eIQnetworks
SecureVue

RSA SecurID Ready Implementation Guide

Last Modified: July 20, 2011

Partner Information

Product Information	
Partner Name	eIQnetworks
Web Site	www.eiqnetworks.com
Product Name	SecureVue
Version & Platform	3.5.1 for Windows
Product Description	The Unified Situational Awareness Platform

Solution Summary

eIQnetworks SecureVue is used to manage company sensitive data which includes configuration, asset and security logs from host systems and network security devices. By implementing RADIUS user authentication, SecureVue supports RSA SecurID Two Factor Authentication. This method of strong authentication allows SecureVue to protect customer's sensitive data more effectively.

RSA SecurID supported features	
SecureVue 3.5.1	
RSA SecurID Authentication via Native RSA SecurID Protocol	N/A
RSA SecurID Authentication via RADIUS Protocol	Yes
On-Demand Authentication via Native SecurID Protocol	N/A
On-Demand Authentication via RADIUS Protocol	Yes
On-Demand Authentication via API	Yes
RSA Authentication Manager Replica Support	N/A
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	Designated Users

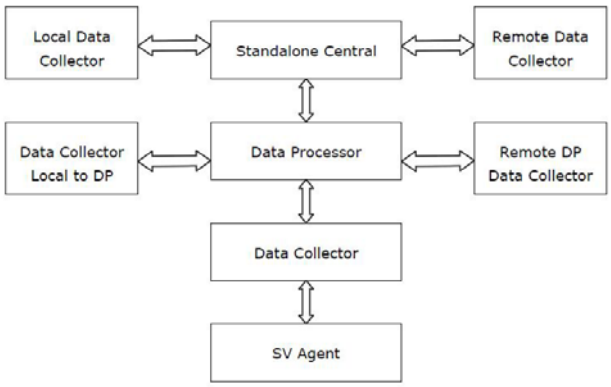
The SecureVue Central component acts as the RADIUS Client. The SecureVue Central manages all RADIUS authentication requests.

Global Central, Regional Central and Standalone Central components manage their own user accounts individually. Data Processors rely on their parent Central to manage authentication and authorization for accessing the data processor.

The RADIUS user accounts must be created individually in SecureVue. In order to successfully log into SecureVue Central or Data Processor, a RADIUS user account must exist both on the radius server and in the SecureVue user manager.

The SecureVue RADIUS implementation manages user accounts on an individual basis rather than allowing all radius users on a radius server access to SecureVue.

A RADIUS user can be granted permissions and roles in the same manner as local users and active directory users. RADIUS users can be created as all of our supported types which include Administrator, Power User, User and Alert Policy.



Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces

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 SecureVue will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for SecureVue to communicate with 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

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 documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

Product Requirements

Before You Begin

This section provides instructions for configuring the SecureVue 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 SecureVue components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring SecureVue for SecurID Authentication

