



RSA SecurID Ready Implementation Guide

Last Modified: August 8th, 2009

Partner Information

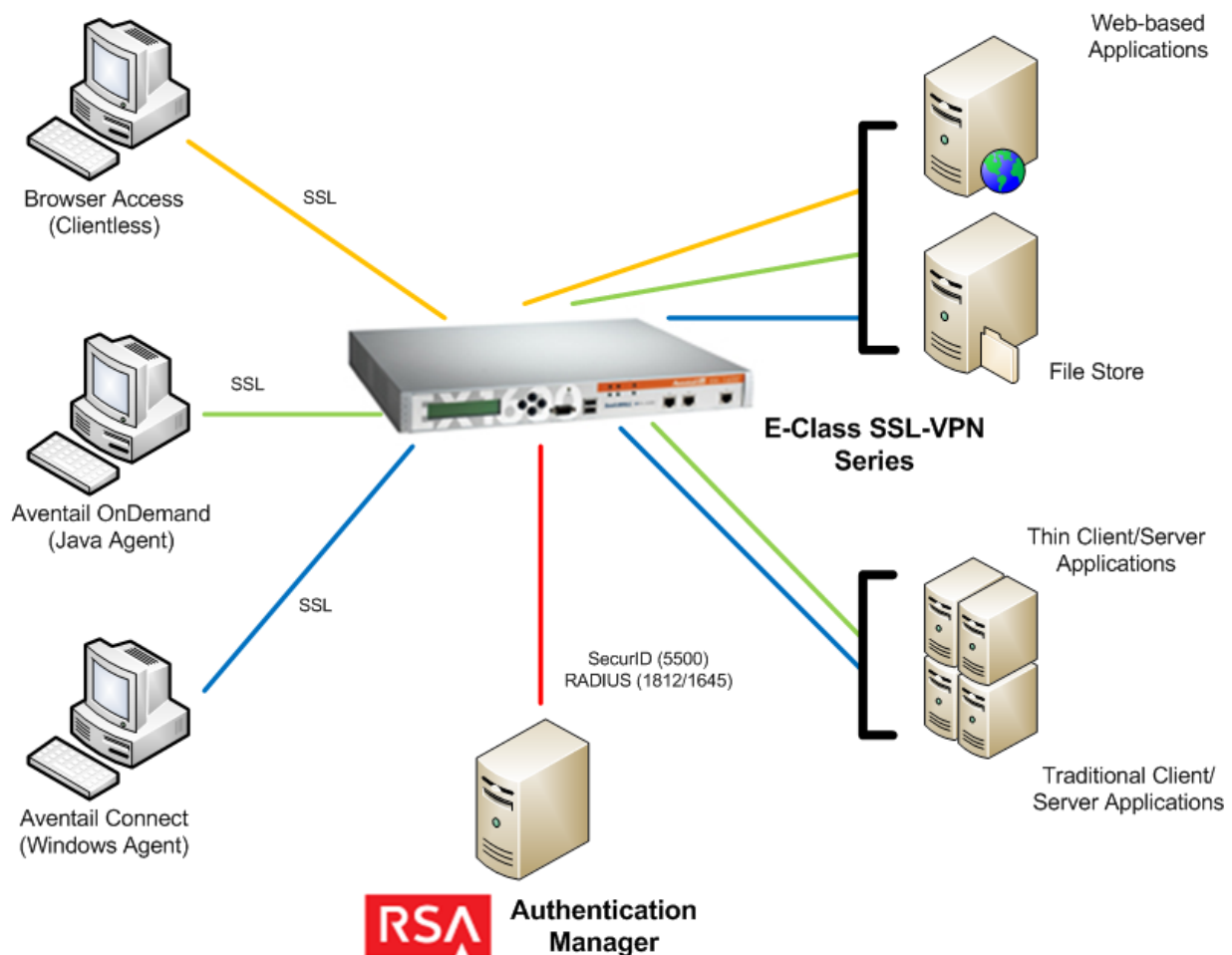
Product Information	
Partner Name	SonicWALL
Web Site	www.sonicwall.com
Product Name	Aventail E-Class SSL-VPN Series
Version & Platform	10.0
Product Description	SonicWALL® Aventail® E-Class Secure Remote Access (SRA) products provide complete application access with full security, control of the end point and unified policy management. Easy to use and control, SonicWALL Aventail E-Class SRAs increase productivity by providing employees and partners with secure, clientless access to the resources they need from any device, anywhere, with unmatched security. SonicWALL Aventail E-Class SRAs also lower total cost of ownership (TCO) by eliminating difficult IPsec VPN deployments and constant support calls.
Product Category	VPNs SSL





