RSA SECURID® ACCESS

Standard Agent
Implementation Guide

Dell SonicWALL SRA vpn v8.1

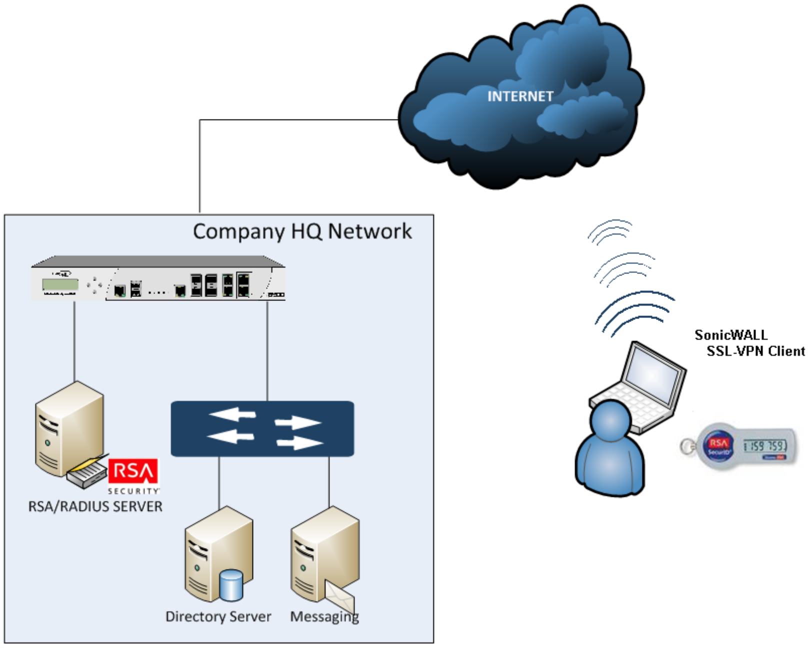
FAL RSA Partner Engineering
Last Modified: 9/23/16

Solution Summary

Dell SonicWALL SRA appliances offer effective solutions for the ever evolving remote access and remote support demands of today's mobile workforce, including remote access, remote support, extranet access, disaster recovery, secure wireless, mobile enterprise, policy enforcement, and network access control. SonicWALL SRA appliances can be configured to communicate with RSA Authentication Manager through the RADIUS protocol. This integration enables strong two factor authentication for users accessing protected resources through the Virtual Private Network (VPN).

Note: For instructions configuring the Dell SonicWALL VPN clients, see the RSA SonicWALL VPN Clients Implementation Guide.

RSA Authentication Manager supported features	
<Partner Product Name and version>	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	No
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
RSA SecurID Authentication via IPv6	No
On-Demand Authentication via Native SecurID UDP Protocol	No
On-Demand Authentication via Native SecurID TCP Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	No
RSA Authentication Manager Replica Support	No
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	Yes


INTERNET
Company HQ Network
RSA SECURITY
RSA/RADIUS SERVER
Directory Server
Messaging
SonicWALL
SSL-VPN Client
RSA SecurID
159 759

RSA Authentication Manager Configuration

Agent Host Configuration

To facilitate communication between the SRA VPN and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the SRA VPN and contains information about communication and encryption.

RSA Authentication Manager 8.2 introduced a new TCP-based authentication protocol and corresponding agent API. RSA Authentication Manager 8.2 and newer also maintains support for the existing UDP-based authentication protocol and agents. The agent host records for TCP and UDP agents are configured similarly, but there are some important differences.

Include the following information when configuring a UDP-based agent host record.

- Hostname
- IP addresses for network interfaces

! > Important: The UDP-based authentication agent's hostname must resolve to the IP address specified.

Include the following information when configuring a TCP-based agent host record.

- RSA agent name (in the hostname field)

! > Important: The RSA agent name is specified in the rsa_api.properties file.

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with SMA SRA VPN will occur.

If SRA VPN will be communicating with RSA Authentication Manager via RADIUS, then a RADIUS client that corresponds to the agent host record must be created in the RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:

- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

! > Important: The RADIUS client's hostname must resolve to the IP address specified.

