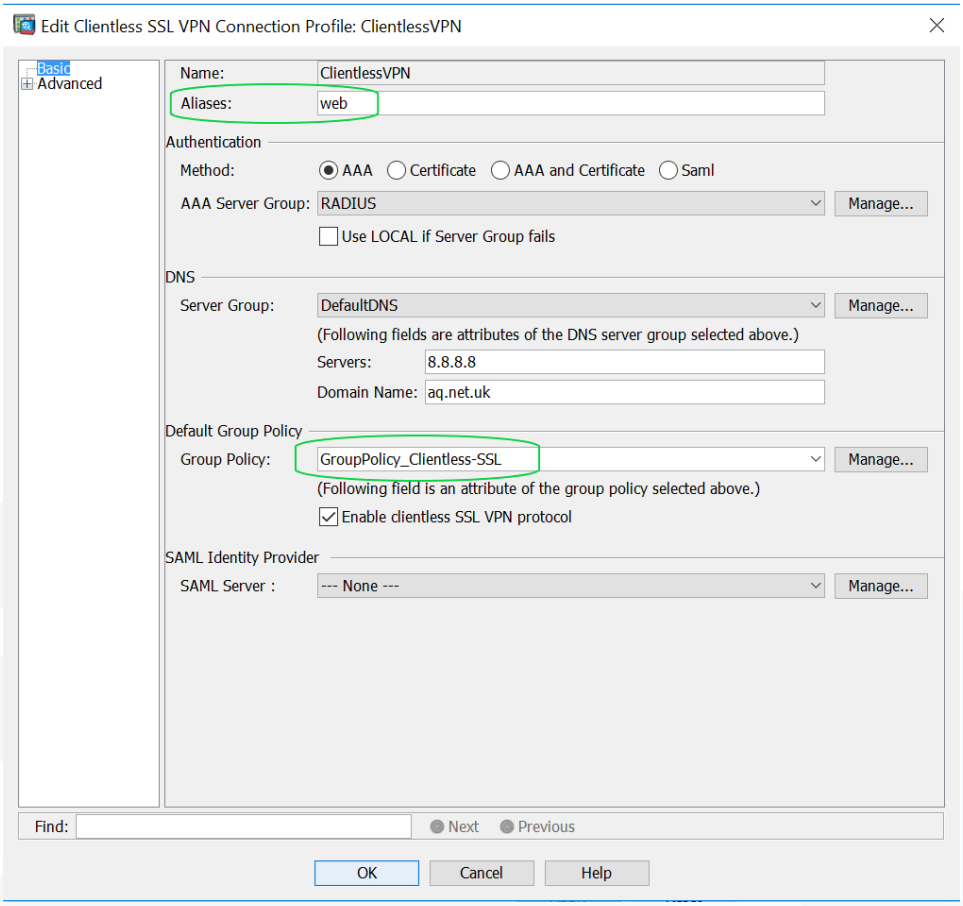
- Run the Cisco Clientless SSL VPN Wizard from the Cisco ASDM and give it a meaningful Connection Profile name e.g. Clientless-SSL
- Navigate to Wizards\VPN Wizards\ Clientless SSL VPN Wizard…. From the Cisco ASDM tool bar.
- *Note: Select the previously configured group RADIUS when the wizard asks for Authentication methods.*
- As best practice it is advisable to create a new Group Policy for the Clientless SSL VPN. When the Wizard asks for group policy, select Create New Group Policy and give it a meaningful name e.g. GroupPolicy_Clientless-SSL
- Complete the Wizard and select Finish
- On completion of all steps in the Wizard, navigate to the Remote Access VPN connections section. Configuration\Remote Access VPN\Clientless SSL VPN\Connection Profiles
- From the Connection Profiles home page, make sure "Allow user to select connection profile on the login page" is selected.



1.6.2 Aliases

On completion of the Wizard, we will need to create an alias for the newly created Clientless-SSL profile.

