SonicWall® SMA 100 Series

Security Best Practice Guide

SMA 200/400
SMA 210/410
SMA 500v for ESXi
SMA 500v for Hyper-V
SMA 500v for AWS
SMA 500v for Azure

January 2021

Overview

Welcome to the SonicWall® SMA 100 Series Security Best Practice Guide. This Best Practice Guide is a reference guide for owners and administrators of the SonicWall SMA 100 series. It presents best practice and industry recognized hardening suggestions for SMA 100 series product line.

Topics:

For additional information on any of the features referenced in this guide, please refer to the SMA 100 Series 10.0 Administration Guide.

ⓘ **NOTE:** This guide will be periodically reviewed and updated for accuracy.

Multi-Factor Authentication

Multi-factor authentication (MFA), sometimes referred to as **two-factor authentication** or **2FA,** is an electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is). MFA protects the user from an unknown person trying to access their data such as personal ID details or financial assets.

There are three basic factors to authentication:

- Something you know: This could be a PIN code, the answers to your security questions, or your password
- Something you have: This generally refers to a physical object, such as a security token, smart card, or phone.
- Something you are: This refers to biometric data, and usually comes in the form of your fingerprint or facial scan — such as with Apple's Touch ID

Utilizing more than one factor is one of the best methods for keeping connectivity into a network safe. Most hackers that breach networks do so by obtaining the username and password of individuals. They can compromise your credentials, and even manipulate their connections to make the authenticating device "think" it is you. However, when a secondary factor is introduced, the hacker would not have access to this information and therefore would be denied access immediately and their session logged.

SonicWall's SMA 100 series incorporates multiple types of factoring functions, that when combined, can ensure the authenticity of the end user. Turning on these features are considered ***critical*** in the security of your network and should always be your number one priority when setting up remote connectivity appliances or software.

ⓘ **NOTE: Due to the critical importance of 2FA, we are providing detailed instructions on the setup of this feature.**

One of the most secure **(and highly recommended)** methods for secondary authentication is using a provider that supports SAML (Security Assertion Markup Language), or a TOTP (Time-Based One-Time Password) provider. SonicWall's SMA 100 series has support for both types of factoring providers – Please reference the SonicWall Feature guide for detailed walkthrough on how to setup these features with different providers. https://www.sonicwall.com/techdocs/pdf/sma-10-2-feature-guide.pdf

Two popular and commonly used solutions for secondary factor-based authentication are the Microsoft Authenticator and Google Authenticator. To enable 2FA using Google or Microsoft Authenticator, please refer to the following knowledge base article: https://www.sonicwall.com/support/knowledge-base/how-can-i-configure-time-based-one-time-password-totp-in-sma-100-series/180818071301745/

Enable One-Time Password (OTP) Using Phone or Email

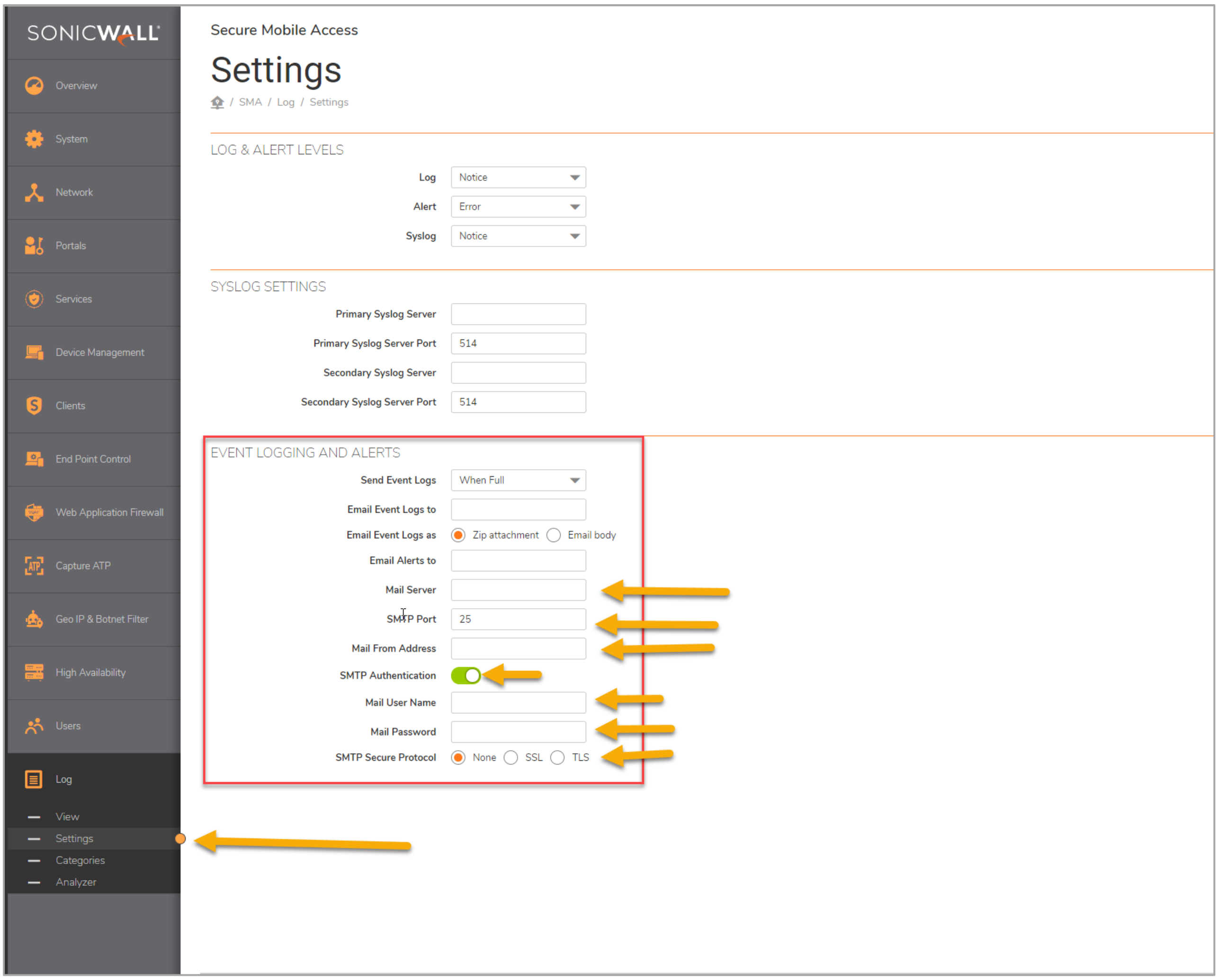
If you do not have the ability to use one of the above highly recommended solutions for secondary factor authentication, SonicWall's SMA 100 series does offers a One Time Password (OTP) option that can be used as a secondary factor (2FA). This token can be sent to the requesting individual via email or SMS text.

To get started with the OTP setup, you should be prepared to choose the method that suites your organizations need the best. A User can be given the option to choose any of the three if the admin desires to allow this.

Configuring One-Time Passwords for Email

ⓘ **NOTE:** Email is sent as a relayed message from the SonicWall SMA 100 series through a mail host. You must ensure your mail host can accept the relay. Most mail hosts will allow this with password authentication and using special designated port. Some require specific types of transport methods in order to relay. Please have this information ready prior to proceeding with the below instructions.

1. In the left menu, navigate to **Log** > **Settings**.
2. Navigate to the **Event Logging and Alerts** section.
3. In the **Mail Server** field, enter the mail server that the appliance will send the relay request to. *Example: smtp.office365.com*
4. In the **SMTP Port** field, enter the recipient port details for relay requests. *Example: Port 587*
5. In the **Mail from Address** field, enter the sender's email address. This will be the display email address from which the emails are sent. Please note, some email relay services require this address to be a valid account. If you do not wish to have your email displayed, then consider adding an additional email user to your account with the appropriate name you wish to use here.
6. Enable **SMTP Authorization**. Most mail relays require authentication. If you know your organization does NOT require this – then do not enable this field. However, if you are unsure, or are sure they do require, then please enable this setting.
7. If **SMTP Authorization** is enabled, now enter the username and password used to log into your email server.
8. If your mail service requires a secure transport to sign in, please select it next to the **SMTP Secure Protocol**. Most mail services will require TLS to authenticate and relay. Some services will allow SSL but is less frequent and less secure.
9. Click **Accept**. If successful, you will receive a green bar at the top indicating your settings have been saved.



Secure Mobile Access

Settings

/ SMA / Log / Settings

LOG & ALERT LEVELS

Log: Notice

Alert: Error

Syslog: Notice

SYSLOG SETTINGS

Primary Syslog Server:

Primary Syslog Server Port: 514

Secondary Syslog Server:

Secondary Syslog Server Port: 514

EVENT LOGGING AND ALERTS

Send Event Logs: When Full

Email Event Logs to:

Email Event Logs as: ● Zip attachment ○ Email body

Email Alerts to:

Mail Server:

SMTP Port: 25

Mail From Address:

SMTP Authentication: ●

Mail User Name:

Mail Password:

SMTP Secure Protocol: ● None ○ SSL ○ TLS

Configuring One-Time Passwords for SMS

You can use this feature to send short message with a one-time password (OTP) code to the users to log in to the appliance.

SonicWall SMA 100 series offers the ability to communicate with two different SMS service providers:

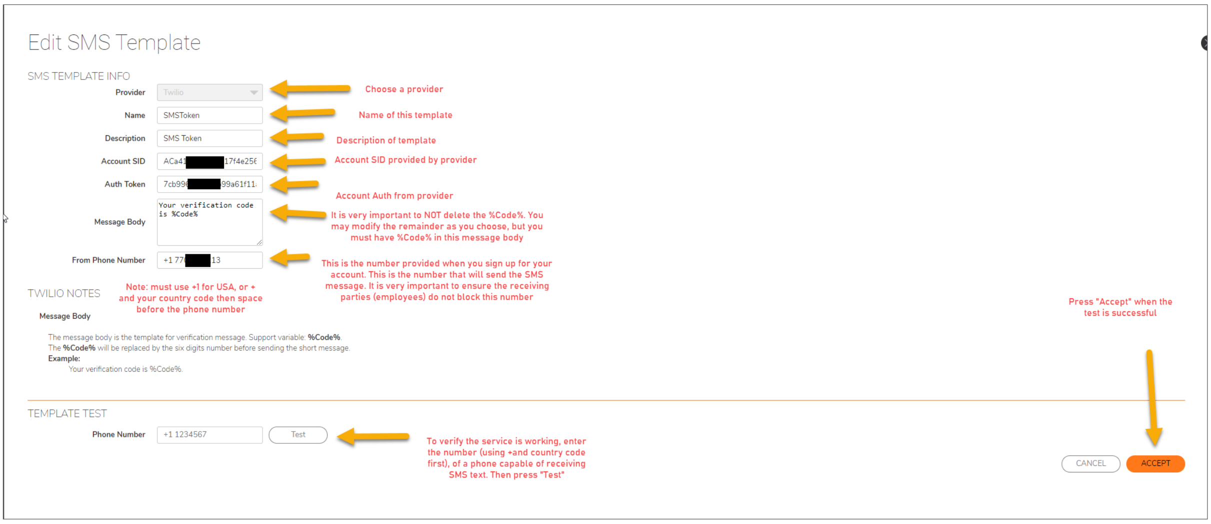
- AliSMS : Connect to the World with Alibaba Cloud SMS
- Twilio: Communication APIs for SMS, Voice, Video and Authentication

Note: for the purpose of this example, Twilio will be used.

To add an SMS Template:

1. To add a policy, navigate to the **Services > SMS Templates** screen within the Secure Mobile Access management interface and select SMS Templates.
2. Click **Add SMS Template**.
3. Select the SMS Provider. The two providers are Aliyun and Twilio. You can add multiple provider templates in the appliance and use them in different domains or user levels.
4. Enter a template **Name**.

5. Enter **Description** for the SMS Template. Select the International check box, if applicable.
6. Enter **Account SID**.
7. Enter **Auth Token**.
8. Type in the message your text message will say when the user receives the code. Please Note: you MUST include the %Code% in your body, or you will NOT receive the code.
9. Enter the phone number of your SMS service account. This is the number that will SEND the text message. You must enter "+" and then the country code, followed by a space. Please ensure that your employees do not block this number on their mobile device.
10. Enter a test number that can be used to receive an SMS text. Enter your number like this example (using USA country code: +1 4045551234)
11. Once the test is successful and you receive a green success banner.
12. Click **Accept** to confirm the changes.



Edit SMS Template

SMS TEMPLATE INFO

Provider: Twilio — Choose a provider

Name: SMSToken — Name of this template

Description: SMS Token — Description of template

Account SID: ACa41[redacted]17f4e25€ — Account SID provided by provider

Auth Token: 7cb99€[redacted]99a61f11: — Account Auth from provider

Message Body: Your verification code is %Code% — It is very important to NOT delete the %Code%. You may modify the remainder as you choose, but you must have %Code% in this message body

From Phone Number: +1 77[redacted]13 — This is the number provided when you sign up for your account. This is the number that will send the SMS message. It is very important to ensure the receiving parties (employees) do not block this number

Note: must use +1 for USA, or + and your country code then space before the phone number

TWILIO NOTES

Message Body

The message body is the template for verification message. Support variable: **%Code%**.
The **%Code%** will be replaced by the six digits number before sending the short message.
Example:
Your verification code is %Code%.