Configure Radius

1. Click **Setup > User**. (Figure 1)

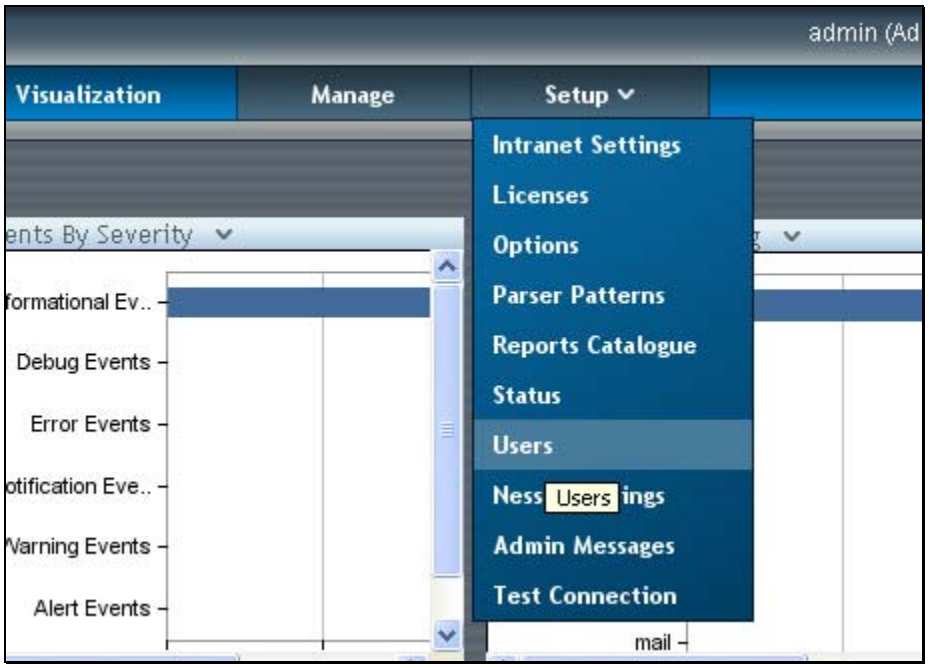


Figure 1

2. From the **User Manager** dialog, click **External Authentication** and click the **Configure Radius** button. (Figure 2)

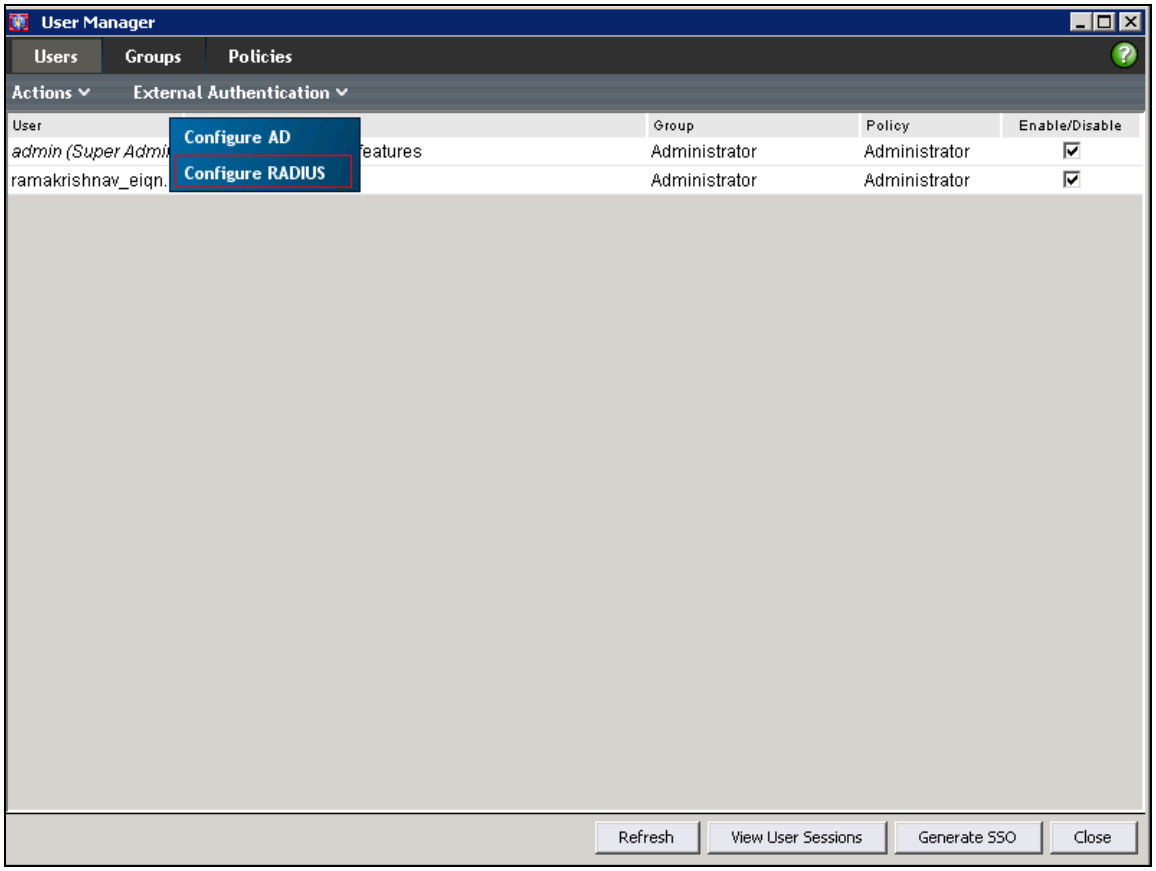


Figure 2

3. In the **Configure Radius Server** dialog, click **Add**.
4. The **RADIUS Server Details** dialog will appear. (Figure 3)

