

INTEGRATION GUIDE

# How to Configure Cisco ASA to secure VPN access with Portnox CLEAR

## Introduction

This document guides you step by step how to configure your VPN environment using Portnox CLEAR to enable secure and trusted cloud-based RADIUS access with an optional push-to-access MFA.

## Preliminary Actions

Before configuring VPN authentication, you need to verify the following:

- 1) Verify your organization is registered on Portnox CLEAR Cloud Services: <https://clear.portnox.com/>
- 2) In the CLEAR portal, go to **Settings > Services** and expand **CLEAR RADIUS Service**. Then:
  - a. If the **Enable Cloud RADIUS** checkbox is not checked, click **Edit** and check the **Enable Cloud RADIUS** checkbox.
  - b. Note the RADIUS server details which you will need when configuring VPN access:
    - **Cloud RADIUS IP** – this is the IP address of the CLEAR RADIUS server
    - **Authentication port**
    - **Accounting port**
    - **Shared Secret** – this is the RADIUS client shared secret
- 3) In the CLEAR portal, go to **Settings > Groups** and create a group for VPN users, or edit an existing one. In the **group settings > VPN Access** select the following:
  - Allowed authentication type = credentials.
  - (optional) Multi-Factor Authentication = push-to-access on mobile only.  
Note, MFA on mobile devices require AgentP to be enrolled on the mobile device.
  - For implementation with AgentP, check the: validate risk score for all managed devices.

# Configuring Cisco ASA VPN

In the following steps, we configure the VPN authentication to be secured and protected based on RADIUS authentication. The following steps should be performed in the Cisco ASA console.

## Step 1 - Creating a RADIUS Authentication Server

- 1) Create a RADIUS server group by navigating to **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups** and clicking **Add**.

The screenshot displays the Cisco ASDM 7.8(1) interface for configuring AAA Server Groups. The breadcrumb navigation at the top reads: **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**. The main content area is titled "AAA Server Groups" and contains a table with the following columns: Server Group, Protocol, Accounting Mode, Reactivation Mode, Dead Time, Max Failed Attempts, and Realm Id. A single entry is visible: LOCAL, LOCAL, (blank), (blank), (blank), (blank), and LOCAL. To the right of the table are buttons for "Add", "Edit", and "Delete". Below the table is a search field labeled "Find:" and a "Match Case" checkbox. Underneath is a section titled "Servers in the Selected Group" with a table for adding servers, including columns for "Server Name or IP Address", "Interface", and "Timeout". To the right of this table are buttons for "Add", "Edit", "Delete", "Move Up", "Move Down", and "Test". At the bottom of the main content area is a search field and a "Match Case" checkbox. The left sidebar shows the navigation tree with "AAA Server Groups" selected under "AAA/Local Users". The bottom of the interface features "Apply" and "Reset" buttons.

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts	Realm Id
LOCAL	LOCAL					LOCAL

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

- 2) In the Add AAA Server Group window that appears:
  - a. Specify a name for the **AAA Server Group**.
  - b. In **Protocol** select **RADIUS**.
  - c. Enter a **Realm-id**.

The screenshot shows the 'Add AAA Server Group' dialog box. The 'AAA Server Group' field is highlighted with a blue box and contains the text 'CLEAR'. The 'Protocol' dropdown menu is set to 'RADIUS'. The 'Realm-id' field contains the number '1'. Below these fields, there are several radio button options: 'Accounting Mode' with 'Simultaneous' and 'Single' (selected), and 'Reactivation Mode' with 'Depletion' (selected) and 'Timed'. There are also input fields for 'Dead Time' (10 minutes) and 'Max Failed Attempts' (3). Below these are three unchecked checkboxes: 'Enable interim accounting update' (with a sub-field for 'Update Interval' set to 24 Hours), 'Enable Active Directory Agent mode', and 'ISE Policy Enforcement' (with a sub-field for 'Dynamic Authorization Port' set to 1700). At the bottom, there is a 'VPN3K Compatibility Option' dropdown menu and three buttons: 'OK', 'Cancel', and 'Help'.

- 3) Select the AAA server group you created, and in the **Servers in the Selected Group** section, click **Add**.