Press "Accept" when the test is successful

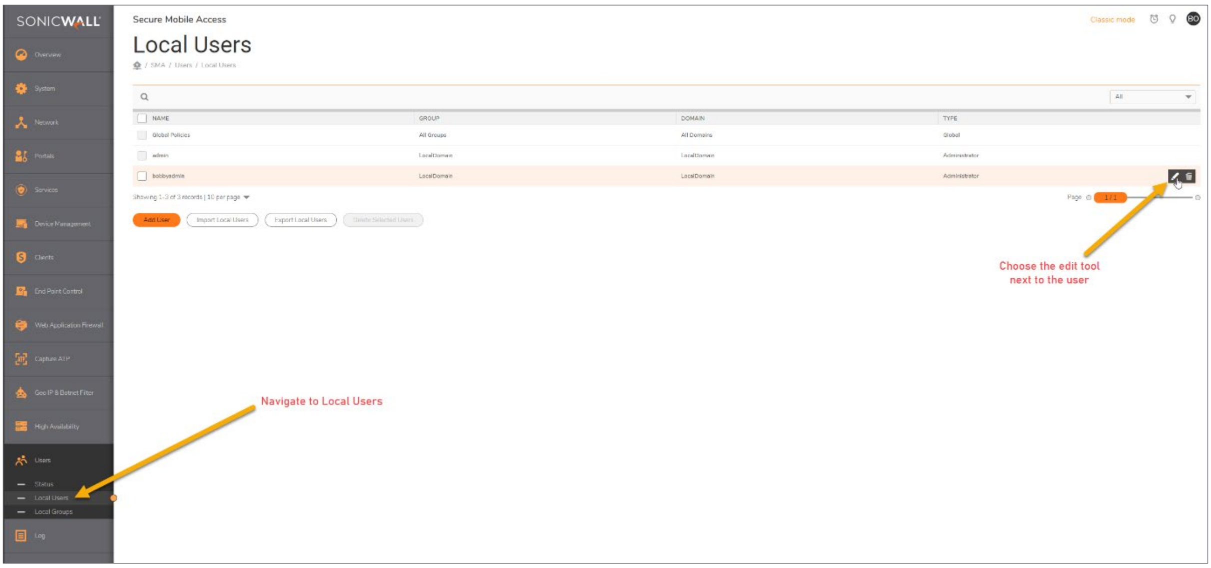
TEMPLATE TEST

Phone Number: +1 1234567 — To verify the service is working, enter the number (using +and country code first), of a phone capable of receiving SMS text. Then press "Test"

Enabling One-Time Password

Now that you successfully have setup your method(s) for receiving your second factor, you can now enable this feature in your users' accounts. This setup must be done per user and is unavailable in the group setting.

1. Navigate to **User** and then choose **Local users**
2. Choose the user that you wish to enable OTP
3. Next to that user, click **Edit**. (pencil icon)



Secure Mobile Access

Local Users

/ SMA / Users / Local Users

NAME	GROUP	DOMAIN	TYPE
Global Policies	All Groups	All Domains	Global
admin	LocalDomain	LocalDomain	Administrator
bobbyadmin	LocalDomain	LocalDomain	Administrator

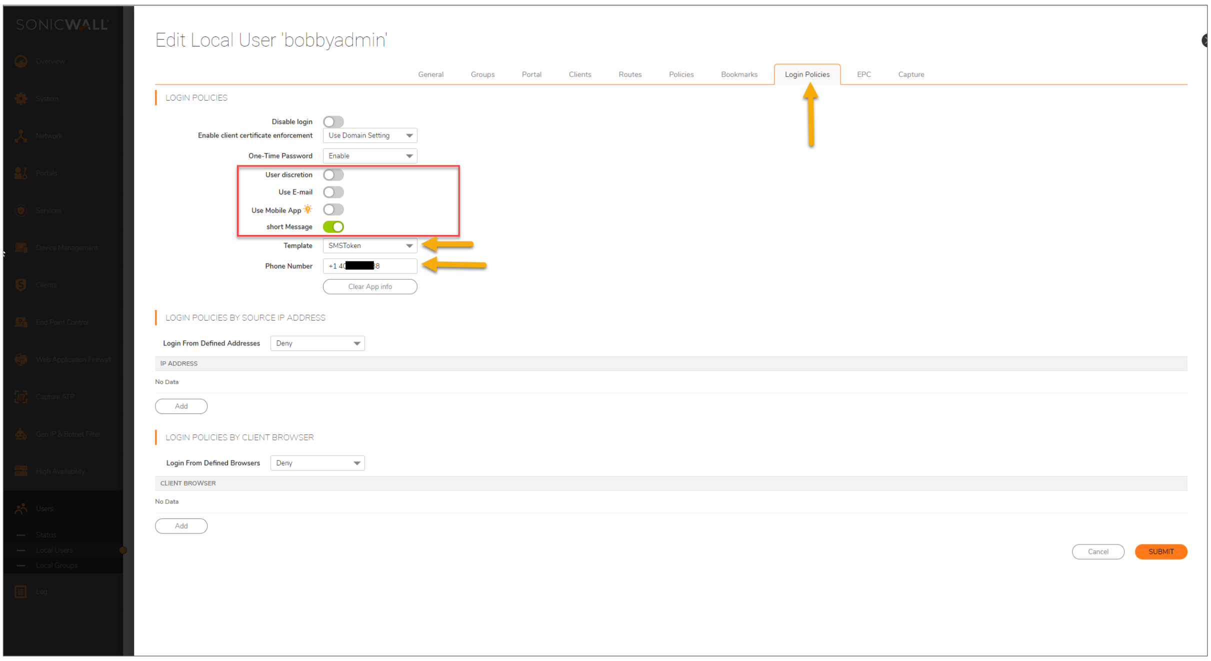
Showing 1-3 of 3 records | 10 per page

Choose the edit tool next to the user

Navigate to Local Users

4. Click the tab labeled **Login Policies**.
5. Choose how to deliver the token:
    a. **Users discretion:** This will display all three methods as options. You may choose which ones you wish to display for the user by ensuring a check mark is next to each one.
    b. **Use Email:** This will enable the token to be sent via email. The users email address will need to be entered into their user info under the general tab
    c. **Use App:** This will allow you to use Google or Microsoft Authenticator, Duo, or any RADIUS BASED 2FA product that you have setup following the directions in the KB referenced above for 2FA
    d. **Use Short Message**: This will enable the SMS text message option

ⓘ **NOTE:** You will need to enable this first in order to select the SMS template and enter the users phone number (Mobile device capable of receiving a text message) then you may choose user discretion as noted above



Edit Local User 'bobbyadmin'

LOGIN POLICIES

Disable login ○
Enable client certificate enforcement: Use Domain Setting
One-Time Password: Enable
User discretion ○
Use E-mail ○
Use Mobile App ○
short Message ●
Template: SMSToken
Phone Number: +1 40[redacted]8

LOGIN POLICIES BY SOURCE IP ADDRESS

Login From Defined Addresses: Deny

IP ADDRESS

No Data

LOGIN POLICIES BY CLIENT BROWSER

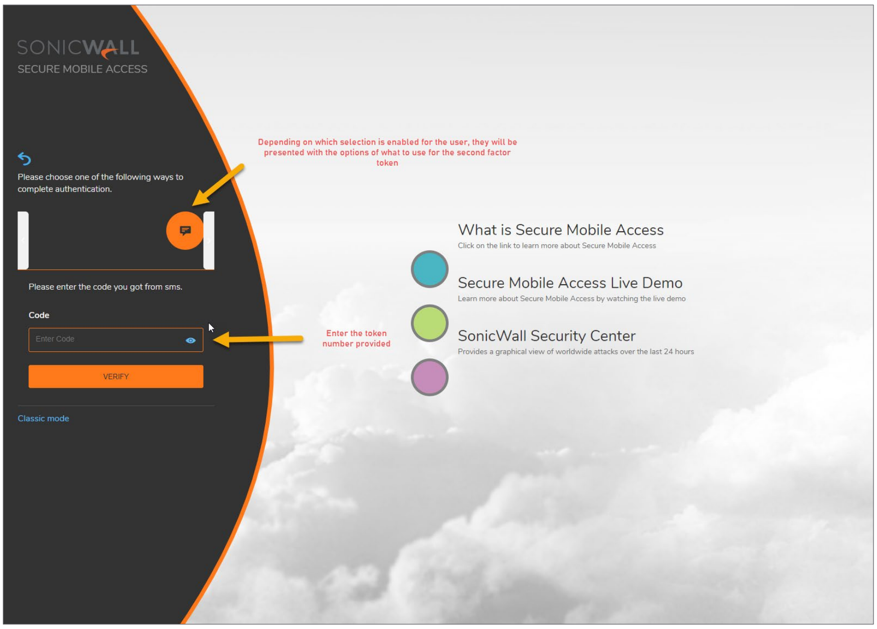
Login From Defined Browsers: Deny

CLIENT BROWSER

No Data

2FA and OTP User Experience

When the user attempts to log into the Virtual office, or if they attempt to log in via the NetExtender Client, they will be presented with the second factor (2FA) challenge question.



SONICWALL
SECURE MOBILE ACCESS

Please choose one of the following ways to complete authentication.

Please enter the code you got from sms.

Code

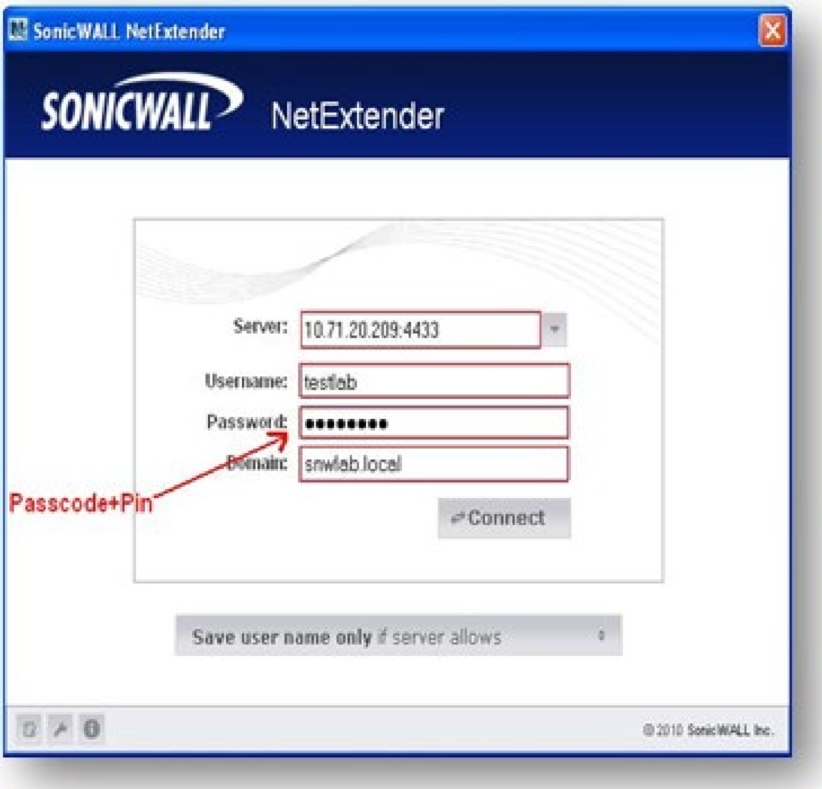
Enter Code
VERIFY
Classic mode

Depending on which selection is enabled for the user, they will be presented with the options of what to use for the second factor token

Enter the token number provided

What is Secure Mobile Access
Click on the link to learn more about Secure Mobile Access
Secure Mobile Access Live Demo
Learn more about Secure Mobile Access by watching the live demo
SonicWall Security Center
Provides a graphical view of worldwide attacks over the last 24 hours

If you are using a 3rd party 2FA application, such as Duo or RSA, you must enter the password plus the PIN.



Server: 10.71.20.209:4433

Username: testlab

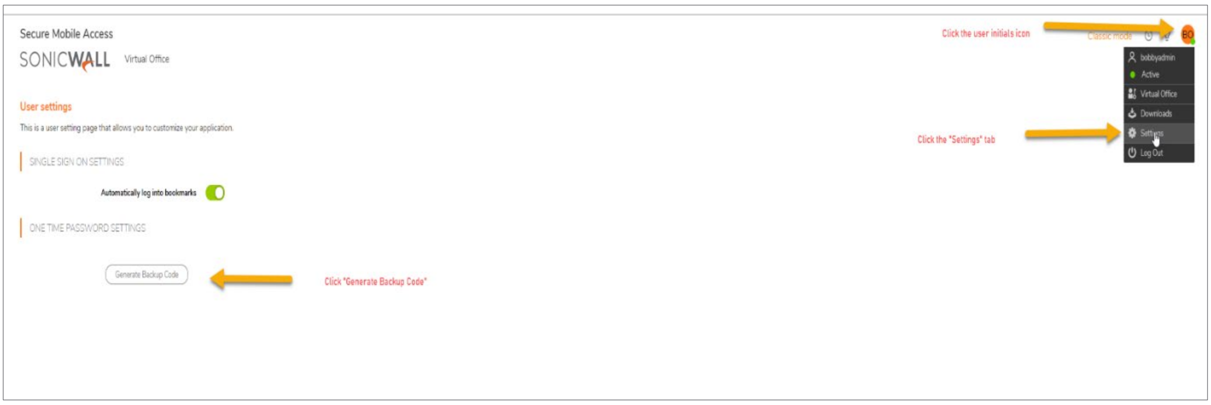
Password: ●●●●●●●●●

Domain: snwlab.local

User Backup Codes

A user can create a backup code after successfully logging in the first time. This option is only available if 2FA is setup. The backup code is designed as a failsafe option in the event the user misplaces the 2FA device / token or is unable to receive it due to their location. Examples would be while in flight where SMS messages may not function properly or where the user can only have one device connected to the wireless network.