Solution Summary

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication, RADIUS
List Library Version Used	5.0.3.2
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	Yes (1)
RSA Authentication Agent Host Type for 6.1	Communication Server
RSA Authentication Agent Host Type for 7.1	Standard Agent
RSA SecurID User Specification	Designated Users, All Users, Default Method
RSA SecurID Protection of Administrative Users	No
RSA Software Token and RSA SecurID 800 Automation	No





Product Requirements

Partner Product Requirements: Aventail E-Class	
Firmware	10.0

Agent Host Configuration

! > Important: “Agent Host” and “Authentication Agent” are synonymous. “Agent Host” is a term used with the RSA Authentication Manager 6.x servers and below. RSA Authentication Manager 7.1 uses the term “Authentication Agent”.

! > Important: All “Authentication Agent” types for 7.1 should be set to “Standard Agent”.

To facilitate communication between the Aventail E-Class SSL-VPN Series 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 Aventail E-Class SSL-VPN Series within its database and contains information about communication and encryption. You will also need to configure a RADIUS client.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces

When adding the Agent Host Record, you should configure the Aventail E-Class SSL-VPN Series as Standard Agent. This setting is used by the RSA Authentication Manager to determine how communication with the Aventail E-Class SSL-VPN Series will occur.

To create the RADIUS client record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces
- RADIUS Secret

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host, and RADIUS client records.



RSA SecurID files

RSA SecurID Authentication Files	
Files	Location
sdconf.rec	In Memory
Node Secret	In Memory
sdstatus.12	In Memory
sdopts.rec	Not implemented

 **Note:** Go to the appendix of this document to get detailed information regarding these files.

Partner Product Configuration

Before You Begin

This section provides instructions for integrating the partners' product 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 vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Documenting the Solution

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

Interoperability between RSA Authentication Manager and the Aventail E-Class SSL-VPN Series is achieved by authenticating to the RSA Authentication Manager via either the SecurID Native or RADIUS protocol.

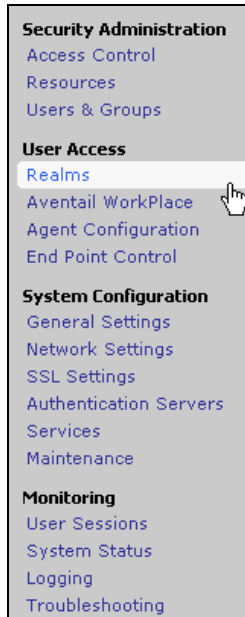
This guide assumes you've successfully installed and configured the Aventail E-Class SSL-VPN Series by running the Aventail Setup Tool and have access to the Aventail Management Console (AMC). Please refer to the appropriate administration guides for detailed instructions. It's recommended that users be configured to authenticate via the Aventail E-Class SSL-VPN Series local password to ensure resources can be served up before configuring for SecurID.

Once the Aventail E-Class SSL-VPN Series is configured, you can then enable authentication via either the SecurID Native or RADIUS protocol.

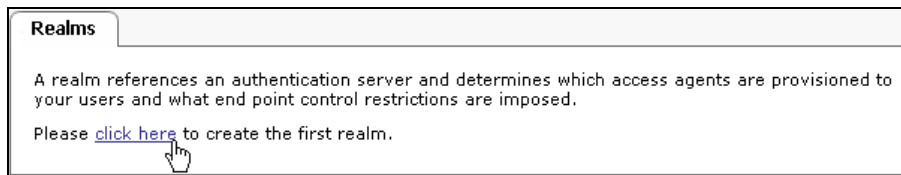


Configure Native SecurID Authentication

1. From the Management Console under **User Access** select the hyperlink for **Realms**.



2. Select **click here** under **Realms** to create a default realm.



3. Input a **Name** for the realm and add a description (**Optional**).
4. Click **New** next to the field titled **Authentication Server** to create a server configuration.