- Enter the **RADIUS Domain**. This domain name will be entered by the end users when they authenticate to SecureVue. (for this example we are using the name rsa)
- Enter the RADIUS Server **IP Address**.
- Enter the RADIUS **Authentication Port**.
- Select **PAP** for **Authentication Protocol**.
- Enter the **shared secret** that is configured on the RADIUS server for the SecureVue Central RADIUS Client.

5. **Save** RADIUS Server Details.

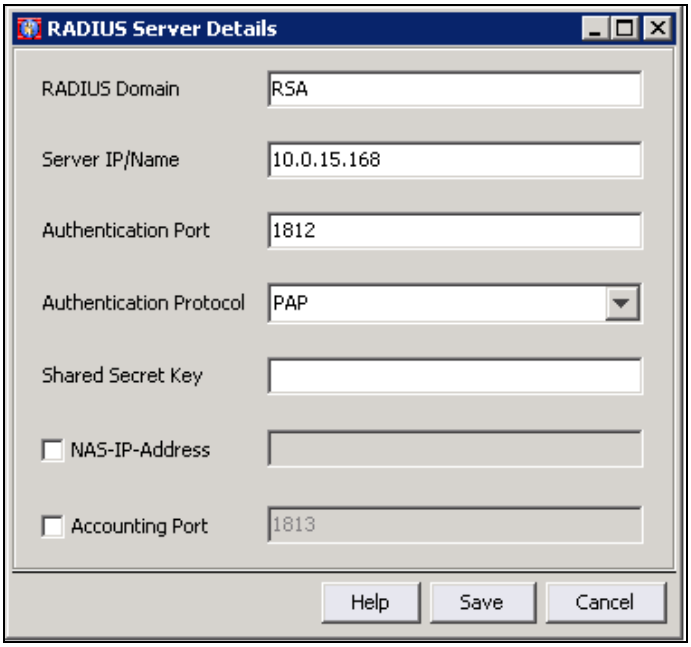


Figure 3

6. Select the **Users** tab in the **User Manager** dialog. Clicks **Actions** and click **Add** Button. (Figure 4)

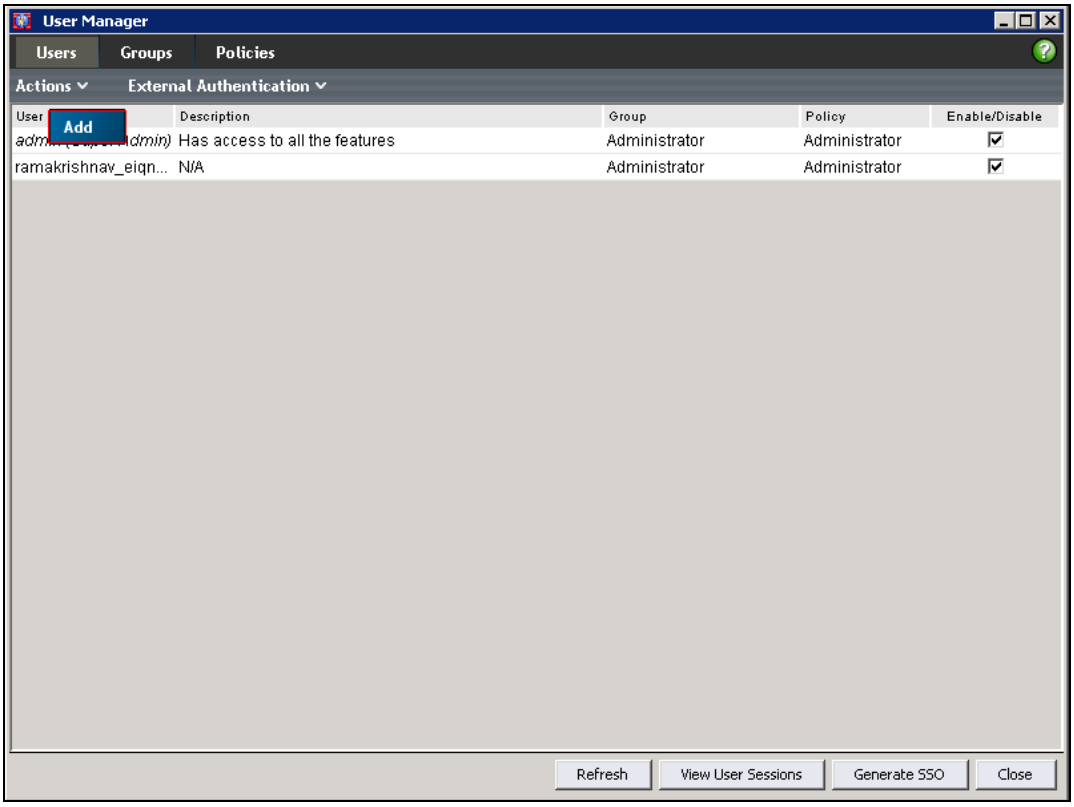


Figure 4

7. Select **Add RADIUS User** from the **Create New User** dialog, and then click **Next**. (Figure 5)