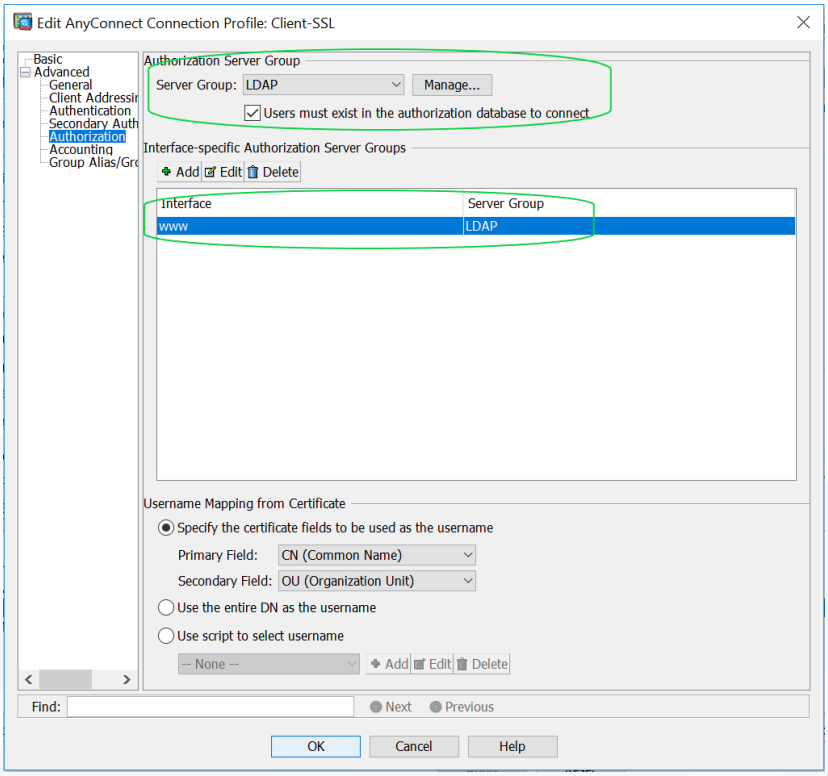
- Highlight and edit the newly created Clientless-SSL Profile
- Create a meaningful name under the Aliases section e.g. Web
- Make sure the Group Policy created during the VPN Wizard is selected from the list



1.6.3 Authorisation

The following section will configure the ASA to check the user logging in, is present in the LDAP directory before allowing access.

- Whilst editing the Connection Profile, select the Advanced\Authorization section
- Select from the list, the previously created LDAP Group and select Users must exist in the authorisation database to connect
- Click OK to continue

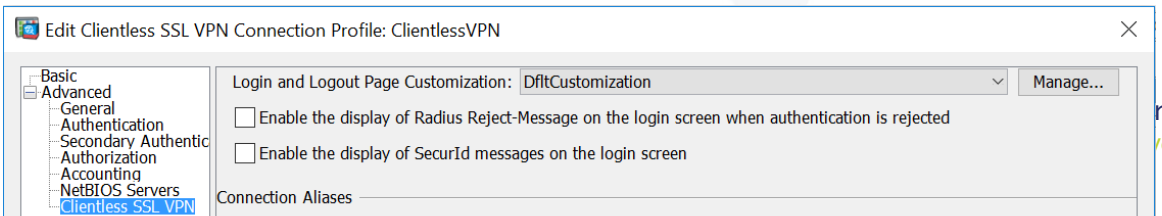


1.6.4 Group URL

This section will configure a group URL that will automatically select the correct connection profile for the Clientless SSL VPN when the user browses to the Cisco ASA with the included alias.
This URL can be bookmarked in the client's browser to return to the same URL for connectivity.

- From within the same Clientless SSL VPN Connection profile select Clientless SSL VPN from the left-hand navigation.
- Make sure the Connection Aliases configured earlier is ticked
- Under Group URL's, select Add and type in the full URL that the user will use to access the Clientless SSL VPN portal, appending the alias created earlier e.g. /web
- Select Disable CSD for both AnyConnect and Clientless SSL VPN
- Click OK to continue

Note: When clients browse to the Clientless VPN portal, please use the URL you defined under Group URL's. If the alias is not used it will present a drop-down box for the client to select at login.



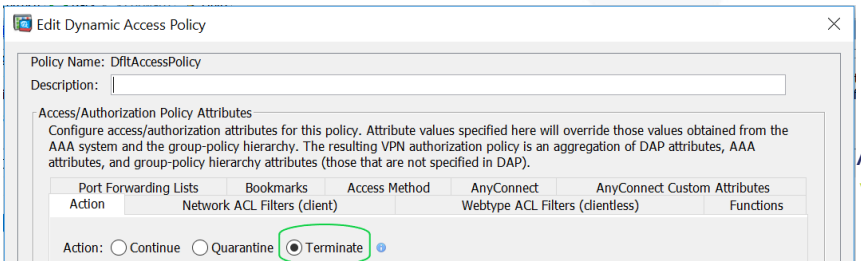
1.7 Dynamic Access Policies

The following section describes steps required to configure the Cisco ASA to authenticate with SecurEnvoy's MFA solution, using LDAP groups to create individual polices against the LDAP directory group that the user is part of, restricting what applications or networks they are allowed to access. These groups are reutilised for both the Client based VPN profile as well as the Clientless VPN Portal access.