Please refer to the appropriate RSA documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

Partner Product Configuration

Before You Begin

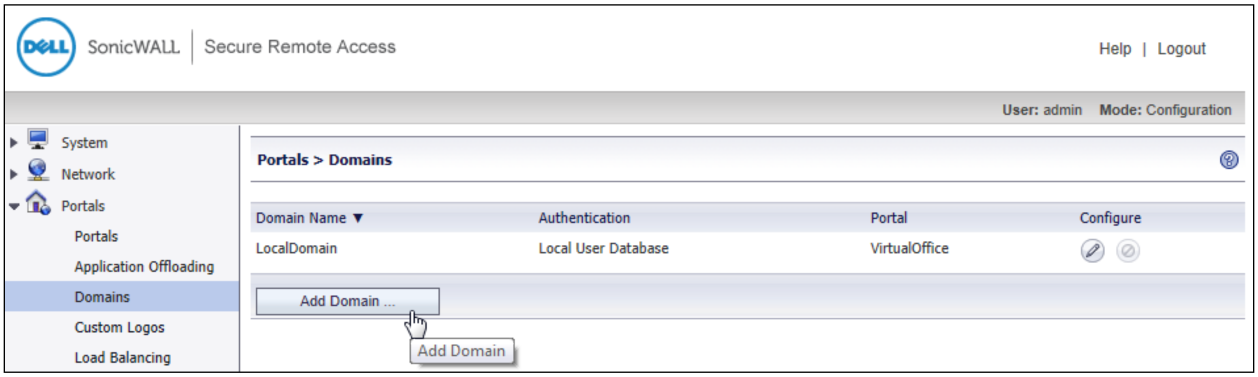
This section provides instructions for configuring the SRA VPN with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All SRA VPN components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