Configure Realm [Realms > Configure Realm](#)

General | Communities

Configure the general settings for the realm.

Name:* Description: Your users will select or type the realm Name during login. Choose a name that clearly describes the user community.

Status: Enabled Disabled

Display this realm Hiding a realm removes its name from the list on the login page, and requires the user to type the realm name.

Authentication server:

Enable RADIUS accounting

Advanced



5. Select the radio button for **RSA ACE** under the **Authentication Server** section and **Token/SecurID** under the **Credential type** section.
6. Select **Continue...**

New Authentication Server [Authentication Servers > New Authentication Server](#)

Choose the protocol used to access your user store, and specify how users will authenticate. Click **Continue** to configure the authentication server.

User store

Choose the directory type or authentication method:

Authentication directory

- Microsoft Active Directory A single domain.
- Microsoft Active Directory Tree A single root domain and all child domains.
- LDAP
- RADIUS
- RSA ACE**
- Public key infrastructure (PKI)

Single sign-on server

- RSA ClearTrust Sign-on to ClearTrust is supported only from a Web browser.

Local user storage

- Local users The local user store is not intended for use in a production environment.

Credential type

Specify how users will authenticate:

- Digital certificate
- Token/SecurID**
- Username/Password

7. For configuring the **RSA ACE** server, enter the information for:
 - Name
 - RSA ACE configuration file
- Click **Save** to continue.

Configure Authentication Server [Authentication Servers > Configure Authentication Server](#)

Configure authentication settings for an RSA ACE server.

Credential type: Token/SecurID

Name:*

RSA ACE configuration file:* The configuration file, sdconf.rec, can be downloaded from your RSA ACE server.



- To complete the addition of the new Authentication Realm, click the **Finish** button.

Configure Realm [Realms > Configure Realm](#)

General | Communities

Configure the general settings for the realm.

Name:* Description: Your users will select or type the realm Name during login. Choose a name that clearly describes the user community.

Status: Enabled Disabled

Display this realm

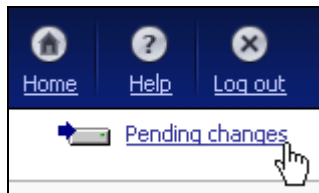
Hiding a realm removes its name from the list on the login page, and requires the user to type the realm name.

Authentication server:

Enable RADIUS accounting

Advanced

- Click on **pending changes** in the upper right hand corner. When the dialog box appears, click **Apply Changes**.



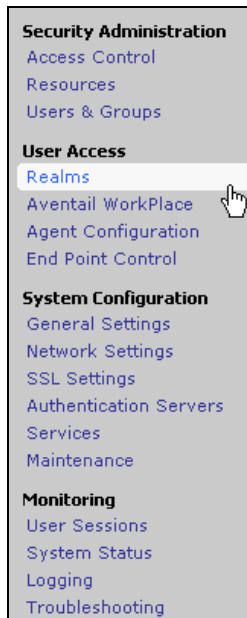
Apply Pending Changes

Apply or discard pending configuration changes. Depending on your configuration, applying changes may take a few minutes to restart services.