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts	Realm Id
CLEAR	RADIUS	Single	Depletion	10	3	1
LOCAL	LOCAL					

Find:   Match Case

Servers in the Selected Group

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

Find:   Match Case

LDAP Attribute Map



- 4) In the Edit AAA Server window that appears:
- Enter the following CLEAR RADIUS server details, which you noted in [Preliminary Actions](#), step 2(b):
    - In **Server Name or IP Address**, enter the Cloud RADIUS IP.
    - In **Server Authentication port**, enter the Authentication port.
    - In **Server Accounting port**, enter the Accounting port.
    - In **Server Secret Key**, enter the Shared Secret.
  - Update the **Timeout** to 30 seconds.
  - Verify that the **Microsoft CHAPv2 Capable** checkbox is checked.
  - Click **OK**.

The screenshot shows the 'Edit AAA Server' dialog box. The 'Server Group' is set to 'CLEAR' and the 'Interface Name' is 'management'. The 'Server Name or IP Address' field is redacted. The 'Timeout' is set to '30 seconds'. Under 'RADIUS Parameters', the 'Server Authentication Port' and 'Server Accounting Port' are redacted, 'Retry Interval' is '10 seconds', 'Server Secret Key' is redacted, 'Common Password' is empty, and 'ACL Netmask Convert' is 'Standard'. The 'Microsoft CHAPv2 Capable' checkbox is checked. The 'SDI Messages' section shows 'Message Table' selected. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

## Step 2 - Configuring the VPN connection profile

- 1) Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**, and in the **Connection Profiles** section click **Add**.

The screenshot shows the Cisco ASDM 7.8(1) for ASA interface. The breadcrumb navigation is **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**. The left sidebar shows the **Remote Access VPN** tree with **AnyConnect Connection Profiles** selected. The main content area is titled **AnyConnect Connection Profiles** and contains the following sections:

- Access Interfaces:** Includes a checkbox to enable Cisco AnyConnect VPN Client access on selected interfaces. Below it is a table for interface configuration:
 

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).**
- Connection Profiles:** Contains a table of existing profiles:
 

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

The **Add** button in the **Connection Profiles** section is highlighted with a red box. At the bottom of the page are **Apply** and **Reset** buttons.

2) In the Edit AnyConnect Connection Profile window that appears:

a. In the **Basic** tab:

- Specify a **Name** for the connection profile.
- Specify **Aliases** for the connection profile.
- Select the **AAA server group** that was created in Step 1).
- Select **Client Address Pools**.
- Check the **Enable SSL VPN client protocol** checkbox.
- Specify **DNS servers**.
- Specify **Domain Name**.

Edit AnyConnect Connection Profile: CLEAR-VPN

Basic

Advanced

Name: CLEAR-VPN

Aliases: CLEAR

Authentication

Method: AAA

AAA Server Group: CLEAR

Use LOCAL if Server Group fails

SAML Identity Provider

SAML Server : --- None ---

Client Address Assignment

DHCP Servers:

None  DHCP Link  DHCP Subnet

Client Address Pools: VPN-Subnet

Client IPv6 Address Pools:

Default Group Policy

Group Policy: DfltGrpPolicy

(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:

Domain Name: [REDACTED]

