SONICWALL®

Integration Guide

Configuring TOTP (Multi-Factor Authentication) Using Microsoft Authenticator on SonicWall® Next Generation Firewalls

April 2019

This document describes how to configure time-based, one-time password (TOTP), multi-factor authentication. It focuses on using Microsoft Authenticator with SonicWall next generation firewalls.

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 password keep changing and is valid for 30 seconds at a time. Because the TOTP password 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. These include Microsoft Authenticator, Google Authenticator, and Duo Mobile, for example. 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 passcodes, you can add any online account, like access through a SonicOS 6.5 firewall, to Microsoft Authenticator.

SonicOS Options

Starting with SonicOS 6.5.3, SonicWall provides several options for managing password authentication:

- **Disabled**: no password authentication is required.
- **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.
- **TOTP**: a time-based, one-time password (TOTP) is used with two-factor authentication (2FA). To take advantage of two-factor authentication, users must download a TOTP client application, such as Microsoft Authentication, on their smartphone.

System Requirements

To take advantage of the two-factor authentication, you should have a SonicWall Next Generation Firewall running SonicOS 6.5.3 at a minimum.

Before enabling two-factor authentication on the firewall, 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 2FA in SonicOS 6.5

To set up the authentication you have to work in both SonicOS and in Microsoft Authenticator. The following outlines the general steps:

1 Create or setup a user on the firewall with the **TOTP** option as described in the following sections:

- Adding a New User with 2FA
- Editing 2FA for a User
- Adding a Group
- Editing a Group
- Setting Up the Administrator

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

2 When the user logs in, the firewall asks the user to update the password followed by a QR code along with instructions to install the Microsoft Authenticator. (Refer to Authenticating with the Firewall for more information.)

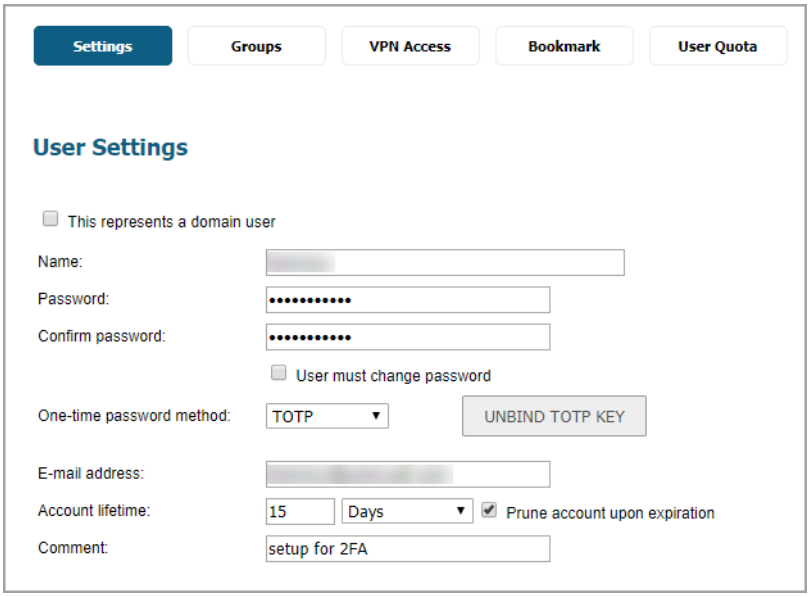
3 The user follows the instructions and the TOTP is enabled for two-factor authentication.

Adding a New User with 2FA

To add a new user with two-factor authentication:

1 After logging into the SonicOS firewall, navigate to **MANAGE | System Setup | Users > Local Users & Groups**.

2 Click **Add**.



3 Setup the **Name**, **Password**, and **Confirm password** as you would for a normal user.

4 Check the box for **User must change password**. The ensures that the user must change the password when they log in the first time.

5 In the field for **One-time password method**, select **TOTP**.

> **NOTE:** If you click on **UNBIND TOTP KEY**, the QR code that was used to setup TOTP is no longer valid for that particular user.

6 Add the user's **Email address**.

7 In Account lifetime, choose how long you want this user's settings to last. The example above shows a 15-day life. You can choose a set number of minutes, hours or days, or you can choose to have it never expire.

8 Add a **Comment**, if desired.

9 Click **OK**.

Editing 2FA for a User

Editing a user is very similar to adding a new user.

To change 2FA for an existing user:

1 After logging into the SonicOS firewall, navigate to **MANAGE | System Setup | Users > Local Users & Groups**.

2 In the table, select the user that you want to edit by checking the box on the left.

3 Click the **Edit** icon in the **Configure** column.

4 Check the box for **User must change password**. The ensures that the user must change the password when they log in the first time.