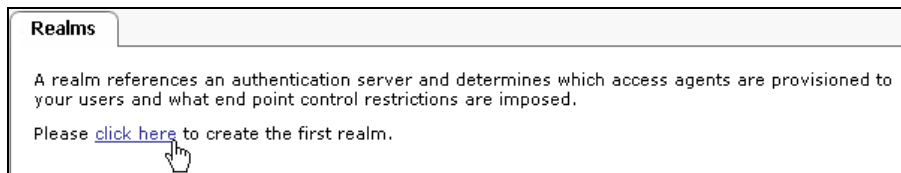


Configure RADIUS SecurID Authentication

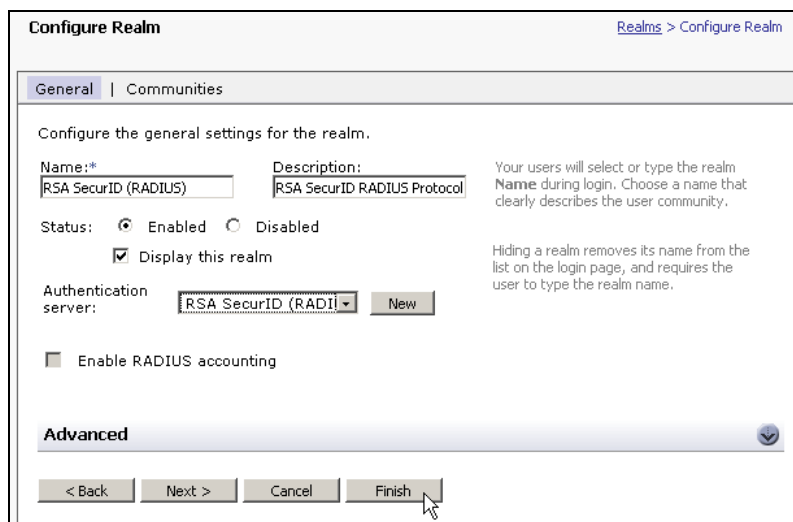
1. From the Management Console select under **User Access** the hyperlink for **Realms**.



2. Select **click here** under **Realms** to create a default realm.



3. Input a **Name** for the realm and add a description (**Optional**).
4. Click **New** next to the field titled **Authentication Server** to create a server configuration.





5. Select the radio button for **RADIUS** under the **Authentication directory** section and **Token/SecurID** under the **Credential type** section.

New Authentication Server [Authentication Servers > New Authentication Server](#)

Choose the protocol used to access your user store, and specify how users will authenticate. Click **Continue** to configure the authentication server.

User store

Choose the directory type or authentication method:

Authentication directory

- Microsoft Active Directory A single domain.
- Microsoft Active Directory Tree A single root domain and all child domains.
- LDAP
- RADIUS**
- RSA ACE The appliance supports one RSA ACE authentication server.
- Public key infrastructure (PKI)

Single sign-on server

- RSA ClearTrust Sign-on to ClearTrust is supported only from a Web browser.

Local user storage

- Local users The local user store is not intended for use in a production environment.

Credential type

Specify how users will authenticate:

- Digital certificate
- Token/SecurID**
- Username/Password

6. Select **Continue...**
7. For configuring the RADIUS server, enter the information for:
 - Primary RADIUS Server
 - Secondary RADIUS Server (**Optional**)
 - Shared Secret

(Optional) Click on the **circular image** of the arrow to expand the **Advanced** options. Under the **Advanced** options input:

- Check the box for **Customize authentication server prompts** and change the proof box contents from **Password:** to **Passcode:**.

Custom prompts

Use this area to change the prompts and other text on the login page.

Customize authentication server prompts

Title:

Message:

Identity: Proof:



Click the button labeled **Save** to continue.

Configure Authentication Server [Authentication Servers > Configure Authentication Server](#)

Configure authentication settings for a RADIUS server.

Credential type: Token/SecurID

Name:*

General

Primary RADIUS server:*

Secondary RADIUS server:

Shared secret: *

Match RADIUS groups by:

Retry interval:
 seconds

Advanced

8. To complete the addition of the new Authentication Realm, click the **Finish** button.

Configure Realm [Realms > Configure Realm](#)

General | Communities

Configure the general settings for the realm.

Name:* Description: Your users will select or type the realm Name during login. Choose a name that clearly describes the user community.

Status: Enabled Disabled
 Display this realm

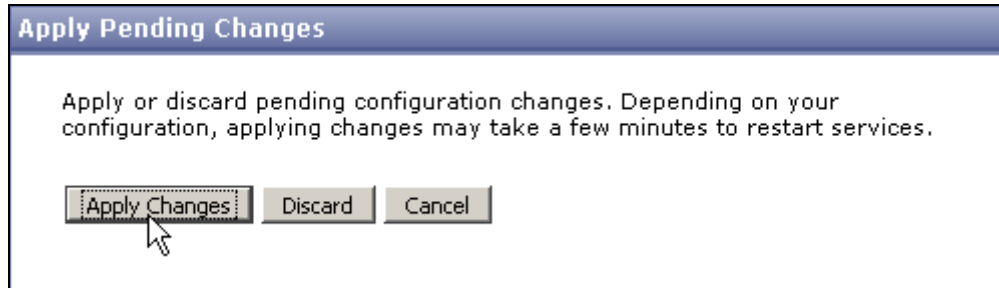
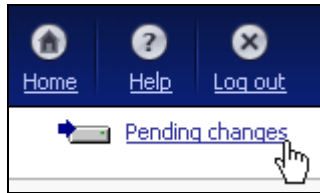
Authentication server:

Enable RADIUS accounting

Advanced



9. Click on **pending changes** in the upper right hand corner. When the dialog box appears, click **Apply Changes**.





End-user Experience

Access the Aventail E-Class SSL VPN Series via a web browser. If multiple **Realms** exist, the user will have to select which to use.