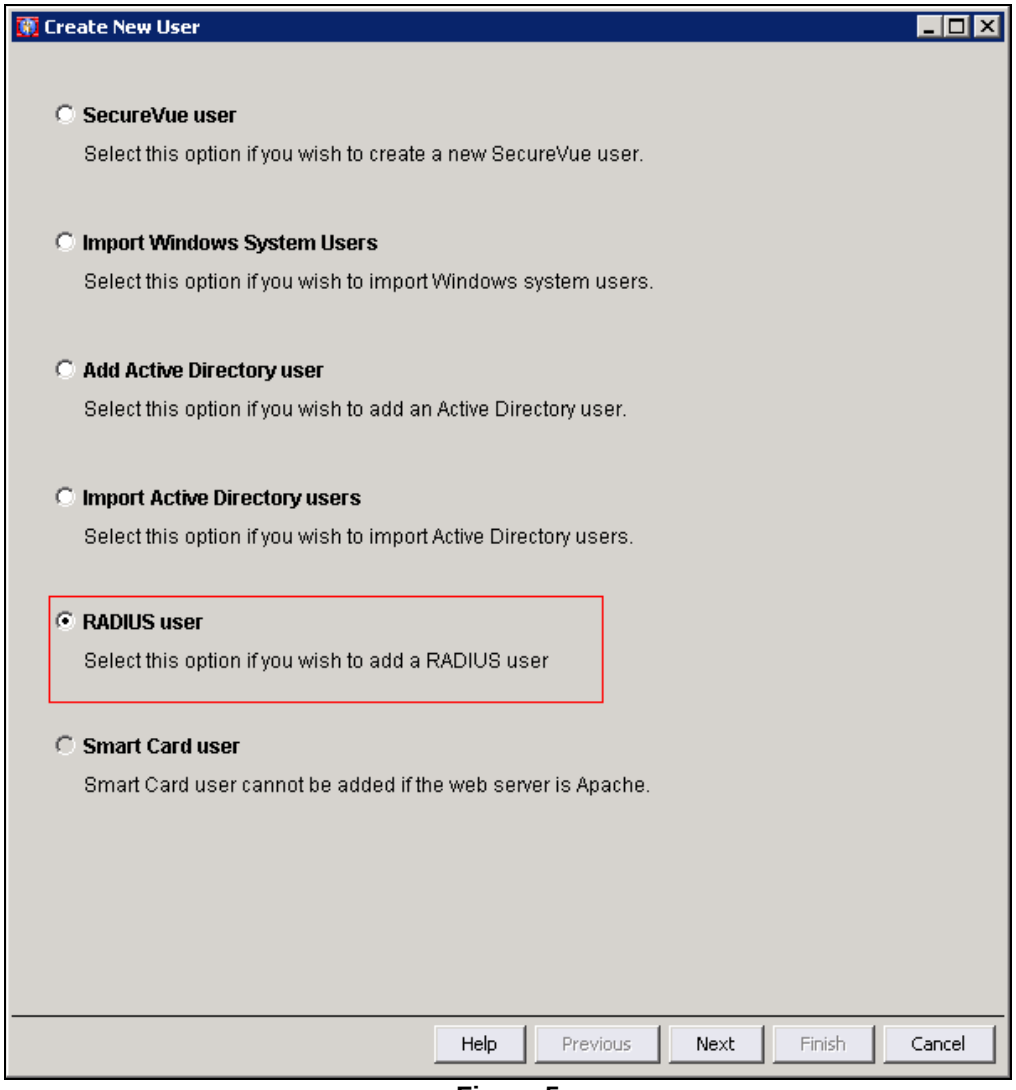


Figure 5

8. The **Create New User** dialog will appear. (Figure 6)

- Select the **RADIUS Domain** from the drop down list. (This example used “rsa”)
- Enter the **user name** that corresponds to the one configured on your RADIUS server that you would like to log in as.
- Enter a **Description**.(optional)