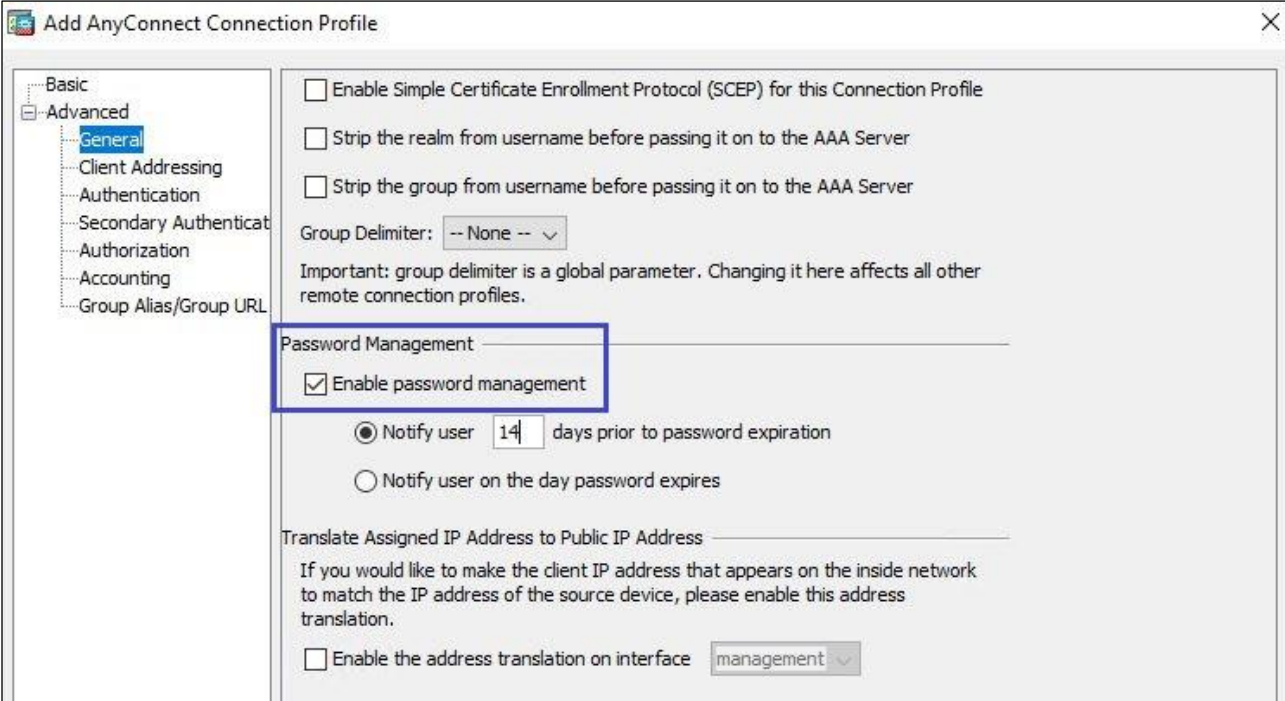
Find: [REDACTED] Next Previous

OK Cancel Help



b. In the **Advanced** tab:

- Check the **Enable password management** checkbox.



The screenshot shows the 'Add AnyConnect Connection Profile' dialog box. The 'Advanced' tab is selected, and the 'General' sub-tab is active. The 'Enable password management' checkbox is checked and highlighted with a blue box. Other options include 'Enable Simple Certificate Enrollment Protocol (SCEP) for this Connection Profile', 'Strip the realm from username before passing it on to the AAA Server', and 'Strip the group from username before passing it on to the AAA Server'. The 'Group Delimiter' is set to '-- None --'. A note states: 'Important: group delimiter is a global parameter. Changing it here affects all other remote connection profiles.' Below this, there are radio buttons for 'Notify user 14 days prior to password expiration' (selected) and 'Notify user on the day password expires'. At the bottom, there is a section for 'Translate Assigned IP Address to Public IP Address' with a checkbox and a dropdown menu set to 'management'.

c. Click **Apply**.

3) Verify that:

- a. In the **Access Interfaces** section, the **Enable Cisco AnyConnect VPN Client access on the interface selected in the table below** checkbox is checked.
- b. In the **Login Page Settings** section, the **Allow user to select connection profile on the login page** checkbox is checked.

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user authentication.

**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
management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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.

Find: 


 Match Case

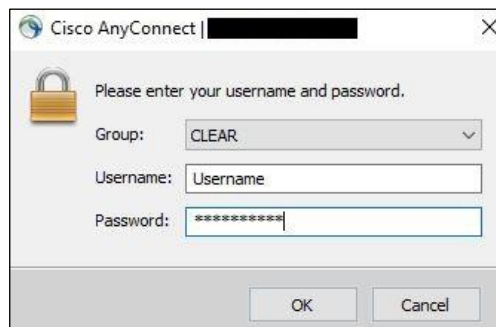
Name	SSL Enabled	IPsec Enabled
DefaultRAGroup	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DefaultWEBVPNGroup	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CLEAR-VPN	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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

# Instructions for Supplying VPN Credentials

## Supplying VPN Credentials without MFA

For successful VPN authentication using Portnox CLEAR RADIUS, users are required to provide their username + password:



## Supplying VPN Credentials with push-to-access MFA

For successful VPN authentication using Portnox CLEAR RADIUS and push-to-access MFA, users are required to provide their username + password and allow the push notification on their mobile device:

