

# SafeNet Authentication Client Integration Guide

---

Using SAC CBA with SonicWALL Secure Remote  
Access



THE  
DATA  
PROTECTION  
COMPANY

# Document Information

<b>Document Part Number</b>	007-012819-001
<b>Release Date</b>	November 2014

## Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

## Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

<b>Contact Method</b>	<b>Contact Information</b>
<b>Mail</b>	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
<b>Email</b>	<a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a>

# Contents

Third-Party Software Acknowledgement .....	4
Description .....	4
Applicability .....	5
Environment .....	5
Audience .....	5
Prerequisites .....	5
CBA Authentication Flow using SAC .....	6
Configuring SonicWALL Secure Remote Access .....	7
Importing a Root CA Certificate .....	7
Creating a Realm .....	10
Creating a User .....	14
Applying Configuration Changes .....	16
Running the Solution .....	18
Using a Web Browser .....	18
Using the Connect Tunnel Application .....	21
Appendix: Configuring Remote Desktop .....	24
Support Contacts .....	29

## Third-Party Software Acknowledgement

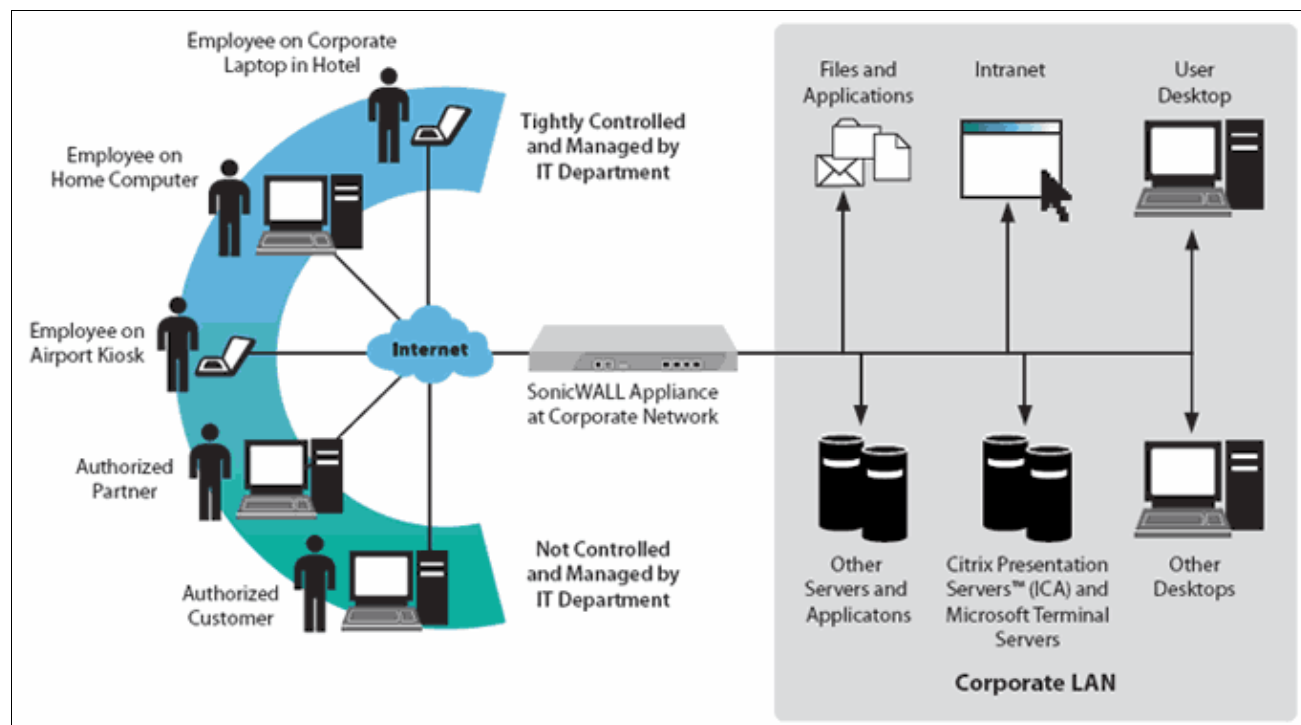
This document is intended to help users of SafeNet products when working with third-party software, such as SonicWALL Secure Remote Access.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

## Description

SafeNet Authentication Client (SAC) is a Public Key Infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. It utilizes a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

SonicWALL Secure Remote Access appliances extend secure remote networking over an SSL VPN to potentially thousands of locations to provide anytime, anywhere access. The encrypted SSL VPN tunnel protects the transmitted data. In addition, as an added layer of protection, granular access controls allow the administrator to delegate access privileges to different individuals or groups so that they can access only specific, defined resources. SonicWALL Secure Remote Access appliances integrate seamlessly with virtually any firewall.



*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*

The SonicWALL Secure Remote Access appliance can be configured to communicate with SAC to perform certificate-based authentication (CBA).

## Applicability

---

The information in this document applies to:

- **SafeNet Authentication Client (SAC)** – SafeNet's public key infrastructure (PKI) middleware

## Environment

---

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Client (SAC) 8.3** – SafeNet's public key infrastructure (PKI) middleware
- **SonicWALL E-Class SRA Virtual Appliance 11.0**

## Audience

---

This document is targeted to system administrators who are familiar with SonicWALL Secure Remote Access and are interested in adding Certificate Based Authentication capabilities using SAC.

## Prerequisites

---

- SafeNet Authentication Client 8.3 should be installed on all the client machines.
- A root Certificate Authority (CA) certificate should be available.
- A user must have a SafeNet token with appropriate certificate (with private key) enrolled from the root Certificate Authority.
- SonicWALL Secure Remote Access should be installed and configured for basic authentication prior to implementing certificate-based authentication using SafeNet Authentication Client.

## CBA Authentication Flow using SAC



1. A user attempts to connect to the VPN using a web browser (for WorkSpace) or the Connect Tunnel application.
2. The user selects a realm and plugs in the SafeNet token with an appropriate certificate.
3. The web browser or the Connect Tunnel application looks for a valid user certificate as per the realm selected. User selects the certificate and enters the token password.
4. If the token password is correct, the user is successfully authenticated and gets connected to the VPN or WorkSpace.