- Enter an **Email Address**.(optional)
- Select the **SecureVue Group** that you would like this user to be a member of.. (we will use administrator in this example)

9. Click **Finish**.

Note: The Validate User Button is a troubleshooting tool that can be used to validate the username and password if desired.

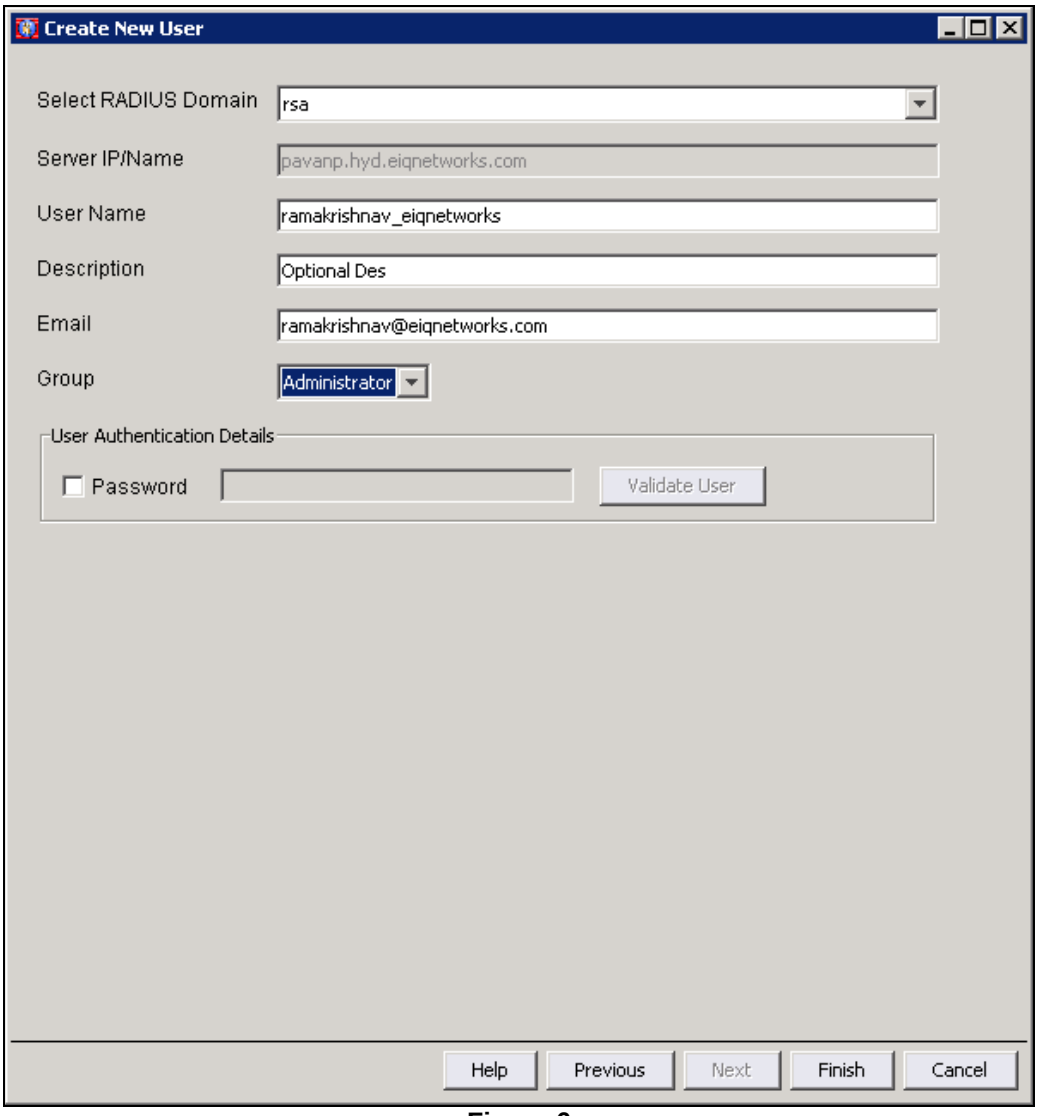
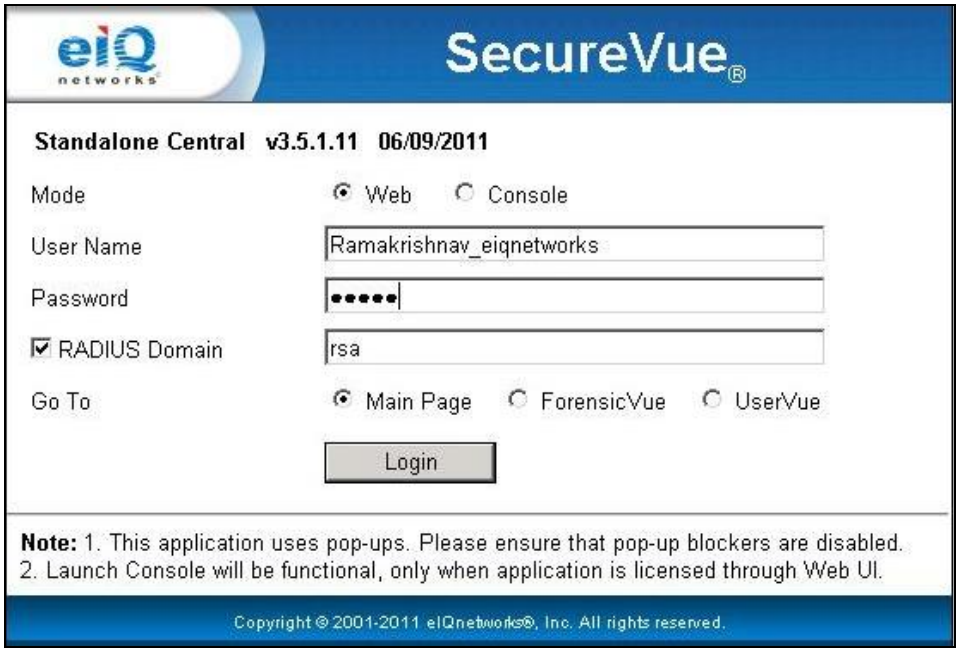


