Integration Guide: Secure Mobile Access 1000 and Duo Mobile

August 2019

This document describes how to configure one-time password (OTP), multi-factor authentication from Duo Mobile (Cisco) for SonicWall® Secure Mobile Access (SMA) 1000 appliances.

Topics:

• Authentication Overview
• System Requirements
• Configuring for Multi-Factor Authentication
• Testing Your Integration

Authentication Overview

This section gives an overview of multi-factor authentication as it relates to DUO and SMA 1000.

About OTP

One-time password (OTP) is a multi-factor authentication system that utilizes an algorithm to generate a one-time code. The code is sent to the user, usually on a mobile device, to be entered as part of the authentication process.

Several third parties have password applications that you can integrate with your SonicWall system. This document focuses on authentication through Duo, by Cisco.

About Duo Authentication

Duo has several options for securing your authentication of users. Refer to information on the Duo website to determine which method works best for your SonicWall solution.

There are three main methods the receiver can use to authenticate with Duo:

• **DUO push**: A prompt comes up on the screen from the Duo app that has been downloaded on the user’s mobile device.
• **Phone call**: A call comes to the mobile device requesting the user to click one or more buttons to authenticate.
• **Passcode**: A passcode comes by email or SMS/Text to the user’s mobile device, which the user then enters as part of the authentication process.

About RADIUS

RADIUS is a protocol, or language SMA 1000 uses to authenticate users through the DUO authentication process. The SMA appliance uses RADIUS to communicate with the DUO authentication system.
System Requirements

The requirements for this integration are an SMA 1000 system and a mobile device on which the DUO app can be downloaded.

Configuring for Multi-Factor Authentication

There are three steps required to set up authentication for an interface with Duo Mobile. These are described below:

Topics:

- SMA Configuration
- Server Side Configuration for DUO
- Registering the RADIUS User @ DUO Account

SMA Configuration

*Configure SMA for Multi-Factor Authentication using the following steps:*

1. Log into the SMA Appliance Management Console (AMC) and go to System Configuration>User Store>Authentication Directory > RADIUS to bring up the Edit Authentication Server screen.
2 Type **RADIUS DUO** in the **Name** field of the **Edit Authentication** screen.
3 Type the **IP/HostName:Port** of the Duo Proxy Server in the **Primary RADIUS server** field.
4 Type your password in the **Shared secret** field.
5 Type **20** in the **Connection timeout** field, then click **Save**.

6 Create a **Realm** associated with the **RADIUS DUO Authentication Server**.
Server Side Configuration for DUO

The following steps are needed to configure RADIUS for Duo access. For more information about configuring for Duo, refer to: https://duo.com/docs/radius

1. Log into the Backend RADIUS server.
2. Go to Start > Administrative tools > Network Policy Server.
3. Click on RADIUS Clients and Servers > RADIUS Clients > New.

4. Click Settings to give the client a Friendly name.

5. In Address (IP or DNS) field, type the IP Address, and click Verify.
6 Click **Resolve > OK**, to bring up the **Properties** screen.

7 In the **Shared secret** field, type your password. Confirm and click **OK**.
8 Go to `C:\Program Files(x86)\Duo Security Authentication Proxy\conf\authproxy.cfg`.

9 Edit the `authproxy.cfg` file.

10 Add an entry for your appliance.
   
   ```
   radius_ip_2= Host name or IP
   radius_secret_2= your password
   ```

11 Stop and restart DuoAuthProxy using `run as Administrator`. 
12 At Active Directory Users and Computers > SMA1000.duo.com > Users, create an Active Directory User on the same Backend server.
Registering the RADIUS User @ DUO Account

The third step in the process is registering the RADIUS user in the DUO account.

Register the new RADIUS user with the following steps:

1. Log into the Duo Admin Panel (https://admin.duosecurity.com)
   - User name: your user name
   - Password: your password

2. On the DUO Dashboard, go to Users > Add User, and type test.

3. Scroll down to Phones, and click Add Phone.

4. Add the phone number of your mobile device.
5 Edit User: test, if desired, by adding 1 to 4 aliases.

6 Scroll down to Phones and click on the phone number.

7 Click on Reactivate Duo Mobile.

8 Go to Dashboard > Phone # > Activate Duo Mobile, and click Generate DUO Mobile Activation Code.
9 Be sure the boxes are checked as you desire, and click **Send Instructions by SMS/Text**.

10 Check on your registered mobile device to be sure you have received the SMS/Text with a link to activate the app.
11 Click on the link received by SMS/Text on your registered mobile device to activate the app. This completes the integration between SMA 1000 and DUO Mobile.
Testing Your Integration

To test your integration, try authenticating to CT using a user who is registered in DUO: test.
12 Verify that you have received a Request Waiting on the DUO App on your mobile device. Tap to respond.
13 Click Approve for the Login Request on the mobile device.

14 Verify that the Authentication was successful.

15 Click OK and the SonicWall VPN icon appears.