- Navigate to Configuration\Remote Access VPN\Network (Client) Access\Dynamic Access Policies

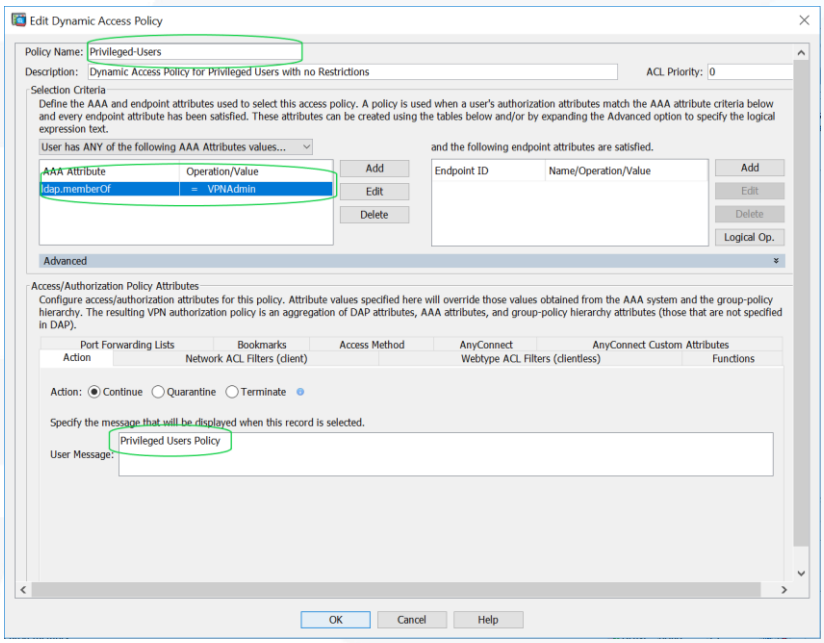
The first thing we need to do is make sure the default policy blocks or denies access to users if they are not approved to connect and login.

- Highlight DfltAccessPolicy and click Edit
- Under the Action tab, select Action: Terminate
- Click OK to continue

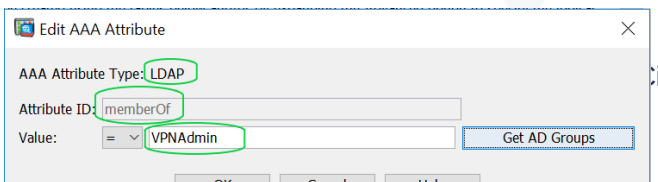


We will now create Dynamic Access Polices that determine a user's privileges based on a particular LDAP group.

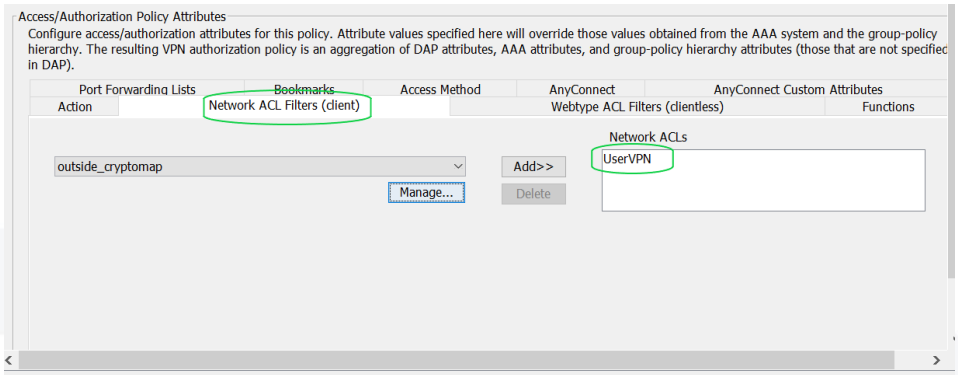
- Navigate to Configuration\Remote Access VPN\Network (Client) Access\Dynamic Access Policies
- Select Add to create a new Dynamic Access Policy and provide a meaningful name under Policy Name E.g. Privileged-User
- Define which LDAP group the user will be matched against in order to be assigned this policy by selecting Add from the Selection Criteria



- We will now select the LDAP group by selecting LDAP from the list AAA Attribute Type
- Make sure the Attribute ID: has memberOf specified in the field
- Select Get AD Groups and browse for the AD group that you would like to match against this Dynamic Access Policy
- Click OK to continue



- Dependent on the level of restrictions required on the Dynamic Access Policy, it is possible to define an ACL restricting the users network access to applications or locations.
- Select the Network ACL Filters (Client) tab under Access/Authorisation Policy Attributes and select from the drop-down list or create (Manage) a new ACL that can be assigned to the group.



Please Reach Out to Your Local SecurEnvoy Team...

UK & IRELAND

The Square, Basing View
Basingstoke, Hampshire
RG21 4EB, UK

Sales

E sales@SecurEnvoy.com
T 44 (0) 845 2600011

Technical Support

E support@SecurEnvoy.com
T 44 (0) 845 2600012

EUROPE

Freibadstraße 30,
81543 München,
Germany

General Information

E info@SecurEnvoy.com
T +49 89 70074522

ASIA-PAC

Level 40 100 Miller Street
North Sydney
NSW 2060

Sales

E info@SecurEnvoy.com
T +612 9911 7778

USA - West Coast

Mission Valley Business Center
8880 Rio San Diego Drive
8th Floor San Diego CA 92108

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA - Mid West

3333 Warrenville Rd
Suite #200
Lisle, IL 60532

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA – East Coast

373 Park Ave South
New York,
NY 10016

General Information

E info@SecurEnvoy.com
T (866)777-6211

SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com