# Configuring SonicWALL Secure Remote Access

Configuring SonicWALL Secure Remote Access for CBA authentication requires:

- Importing a Root CA Certificate
- Creating a Realm
- Creating a User
- Applying Configuration Changes

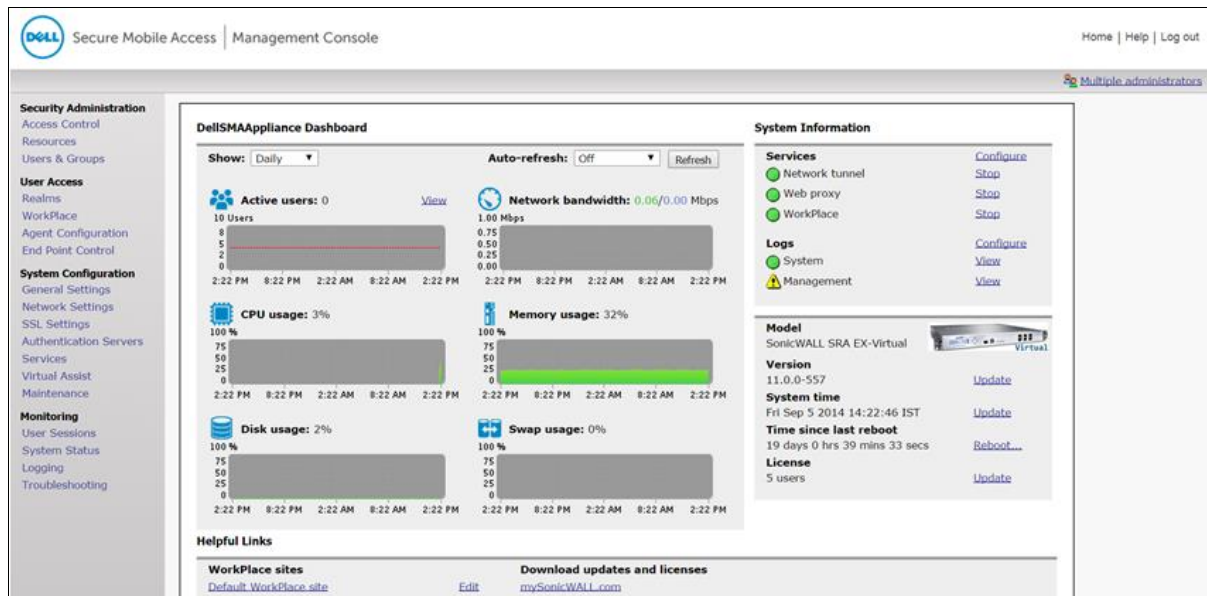
To perform these configuration settings, log in to the SonicWALL Secure Remote Access appliance with administrator credentials.

## Importing a Root CA Certificate

A root CA certificate is added on the SonicWALL Secure Remote Access appliance. This root CA certificate is used to authenticate users with a valid user certificate.

**To import a certificate:**

1. Open the **SonicWALL Management Console**.



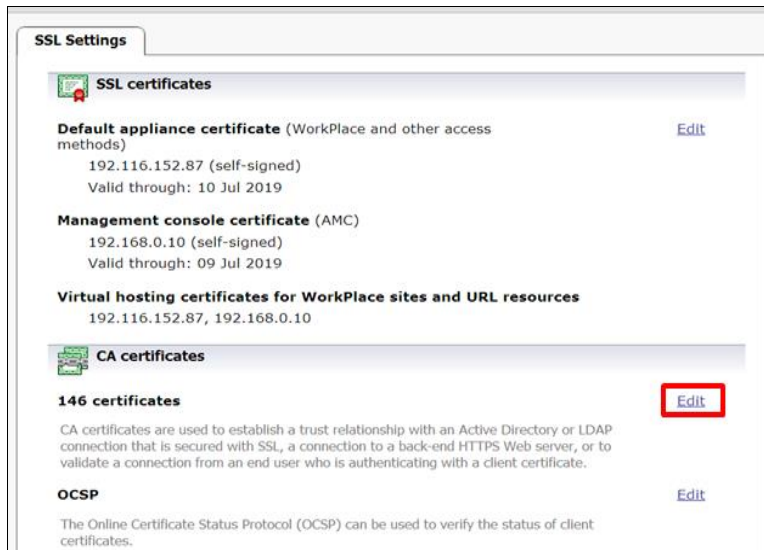
*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*

2. On the **Secure Mobile Access Management Console** window, in the left pane, under **System Configuration**, click **SSL Settings**.



(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

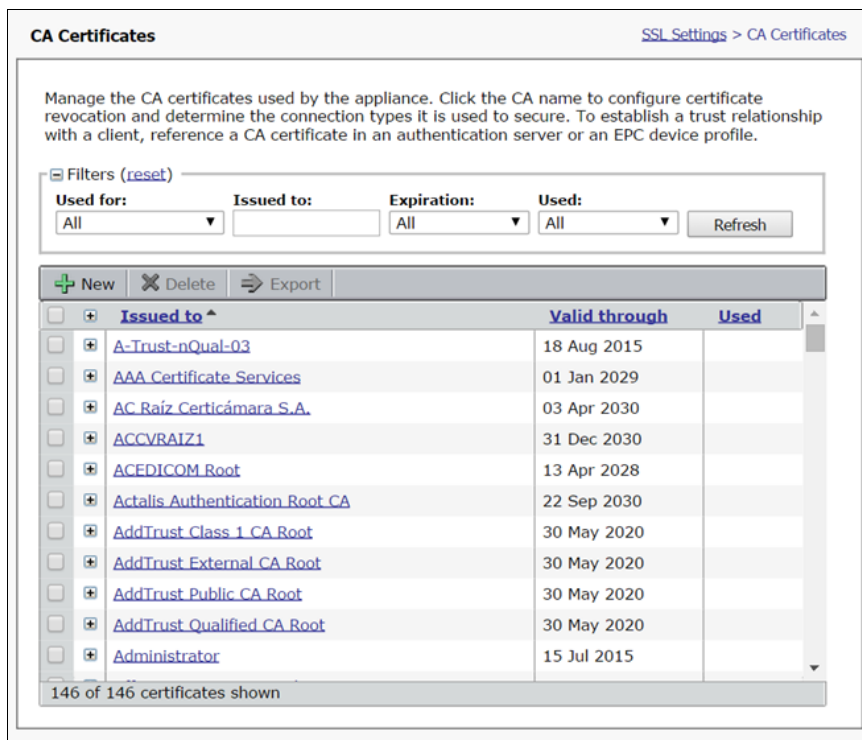
3. On the **SSL Settings** tab, under **CA certificates**, click the first **Edit** link (see the red box in the image below).



(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

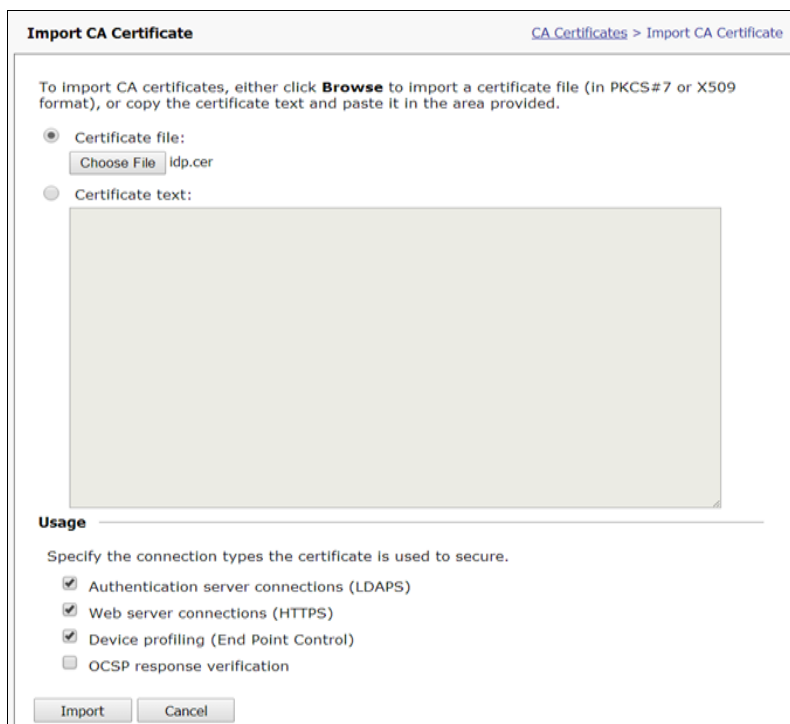


4. On the **CA Certificates** window, click **New**.



(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

5. On the **Import CA Certificates** window, select **Certificate file**, and then click **Choose File** to browse and select the root CA certificate.