1. After successful login to the virtual office, click on the circle with your initials in the upper right corner.
2. Choose **Settings**.
3. Choose **Generate Backup Keys**.



User settings

This is a user setting page that allows you to customize your application.

SINGLE SIGN ON SETTINGS

Automatically log into bookmarks

ONE TIME PASSWORD SETTINGS

Click the user initials icon

Click the "Settings" tab

Click "Generate Backup Code"

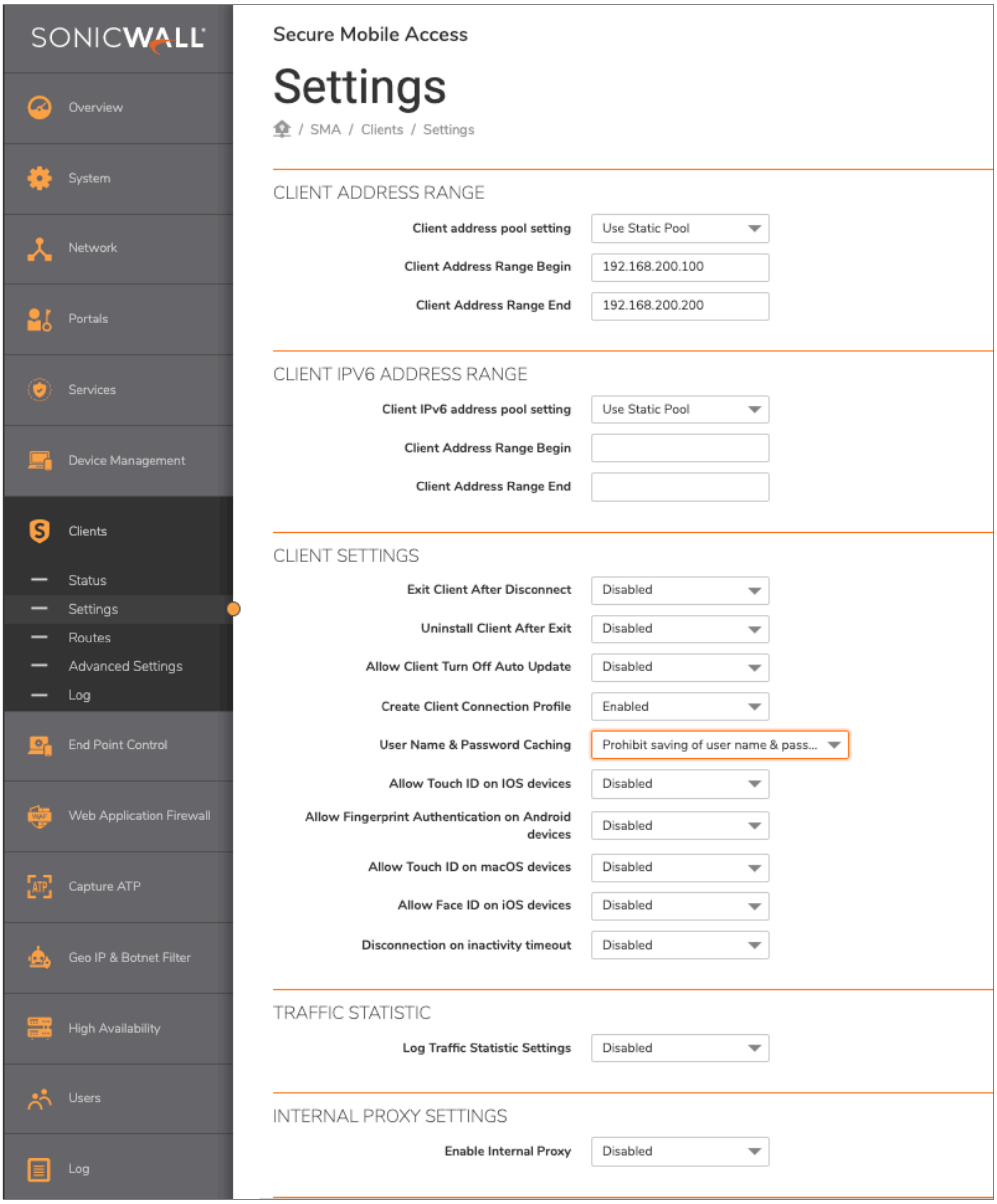
4. After clicking the **Generate Backup Key** button, a text file will be downloaded to your computer. This text file will contain the backup keys that can be used. These are a 1 time use only key. Do not lose them. If you press the button more than once, it will generate additional text files, however only the last set of numbers will be valid for use.

Additional Configuration Recommendations for Security Best Practices

- Prohibit Saving Username and Password
- Hide Domain List on Portal Login Page
- Enable HTTP Strict Transport Security (HSTS) for SMA
- Enforce Login Uniqueness
- Enforce Client Source Uniqueness
- Enable “Login Schedule”
- Enable “Logout Schedule”
- Enforce Password Complexity
- Enable Client Certificate Enforcement (Advanced Security Feature)
- Restrict Request Headers
- Use a Public Certificate
- Allow Touch ID and Face ID on Mac, Apple IOS and Android Devices
- Disconnection on Inactivity Timeout
- Disable the Default Admin Account
- Allow Policy Match Logging
- Setup Connection Policies
- Device Registration
- End Point Control
- GEO IP Fencing
- Capture ATP for the SMA 100 Series

Prohibit Saving Username and Password

While this can be a convenience to the individual user, saving the username and password on a workstation can be dangerous.



Secure Mobile Access

Settings

/ SMA / Clients / Settings

CLIENT ADDRESS RANGE

Client address pool setting	Use Static Pool
Client Address Range Begin	192.168.200.100
Client Address Range End	192.168.200.200

CLIENT IPV6 ADDRESS RANGE

Client IPv6 address pool setting	Use Static Pool
Client Address Range Begin	
Client Address Range End	

CLIENT SETTINGS

Exit Client After Disconnect	Disabled
Uninstall Client After Exit	Disabled
Allow Client Turn Off Auto Update	Disabled
Create Client Connection Profile	Enabled
User Name & Password Caching	Prohibit saving of user name & pass...
Allow Touch ID on IOS devices	Disabled
Allow Fingerprint Authentication on Android devices	Disabled
Allow Touch ID on macOS devices	Disabled
Allow Face ID on iOS devices	Disabled
Disconnection on inactivity timeout	Disabled

TRAFFIC STATISTIC

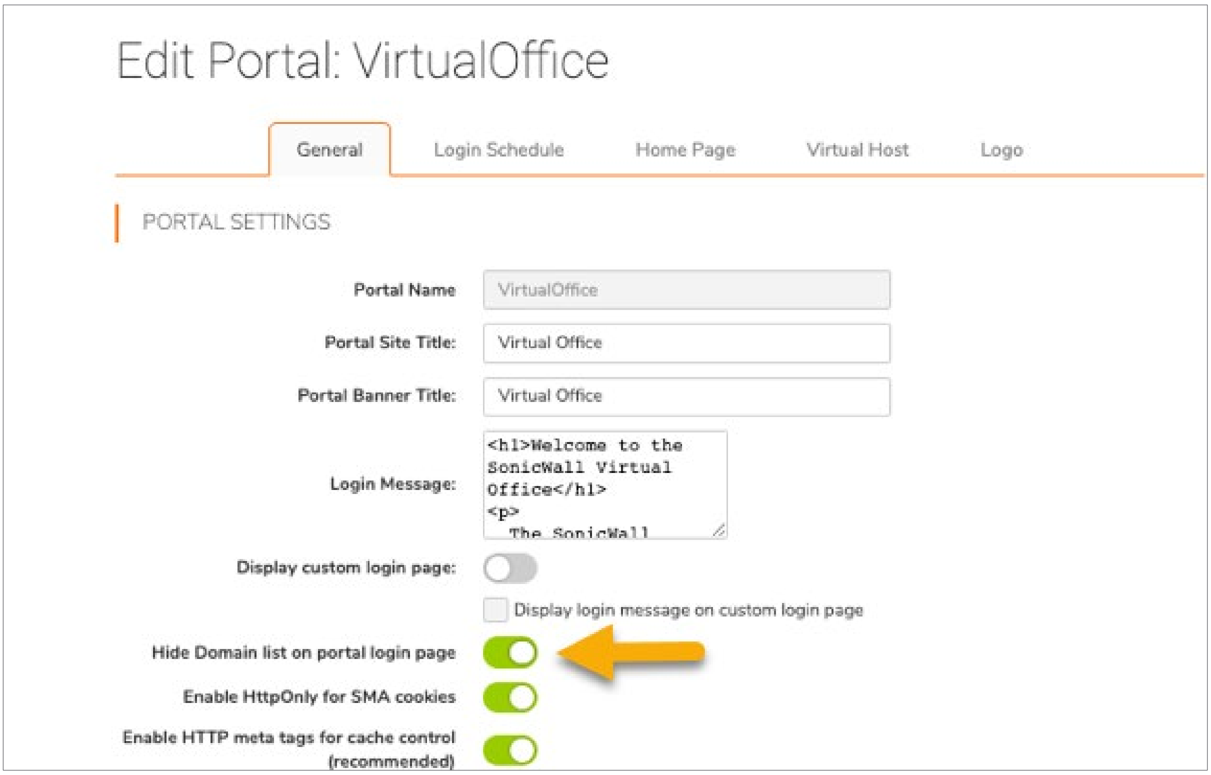
Log Traffic Statistic Settings	Disabled

INTERNAL PROXY SETTINGS

Enable Internal Proxy	Disabled

Hide Domain List on Portal Login Page

By hiding the domain name, this makes it more difficult for a threat actor to attempt unauthorized access. Your users should know the domain name of the organization.



Edit Portal: VirtualOffice

PORTAL SETTINGS

Portal Name: VirtualOffice

Portal Site Title: Virtual Office

Portal Banner Title: Virtual Office

Login Message:

```
<h1>Welcome to the
SonicWall Virtual
Office</h1>
<p>
  The SonicWall
```

Display custom login page: ○ (off)

□ Display login message on custom login page

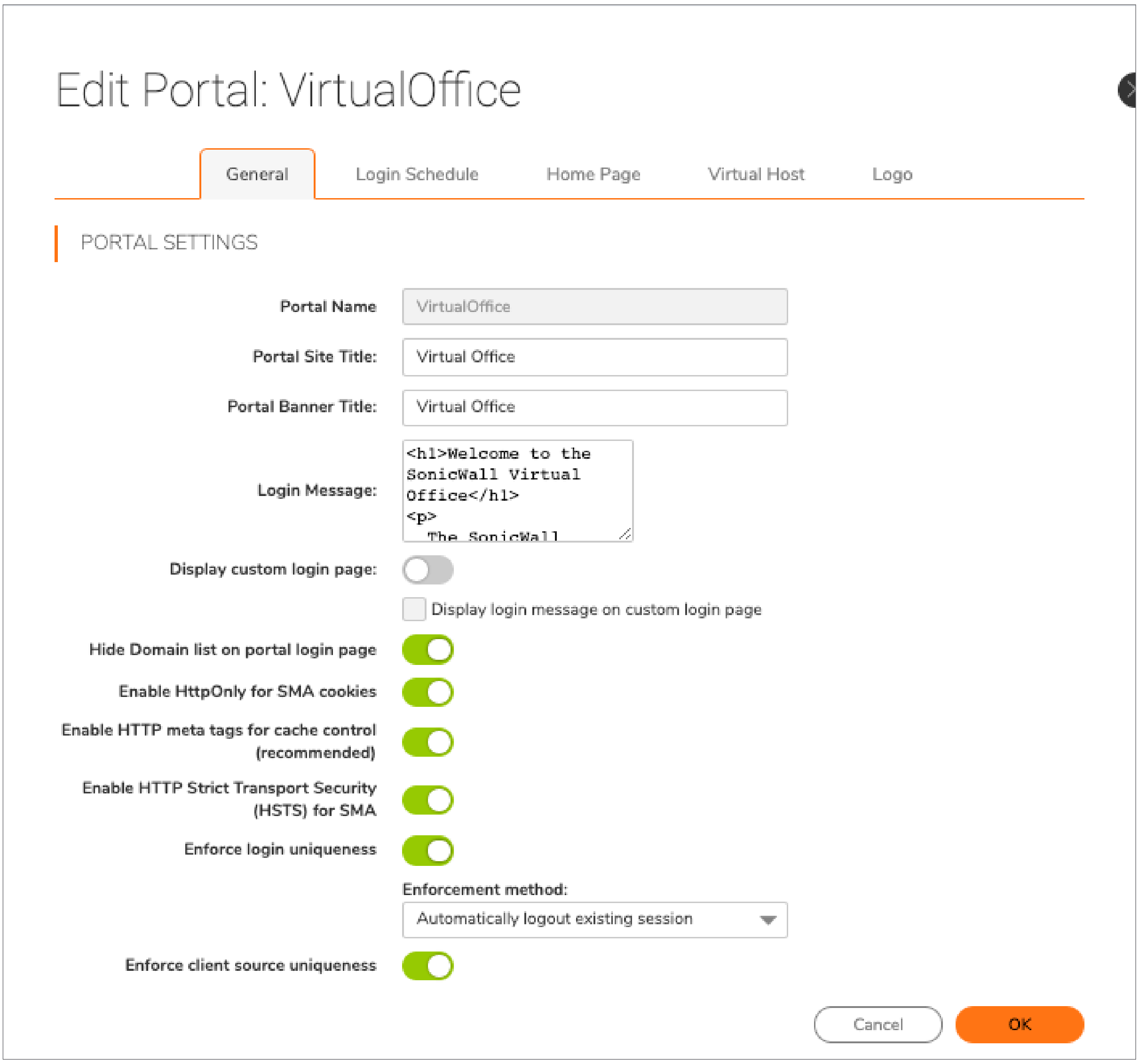
Hide Domain list on portal login page: ● (on)

Enable HttpOnly for SMA cookies: ● (on)

Enable HTTP meta tags for cache control (recommended): ● (on)

Enable HTTP Strict Transport Security (HSTS) for SMA

This feature forces the connection to be HTTPS and does not allow HTTP connections. Without this, a user could connect to the portal using an HTTP connection to authenticate, then the appliance would convert the session to HTTPS.



