Integration Guide

Configuring TOTP (Multi-Factor Authentication) Using Google Authenticator on SonicWall® SMA Appliance

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 Google Authenticator integration.

- Authentication Overview
- System Requirements
- Managing TOTP-Based Two-Factor Authentication in SMA
- Authenticating with the SMA Appliance

Authentication Overview

Topics:

- About TOTP
- About Google Authenticator
- SMA Two-Factor Authentication Options

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 Google Authenticator.

About Google Authenticator

By using Google Authenticator, you can help strengthen your account security by generating verification codes on your phone. The Google Authenticator requires a second step of verification when you sign in. In addition to your password, you need the code generated by Google Authenticator on your phone.

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 username 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 or OTP via mobile application**: enables user to use the 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 Google 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 TOTP-based two-factor authentication on your appliance, Google Authenticator must be set up on the user's smartphone. For information on how to download and install the Google Authenticator application for users, information available at Google Authenticator.

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 Google 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 User
- Editing a Domain
- Editing a Domain
- Setting Up the Administrator
- Editing 2FA for a User in Virtual Office
- Authenticating with the SMA Appliance

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

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

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

Editing 2FA for a User

To edit 2FA for a user:

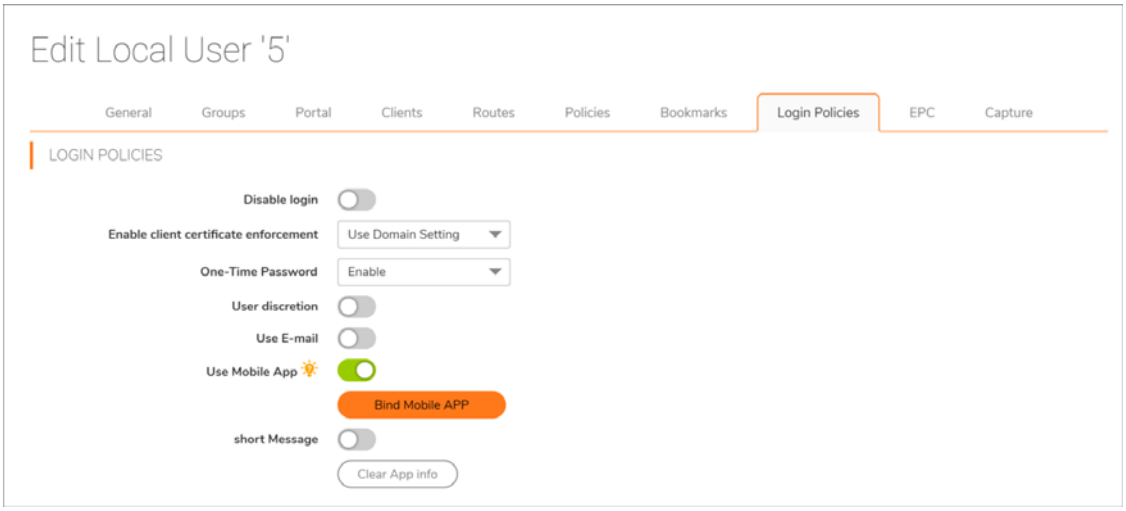
1 In the SMA web-based management interface, navigate to **Users > Local Users**.

2 Hover over a user account and click <edit icon> that appears.

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 changes the password in the next login.

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 Editing 2FA for a User in Virtual Office to configure TOTP-based 2FA for a user from the client side of the SMA.