(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

6. On the **Import CA Certificates** window, click **Import**.

The root CA certificate is imported successfully.



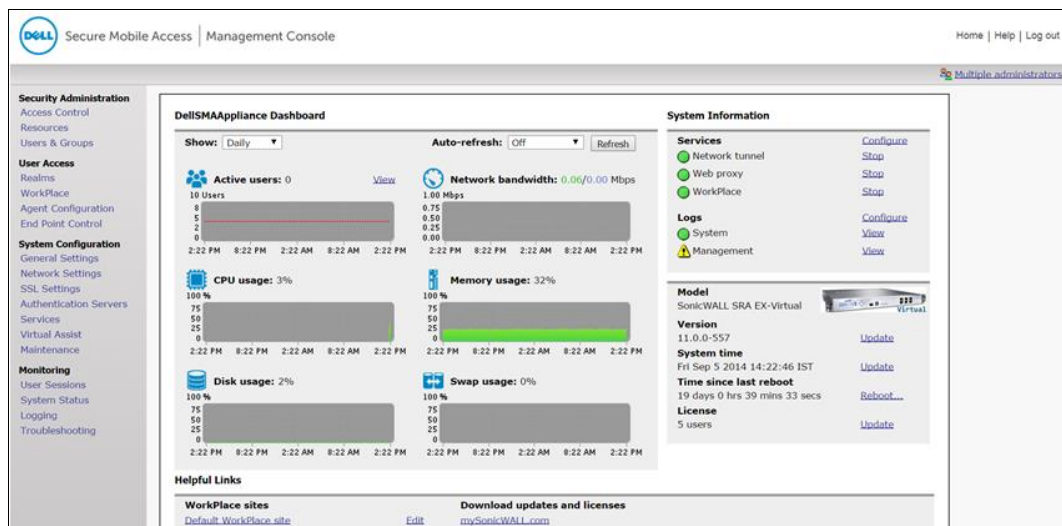
(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

## Creating a Realm

A realm references an authentication server and determines which access agents are provisioned to users and which endpoint control restrictions are imposed.

**To create a realm:**

1. Open the **SonicWALL Management Console**.



(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

2. On the **Secure Mobile Access Management Console** window, in the left pane, under **User Access**, click **Realms**.



*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*

3. In the upper right corner of the window, click the **New realm** link.



*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*

4. On the **Configure Realm** window, on the **General** tab, complete the following details:
  - a. In the **Name** field, enter a name for the realm.
  - b. In the **Authentication server** field, click **New**.

The screenshot shows the 'Configure Realm' window with the 'General' tab selected. The window title is 'Configure Realm' with a breadcrumb 'Realms > Configure Realm'. Below the tabs, there's a section 'Configure the general settings for the realm.' containing fields for 'Name:\*' (with a text input), 'Description:' (with a text input), and 'Status:' with radio buttons for 'Enabled' (selected) and 'Disabled'. There's a checkbox for 'Display this realm' which is checked. The 'Authentication server:' section has a dropdown menu showing 'Choose one' and a 'New' button. Below that is a checkbox for 'Enable accounting records'. At the bottom, there's an 'Advanced' section with a dropdown arrow. Navigation buttons at the bottom are '< Back', 'Next >', 'Cancel', and 'Finish'.

(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

- c. On the **New Authentication Server** window, under **Authentication directory**, select **Public key infrastructure (PKI)**, and then click **Continue**.

The screenshot shows the 'New Authentication Server' window with a breadcrumb 'Authentication Servers > New Authentication Server'. The main instruction is 'Choose the protocol used to access your user store, and specify how users will authenticate. Click **Continue** to configure the authentication server.' Under the 'User store' section, it says 'Choose the directory type or authentication method:'. The 'Authentication directory' section has radio buttons for: 'Microsoft Active Directory (Basic)' (with note 'A single domain.'), 'Microsoft Active Directory (Advanced)' (with note 'Multiple domains in a tree or forest.'), 'LDAP', 'RADIUS', 'RSA Authentication Manager', 'Public key infrastructure (PKI)' (selected), and 'CA SiteMinder'. The 'Single sign-on server' section has a radio button for 'RSA ClearTrust' (with note 'Sign-on to ClearTrust is supported only from a Web browser.'). The 'Local user storage' section has a radio button for 'Local users' (with note 'The appliance supports one local user authentication server.'). The 'Credential type' section says 'Specify how users will authenticate:' and has radio buttons for 'Digital certificate' (selected), 'Token/SecurID', and 'Username/Password'. At the bottom are 'Continue...' and 'Cancel' buttons.

(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

- d. On the **Configure Authentication Server** window, complete the details as specified below, and then click **Save**.

<b>Name</b>	Enter a name for the authentication server.
<b>Trusted CA certificates</b>	In the <b>All CA certificate</b> list, select the root CA certificate that you have imported, and then click <b>&gt;&gt;</b> . The certificate is added to the <b>Trusted CA certificates</b> list.

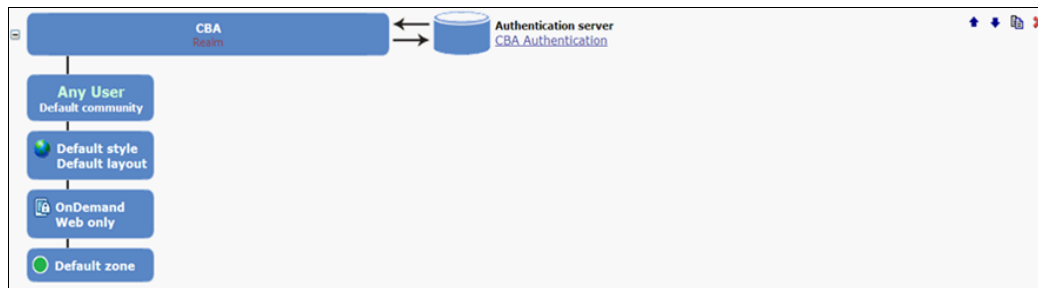
(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

On the **Configure Realm** window, the newly created authentication server is populated in the **Authentication Server** field.