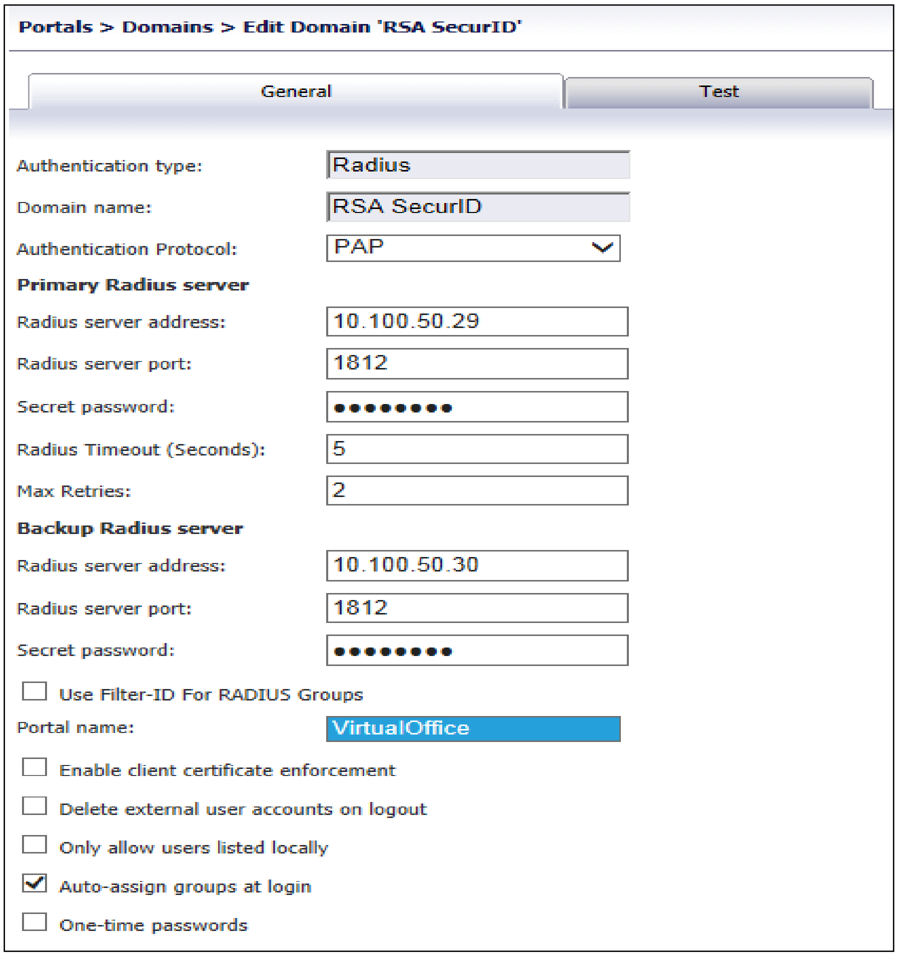
DellSonicWALL SRA VPN Configuration

1. Login to the SonicWALL SRA appliance via web browser; navigate to **Portals > Domains**.



Domain Name ▼	Authentication	Portal	Configure
LocalDomain	Local User Database	VirtualOffice	

2. Click the Add Domain button.



Portals > Domains > Edit Domain 'RSA SecurID'

Authentication type:	Radius
Domain name:	RSA SecurID
Authentication Protocol:	PAP
Primary Radius server	
Radius server address:	10.100.50.29
Radius server port:	1812
Secret password:	●●●●●●●●
Radius Timeout (Seconds):	5
Max Retries:	2
Backup Radius server	
Radius server address:	10.100.50.30
Radius server port:	1812
Secret password:	●●●●●●●●

