SONICWALL®

Integration Guide

Configuring TOTP (Multi-Factor Authentication) Using Microsoft Authenticator on SonicWall® Secure Mobile Access Appliances

May 2019

SMA 200/400

SMA 500v for ESXi

SMA 500v for Hyper-V

This document describes how to configure time-based, one-time password (TOTP), multi-factor authentication for Secure Mobile Access (SMA) appliances running SMA 10.0. This document focuses on Microsoft Authenticator integration.

Topics:

Authentication Overview

Topics:

About TOTP

The time-based, one-time password (TOTP) is a multi-factor authentication scheme that utilizes an algorithm to generate a one-time code. TOTP is an alternative to traditional two-factor authentication methods. The TOTP keeps changing and is valid for 30 seconds at a time. Because the TOTP changes frequently, it is considered more secure than a standard OTP solution.

Several third parties have password applications that you can integrate into your SonicWall infrastructure, for example, Microsoft Authenticator, Google Authenticator, and Duo Mobile. This document focuses on Microsoft Authenticator.

About Microsoft Authenticator

By using Microsoft Authenticator, you can help strengthen your account security. For your second level of security you can use a fingerprint, face recognition or a PIN (personal identification code) through the authenticator. Because Microsoft Authenticator also supports the industry standard for time-based, one-time passwords, you can add any online account, like access Secure Mobile Access (SMA), to Microsoft Authenticator.

SMA Two-Factor Authentication Options

SMA appliance provides several options for managing password authentication, starting with Secure Mobile Access 9.0.

- **OTP via email**: one-time password (OTP) authentication is verified one time through email. The user gets a temporary password, by email, after they log in with their regular user name and password. Once they input the password from their email, the login process completes.
- **OTP via SMS:** enables user to use an SMS code for one-time password authentication.
- **TOTP via mobile application**: enables user to use OTP authentication in which the OTP (generated using a mobile application) keeps changing and is valid for 30 seconds at a time. To take advantage of time-based, one-time password (TOTP) authentication, users must download a TOTP client application, such as Microsoft Authenticator, on their smartphone.

System Requirements

To take advantage of the TOTP-based two-factor authentication, you should have an SMA appliance running Secure Mobile Access 9.0 at a minimum.

Before enabling two-factor authentication on your SMA appliance, Microsoft Authenticator must be downloaded to the user's smartphone. Microsoft Authenticator is available for Android and iOS phones. For information on how to download and install the application for users, refer to Download and install Microsoft Authenticator app. Administrators can find more information at Azure Active Directory Documentation.

Managing TOTP-Based Two-Factor Authentication in SMA

To set up the authentication you have to work in both SMA web-based management interface and in Microsoft Authenticator. The following outlines the general steps:

1 Create or set up a user on SMA with the TOTP option as described in the following sections:

- Editing 2FA for a UserEditing 2FA for a User
- Adding a Domain
- Editing a Domain
- Setting Up the Administrator
- Configuring 2FA for Users
- Authenticating with the SMA Appliance

The user now has a temporary password to log into the appliance.

2 When the user logs in, SMA shows a QR code along with instructions to install and bind Microsoft authenticator with your appliance. (Refer to Authenticating with the SMA Appliance for more information.)

3 The user follows the instructions and TOTP is enabled for two-factor authentication.

Editing 2FA for a User

To edit 2FA for a user:

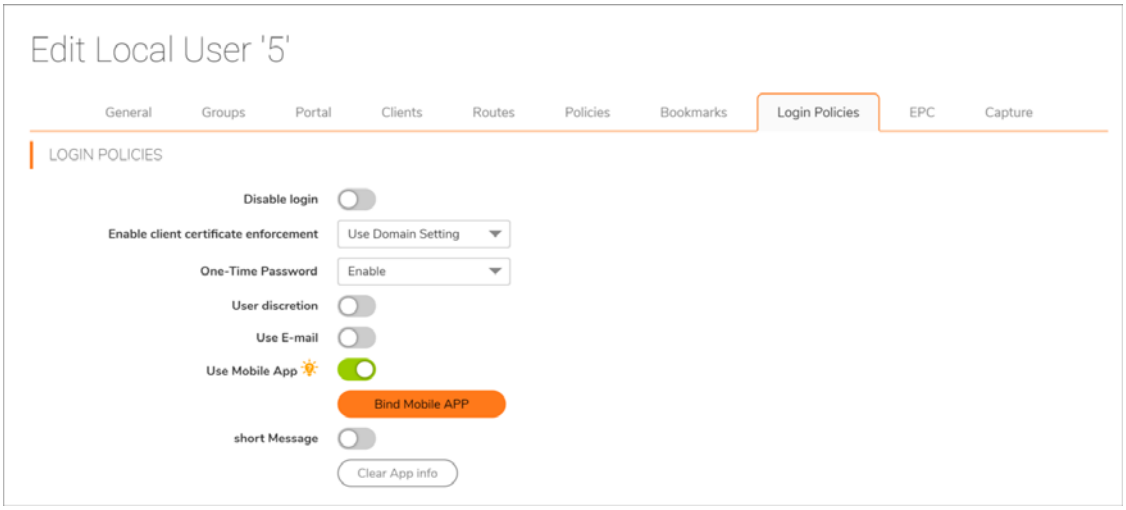
1 In the SMA web-based management interface, navigate to **Users > Local Users**.

2 Hover over a user account and click the **Edit** icon.

3 In the **GENERAL USER SETTINGS** section, enable **Require password change on next logon**.

> **NOTE:** You should enable **Require password change on next logon**, only if **Allow password changes** option is enabled in the domain settings. This ensures that the user must change the password when they log in the next time.