(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

5. Click **Next > Finish**.

A realm is created and its details are displayed.



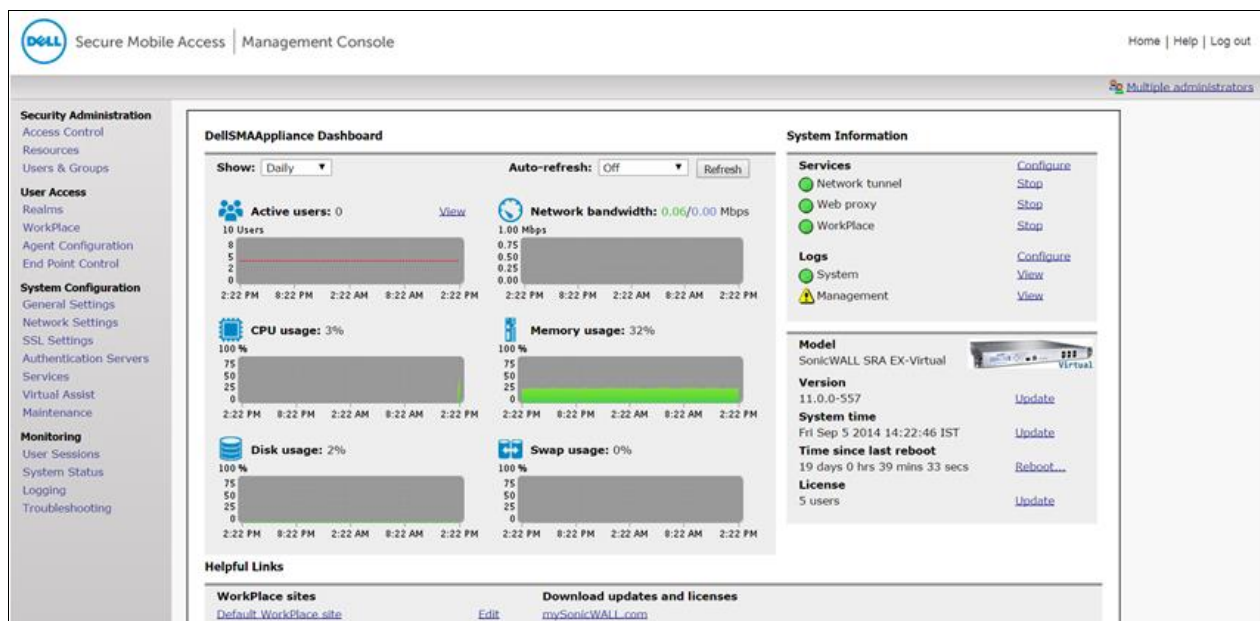
(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

## Creating a User

A user is an individual who needs access to resources on the corporate network. After creating users on the SonicWALL Secure Remote Access appliance, you can reference them in an Access Control Rule to permit or deny access to resources.

**To create a user:**

1. Open the **SonicWALL Management Console**.



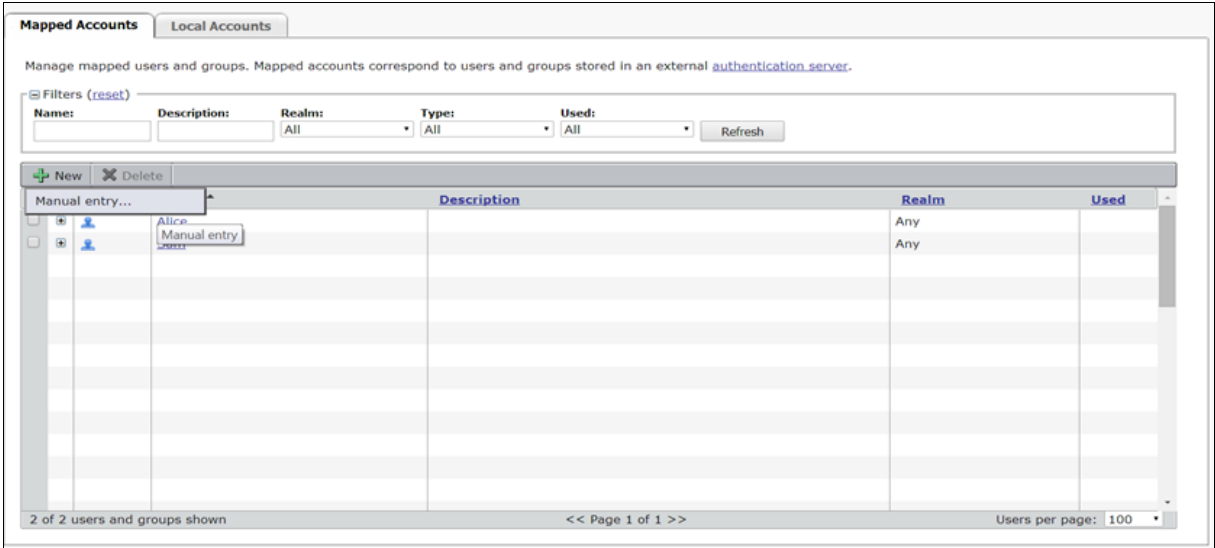
(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

2. On the **Secure Mobile Access Management Console** window, in the left pane, under **Security Administration**, click **Users & Groups**.



(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

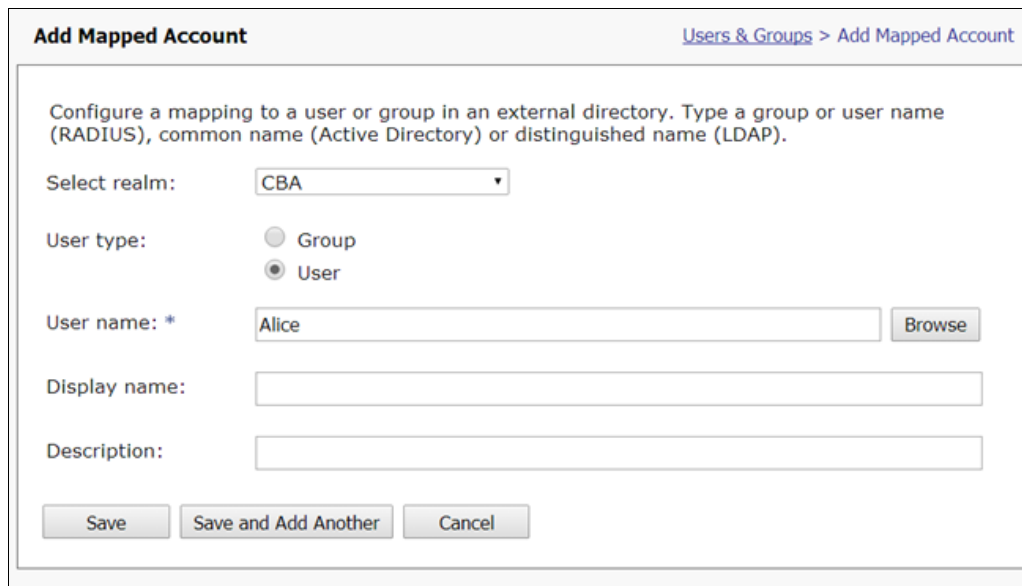
3. On the **Mapped Accounts** tab, click **New > Manual entry**.