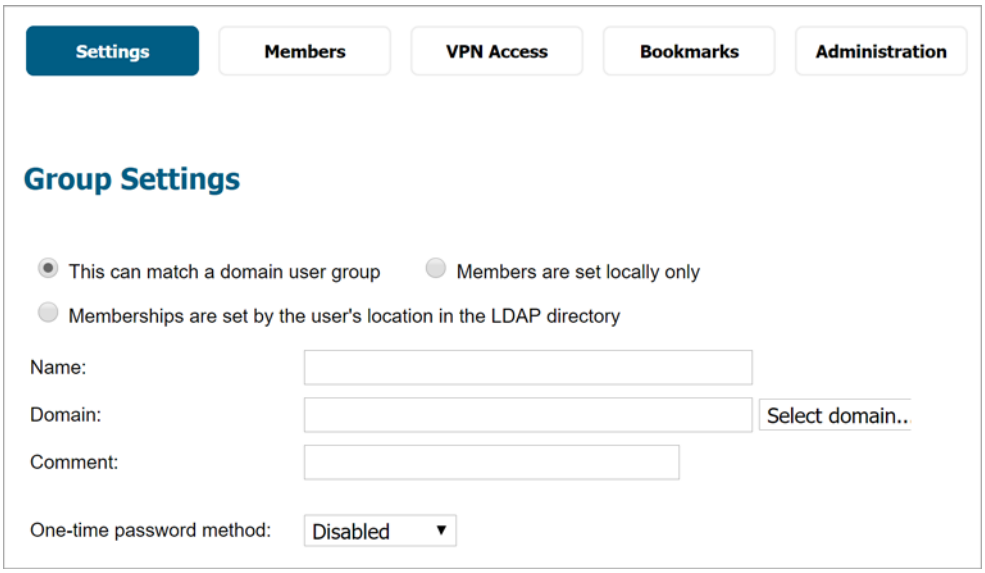
5 In the field for **One-time password method**, select **TOTP**.

6 Click **OK**.

Adding a Group

To add a new user group with two-factor authentication:

1. After logging into the SonicOS firewall, navigate to **MANAGE | System Setup | Users > Local Users & Groups**.
2. Select **Local Groups** at the top of the table.
3. Click **Add**.



4. Configure the group settings as you would for any group on the firewall.
5. In the field for **One-time password method**, select **TOTP**.
6. Click **OK**.

Editing a Group

Editing a group is very similar to adding a new group.

To change 2FA for an existing group:

1. After logging into the SonicOS firewall, navigate to **MANAGE | System Setup | Users > Local Users & Groups**.
2. Select **Local Groups** at the top of the table.
3. Click the **Edit** icon in the **Configure** column for the group you want to change.
4. In the field for **One-time password method**, select **TOTP**.
5. Click **OK**.

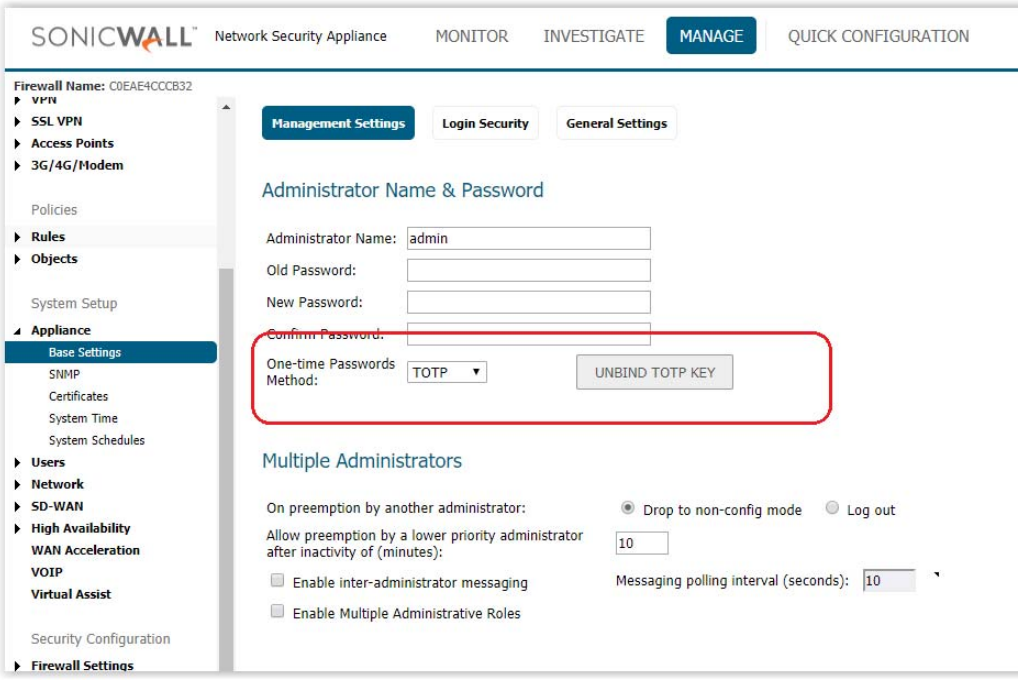
Setting Up the Administrator

Beginning with SonicOS 6.5.4, two-factor authentication applies to the built-in administrator as well.

To set up two-factor authentication for the adminstrator:

1 After logging into the SonicOS firewall, navigate to **MANAGE | Appliance | Base Settings**.

2 Select **Management Settings** at the top of the table.



3 Set up the administrator parameters as usual.

4 In the **Administrator Name & Password** section, select **TOTP** for **One-time Passwords Method**.

> **NOTE:** If you click on **UNBIND TOTP KEY**, the QR code that was used to setup TOTP is no longer valid for that particular user.

5 Click **Accept**.

Authenticating with the Firewall

After setting up for two-factor authentication:

1 Log in from the user interface on the firewall, using the temporary password that was assigned to you. A window similar to the following appears, and you are prompted to change your password:

NOTE: When you log in to the firewall, you can use Microsoft Authenticator by downloading it to your phone.

2 Open the Authenticator application on your phone.

3 Navigate to **Accounts**.

4 Click the **Add** icon.

5 Scan the QR code.

6 Type the PIN from your phone in the **2FA Code** field.

7 Click **OK**.

8 Follow the link to complete your login.

NOTE: Store your emergency scratch code in a safe place away from your phone. It is the only way to log in if you lose your mobile phone.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

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: 4/26/19