Edit Portal: VirtualOffice

PORTAL SETTINGS

Portal Name: VirtualOffice

Portal Site Title: Virtual Office

Portal Banner Title: Virtual Office

Login Message:

```
<h1>Welcome to the
SonicWall Virtual
Office</h1>
<p>
  The SonicWall
```

Display custom login page: ○ (off)

□ Display login message on custom login page

Hide Domain list on portal login page: ● (on)

Enable HttpOnly for SMA cookies: ● (on)

Enable HTTP meta tags for cache control (recommended): ● (on)

Enable HTTP Strict Transport Security (HSTS) for SMA: ● (on)

Enforce login uniqueness: ● (on)

Enforcement method: Automatically logout existing session

Enforce client source uniqueness: ● (on)

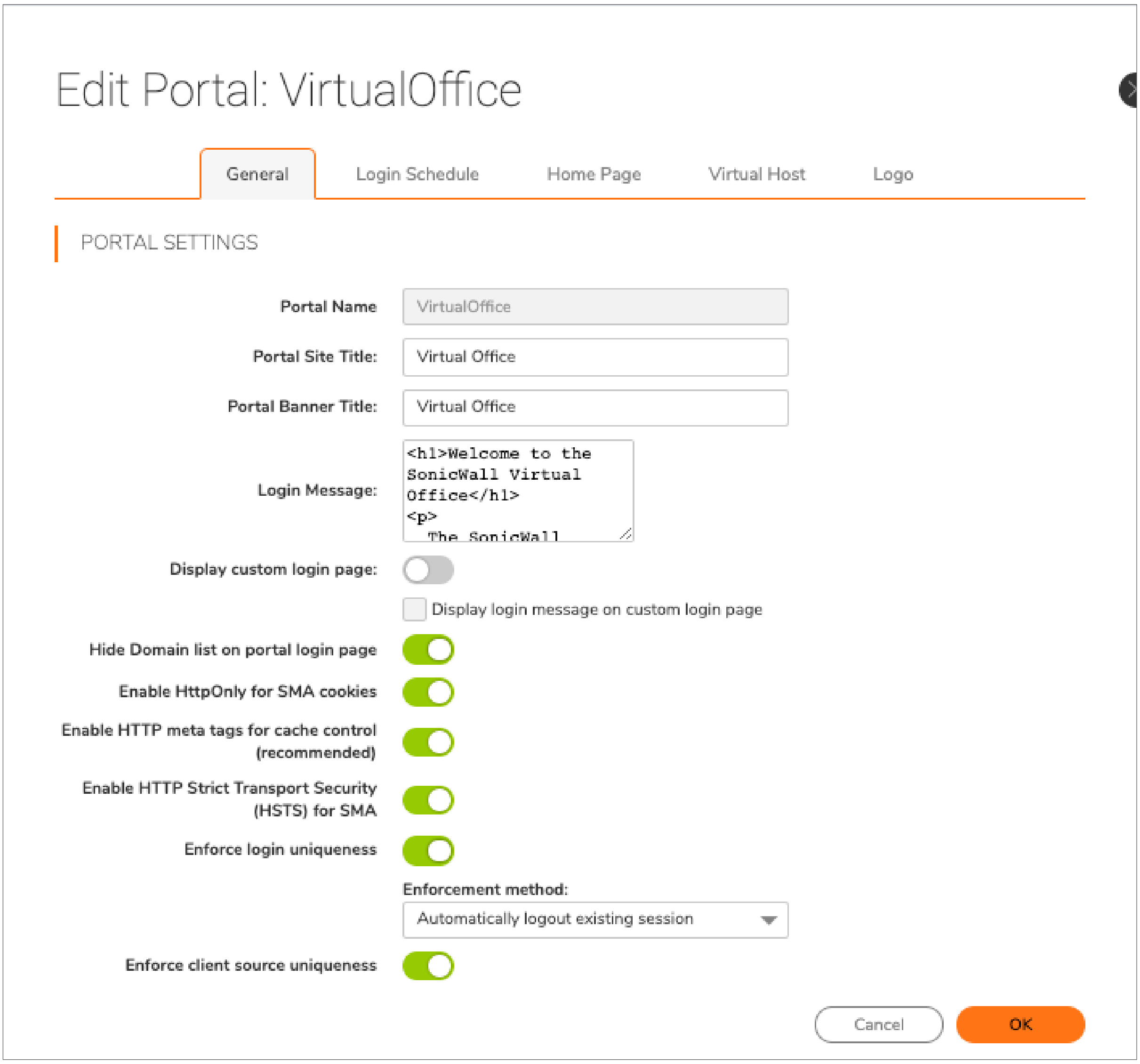
Enforce Login Uniqueness

As a layered security precaution, users should only be allowed to login to a single session. Allowing multiple logins with the same username can lead to an increased risk of a security breach.

You have two options for logging the user out if they try to log in using the same username twice:

- Automatically logout existing session
    - This means the users first session would be disconnected immediately
- Confirm Logout of existing session
    - This would require the user to confirm that my proceeding, their original session will be terminated

Either choice can be used to effectively enhance security.


Edit Portal: VirtualOffice

PORTAL SETTINGS

Portal Name: VirtualOffice

Portal Site Title: Virtual Office

Portal Banner Title: Virtual Office

Login Message:

```
<h1>Welcome to the
SonicWall Virtual
Office</h1>
<p>
  The SonicWall
```

Display custom login page: off

□ Display login message on custom login page

Hide Domain list on portal login page: on

Enable HttpOnly for SMA cookies: on

Enable HTTP meta tags for cache control (recommended): on

Enable HTTP Strict Transport Security (HSTS) for SMA: on

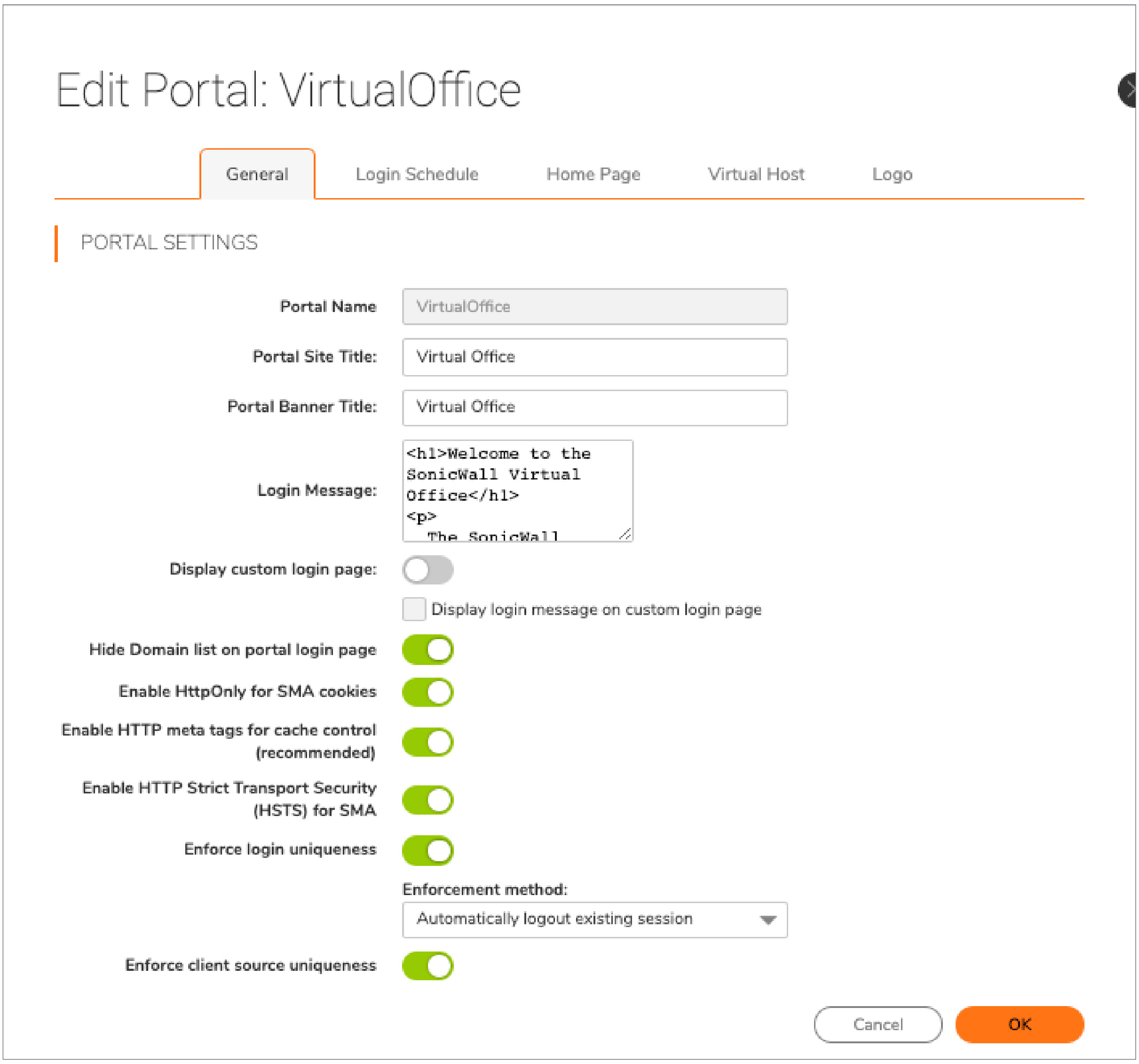
Enforce login uniqueness: on

Enforcement method: Automatically logout existing session

Enforce client source uniqueness: on

Enforce Client Source Uniqueness

Remote connectivity to a network should only be allowed from one device at a time. This setting will only allow once unique device to connect at a time. Trying to connect with a second device using the same username would deny access to the second device attempting to connect.



Edit Portal: VirtualOffice

PORTAL SETTINGS

Portal Name: VirtualOffice

Portal Site Title: Virtual Office

Portal Banner Title: Virtual Office

Login Message:

```
<h1>Welcome to the
SonicWall Virtual
Office</h1>
<p>
 The SonicWall
```

Display custom login page: ○

□ Display login message on custom login page

Hide Domain list on portal login page: ●

Enable HttpOnly for SMA cookies: ●

Enable HTTP meta tags for cache control (recommended): ●

Enable HTTP Strict Transport Security (HSTS) for SMA: ●

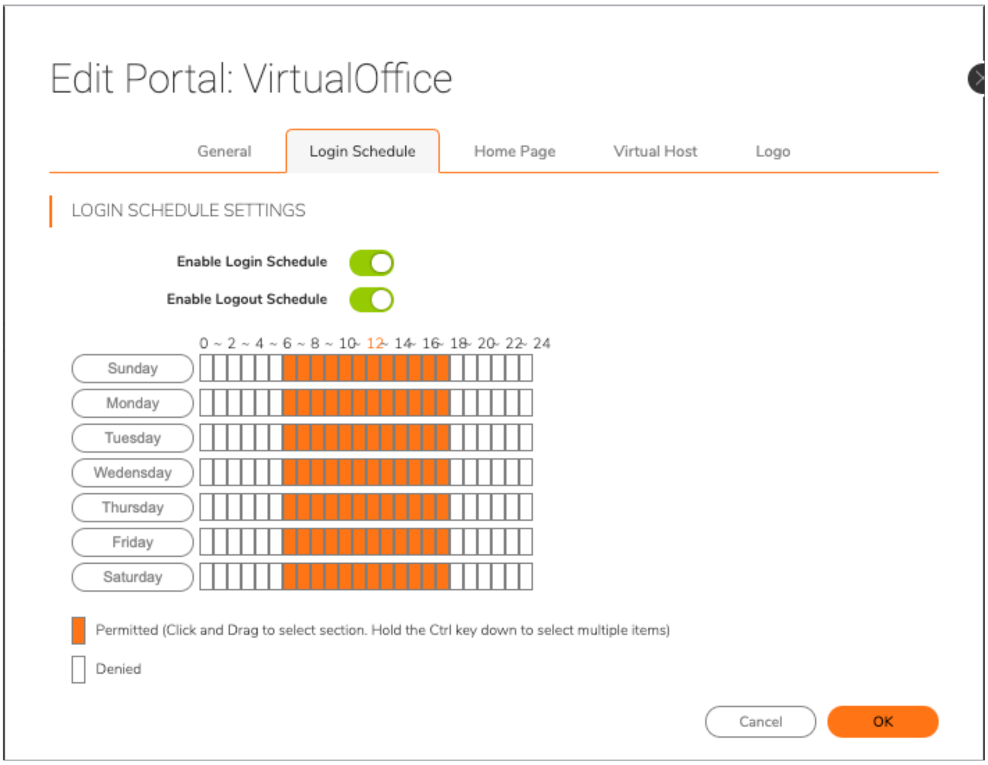
Enforce login uniqueness: ●

Enforcement method: Automatically logout existing session

Enforce client source uniqueness: ●

Enable “Login Schedule”

If your organization has normal office hours, and your users should only be connecting during those hours, then why risk allowing someone to connect before or after. With Login Schedule, you can deny access through the SMA 100 series during off hours.