(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

4. On the **Add Mapped Account** window, complete the details as specified below, and then click **Save**.

<b>Select realm</b>	Select the realm that was created previously.
<b>User type</b>	Select <b>User</b> .
<b>User name</b>	Enter the name of the user. The user name must be same as specified in the Active Directory.
<b>Display name</b>	Enter the name of the user for display.
<b>Description</b>	Enter a description of this mapped account.



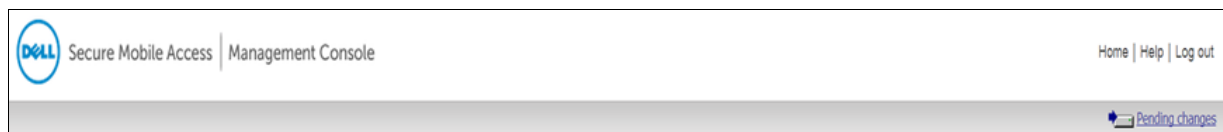
*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*

## Applying Configuration Changes

After you have made the configuration changes, you need to apply them in the system.

### To apply configuration changes:

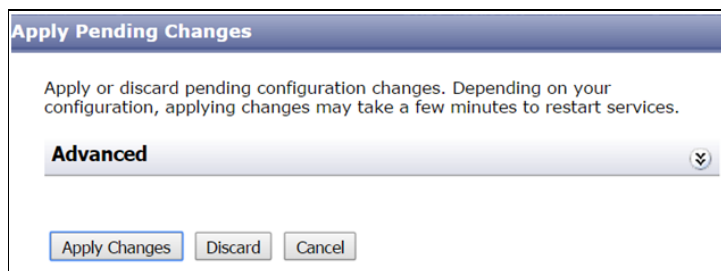
1. Open the **SonicWALL Management Console**.
2. On the **Secure Mobile Access Management Console** window, in the upper right corner, click **Pending changes**.



*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*

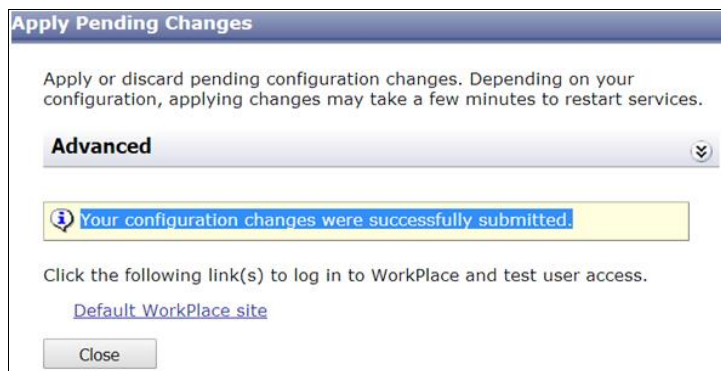


3. On the **Apply Pending Changes** window, click **Apply Changes**.



*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*

The changes are applied and a message is displayed.



*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*

4. Click **Close**.

## Running the Solution

After configuring SonicWALL Secure Remote Access for CBA authentication with SafeNet Authentication Client, users can securely connect using the following methods:

- Using a Web Browser—page 18
- Using the Connect Tunnel Application—page 21

For this integration, the SafeNet eToken 5100 is configured for authentication with the SAC solution.

### Using a Web Browser

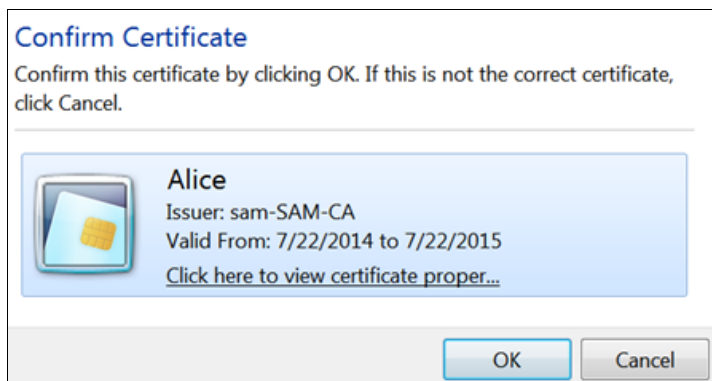
The SonicWALL WorkPlace portal is used to verify this integration solution. The WorkPlace portal provides users with dynamically personalized access to web-based (HTTP) resources. It also gives users access to files and folders from their web browsers on Windows file servers, and to TCP/IP resources through Secure Mobile Access agents that can be provisioned from WorkPlace.

1. Plug in the SafeNet eToken with a valid user certificate.
2. In a web browser, open the SonicWALL Secure Mobile Access Workspace:  
**https://< SonicWALL SRA Appliance Public IP >**
3. In the **Log in to** field, select the configured realm, and then click **Next**.



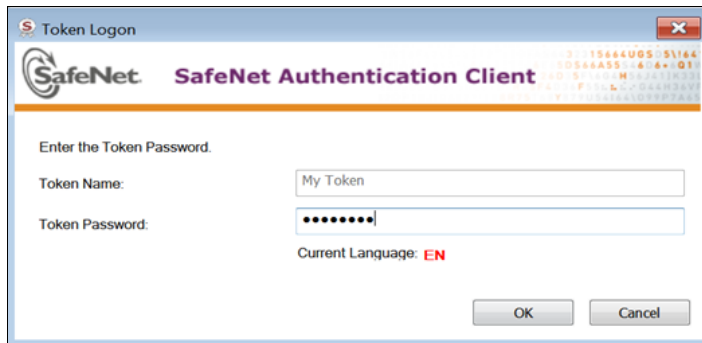
*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*

4. On the **Confirm Certificate** window, select the correct certificate, and then click **OK**.



*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*

5. Use the SafeNet token to generate a passcode, and then enter it in the **Token Password** field. Click **OK** to continue.