4 Click **Login Policies**.



5 From the **One-Time Password** drop-down list, select **Enable**.

6 Enable **Use Mobile App**.

> **NOTE:** To enable user to configure TOTP-based two-factor authentication after logging into Virtual Office, enable **User discretion** and select **Mobile App** as one of the options. See Configuring 2FA for Users to configure TOTP-based 2FA from the client side of the SMA.

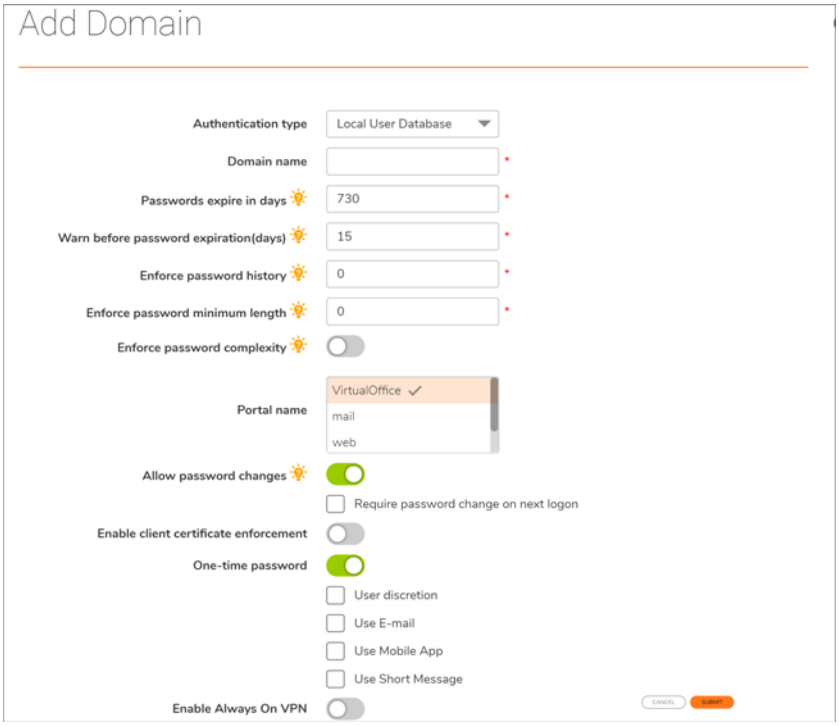
7 Click **SUBMIT** at the lower-right corner of the page.

Adding a Domain

To add a new domain with TOTP-based two-factor authentication:

1 After logging into the SMA management interface, navigate to **Portals > Domains**.

2 Click **ADD DOMAIN**.



3 In the **Add Domain** window, enter the domain name and configure other settings as required.

4 Enable **Allow password changes**.

> **NOTE:** Select **Require password change on next logon**, to ensure that the user must change the password when they log in the first time.

5 Enable **One-time password**.

6 Select **Use Mobile App**.

7 Click **SUBMIT**. A new domain with TOTP-based 2FA is added.

> **NOTE:** To add a user group or user with TOTP-based 2FA, select a TOTP-based 2FA domain when adding a group or user.

Editing a Domain

To edit an existing domain:

1 After logging into the SMA management interface, navigate to **Portals > Domains**.

2 Hover over the domain and click the **Edit** icon.

3 Enable **Allow password changes** and select **Require password change on next logon** checkbox**.**

This ensures that the user must change the password when they log in the next time.

4 In the **Edit Domain** page, select **One-time Password**.

5 Select **Use Mobile App**.

6 Click **SUBMIT**.

Setting Up the Administrator

Two-factor authentication applies to the built-in administrator also and the configuration is similar to that of a user.

To set up TOTP-based two-factor authentication for the administrator:

1. After logging into the SMA management interface, navigate to **Users > Local Users**.
2. Hover over the administrator account and then click the **Edit** icon.
3. Set up the administrator parameters.
4. Click **Login Polices**.
5. From the **One-Time Password** drop-down list, select **Enable**.
6. Enable **Use Mobile App**.
7. Click **SUBMIT** at the lower-right corner of the page.

Configuring 2FA for Users

Users can enable TOTP-based 2FA for their accounts themselves only if the administrator has selected **Mobile App** as one of the user discretion options.

To set up TOTP authentication for users:

1. Log in to SonicWall Virtual Office with the credentials assigned by your administrator.
2. Click the **User** icon at the upper-right of the page.
3. Click **Settings**.
4. In the **ONE TIME PASSWORD SETTINGS** section, enable **one-time password**.
5. Enable **Use Mobile App**.
6. Click **Accept**.

Authenticating with the SMA Appliance

After setting up the two-factor authentication:

1 Log in to the SMA appliance with the credentials assigned by your administrator.

2 Reset the password if prompted.

3 Log in with your new password.

4 If you see multiple options for authentication, select **MOBILE APP**.

NOTE: You see multiple options for authentication when your user account is configured to use any of the supported authentication methods.

The **Mobile APP BINDING** window is displayed.

5 Install Microsoft Authenticator on your phone.

6 Open Microsoft Authenticator from your phone and Click the **Add** icon.

7 Select **Other account**.

8 Scan the QR code from the SMA appliance or enter the text that is displayed when you click **text code** link under the QR code into Microsoft Authenticator to generate OTP.

9 Enter the 6-digit OTP generated from your application into the **Code** field.

10 Click **VERIFY**.

If the bind is successful, you receive a confirmation message.

After Microsoft Authenticator is bound with your SMA user account, a new TOTP is generated every 30 seconds in your Microsoft Authenticator app. You can use this TOTP to securely log in to your SMA appliance.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Last updated: 5/31/19