Edit Portal: VirtualOffice

LOGIN SCHEDULE SETTINGS

Enable Login Schedule ●

Enable Logout Schedule ●

0 ~ 2 ~ 4 ~ 6 ~ 8 ~ 10~ 12~ 14~ 16~ 18~ 20~ 22~ 24

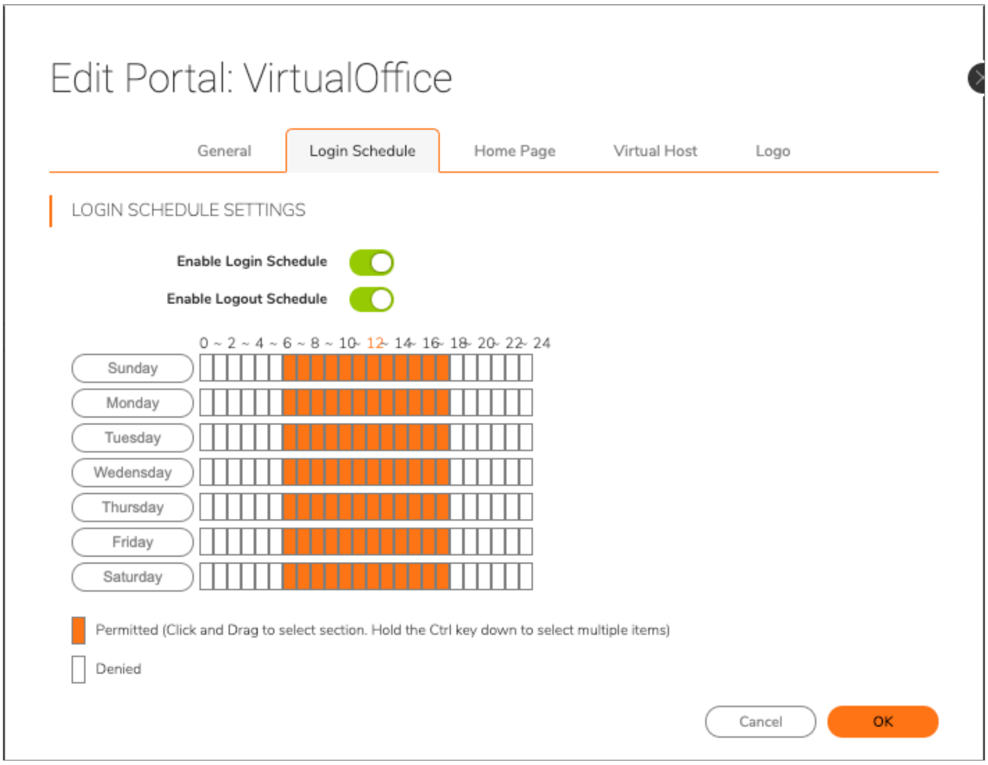
Sunday	□	□	□	□	□	□	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	□	□	□	□	□	□
Monday	□	□	□	□	□	□	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	□	□	□	□	□	□
Tuesday	□	□	□	□	□	□	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	□	□	□	□	□	□
Wedensday	□	□	□	□	□	□	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	□	□	□	□	□	□
Thursday	□	□	□	□	□	□	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	□	□	□	□	□	□
Friday	□	□	□	□	□	□	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	□	□	□	□	□	□
Saturday	□	□	□	□	□	□	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	□	□	□	□	□	□

🟧 Permitted (Click and Drag to select section. Hold the Ctrl key down to select multiple items)

□ Denied

Enable “Logout Schedule”

Many times, users tend to leave their remote network equipment connected, even while they are not in use. Any network activity can keep a client “awake” and avoid disconnecting due to inactivity. Setting up a logout schedule will automatically logout any user session that is connected during your defined time. Many times, threat actors that have remote access to remote user equipment, such as a laptop, will wait until after hours as not to draw attention from the user. This adds feature offers additional security to your network.



Edit Portal: VirtualOffice

LOGIN SCHEDULE SETTINGS

Enable Login Schedule ●

Enable Logout Schedule ●

0 ~ 2 ~ 4 ~ 6 ~ 8 ~ 10- 12- 14- 16- 18- 20- 22- 24

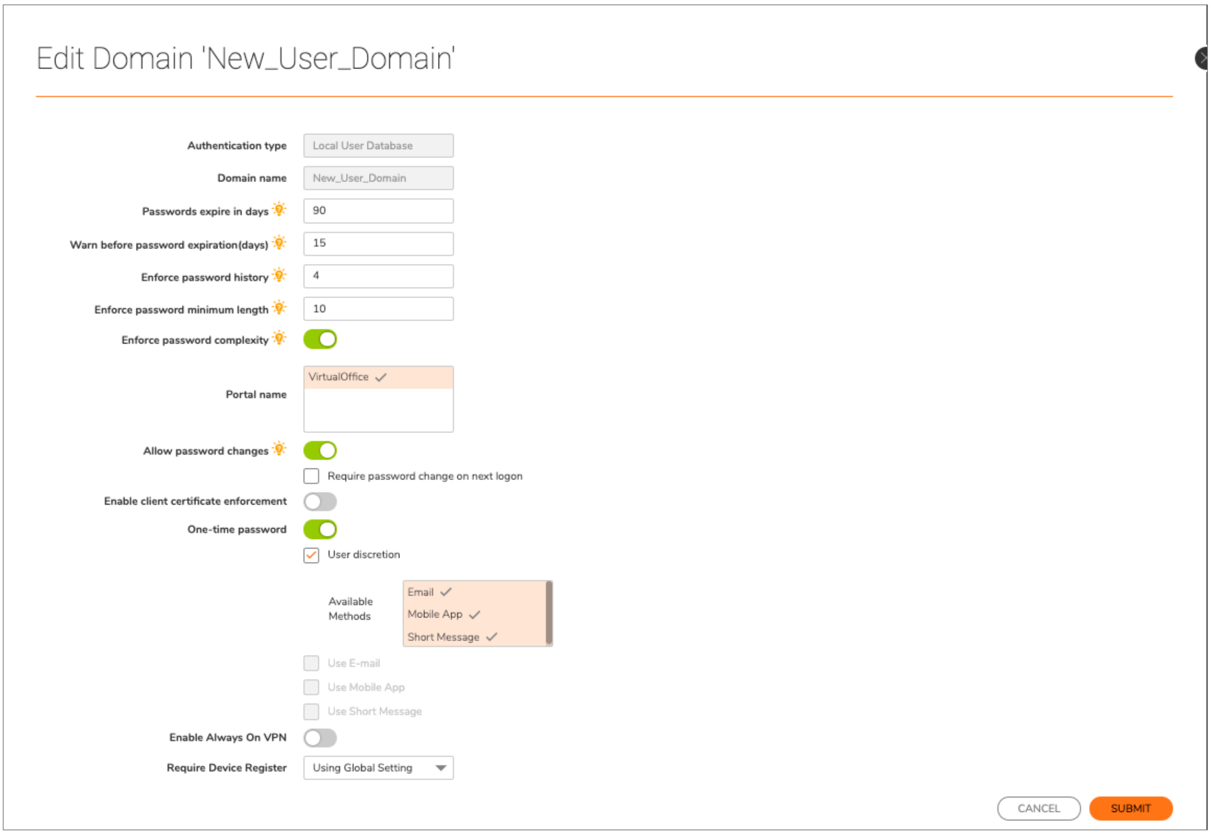
Sunday	□	□	□	□	□	□	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	□	□	□	□	□	□
Monday	□	□	□	□	□	□	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	□	□	□	□	□	□
Tuesday	□	□	□	□	□	□	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	□	□	□	□	□	□
Wedensday	□	□	□	□	□	□	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	□	□	□	□	□	□
Thursday	□	□	□	□	□	□	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	□	□	□	□	□	□
Friday	□	□	□	□	□	□	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	□	□	□	□	□	□
Saturday	□	□	□	□	□	□	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	□	□	□	□	□	□

🟧 Permitted (Click and Drag to select section. Hold the Ctrl key down to select multiple items)

□ Denied

Enforce Password Complexity

Users that can choose their own complex password tend to gravitate toward something they can remember. Those passwords may be short, common names or places, and may include their phone number or social security number. Threat actors have designed and built tools that can run through hundreds of thousands of names and combinations within minutes to guess passwords. Forcing your employees to have a stronger password that have additional complex characters will cause the threat actors to take years to attempt to guess. Common is 8 characters with upper case and numbers. Uncommon would be 12 or more characters with forced upper case and lower case, numbers, and special characters – as an example.



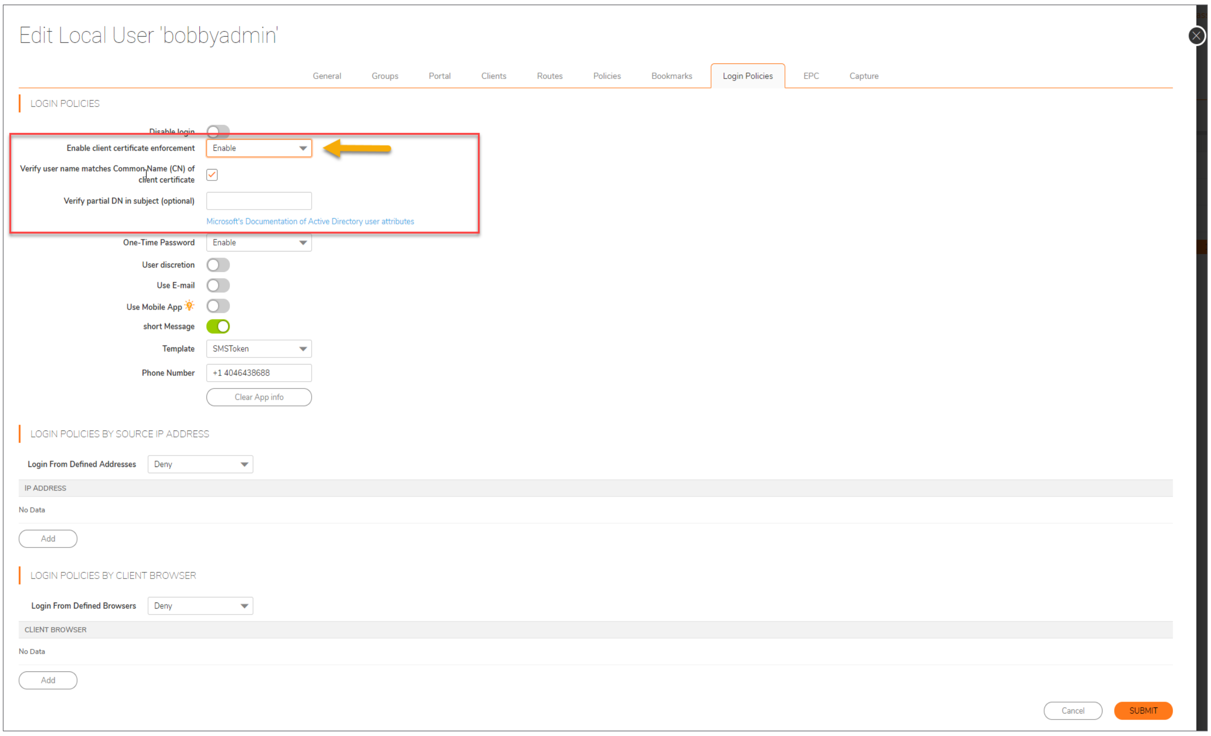
Edit Domain 'New_User_Domain'

Authentication type	Local User Database
Domain name	New_User_Domain
Passwords expire in days	90
Warn before password expiration(days)	15
Enforce password history	4
Enforce password minimum length	10
Enforce password complexity	●
Portal name	VirtualOffice ✓
Allow password changes	●
	□ Require password change on next logon
Enable client certificate enforcement	○
One-time password	●
	☑ User discretion
Available Methods	Email ✓ Mobile App ✓ Short Message ✓
	□ Use E-mail
	□ Use Mobile App
	□ Use Short Message
Enable Always On VPN	○
Require Device Register	Using Global Setting

Enable Client Certificate Enforcement (Advanced Security Feature)

As another means of ensuring the authenticity of a user and their device, administrators can deploy client-side certificates. With this setting enabled, the SonicWall SMA 100 series will verify the client certificate matches what is defined within the user settings. While this is a recommended additional setting for advanced security, it is more complicated in nature. Below we are providing links to Microsoft forums, as well as SonicWall KB's to help you in setting this feature up on your appliance if you choose to incorporate advanced security features.