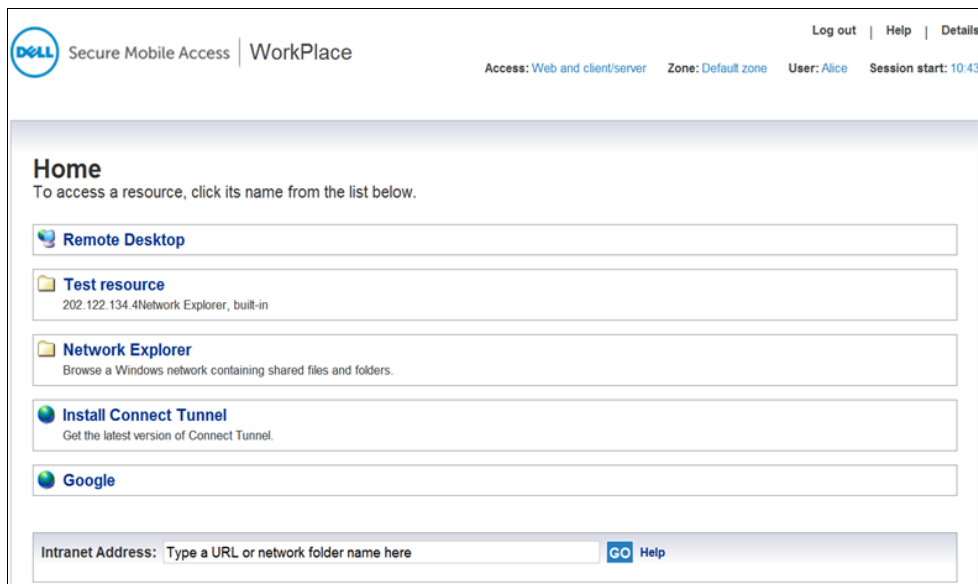


(The screen image above is from Dell®. Trademarks are the property of their respective owners.)



**NOTE:** Allow any Java or security warning that is displayed.

If authentication is successful, the user will be allowed access to the resources configured on WorkPlace.



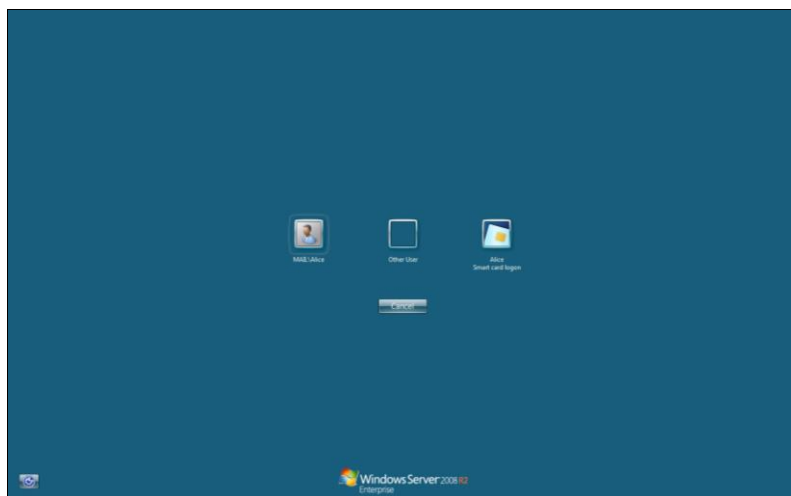
(The screen image above is from Dell®. Trademarks are the property of their respective owners.)



**NOTE:** If you are using SonicWALL for the first time, you will need to install the **Secure Endpoint Manager**. When you are logged in to WorkPlace, you will get an option to install the **Secure Endpoint Manager**. For more information, refer to the SonicWALL documentation.

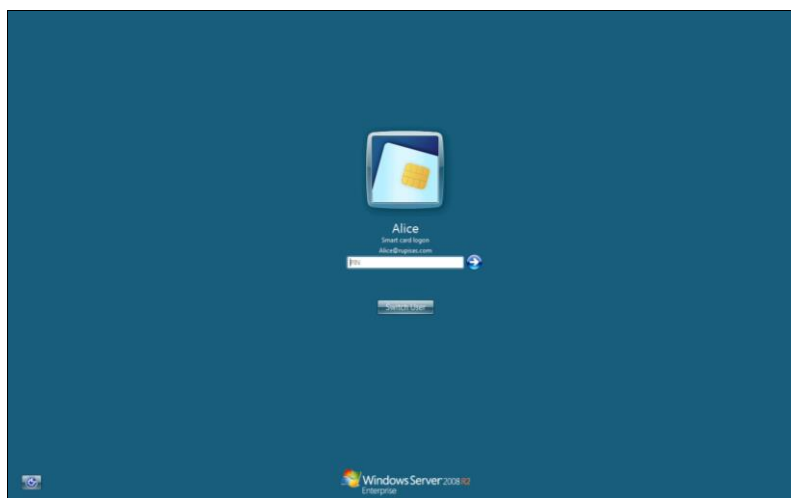
6. On the WorkPlace home window, click **Remote Desktop**.

7. On the **Remote Desktop** window, click **Smart card login**.



*(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)*

8. Enter the eToken password, and then press **Enter**.



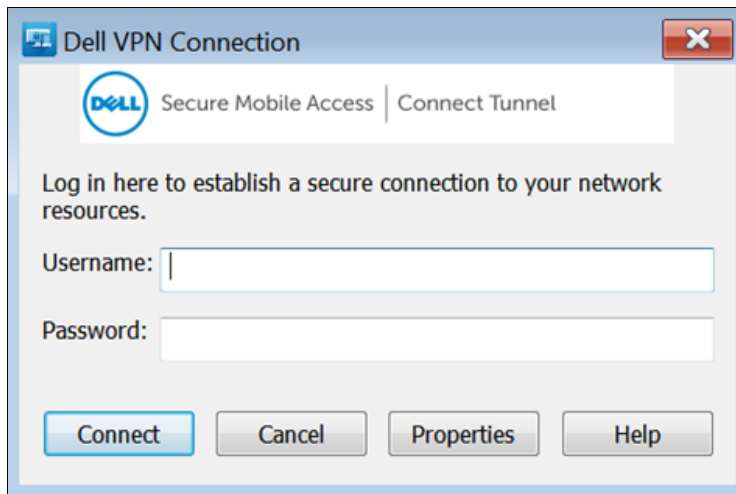
*(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)*

If the credentials are correct, the user will be successfully logged in to the remote session.

## Using the Connect Tunnel Application

The SonicWALL Connect tunnel application allows you to create a VPN connection between your computer and the corporate network for secure data transmission.

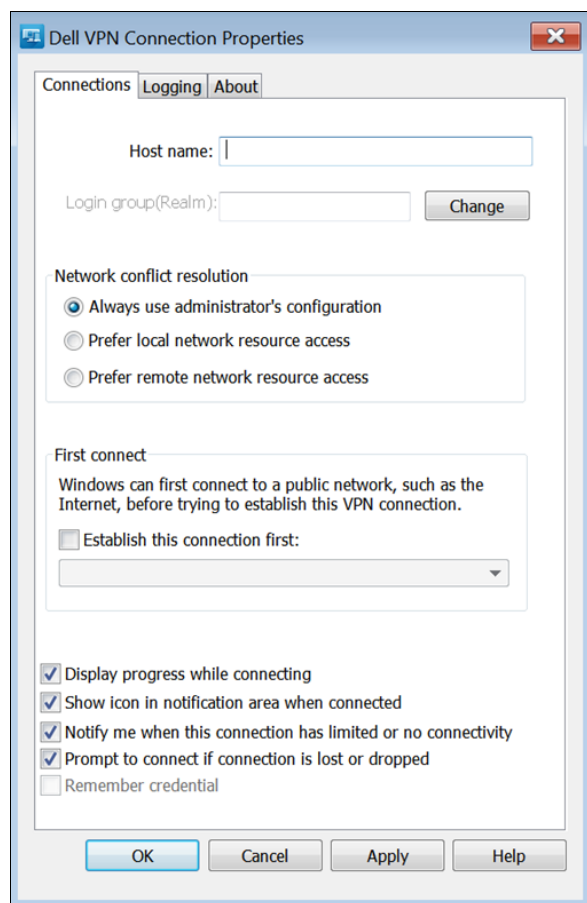
1. Plug in the SafeNet token with a valid user certificate.
2. Start the **Connect Tunnel** application.
3. On the **Dell VPN Connection** window, click **Properties**.



