WLAN & LAN ACESS CONTROL

WLAN & LAN Acess Control

WLAN Radius EAP 802.1X

1. WebADM/OpenOTP/Radius Bridge

This guide explains how to deploy Network Access Control (NAC) using 802.1X protocol and OpenOTP. This solution can be applied both to Wireless LAN and wired LAN networks. For this recipe, you will need to have WebADM/OpenOTP installed and configured. Please, refer to WebADM Installation Guide and WebADM Manual to do so. You have also to install our Radius Bridge product on your WebADM server(s).

For authentication, you have two possible mechanisms.

1. Username and password authentication using EAP-TTLS
2. Certificate authentication using EAP-TLS (Supported from WebADM 1.6.8 & Radius Bridge 1.3.6)

Same configuration can be used in Radius Bridge for both of these scenarios.

2. Radius Bridge Configuration

On your OpenOTP Radius Bridge server, edit the */opt/radiusd/conf/clients.conf* and add a RADIUS client (with IP address and RADIUS secret) for your WLAN controller or access point.

Example:

```
client NAC_CLIENT {
    ipaddr          = <Radius_Client_IP>
    secret          = testing123
}
```

2.1 Enabling EAP-TLS in Radius Bridge

If you wish to use EAP-TLS with user certificates for authentication (instead of username+password), should enable the following settings in */opt/radiusd/conf/radiusd.conf*

```
cert_support = yes
ocsp_url = "https://<webadm_ip>/ocsp/"
```

3. Configuring the RADIUS AAA Server to your Access Point, WLAN Controller or LAN Switch

The next step is to configure wireless to use WPA2 Enterprise security mode and to define the RADIUS server as the authentication

provider for your WLAN. The specific configuration depends on the make and model of you WLAN equipment, two examples are provided by the chapters below.

3.1 For WLAN Access Point

If you have a standalone WLAN access point or router, without a centralized controller, you must configure the RADIUS server to each access point/router.

The below image provides an example of Cisco Linksys wireless router configuration.

3.2 For Cisco WLAN Controller

In this case, we add a RADIUS AAA Server configuration to your Cisco WLAN controller:

1. Login to the WLC GUI.
2. Click Security and RADIUS > Authentication.
3. In the RADIUS Authentication servers page appears, click New to add a new RADIUS Authentication Server.
4. Enter the RADIUS server corresponding to the Radius Bridge configuration on chapter 2.

Next, configure the WLAN networks and settings:

1. Open the WLANs page from the controller web interface.
2. Choose an existing or create a new WLAN.
3. In the “Security” tab, open “AAA Servers” subtab.
4. Select the RADIUS server you configured as the “Authentication server”.
5. Click Apply to save your configuration.

4. Client Configuration for username+password Authentication (EAP-TTLS)

The correct authentication protocol and settings must be configured also into your wireless clients.

> ⚠ Note
>
> To securite EAP-TTLS connection it is critical that you configure your Radius Bridge /opt/radiusd/conf/ca.crt certificate to all the clients to authenticate the Radius server you are connecting to. Without this the client is vulnerable to man in the middle attack and will disclose username and password to malicious access point!

4.1 Windows PCs

The exact configuration depends on the Windows version used.

4.1.1 Windows 10

Windows 10 has native support for the required authentication protocols, so it is possible to connect to the network directly. However, Microsoft has some special [requirements] (https://support.microsoft.com/en-us/help/814394/certificate-requirements-when-you-use-eap-tls-or-peap-with-eap-tls) for the server certificates used in this case.

The current version of Radius Bridge uses certificates generated by WebADM which will comply with these requirements, but older installation must recreate the certificates with an additional configuration. Below is a sample of the required commands that can be used for creating a new server certificate on older Radius Bridge server.

```
cd /opt/radiusd/conf
echo -e "[ xpserver_ext]\nextendedKeyUsage = 1.3.6.1.5.5.7.3.1\n" > xpextensions
openssl genrsa -out radiusd.key 2048
openssl req -sha256 -new -key radiusd.key -out radiusd.csr -subj
"/CN=HOSTNAME/O=ORGNAME"
openssl x509 -req -days 3650 -in radiusd.csr -signkey radiusd.key -out radiusd.crt -
extensions xpserver_ext -extfile xpextensions
```

4.1.2 Windows 7

Windows 7 does not support the required EAP-TTLS authentication natively, so you must either use a 3rd party wireless client or install a WPA supplicant plugin. In this guide, we have used the [GÉANTLink] (https://github.com/Amebis/GEANTLink) plugin.

1. Download the correct version of the GÉANTLink [binary] (https://github.com/Amebis/GEANTLink/releases) (GEANTLink32.msi or GEANTLink64.msi).
2. Install the plugin on the Windows client.
3. Configure the WLAN settings as in the below images.

4. You must transfer the /opt/radiusd/conf/radiusd.crt from the Radius Bridge server and select it with “Add CA from File”.

4.2 MacOS / iOS

Users cannot directly configure the correct settings in MacOS and iOS, instead the configuration must be created using Apple Configurator 2. Please see below picture for a sample configuration.

4.3 Android

Android has native support of the required protocols. Below picture provides a sample of the settings.

4.4 Linux

Most Linux clients also have native support and the connection can be configured graphically. Below is a screenshot of Ubuntu 17.10 Network Manager.

5. Client Configuration for User Certificate Authentication (EAP-TLS)

The correct authentication protocol and settings must be configured also into your network clients.

5.1 Generating and Downloading required Certificates

All the required certificates can be downloaded either from the Self-Service portal or from the WebADM administrative interface. This guide explains the process using the Self-Service portal. First log into the Self-Service portal with your username, then select the PKI page.

On the PKI page, first click the “Get WebADM CA Certificate” to CA Certificate.

Next, click the “Add new Certificate” button to generate a user certificate followed by clicking the “Download” button.

⚠ Note

Please note that the certificate password is required in the following steps and it is only available on this page. It cannot be recovered later.

You should now have the required certificates for client configuration.

5.2 Windows PCs

The exact configuration depends on the Windows version used.

5.2.1 Windows 10

Windows 10 has native support for the required authentication protocols, so it is possible to use certificates for authentication without additional software.

First we must install the CA certificate of your WebADM to the Windows client. Open the CA certificate in Windows and click “Install Certificate”.

Click “Next” on the following page in Certificate Import Wizard.

On the next page, select the certificate store in which the certificate should be installed. You must install the certificate in the “Trusted Root Certification Authorities”. Click “Next” followed by “Finish” on the next page.

Next we install the user certificate downloaded from Self-Service to the Windows client. Open the user certificate, select “Current User” in the wizard and click “Next” two times.

When the wizard asks for the password for the certificate, input the password you’ve received in the Self-Service desk when downloading the certificate.

You can let Windows select the certificate store for the user certificate automatically. Click “Next” followed by “Finish”.

Now we can connect to the wireless network, find the network in question from your network connections and click “Connect”.

When you are prompted for username and password, select “Connect using a certificate”.

Choose the user certificate you’ve installed previously, click “OK” followed by “Connect”.

5.3 MacOS / iOS

In MacOS, open the downloaded user certificate to install it into the keychain. Input the password you’ve received from the Self-Service Desk.

Once the user certificate is in your keychain, you can select the wireless network to connect to. In the following screen, select “Mode: EAP-TLS”, use the installed user certificate as the identity and click “Join”.

5.4 Android

Android has native support of the required protocols, although this might depend on the specific version of Android. First, transfer the downloaded certificate on your phone, and then configure the wireless network.

5.5 Linux

Most Linux clients also have native support and the connection can be configured graphically. Below is a screenshot of Ubuntu 18.04 Network Manager.

⚠ Note

Don’t forget to authorize the communication on 1812 UDP port (default RADIUS port for the authentication) from your ASA system to your Radius Bridge instance at the firewall level.

6. Radius Return Attributes

Radius return attributes can be used with both EAP-TTLS and TLS starting from WebADM 1.7.9-1 and Radius Bridge 1.3.11. This is a powerful mechanism which allows you to centrally control various characteristics of the network connection on per user/group basis, for example:

-VLAN allocation

-Access Control List Configuration

-Quality of Service Policies

Please refer to your network equipments documentation on which attributes can be used for your specific use case. The related WebADM configuration is explained in Radius Attributes guide.