□ Use Filter-ID For RADIUS Groups

Portal name: VirtualOffice

□ Enable client certificate enforcement

□ Delete external user accounts on logout

□ Only allow users listed locally

☑ Auto-assign groups at login

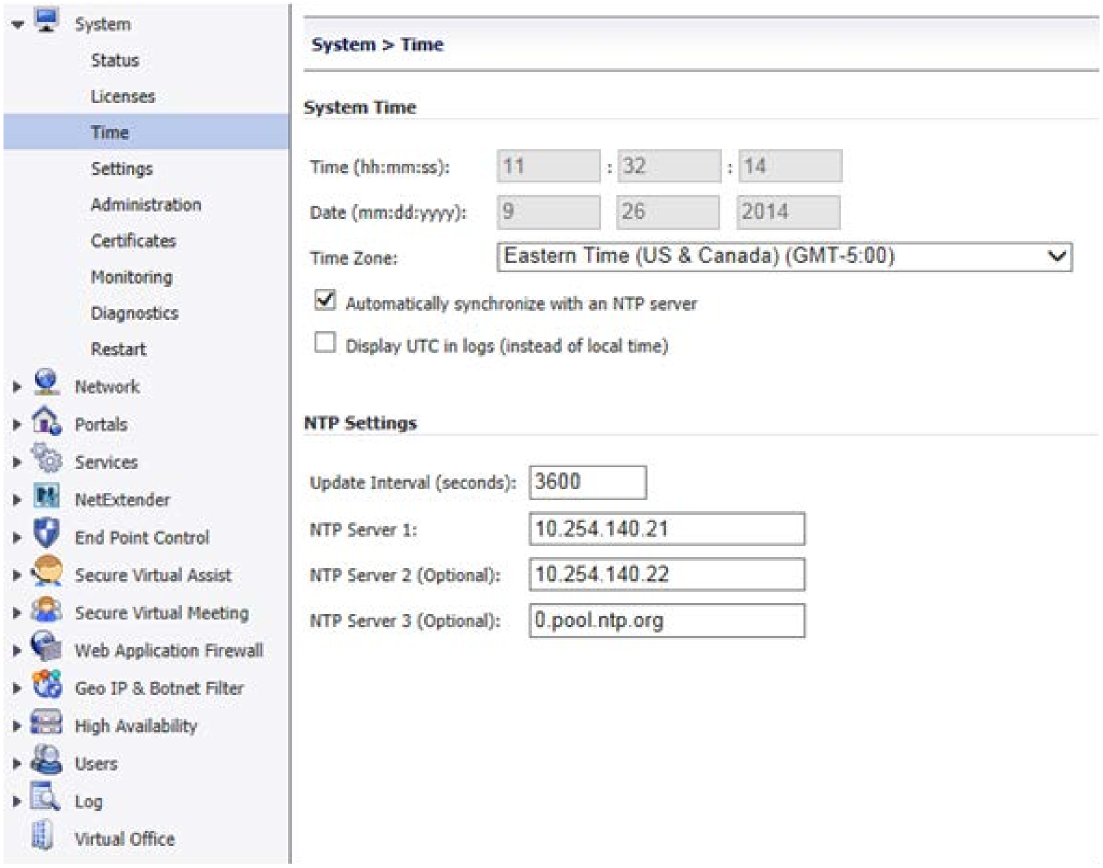
□ One-time passwords

3. In the Authentication type pull-down menu, select Radius.
4. Enter a descriptive name for the authentication domain in the Domain name field (e.g. RSA SecurID). This is the domain name users will select when authenticating to the SonicWALL SRA appliance via SecurID.
5. Enter the IP address of the RADIUS server in the Radius server address field.
6. Enter the RADIUS server port in the Radius server port field.
7. Enter the authentication secret in the Secret password field.

! > Important: The RADIUS secret password entered above must match the Shared Secret for this Radius Client within the RSA Authentication Manager console.

Time Synchronization

RSA SecurID two-factor authentication depends heavily on time synchronization; it is import that the internal clock for the SonicWALL SRA appliance and the RSA Authentication Manager server(s) are set to the correct date and time. On the SonicWALL SRA appliance, navigate to System > Time then adjust the date or time accordingly. To keep the server in-sync, use an NTP server whenever possible.



System > Time

System Time

Time (hh:mm:ss): 11 : 32 : 14

Date (mm:dd:yyyy): 9 26 2014

Time Zone: Eastern Time (US & Canada) (GMT-5:00)

☑ Automatically synchronize with an NTP server

☐ Display UTC in logs (instead of local time)