*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*

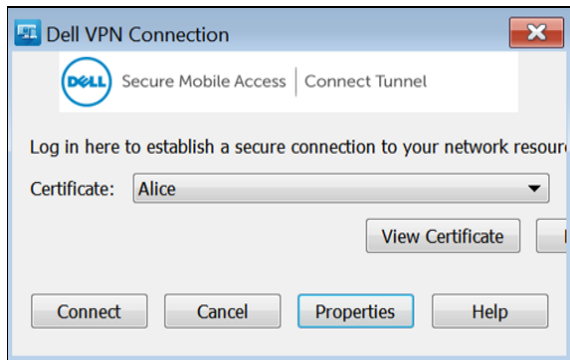
4. On the **Dell VPN Connection Properties** window, on the **Connections** tab, complete the following details, and then click **OK**.

<b>Host name</b>	Enter the public IP address of the SonicWALL Secure Remote Access appliance.
<b>Login group (Realm)</b>	Click <b>Change</b> and then select the realm.



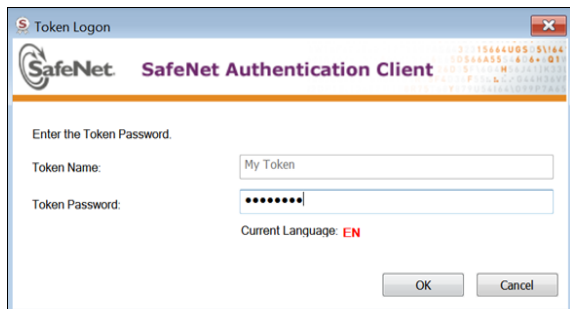
*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*

5. On the **Dell VPN Connection** window, select a certificate in the **Certificate** field, and then click **Connect**.



*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*

6. Use the SafeNet token to generate a passcode, and then enter it in the **Token Password** field. Click **OK** to continue.



If authentication is successful, a VPN connection will be established.

## Appendix: Configuring Remote Desktop

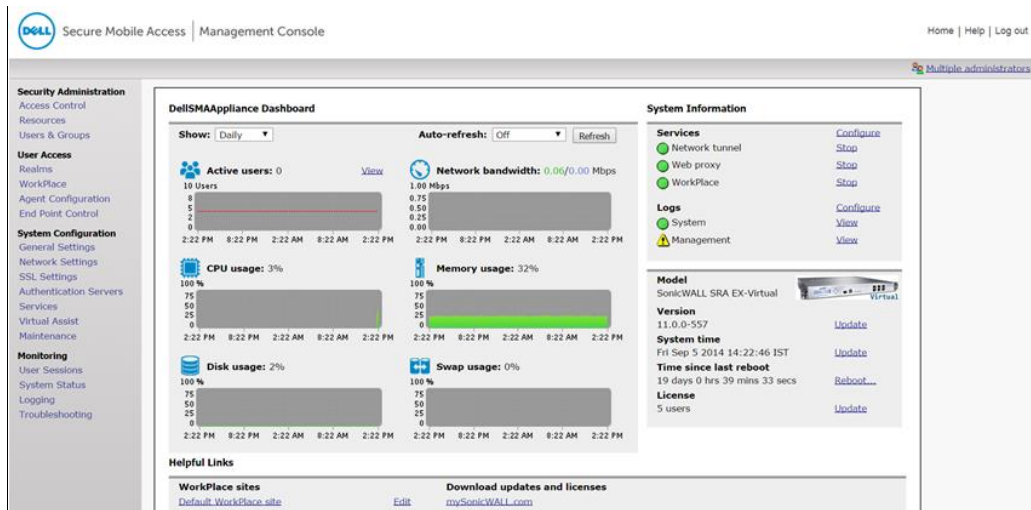
To access a resource after securely connecting to SonicWALL Secure Remote Access, you need to add that resource on the SonicWALL WorkSpace.

In this configuration, you need to:

- Add remote desktop as a resource on the SonicWALL WorkSpace
- Configure remote desktop to allow SafeNet eToken for smart card logon

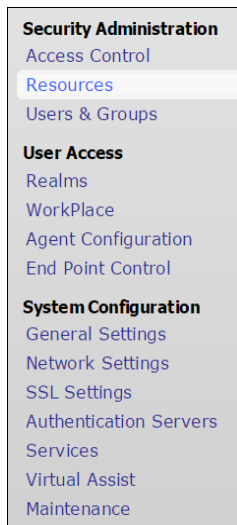
**To add and configure remote desktop:**

1. Open the **SonicWALL Management Console**.



*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*

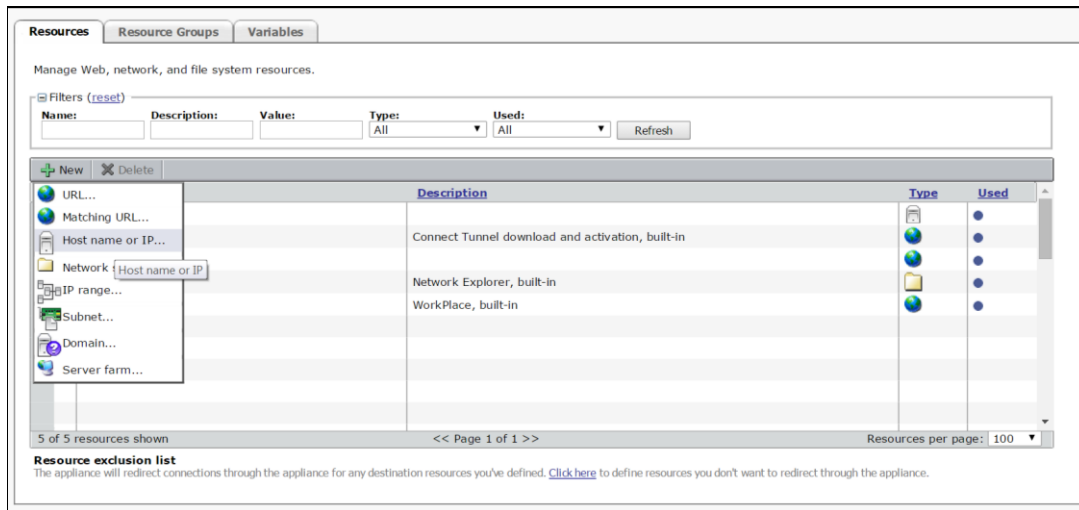
2. On the **SonicWALL Management Console**, in the left pane, under **Security Administration**, click **Resources**.