- How can I enable client Certificate check for HTTPS management on the SonicWall?
- Client Certificate Authentication (Part 1) - Microsoft Tech Community



Edit Local User 'bobbyadmin'

LOGIN POLICIES

Disable login ○

Enable client certificate enforcement: Enable

Verify user name matches Common Name (CN) of client certificate ☑

Verify partial DN in subject (optional):

Microsoft's Documentation of Active Directory user attributes

One-Time Password: Enable

User discretion ○

Use E-mail ○

Use Mobile App ○

short Message ●

Template: SMSToken

Phone Number: +1 4046438688

LOGIN POLICIES BY SOURCE IP ADDRESS

Login From Defined Addresses: Deny

IP ADDRESS
No Data

LOGIN POLICIES BY CLIENT BROWSER

Login From Defined Browsers: Deny

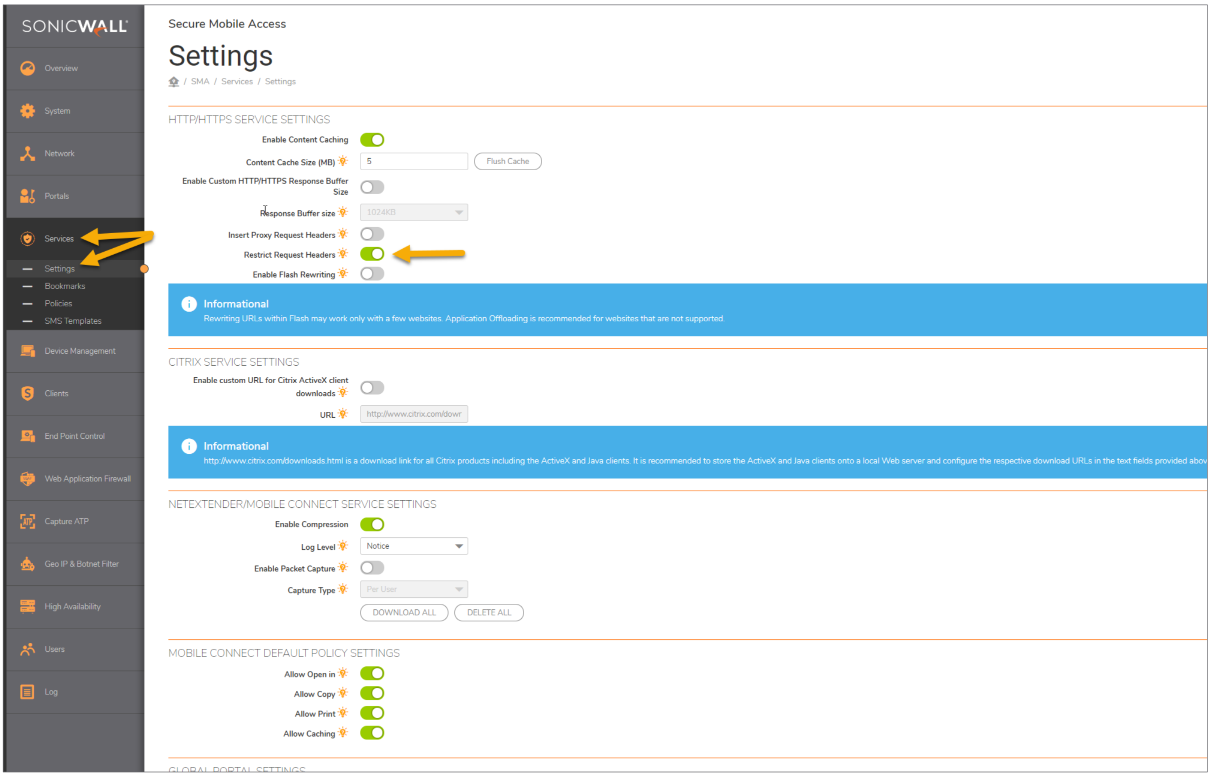
CLIENT BROWSER
No Data

Restrict Request Headers

A request header is an HTTP header that can be used in an HTTP request to provide information about the request context, so that the server can tailor the response. For example, the Accept- headers indicate the allowed and preferred formats of the response.

Threat actors attempting to gain control of websites will typically inject code into a request header. If the website is not protected, it may "dump" memory back as the reply – allowing the threat actor to possibly have access to passwords and usernames that are active.

By enabling this feature, the SonicWall SMA 100 series will not allow anything except what is expected in the header – thus not allowing for injection type attacks on the webservice.



Secure Mobile Access

Settings

/ SMA / Services / Settings

HTTP/HTTPS SERVICE SETTINGS

Enable Content Caching ☑

Content Cache Size (MB) 5 Flush Cache

Enable Custom HTTP/HTTPS Response Buffer Size ☐

Response Buffer size 1024KB

Insert Proxy Request Headers ☐

Restrict Request Headers ☑

Enable Flash Rewriting ☐

Informational
Rewriting URLs within Flash may work only with a few websites. Application Offloading is recommended for websites that are not supported.

CITRIX SERVICE SETTINGS

Enable custom URL for Citrix ActiveX client downloads ☐

URL http://www.citrix.com/dowr

Informational
http://www.citrix.com/downloads.html is a download link for all Citrix products including the ActiveX and Java clients. It is recommended to store the ActiveX and Java clients onto a local Web server and configure the respective download URLs in the text fields provided abov

NETEXTENDER/MOBILE CONNECT SERVICE SETTINGS

Enable Compression ☑

Log Level Notice

Enable Packet Capture ☐

Capture Type Per User

DOWNLOAD ALL DELETE ALL

MOBILE CONNECT DEFAULT POLICY SETTINGS

Allow Open in ☑

Allow Copy ☑

Allow Print ☑

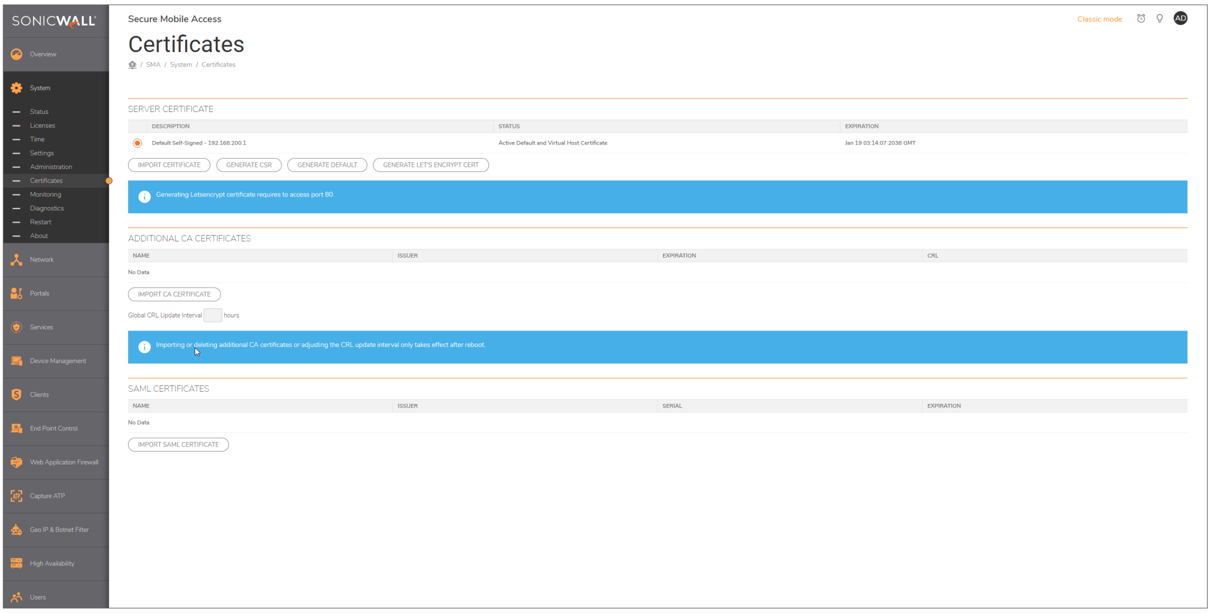
Allow Caching ☑

GLOBAL PORTAL SETTINGS

Use a Public Certificate

The SonicWall SMA appliance includes a self-signed certificate to provide SSL connectivity to the appliance for configuration. While this certificate can be used for normal operation of the appliance, it is highly recommended to use a public certificate from a trusted (and supported) public certificate authority. This will not only offer your users a higher level of security knowing they are connecting to your organization, but it will also allow them easier use of virtual office without the browser security warning from the self-signed certificate.

- How to create a Certificate Signing Request (CSR) and import a signed certificate on SMA 1000 series appliance?



Secure Mobile Access

Certificates

/ SMA / System / Certificates

SERVER CERTIFICATE

	DESCRIPTION	STATUS	EXPIRATION
●	Default Self-Signed - 192.168.200.1	Active Default and Virtual Host Certificate	Jan 19 03:14:07 2038 GMT

Generating Letsencrypt certificate requires to access port 80.

ADDITIONAL CA CERTIFICATES

NAME	ISSUER	EXPIRATION	CRL
No Data			

Global CRL Update Interval hours

Importing or deleting additional CA certificates or adjusting the CRL update interval only takes effect after reboot.

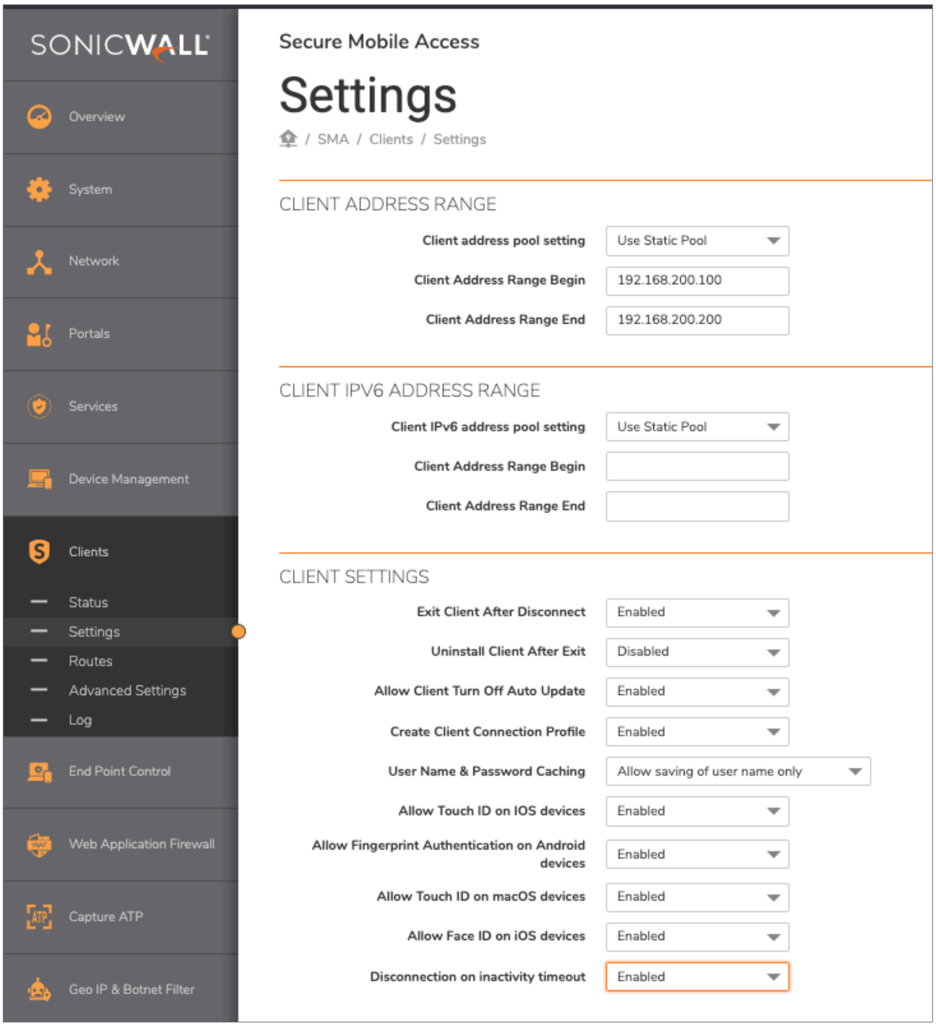
SAML CERTIFICATES

NAME	ISSUER	SERIAL	EXPIRATION
No Data			

Allow Touch ID and Face ID on Mac, Apple IOS and Android Devices

As part of the 2FA mechanism mentioned in the beginning of this best practice guide, this incorporates the “Something you are”. By allowing your users to utilize the additional security vectors incorporate in their devices, this provides additional layers of security to identify the user connecting is the intended user

- SMB SSL-VPN: How to enable Mobile Connect touch ID authentication



Secure Mobile Access

Settings

/ SMA / Clients / Settings

CLIENT ADDRESS RANGE

Client address pool setting	Use Static Pool
Client Address Range Begin	192.168.200.100
Client Address Range End	192.168.200.200

CLIENT IPV6 ADDRESS RANGE

Client IPv6 address pool setting	Use Static Pool
Client Address Range Begin	
Client Address Range End	

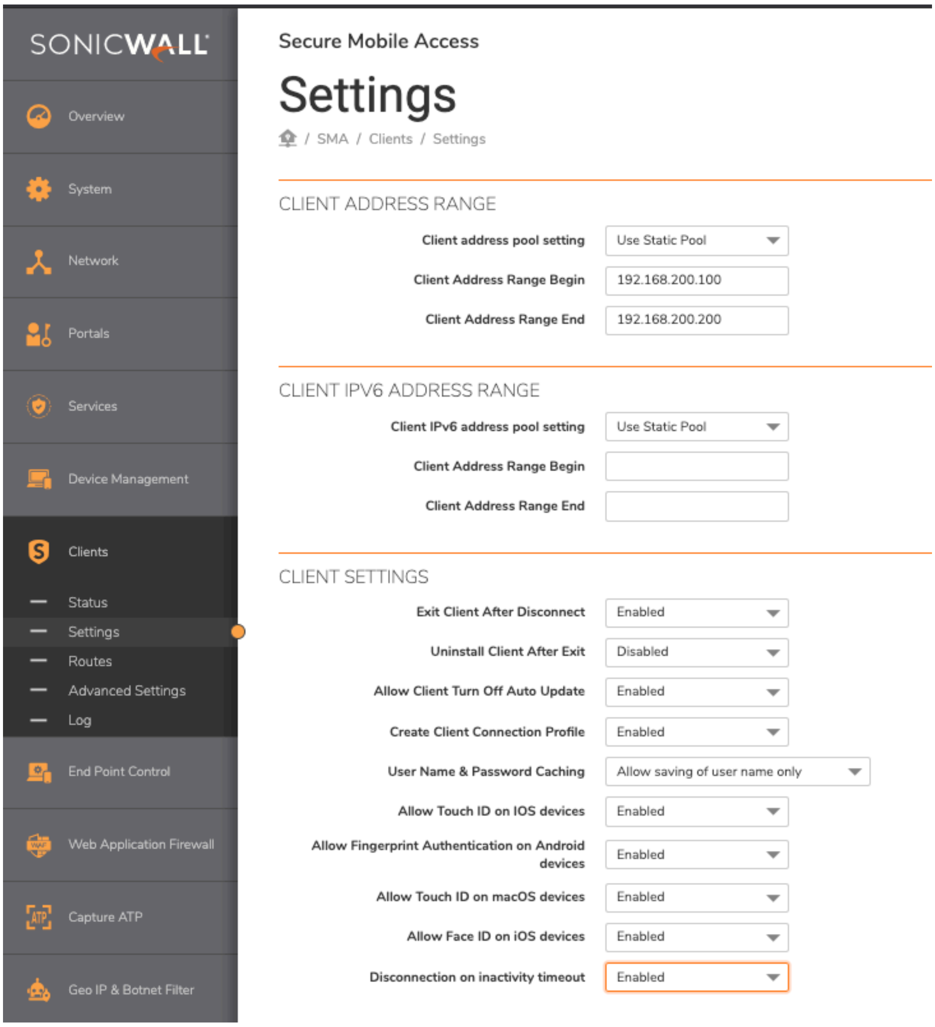
CLIENT SETTINGS

Exit Client After Disconnect	Enabled
Uninstall Client After Exit	Disabled
Allow Client Turn Off Auto Update	Enabled
Create Client Connection Profile	Enabled
User Name & Password Caching	Allow saving of user name only
Allow Touch ID on IOS devices	Enabled
Allow Fingerprint Authentication on Android devices	Enabled
Allow Touch ID on macOS devices	Enabled
Allow Face ID on iOS devices	Enabled
Disconnection on inactivity timeout	Enabled