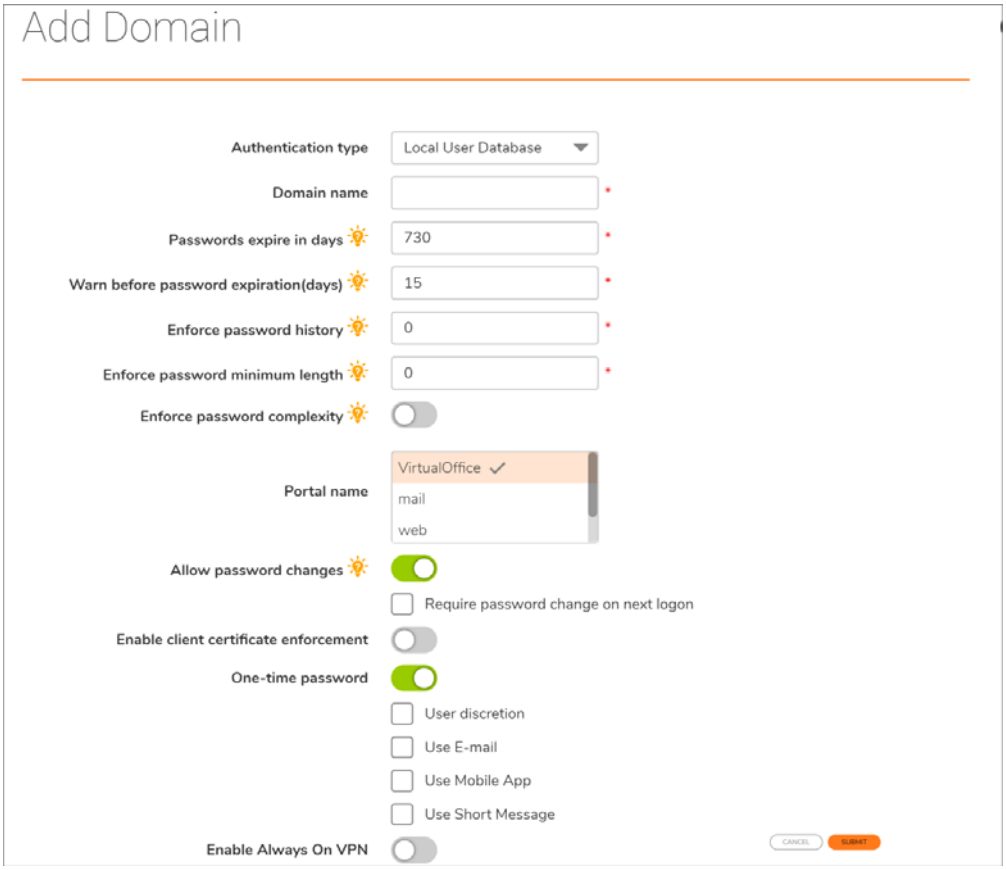
7 Click **SUBMIT** at the lower-right corner of the page.

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**.

> **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> that appears.

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 click <edit icon> that appears.

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.

Editing 2FA for a User in Virtual Office

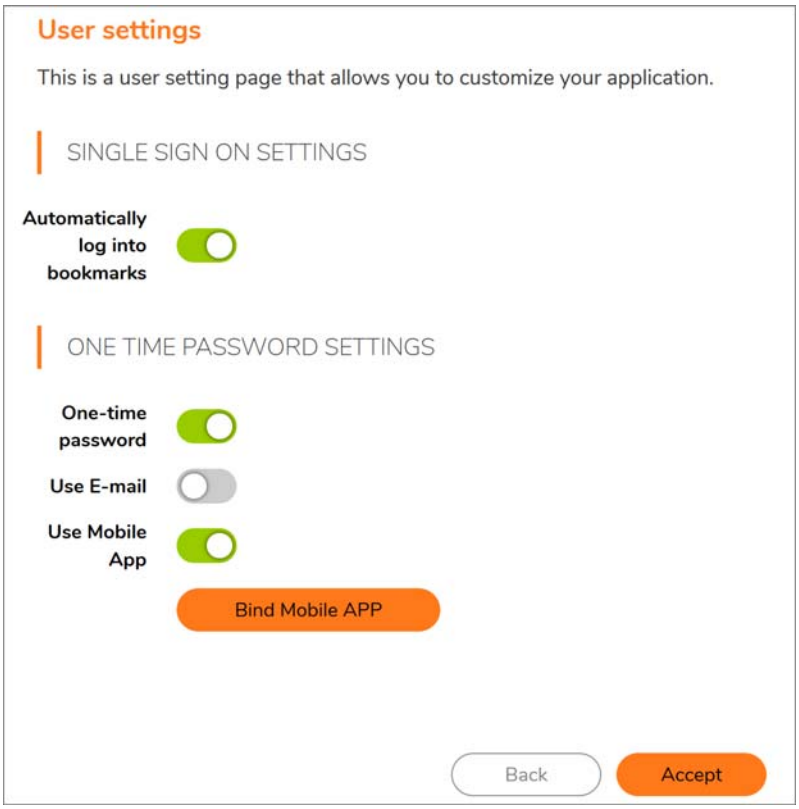
Users can enable TOTP-based 2FA for their accounts themselves only if the administrator has enabled **One-Time Password** and has selected **Mobile App** as one of the User discretion options.

1 Log in to the Virtual Office with the credentials assigned by your administrator.

2 Click <user icon> at the upper-right corner 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 your 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 Google Authenticator application on your phone.

6 Open Google Authenticator and click **BEGIN**.

7 Click **Scan a barcode,** scan the QR code from your appliance or enter the text code that is displayed when you click **text code** into Google Authenticator to generate an OTP.

8 Enter the 6-digit OTP generated from your application in the **Code** field.

9 Click **VERIFY**.

If the bind is successful, a confirmation message appears, and you are logged into Virtual Office.

After Google Authenticator is bound with your SMA user account, TOTP is generated in your Google Authenticator application that changes every 30 seconds. From next login, use the OTP from Google Authenticator application to complete authentication.

Copyright © 2019 SonicWall Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/eupa.

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