*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*



- On the **Resources** tab, click **New > Host name or IP**.



(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

- On the **Add Resource** window, complete the following fields, and then click **Save**.

<b>Name</b>	Enter a name for the resource; for example, <b>Remote Desktop</b> .
<b>Host name or IP Address</b>	Enter a host name or IP address of the machine you want to access as a remote desktop.

**Add Resource - Host Name or IP Address**
[Resources > Add Resource](#)

Create or modify a resource.

Name:\*  Description:

Host name or IP address:\*   A host name can include \* and ? wildcard characters.

**Resource group**

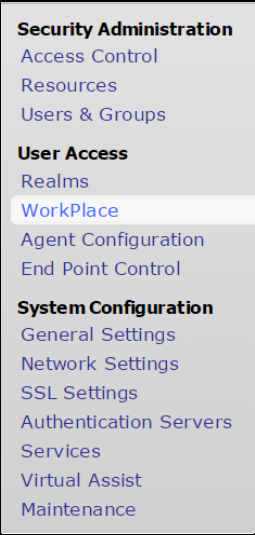
Add this resource to group:  To simplify policy administration, group resources with similar access requirements in Resource Groups.

New group name:

**Advanced**

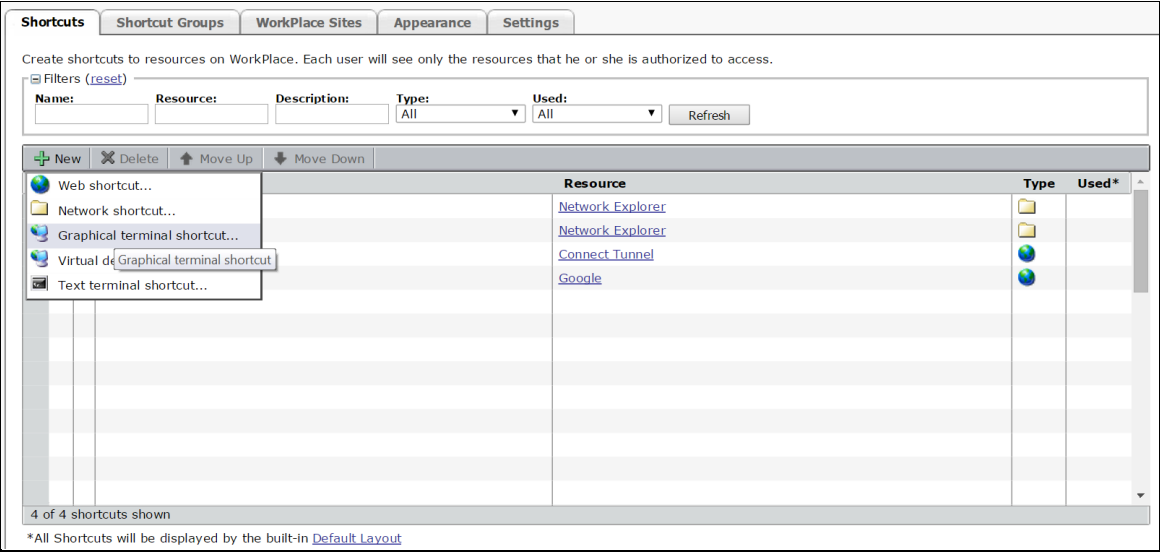
(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

5. On the **SonicWALL Management Console**, in the left pane, under **User Access**, click **WorkPlace**.



(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

6. On the **Shortcuts** tab, click **New > Graphical terminal shortcut**.



(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

7. On **General** tab, complete the following fields, and then click **Finish**.

<b>Position</b>	Select the position at which the shortcut will be displayed on WorkPlace.
<b>Resource</b>	Select the resource created previously; for example, <b>Remote Desktop</b> .
<b>Link text</b>	Enter a name for the resource; for example, <b>Remote Desktop</b> .

**Add Graphical Terminal Shortcut** [WorkPlace Shortcuts > Add Graphical Terminal Shortcut](#)

General | Advanced

Add or edit an WorkPlace link for accessing a Windows Terminal Services or Citrix host.

Position:\*  
1 ▼

Resource:\*  
Remote Desktop ▼

Link text:\*  
 {variable} Type the hyperlink text you want to show to the user.

Description:  
 {variable} The description appears beneath the hyperlink

**Shortcut group**

Add this shortcut to group: Standalone shortcuts ▼ To group shortcuts in the WorkPlace portal, group shortcuts with similar usage requirements in Shortcut Groups.

New group name:

< Back Next > Cancel Finish

(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

8. On the **Shortcuts** tab, click on the link text of the resource; for example **Remote Desktop**.

**Shortcuts** | Shortcut Groups | WorkPlace Sites | Appearance | Settings

Create shortcuts to resources on WorkPlace. Each user will see only the resources that he or she is authorized to access.

Filters (reset)  
Name:  Resource:  Description:  Type: All ▼ Used: All ▼ Refresh

+ New ✕ Delete ↑ Move Up ↓ Move Down

	Link text	Resource	Type	Used*
<input type="checkbox"/>	1 Remote Desktop	Remote Desktop		
<input type="checkbox"/>	2 Test resource	Network Explorer		
<input type="checkbox"/>	3 Network Explorer	Network Explorer		
<input type="checkbox"/>	4 Install Connect Tunnel	Connect Tunnel		
<input type="checkbox"/>	5 Google	Google		

5 of 5 shortcuts shown

\*All Shortcuts will be displayed by the built-in [Default Layout](#)

(The screen image above is from Dell®. Trademarks are the property of their respective owners.)

9. On the **Edit Graphical Terminal Shortcut** window, click the **Advanced** tab.
10. Scroll down to the **Resource redirection** section. Under **Allow access to local**, select **SmartCards**, and then click **Save**.

☐ Use Java client (does not support advanced session options)

☐ Use Browser based RDP client (does not support advanced session options)

**Single sign-on**

☐ None (prompt user)

☒ Forward user's session credentials

Domain:  {variable}

☐ Forward static credentials

Username:  {variable}

Password:  {variable}

Domain:  {variable}

**Resource redirection**

☐ Bring remote audio to local computer

☒ Share clipboard between local and remote computers

Allow access to local:

☐ Drives ☒ SmartCards ☐ Ports

☐ Printers ☐ Plug-and-play devices

**Connection properties** [Edit Graphical Terminal Shortcut](#)

☒ Automatically reconnect if session is interrupted

☐ Connect to admin/console session

☐ Enable Wake-on-LAN (WoL)

MAC/Ethernet address:  {variable}

Wait time for boot-up:  seconds

☐ Send WoL packet to hostname or IP address

*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*

After you have made these configuration changes, you need to apply them in the system. To apply configuration changes, refer to “Applying Configuration Changes” on page 16.

## Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

**Table 1: Support Contacts**

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	<a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a> Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	