Disconnection on Inactivity Timeout

As a security precaution, administrators should not allow their users to remain connected via a VPN connection if no data is passing through for an extended amount of time. If a user were to leave a session active and a threat actor gained access to their device while the user was not present, then the threat actor could gain access to the network utilizing the user's credentials.

- Inactivity timeout for NetExtender



Secure Mobile Access

Settings

/ SMA / Clients / Settings

CLIENT ADDRESS RANGE

Client address pool setting	Use Static Pool
Client Address Range Begin	192.168.200.100
Client Address Range End	192.168.200.200

CLIENT IPV6 ADDRESS RANGE

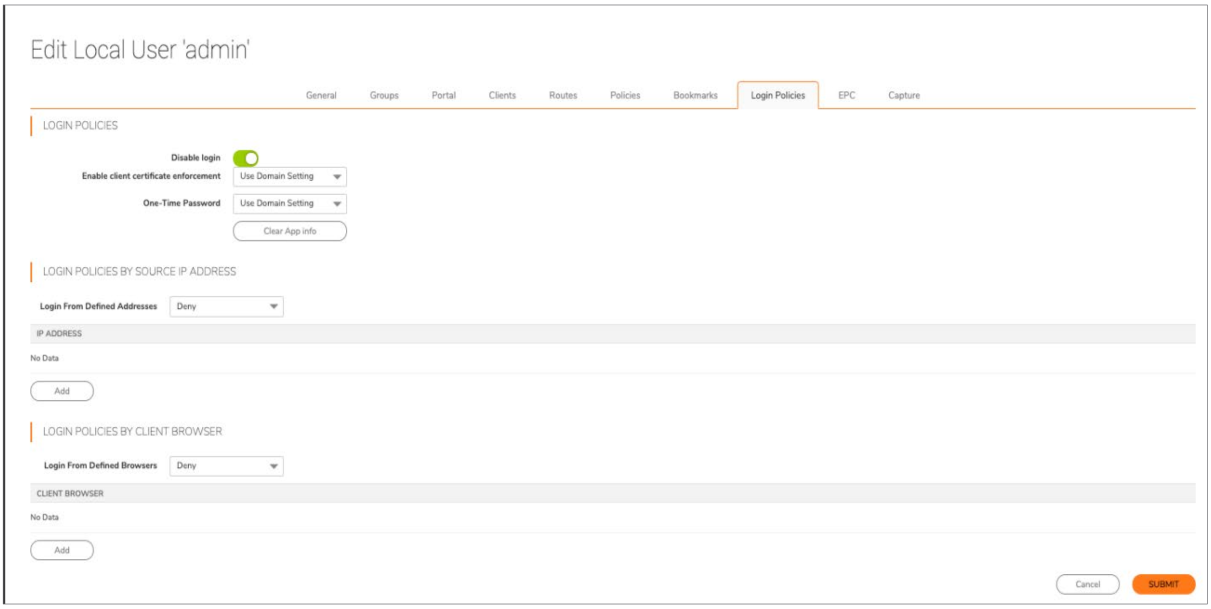
Client IPv6 address pool setting	Use Static Pool
Client Address Range Begin	
Client Address Range End	

CLIENT SETTINGS

Exit Client After Disconnect	Enabled
Uninstall Client After Exit	Disabled
Allow Client Turn Off Auto Update	Enabled
Create Client Connection Profile	Enabled
User Name & Password Caching	Allow saving of user name only
Allow Touch ID on IOS devices	Enabled
Allow Fingerprint Authentication on Android devices	Enabled
Allow Touch ID on macOS devices	Enabled
Allow Face ID on iOS devices	Enabled
Disconnection on inactivity timeout	Enabled

Disable the Default Admin Account

As a security precaution, it is recommended to disable the default user account for login access. To do this, you must first create a NEW administrator. It is recommended to use a different username than “Admin or Administrator”. Test the new administrator login PRIOR to disabling the default admin account.



Edit Local User 'admin'

LOGIN POLICIES

Disable login: ●

Enable client certificate enforcement: Use Domain Setting

One-Time Password: Use Domain Setting

LOGIN POLICIES BY SOURCE IP ADDRESS

Login From Defined Addresses: Deny

IP ADDRESS

No Data

LOGIN POLICIES BY CLIENT BROWSER

Login From Defined Browsers: Deny

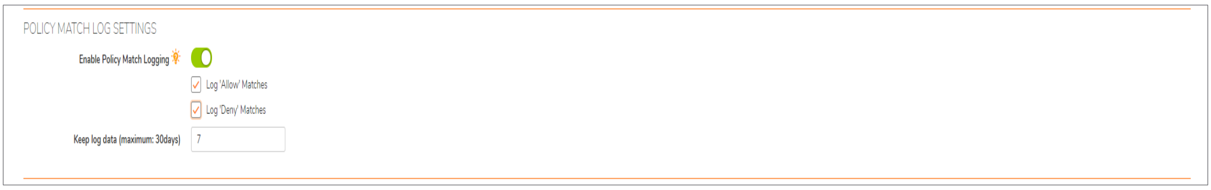
CLIENT BROWSER

No Data

Allow Policy Match Logging

Found under the Settings tab, this feature will help better track users and what they are doing. It will also allow you to see those who try and connect and go to places they are not allowed.

- How to enable the logs to track Access Policies matched by users



POLICY MATCH LOG SETTINGS

Enable Policy Match Logging ●

☑ Log 'Allow' Matches

☑ Log 'Deny' Matches

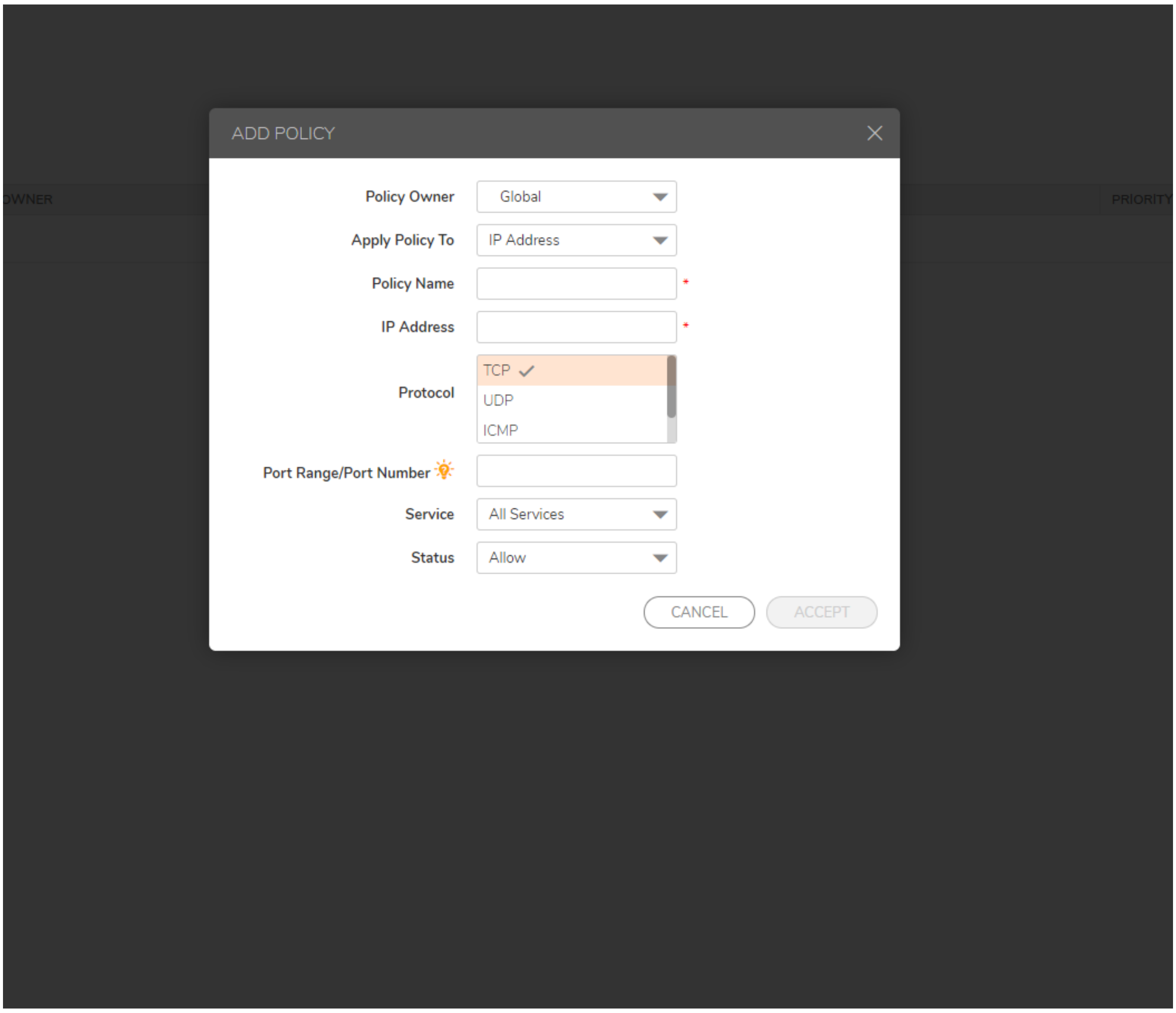
Keep log data (maximum: 30days) 7

Setup Connection Policies

Allowing users into a network from a remote location is a nice convenience. However, as we have discussed in this guide, this allows for heightened security risk from compromised remote individuals. To help better tighten security, adding connection policies globally and to the individual will help control the possibility of malware which may be embedded on a user's workstation.

If a user only needs to access a specific server or folder on a specific folder, you can lock down the connection to only allow access to that specific area. If users are only making TCP connections into your backend infrastructure, you could disable UDP protocols, which are sometimes used to deliver malicious payloads.

- SMA 100 Series: Information on Access Policy Hierarchy



ADD POLICY

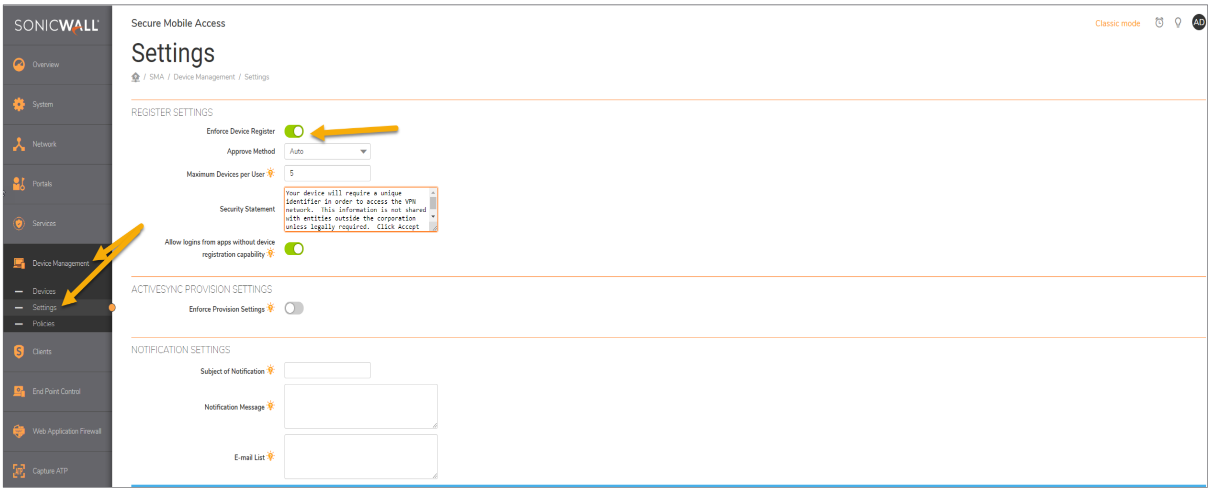
Policy Owner	Global
Apply Policy To	IP Address
Policy Name	*
IP Address	*
Protocol	TCP ✓ UDP ICMP
Port Range/Port Number	
Service	All Services
Status	Allow

Device Registration

In some cases, you may not be able to offer 2FA. This is true in the example of a kiosk which has no human interaction. With Device Registration, you will be able to register the unique identity of the connecting device, and only that device with that unique ID will be able to connect with the username and password associated to it

This is a good way to ensure additional security controls in your network, and to ensure users are not changing devices or using devices such as workstations in hotels or other public places.

- How to restrict users based on DeviceID using Device policies.



Secure Mobile Access

Settings

/ SMA / Device Management / Settings

REGISTER SETTINGS

Enforce Device Register: on

Approve Method: Auto

Maximum Devices per User: 5

Security Statement: Your device will require a unique identifier in order to access the VPN network. This information is not shared with entities outside the corporation unless legally required. Click Accept

Allow logins from apps without device registration capability: on

ACTIVESYNC PROVISION SETTINGS

Enforce Provision Settings: off

NOTIFICATION SETTINGS

Subject of Notification

Notification Message

E-mail List

End Point Control

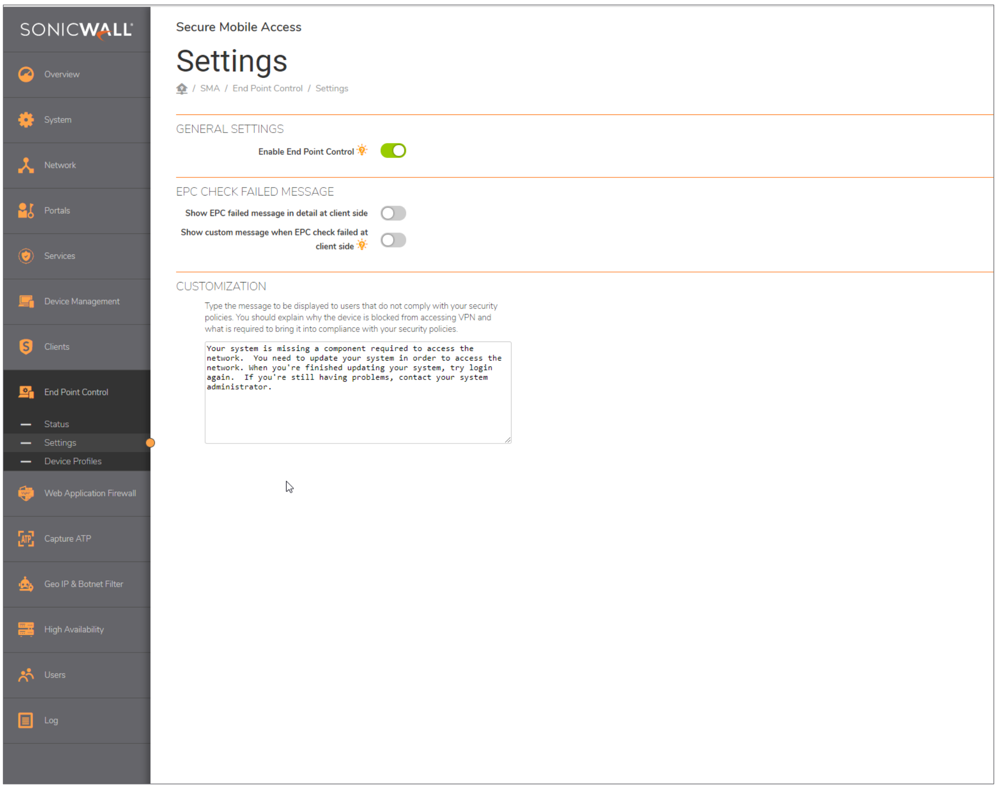
The SonicWall SMA 100 series incorporates advanced endpoint control functionality. While this is often an overlooked part of the product, it is a very important security addition.

End Point Control allows you to make verifications of different aspects of the connecting device:

- Does the connecting device have an anti-virus client?
- Is the connecting device a member of my domain?
- Does the connecting device have the specific file or folder that was hidden in a specific location?

End Point Control is an advanced security feature that will enable the administrator additional protection of the company network

- SRA/SMB SSL-VPN: How to apply EPC (End Point Control) restrictions to Users/Groups based on Windows



Secure Mobile Access

Settings

/ SMA / End Point Control / Settings

GENERAL SETTINGS

Enable End Point Control ●

EPC CHECK FAILED MESSAGE

Show EPC failed message in detail at client side ○

Show custom message when EPC check failed at client side ○

CUSTOMIZATION

Type the message to be displayed to users that do not comply with your security policies. You should explain why the device is blocked from accessing VPN and what is required to bring it into compliance with your security policies.

```
Your system is missing a component required to access the
network.  You need to update your system in order to access the
network. When you're finished updating your system, try login
again.  If you're still having problems, contact your system
administrator.
```

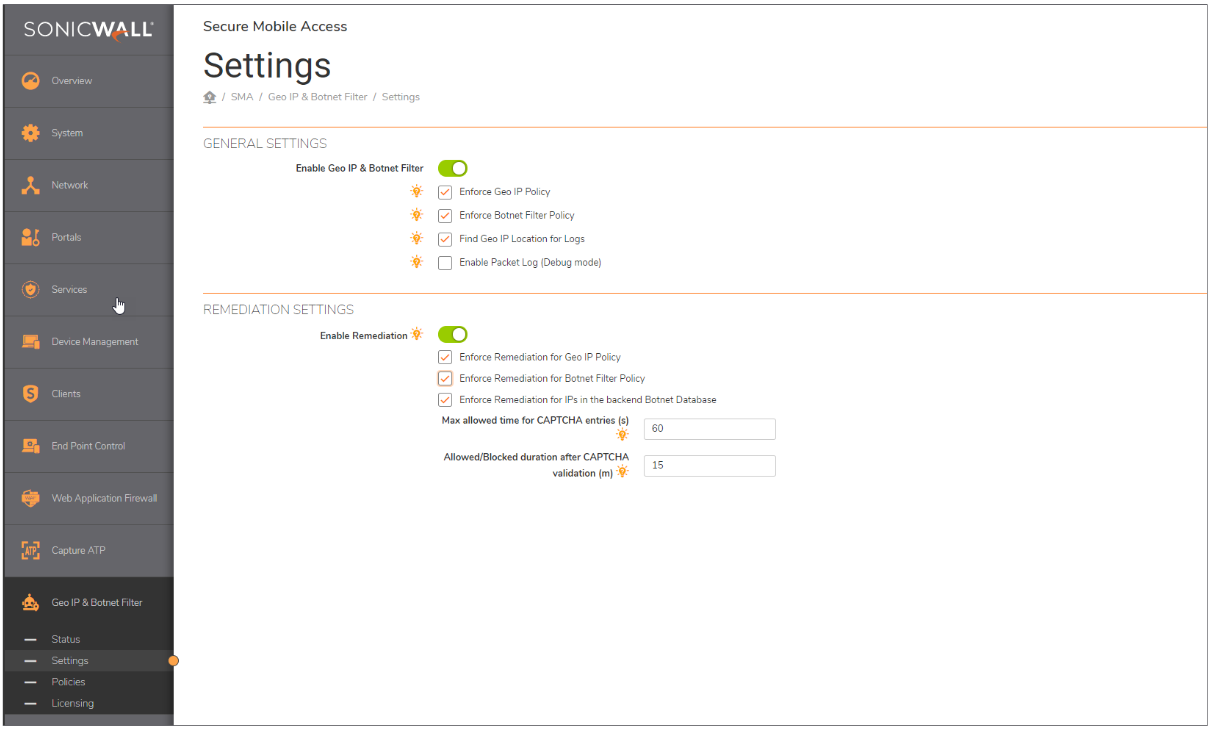
GEO IP Fencing

The SonicWall SMA 100 series contains a very advanced geo fencing capability. This feature allows the administrator to block access from countries that are not a travel destination for employees, or a location that a customer or client would be connecting from. By adding this layer of security, you can reduce the number of attacks by a significant amount. Most threats to networks occur from outside the resident country where the appliance is located.

The SMA 100 series can also add the geo location within the connectivity logs. This helps identify not only where the users are coming from (authorized users), but also helps identify where threat actors may be residing.

In the event your organization is international, and you still wish to put a policy in place to help keep bad actors from using auto dialers to try and connect to your system- you can enable the CAPTCHA feature. This would require a human to identify the letters and numbers in a random picture and manually enter this information before being allowed to connect from outside your geo fence area. Those who guess wrong after a set amount of time would be denied

- SMB-SSL VPN: How to block access to the SRA device from specific source IP address or range using Geo-IP/Botnet filter



Secure Mobile Access

Settings

/ SMA / Geo IP & Botnet Filter / Settings

GENERAL SETTINGS

Enable Geo IP & Botnet Filter ●

☑ Enforce Geo IP Policy

☑ Enforce Botnet Filter Policy

☑ Find Geo IP Location for Logs

□ Enable Packet Log (Debug mode)

REMEDIATION SETTINGS

Enable Remediation ●

☑ Enforce Remediation for Geo IP Policy

☑ Enforce Remediation for Botnet Filter Policy

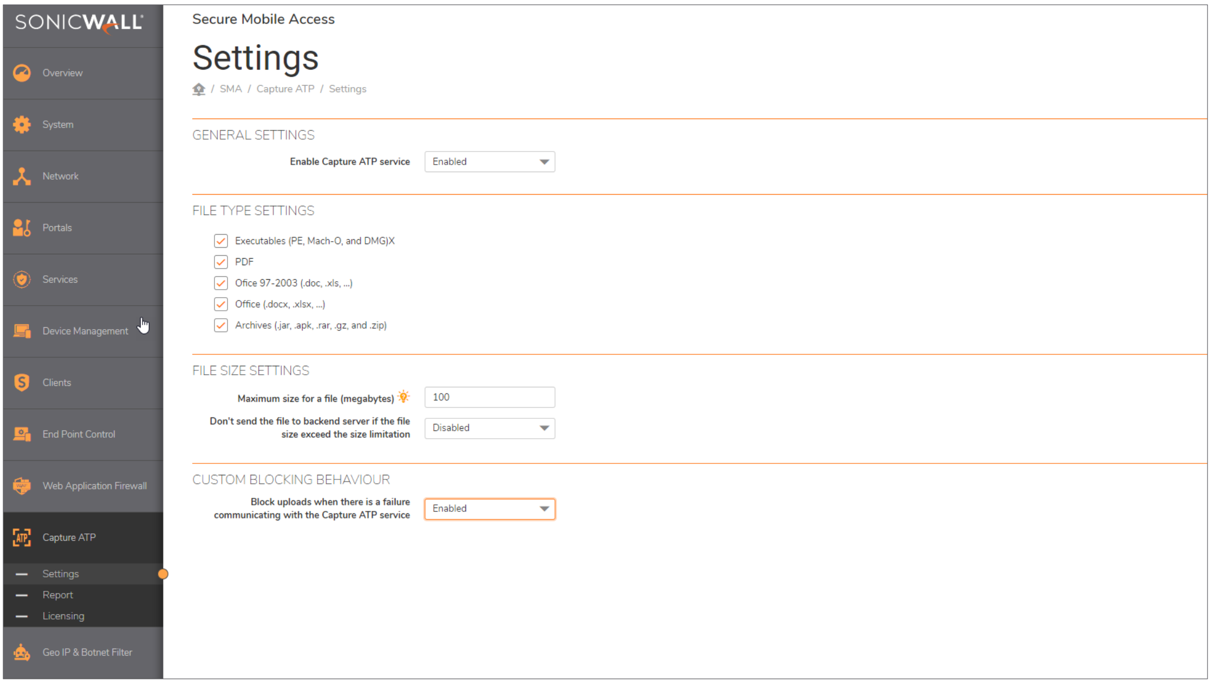
☑ Enforce Remediation for IPs in the backend Botnet Database

Max allowed time for CAPTCHA entries (s): 60

Allowed/Blocked duration after CAPTCHA validation (m): 15

Capture ATP for the SMA 100 Series

A unique feature from SonicWall is the availability of Capture ATP. With this enabled on your SMA 100 device, clients that are connected and passing traffic into your network would have that traffic inspected by the SonicWall Capture ATP service. This is a cloud-based sandbox solution which incorporates RTDMI (Real Time Deep Memory Inspection). With this feature enabled – if a threat actor was to gain access to a remote computer device and attempted to upload a malicious payload to the network, Capture ATP could potentially identify the threat and block it.



Secure Mobile Access

Settings

/ SMA / Capture ATP / Settings

GENERAL SETTINGS

Enable Capture ATP service: Enabled

FILE TYPE SETTINGS

☑ Executables (PE, Mach-O, and DMG)X
☑ PDF
☑ Ofice 97-2003 (.doc, .xls, ...)
☑ Office (.docx, .xlsx, ...)
☑ Archives (.jar, .apk, .rar, .gz, and .zip)

FILE SIZE SETTINGS

Maximum size for a file (megabytes): 100

Don't send the file to backend server if the file size exceed the size limitation: Disabled

CUSTOM BLOCKING BEHAVIOUR

Block uploads when there is a failure communicating with the Capture ATP service: Enabled

General Considerations

- Always ensure security services are active and enabled
- Review new firmware releases. Inspect the Firmware *Getting Started Guide* for important information on patches and / or additional features that may be implemented on the product
- Ensure you are on the latest firmware when possible
- Review the access that grated to remote users – do not give more than is needed
- Always use 2FA – this is a critical feature that must be enabled in all remote environments

SonicWall Support

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

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 and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- 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.

About This Document

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

Last updated: 2/1/2021

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/license-agreements. Select the language based on your geographic location to see the EUPA that applies to your region.