The screenshot shows the top of the login page with the 'Aventail' logo and 'Aventail WorkPlace' title. Below the title is a blue bar with the text 'Please log in'. Underneath, there is a 'Log in to:' label followed by a dropdown menu. The dropdown menu is open, showing three options: 'RSA SecurID (Native)', 'RSA SecurID (Native)', and 'RSA SecurID (RADIUS)'. A mouse cursor is pointing at the 'RSA SecurID (RADIUS)' option.

Enter a **Username** and insert a **PASSCODE**, then select the button titled **Log in**.

The screenshot shows the full login page. It includes the 'Aventail' logo and 'Aventail WorkPlace' title. Below the title is a blue bar with the text 'Please log in'. Underneath, there is a message: 'Log in here to establish a secure connection to your network resources.' Below this message, there is a 'Log in to:' label followed by the text 'RSA SecurID (Native)'. There are two input fields: 'Username:' with the text 'user' and 'Passcode:' with five dots. Below the input fields is a blue button labeled 'Log in' with a mouse cursor pointing at it.

Certification Checklist for RSA Authentication Manager v6.x

Date Tested: 04/02/2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1.3	Windows Server 2003
SonicWALL Aventail SSL-VPN Series	10.0.1-080	Embedded OS

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
Passcode			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input checked="" type="checkbox"/>
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
RSA SecurID 800 Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
Credential Functionality			
Determine Cached Credential State	<input type="checkbox"/> N/A	Determine Cached Credential State	<input type="checkbox"/>
Set Credential	<input type="checkbox"/> N/A	Set Credential	<input type="checkbox"/>
Retrieve Credential	<input type="checkbox"/> N/A	Retrieve Credential	<input type="checkbox"/>

BSD / PAR

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

Certification Checklist for RSA Authentication Manager 7.x

Date Tested: 04/03/2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows Server 2003
SonicWALL Aventail SSL-VPN Series	10.0.1-080	Embedded OS

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
Deny Numeric PIN	<input checked="" type="checkbox"/>	Deny Numeric PIN	<input checked="" type="checkbox"/>
PIN Reuse	<input checked="" type="checkbox"/>	PIN Reuse	<input checked="" type="checkbox"/>
Passcode			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input checked="" type="checkbox"/>
4 Digit Fixed Passcode	<input checked="" type="checkbox"/>	4 Digit Fixed Passcode	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
RSA SecurID 800 Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A

BSD / PAR

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



Known Issues

User Selectable PIN and SecurID Native Protocol

If a user is in new PIN mode and the PIN is set to User Selectable when the device is configured for SecurID Native protocol, the prompt is incorrectly presented to the user that they must create a new PIN. If the user at this point selects cancel, the system generated PIN will then be presented to the user and authentication continues normally.

First Authentication Failure and SecurID Native Protocol

When the device has first been configured to use SecurID Native protocol for authentication, if the first attempt is a failure, the device may not try to authenticate against Authentication Manager again. To correct this behavior, the device may be power-cycled, it will then make requests to the Authentication Manager server. After a successful authentication has occurred, the device will continue to operate normally when failed authentication happens.



Appendix

Node Secret:

This file is stored on the device; it can be reset by deleting the Authentication Server from the device configuration under **System Configuration > Authentication Servers**.

sdconf.rec

This file is stored on the device; it can be reset by deleting the Authentication Server from the device configuration under **System Configuration > Authentication Servers**.

sdopts.rec:

This option has not been implemented.

sdstatus.12:

This file is stored on the device; it can be reset by deleting the Authentication Server from the device configuration under **System Configuration > Authentication Servers**.