



RSA SecurID Ready Implementation Guide

Last Modified: March 27, 2008

Partner Information

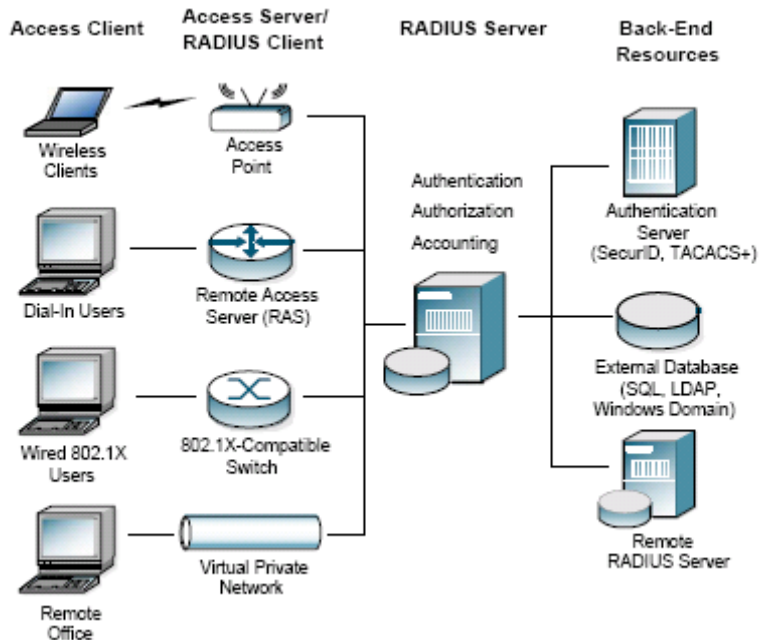
Product Information	
Partner Name	Juniper Networks
Web Site	www.juniper.net
Product Name	Steel Belted RADIUS
Version & Platform	6.10 4280
Product Description	Steel-Belted Radius is a complete implementation of the widely used IETF standards-track RADIUS (Remote Authentication Dial-In User Service) protocols. It acts as a security gateway to your LAN that authenticates, authorizes and accounts for all remote and wireless LAN access. It interfaces with a wide variety of network access servers, including Wireless Access Points, VPN and Dial-in servers and easily authenticates remote and WLAN users against your existing security infrastructure.
Product Category	RADIUS server





Solution Summary

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID
List Library Version Used	5.0.3
RSA Authentication Manager Name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	N/A
Location of Node Secret on Agent	In Registry
RSA Authentication Agent Host Type	Net OS (Windows), UNIX (*nix)
RSA SecurID User Specification	Designated Users, All Users, Default Method
RSA SecurID Protection of Administrative Users	No
RSA Software Token and SD800 Automation	No
Use of Cached Domain Credentials	No





Product Requirements

Minimum software and patch requirements used in this certification include the following:

Partner Product Requirements: Array SPX Series	
Version	
Steel Belted RADIUS	V6.10 or newer
Memory	256MB (512 for servers with 10,000+ users)
Storage	Different per Operating System
Partner Product Requirements: SBR Administrator	
Memory	256MB
Storage	Different per Operating System
Application	Additional Patches
Internet Explorer 7.0, FireFox 1.0.8	All Patch Levels Supported

Agent Host Configuration

To facilitate communication between the Steel Belted RADIUS (SBR) server 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 SBR server within its database and contains information about communication and encryption.

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 SBR Server with the appropriate Agent Host type as documented prior in the Solution Summary section. This setting is used by the RSA Authentication Manager to determine how communication with the SBR server will occur.

 **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 records.



Partner Authentication Agent 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.

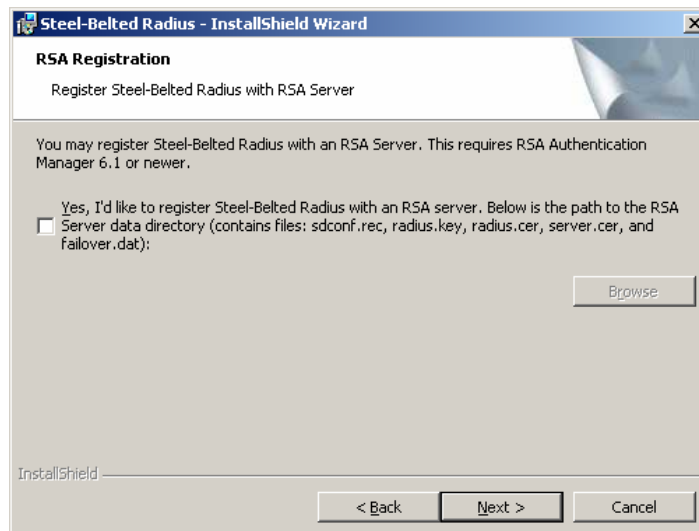
All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Documenting the Solution

Steel Belted RADIUS installation

During the install of Steel Belted RADIUS, you are prompted with the dialogue window below that will add the Steel Belted RADIUS server as a 'RADIUS Server' host type within an RSA Authentication Manager 6.1 or above. There are four files that will need to be selected to register. The following files are located on the Authentication Manager server in the default directory **C:\Program Files\RSA Security\RSA Authentication Manager\data**

- **sdconf.rec**
- **radius.key**
- **radius.cer**
- **server.cer**



If you have configured SBR as an Agent Host during the install as documented above in the 'Agent Host Configuration' section, the process is complete and you can skip to Step 1 of the **RSA SecurID Agent Configuration**. If this has not been performed, please continue to step 3.



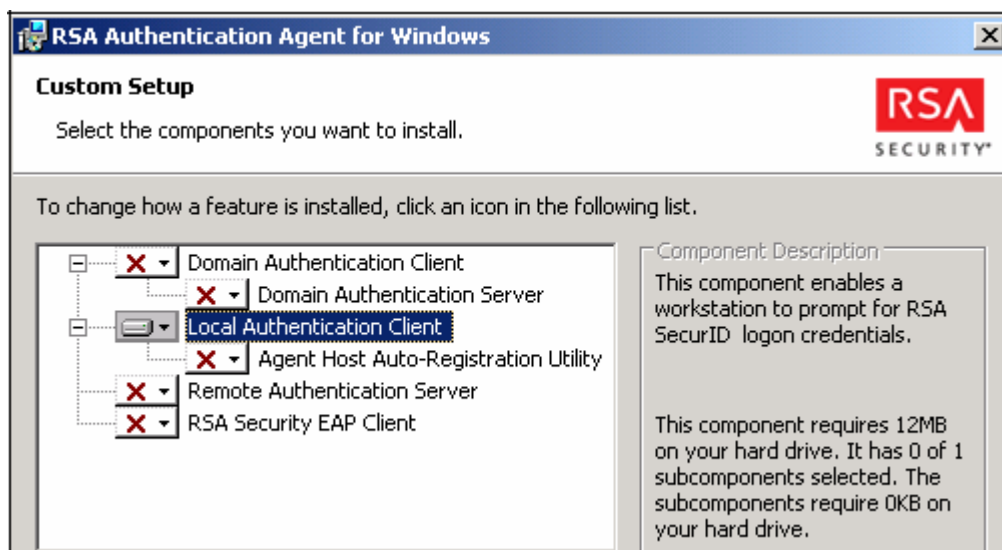
To configure a Steel Belted Radius server to work with an RSA Authentication Manager, the following steps must be performed.

1. Copy the sdconf.rec file from the RSA Authentication Manager to the proper location on the SBR server.
 - *Windows:* %root%\system32
 - *Unix:* the directory that contains the radius daemon on the Steel-Belted RADIUS server.

Note: If you copy the file after the Steel Belted Radius service, or daemon, has been started, you must stop and start Steel Belted Radius before SecurID will work.

RSA SecurID Agent Configuration

1. Install the RSA Authentication Agent on the Steel Belted RADIUS server and select the following options:
 - In **Setup Type**, select **Custom**
 - In **Custom Setup**, select **Local Authentication Client** only. All other client options should not be installed.

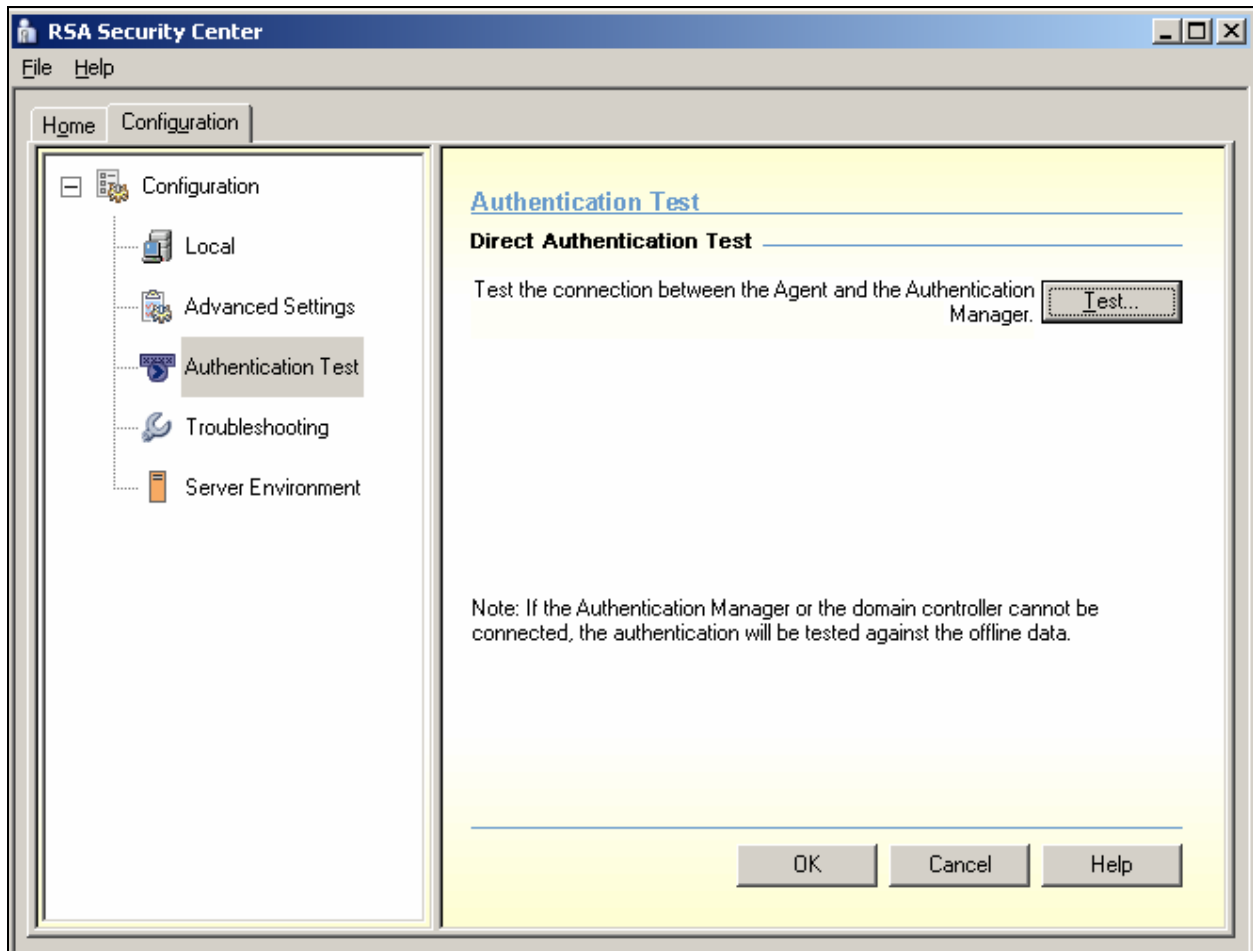


2. Following the remaining onscreen instructions and restart the Steel Belted RADIUS server.



Test RSA SecurID authentication

1. On the SBR server, Click **Start > Control Panel>RSA Security Center**.



3. From the Configuration Tab, click **Authentication Test**.
4. From the Authentication Test / Direct Authentication Test frame, click the Test button and enter the user ID and token PASSCODE for the user you are testing.
5. If the test is successful, continue on the next section of this document.



Configuring RADIUS Clients

1. Login into Steel Belted RADIUS and select **RADIUS Clients** from the left pane.
2. Configure your **RADIUS Clients** (IE: Network Access Devices, etc) making sure the **Shared Secrets** match with what is configured on your Network Access Devices. For purposes of this document, **<ANY>** was chosen.

The screenshot displays the Steel-Belted Radius Global Enterprise Edition (VM2179) web interface. The left sidebar shows a tree view with 'RADIUS Clients' selected. The main area shows a table with columns for Name, Description, IP Address, and Make or Model. A dialog box titled 'Edit RADIUS Client' is open, showing the configuration for a client named '<ANY>'. The 'Name' field is set to '<ANY>', and the 'Make or model' dropdown is set to '- Standard Radius -'. The 'Shared Secret' field is masked with asterisks. The 'Attribute Combination' section has 'Merge' selected under 'Merge Precedence'. The 'Advanced' section has 'Use different shared secret for Accounting' and 'Assume down if no keepalive packets after' options.

Name	Description	IP Address	Make or Model
<ANY>			- Standard Radius -

Edit RADIUS Client

Name: <ANY>

Description:

IP Address:

Range:

Shared Secret: ***** [Validate] [Unmask]

Make or model: - Standard Radius -

Address pool: [View]

Location Group: [View]

Profiles:

Use Profile: [View]

Attribute Combination:

Merge Precedence:

Merge User RADIUS Client

Override

Advanced:

Use different shared secret for Accounting [Edit...]

Assume down if no keepalive packets after [] seconds

[OK] [Cancel]

Certification Checklist

Date Tested: March 14, 2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1.2 (148)	Windows 2003, SP1
RSA Authentication Agent	6.1.1	Windows 2003, SP1
Steel-Belted RADIUS server	6.10 4280 (Standalone)	Windows 2003, SP1
Steel-Belted RADIUS Administrator	6.10 4280	Windows 2003, SP1

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 type="checkbox"/> N/A
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input type="checkbox"/> N/A
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input type="checkbox"/> N/A
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input type="checkbox"/> N/A
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input type="checkbox"/> N/A
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input type="checkbox"/> N/A
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input type="checkbox"/> N/A
PASSCODE			
16 Digit PASSCODE	<input checked="" type="checkbox"/>	16 Digit PASSCODE	<input type="checkbox"/> N/A
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<input type="checkbox"/> N/A
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/> N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input type="checkbox"/> N/A
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 type="checkbox"/> N/A
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 SD800 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
Domain Credential Functionality			
Determine Cached Credential State	<input type="checkbox"/> N/A	Determine Cached Credential State	<input type="checkbox"/>
Set Domain Credential	<input type="checkbox"/> N/A	Set Domain Credential	<input type="checkbox"/>
Retrieve Domain Credential	<input type="checkbox"/> N/A	Retrieve Domain Credential	<input type="checkbox"/>

CMY

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



Certification Checklist For RSA Authentication Manager 7.x

Date Tested: March 27, 2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows 2003, SP1
RSA Authentication Agent	6.1.1	Windows 2003, SP1
Juniper Steal Belted RADIUS	6.10.4280	Windows 2003, SP1

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 type="checkbox"/> N/A
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input type="checkbox"/> N/A
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input type="checkbox"/> N/A
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input type="checkbox"/> N/A
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input type="checkbox"/> N/A
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input type="checkbox"/> N/A
Deny Numeric PIN	<input checked="" type="checkbox"/>	Deny Numeric PIN	<input type="checkbox"/> N/A
PIN Reuse	<input checked="" type="checkbox"/>	PIN Reuse	<input type="checkbox"/> N/A
Passcode			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input type="checkbox"/> N/A
4 Digit Fixed Passcode	<input checked="" type="checkbox"/>	4 Digit Fixed Passcode	<input type="checkbox"/> N/A
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/> N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input type="checkbox"/> N/A
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input type="checkbox"/> N/A
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
PIN Expiration	<input type="checkbox"/> N/A	PIN Expiration	<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
PIN Expiration	<input type="checkbox"/> N/A	PIN Expiration	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A

SWA

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



Known Issues

As of the release of Steel-Belted RADIUS 5.3, a new authentication method was introduced that does NOT require that the SBR server have an entry with the username/suffix/prefix of the user to be SecurID authenticated. Below is an excerpt from a SBR log that outlines the steps SBR uses to authenticate users:

SBR first checks for a Native user:

02/24/2006 09:13:10 Authenticating user KRENNIE with authentication method Native User

Then a SecurID specific user:

02/24/2006 09:13:10 Authenticating user krennie with authentication method SecurID User

Then for a prefix

02/24/2006 09:13:10 Authenticating user krennie with authentication method SecurID Prefix

Then a suffix

02/24/2006 09:13:10 Authenticating user krennie with authentication method SecurID Suffix

SBR then falls to the SecurID authentication method, which is managed completely via the RSA authentication manager, with no entries required on the SBR server.

02/24/2006 09:13:10 Authenticating user krennie with authentication method SecurID

02/24/2006 09:13:10 Performing SecurID user authentication for DEFAULT

(krennie)

02/24/2006 09:13:14 SecurID profile DEFAULT for user krennie success

As you can see the user also received the Default profile for any user being authenticated via the RSA auth manager.



Appendix

ISDN users:

Edit the [SecurID] section of radius.ini. This initialization file is found in the same directory as the Steel-Belted Radius service (for Windows, usually C:\RADIUS\Service) or daemon (for Unix). Ensure that the CachePasscodes field is set to yes and the SecondsToCachePasscodes field is set to an appropriate number of seconds. These settings ensure that authenticated SecurID users will be able to open a second B-channel during an ISDN connection:

```
[SecurID]
CachePasscodes      = yes
SecondsToCachePasscodes = 60
```

EAP Generic Token users:

Edit the [SecurID] section of the eap.ini file. This initialization file is found in the same directory as the Steel-Belted Radius service (for Windows, usually C:\RADIUS\Service) or daemon (for Unix). Ensure the EAP settings in this section are enabled (remove semi-colon character from the front of each line) if you plan to use SecurID authentication with EAP Generic-Token protocol support. The client system must support this protocol as well for this combination to work:

```
[SecurID]
;EAP-Only=0
;First-Handle-Via-Auto-EAP=0
;EAP-Type=Generic-Token,EAP-32,EAP-15
Available-EAP-Types=Generic-Token,EAP-32,EAP-15
Available-EAP-Only-Values=0,1
Available-Auto-EAP-Values=0
```

```
[SecurID User]
;EAP-Only = 0
;EAP-Type = Generic-Token
;First-Handle-Via-Auto-EAP = 0
Available-EAP-Types=Generic-Token
Available-EAP-Only-Values=0,1
Available-Auto-EAP-Values=0
```

```
[SecurID Prefix]
;EAP-Only = 0
;EAP-Type = Generic-Token
;First-Handle-Via-Auto-EAP = 0
Available-EAP-Types=Generic-Token
Available-EAP-Only-Values=0,1
Available-Auto-EAP-Values=0
```

```
[SecurID Suffix]
;EAP-Only = 0
;EAP-Type = Generic-Token
;First-Handle-Via-Auto-EAP = 0
Available-EAP-Types=Generic-Token
Available-EAP-Only-Values=0,1
Available-Auto-EAP-Values=0
```

Note: If you edit the radius.ini or eap.ini files after Steel-Belted Radius has been started, then you must stop and restart Steel-Belted Radius before your changes will take effect.



Enabling System Generated PINS:

In order to allow Steel Belted RADIUS to handle **System Generated PINS**, a configuration change is required. Open the file named **secured.ini** typically located in **C:\Program Files\Juniper Networks\Steel-Belted Radius\Service**. Uncomment **Enable = 1** and **AllowSystemPins = 1**. Restart the RADIUS service once this has been completed.

[Configuration]

Enable = 1

;CheckUserAllowedByClient = 1

DefaultProfile = DEFAULT

AllowSystemPins = 1

Node Secret:

- **Deleting the Node Secret:** On the Steel Belted RADIUS server, Click **Start > Control Panel>RSA Security Center>Advanced Settings**. On the right hand side click **Clear**.