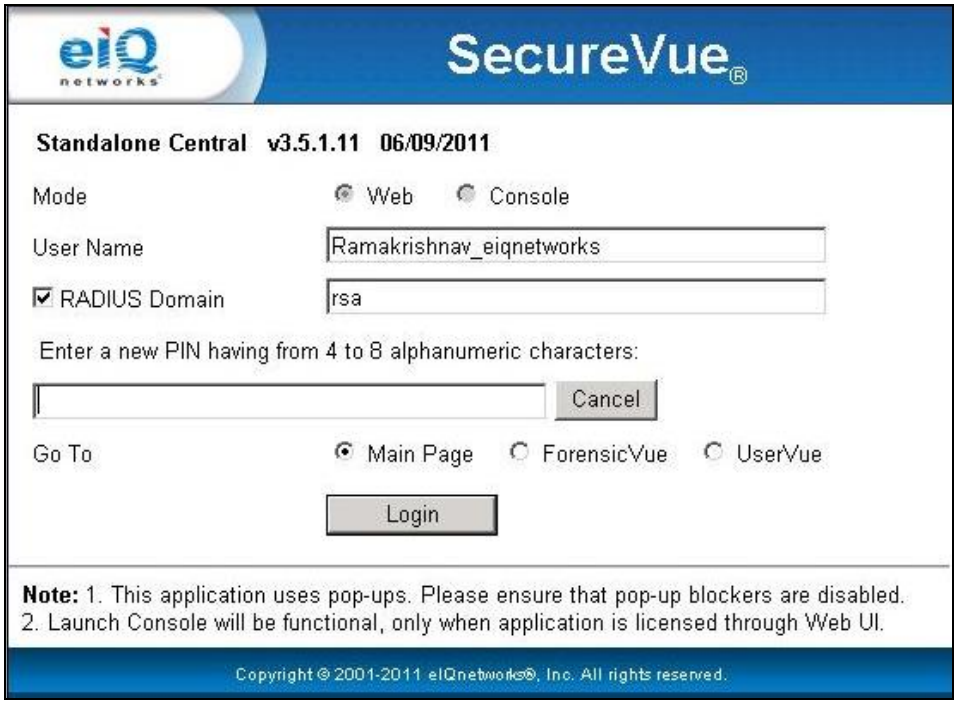
Figure 6

Screens

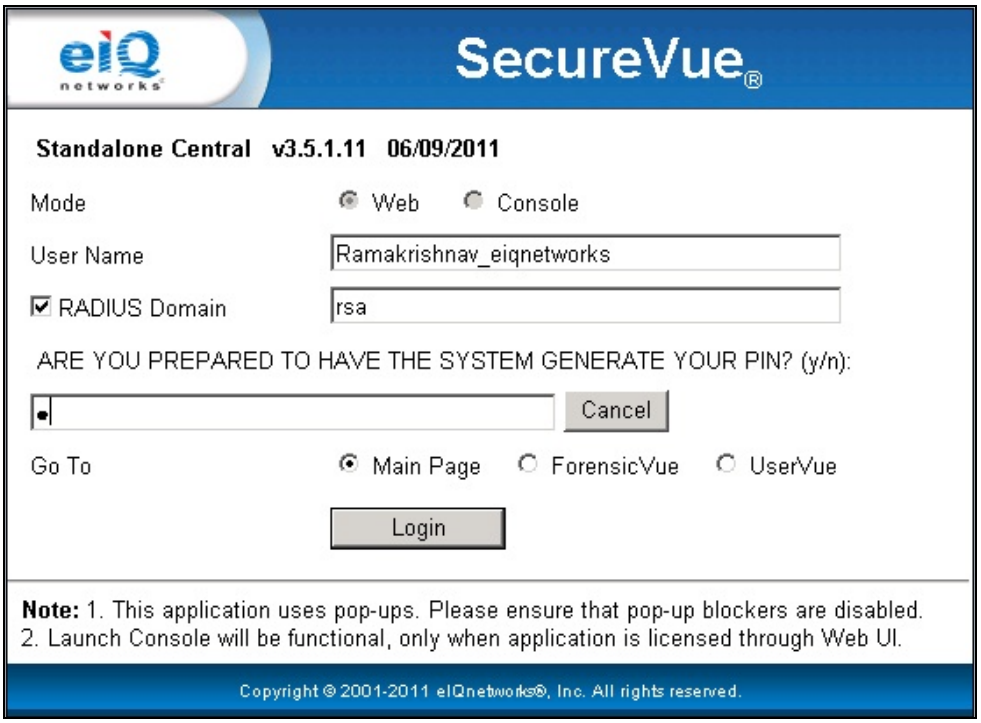
Login screen:

