This document describes how SonicWall Secure Mobile Access (SMA) 1000 is integrated with the Remote Authentication Dial-In User Service (RADIUS) networking protocol. Such integration allows RADIUS to run in the application layer of cloud-based Microsoft Azure Multi-Factor Authentication Server (MFS), which provides two-step verification.

Topics:
- About RADIUS
- Requirements
- Log into SMA
- Configuring Your Server
- Testing the Client Connectivity Using SSL Client

About RADIUS

RADIUS is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service. The application is often used to access internal security networks. RADIUS is also a client/server protocol that runs in an application layer such as Microsoft Azure MFS.

Requirements

- Windows 10, Windows 7 x86 SP1/x64
- Windows 2016/2019 Server
- LDAP servers
- RADIUS Protocol
Log into SMA

1. Go to your SMA client web browser, for example from Windows 10 Enterprise, and connect to the SMA 1000 IP address.
2. Select RADIUS UNPW as the authentication enabled REALM.
3. Click Next.
4. Enter the Username and Password in the text fields provided.
5. Click Log in.
   You are now an authenticated WorkPlace.
7 In the AUTHENTICATION SERVERS section, click New.

8 Under USER STORE, choose RADIUS as the protocol to configure your authentication.

9 Under CREDENTIAL TYPE, select Username/Password and click Continue.

10 On the Edit Authentication Server page, enter RADIUS as the name for your RADIUS server.

11 Enter the IP Address in the Primary RADIUS server text field provided.

12 Enter sonicwall in the Shared secret text field provided.

Check that the connection is working by clicking Test.

13 Click Save to keep your settings.
14 On the Authentication Servers page, under AUTHENTICATION SERVERS, check to make sure the authentication server is referenced by a realm listed.

15 Create a realm associated with your RADIUS Authentication Server by navigating to Monitoring.
Configuring Your Server

Configure your Microsoft Windows 2016 or Microsoft Windows 2019 servers to authenticate using RADIUS.

1. Go to Server Manager | Dashboard > All Servers.
2. On the top right of the Server Manager console, go to Manage > Add Roles and Features.
3. On the left of the Add Roles and Features Wizard screen that displays, choose Server Selection.
4. Select the radio button for Select a server from the server pool, pick Interactive Services Detection under the Display Name column, and click Next.
5. Then, in the Add Roles and Features Wizard screen, choose Server Roles and check the box next to Network Policy and Access Services.
6 Click Next.

7 Check the box for Include management tools and click Add Features.


9 Click Next.
10 Choose **Network Policy and Access Services** and click **Next**.

11 Choose **Confirmation** and click **Install**.
12 Choose **Results** and click **Close** when the installation is complete.
Installing Network Policy Server

1. On the top right of the Server Manager console, go to Tools > Network Policy Server.

2. On the Network Policy Server dialog that displays, right-click NPS (Local) at the top of the left panel to configure it as a RADIUS server.

3. Select Register server in Active Directory from the drop-down list.
4 Click OK to confirm the registration of the server in **Active Directory** and authorize your computer to read users’ dial-in properties from the sma.local domain.

5 Click **OK** again to register your computer to be a member of the **RAS/NPS Servers Group** in that domain.

Creating a Domain Group and RADIUS Users

1 Click the **RADIUS Clients and Servers** section, select **RADIUS Clients**, and choose **New** from the drop-down list.

2 In the **New RADIUS Client** dialog, do the following under the **Settings** tab:
   - Select **Enable this RADIUS Client**.
   - Enter the **Friendly Name**, for example, app214.
   - Enter the **IP or DNS Address** in the text field provided.
   - Select **Manual** to manually type a **Shared secret**.
   - **Confirm the shared secret** in the text field provided.
   - Click **OK**.
3 Expand the Network Policies section and select New.

4 In the New Network Policy dialog, do the following:
   - Specify the Policy name in the text field provided, for example, `sma_policy`.
   - Type of network access server should remain unchanged as Unspecified.
   - Click Next.
Adding a User Group to New Network Policy

1. In the **Network Policies** dialog, select a condition such as **Groups**.

   You need to add conditions under which the RADIUS policy is applied.

2. Select **Windows Groups** as a condition to specify that the connecting user must belong to one of the selected groups.

3. Click **Add**.
4 Select **Group** as the **Object Type**, **sma.local** as the **Location**, and enter the **object name** in the text field. For example, **radius_users**.

5 Click **Add**.
6 Select **Access granted** and click **Next**.

7 Configure one or more authentication methods required for the connection request to match the policy. For EAP authentication you must configure an **EAP type**.

8 Click **Add**.
9 Configure the constraints for the network policy for *Idle Timeout* and specify the maximum time in minutes that the server can remain idle before the connection is disconnected.

- Check the *Disconnect after the maximum idle time* box.
- Select the amount of time from the drop-down list.
- Click *Next*.

10 Configure settings, such as *RADIUS Attributes*, for the connection request for the network policy.
11 Complete the **New Network Policy** by checking the **Policy conditions** and **Policy settings** in the window that displays and click **Finish**.

![Network Policies](image)

**Testing the Client Connectivity Using SSL Client**

*Test the secure connection between the client browser and the SMA:*

1. Launch your client web browser, for example from **Windows 10 Enterprise**, and connect to the **SMA IP Address**.

![Client Connectivity](image)

2. Enter the **Username**, **Password**, and **Domain** in the text fields provided.
3. Click **LOGIN**.
   
   You are authenticated with the Domain LOGIN.
4. Access your **WorkPlace virtual office** and click a resource from the list below.
   
   The options you see depend on your SMA appliance.