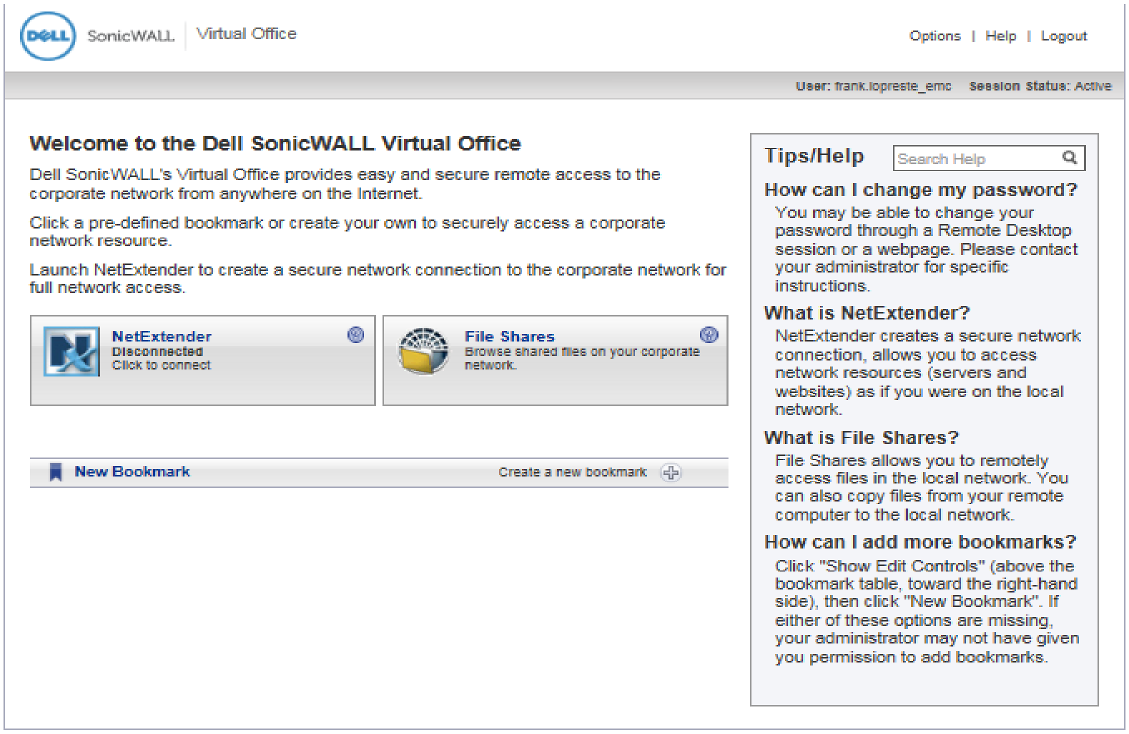
NTP Settings

Update Interval (seconds): 3600

NTP Server 1: 10.254.140.21

NTP Server 2 (Optional): 10.254.140.22

NTP Server 3 (Optional): 0.pool.ntp.org



SonicWALL | Virtual Office
Options | Help | Logout
User: frank.lopreste_emc Session Status: Active

Welcome to the Dell SonicWALL Virtual Office

Dell SonicWALL's Virtual Office provides easy and secure remote access to the corporate network from anywhere on the Internet.

Click a pre-defined bookmark or create your own to securely access a corporate network resource.

Launch NetExtender to create a secure network connection to the corporate network for full network access.

How can I change my password?
You may be able to change your password through a Remote Desktop session or a webpage. Please contact your administrator for specific instructions.

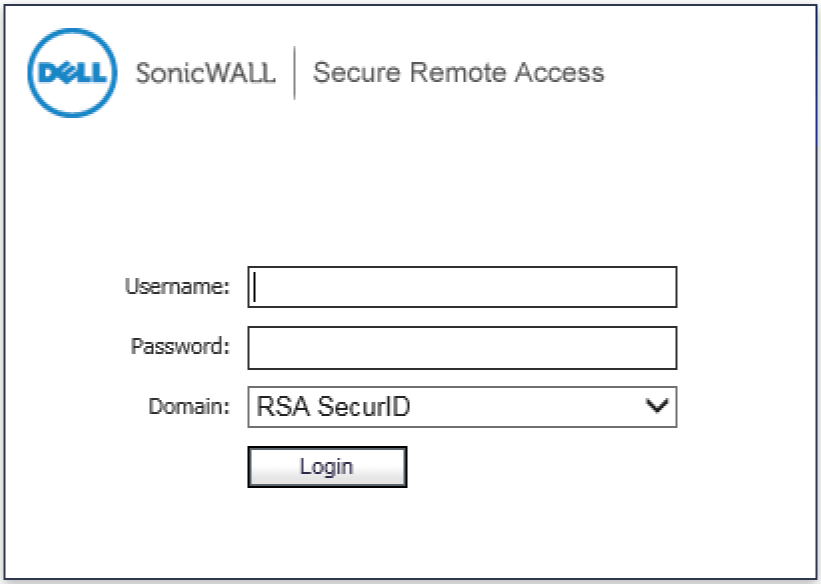
What is NetExtender?
NetExtender creates a secure network connection, allows you to access network resources (servers and websites) as if you were on the local network.

What is File Shares?
File Shares allows you to remotely access files in the local network. You can also copy files from your remote computer to the local network.

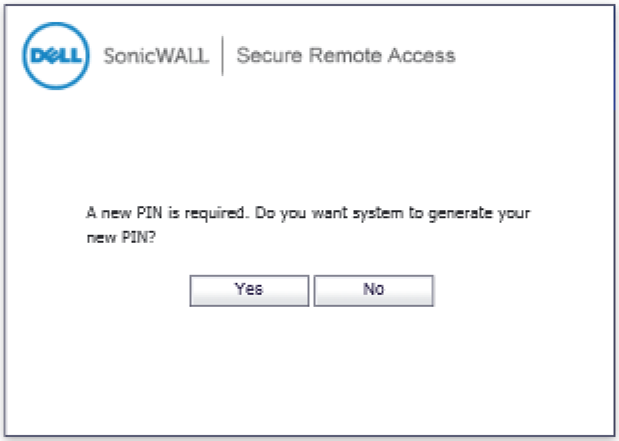
How can I add more bookmarks?
Click "Show Edit Controls" (above the bookmark table, toward the right-hand side), then click "New Bookmark". If either of these options are missing, your administrator may not have given you permission to add bookmarks.

RSA SecurID Login Screens

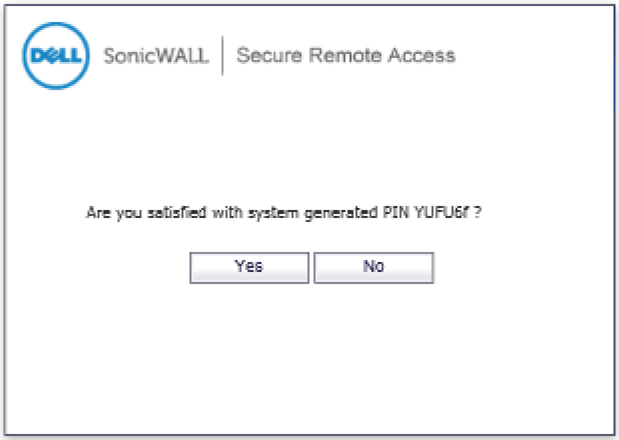
Desktop



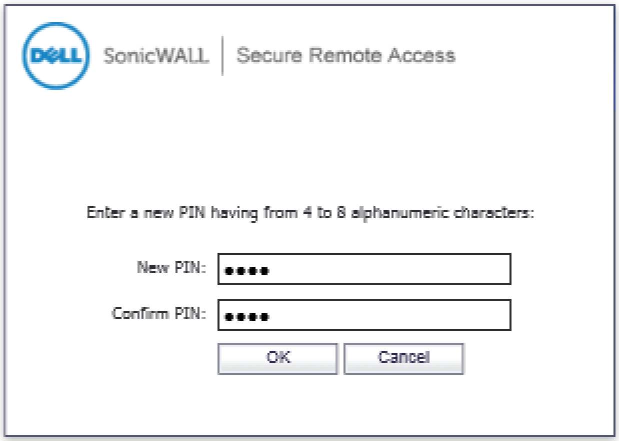
System-generated New PIN:



A new PIN is required. Do you want system to generate your new PIN?



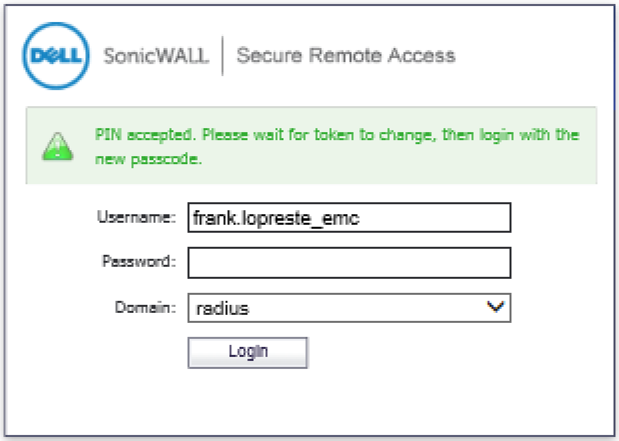
Are you satisfied with system generated PIN YUFU6f ?



Enter a new PIN having from 4 to 8 alphanumeric characters:

New PIN: ●●●●

Confirm PIN: ●●●●

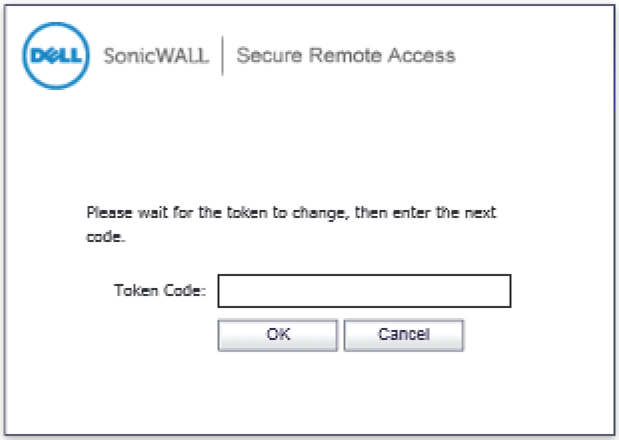


PIN accepted. Please wait for token to change, then login with the new passcode.

Username: frank.lopreste_emc

Password:

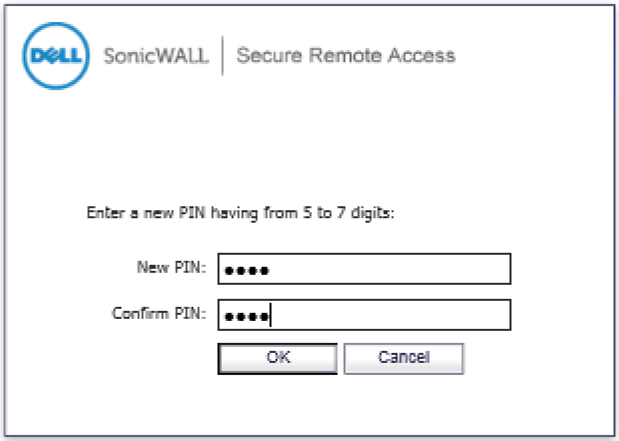
Domain: radius



Please wait for the token to change, then enter the next code.

Token Code:

User-defined New PIN:

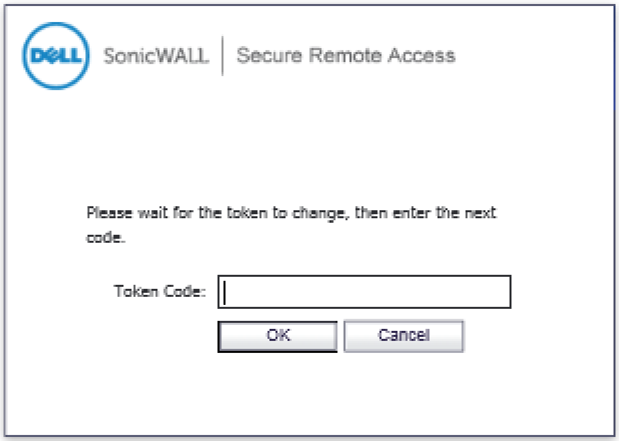


Enter a new PIN having from 5 to 7 digits:

New PIN: ●●●●

Confirm PIN: ●●●●

Next Token Code:



Please wait for the token to change, then enter the next code.

Token Code:

Certification Checklist for RSA SecurID Access

Date Tested: 9/23/16

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.2	Virtual Appliance
RSA Authentication Agent	5.0.3.2	Linux
RSA Software Token	5.0.0	Windows
SRA VPN	8.1	Virtual Appliance

RSA SecurID Authentication

Date Tested: 9/23/16

Mandatory Functionality	Native UDP	Native TCP	RADIUS Client
New PIN Mode			
Force Authentication After New PIN	N/A	N/A	✓
System Generated PIN	N/A	N/A	✓
User Defined (4-8 Alphanumeric)	N/A	N/A	✓
User Defined (5-7 Numeric)	N/A	N/A	✓
Deny 4 and 8 Digit PIN	N/A	N/A	✓
Deny Alphanumeric PIN	N/A	N/A	✓
Deny PIN Reuse	N/A	N/A	✓
Passcode			
16 Digit Passcode	N/A	N/A	✓
4 Digit Fixed Passcode	N/A	N/A	✓
Next Tokencode Mode			✓
Next Tokencode Mode	N/A	N/A	✓
On-Demand Authentication			
On-Demand Authentication	N/A	N/A	✓
On-Demand New PIN	N/A	N/A	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	N/A	✓
No RSA Authentication Manager	N/A	N/A	✓

✓ = Pass ✗ = Fail N/A = Non-Available Function