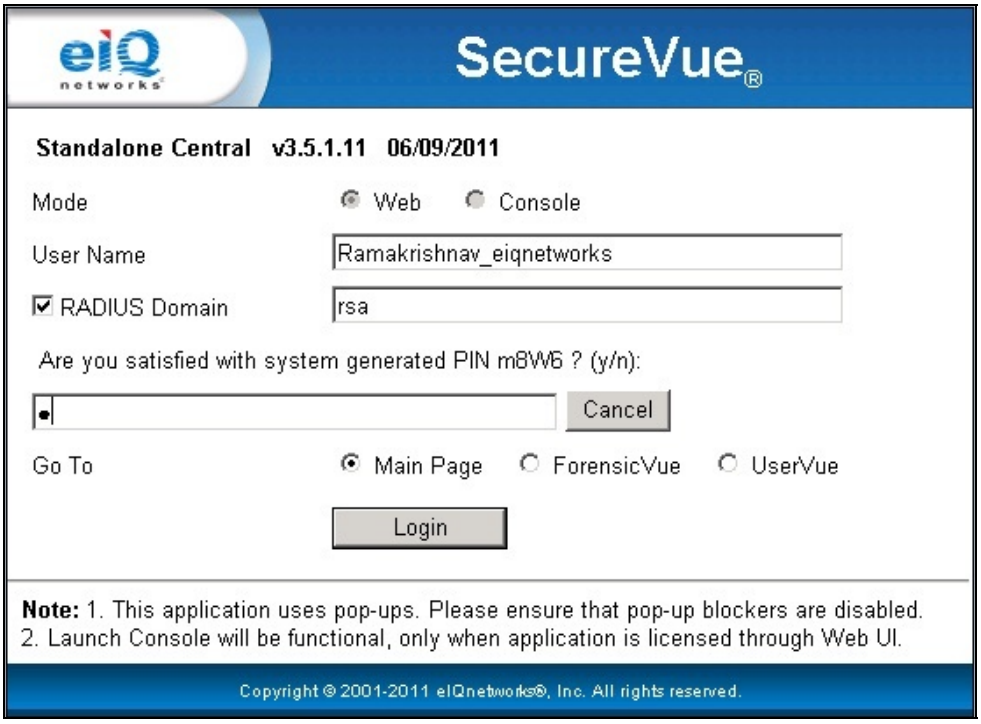


User-generated New PIN:

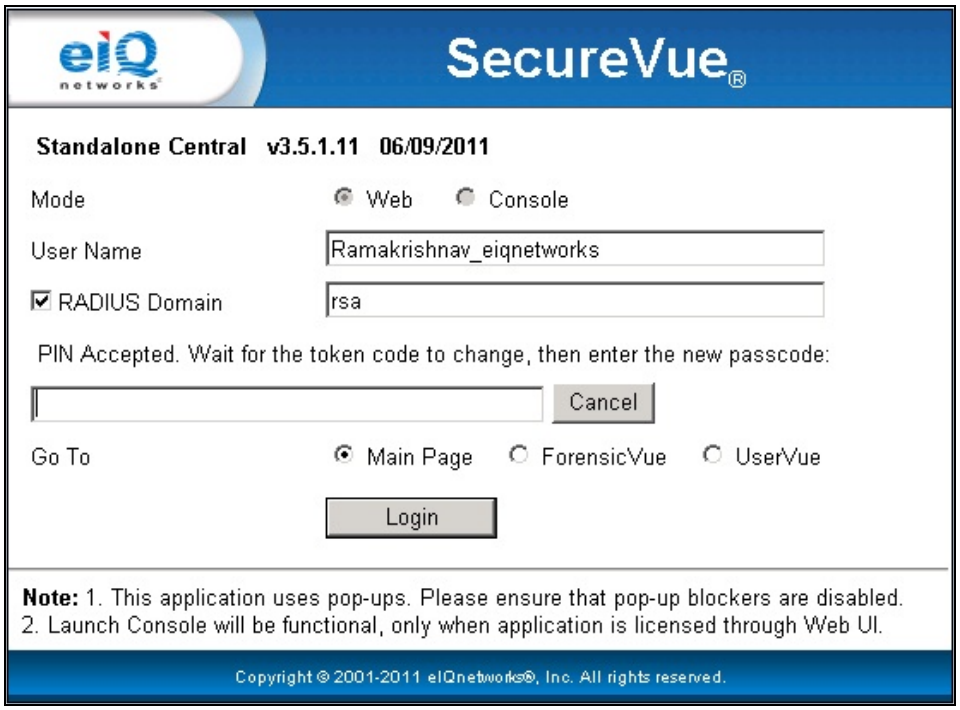


System-generated New PIN:





Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: July 20, 2011

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1SP4	Windows Server 2003 Enterprise
eIQnetworks SecureVue	3.5.1	Windows 2008 SP1

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

GLS / PAR

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration