Xceedium
Xsuite

RSA SecurID Ready Implementation Guide

Last Modified: January 23, 2014

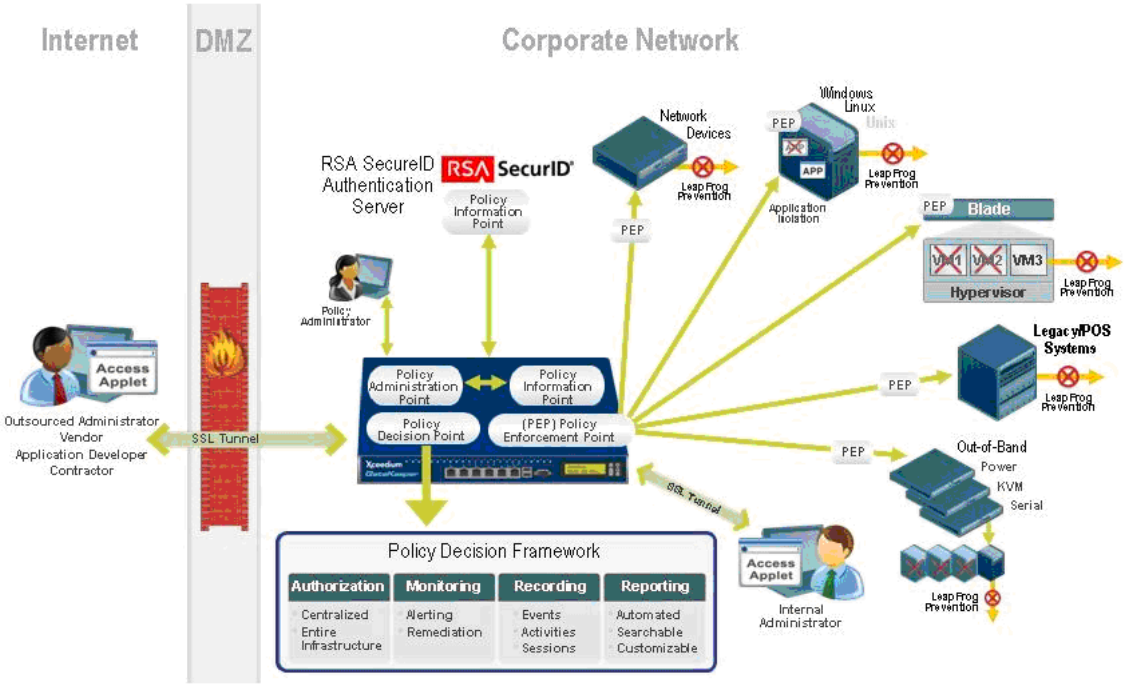
Partner Information

Product Information	
Partner Name	Xceedium
Web Site	www.xceedium.com
Product Name	Xsuite
Version & Platform	2.4
Product Description	Xceedium Xsuite™ protects your organization from security threats associated with privileged users, individuals and applications that have unfettered administrative access to your most sensitive IT infrastructure and business data. Xceedium's highly scalable solution employs role-based privilege access control, ensuring that privileged users, such as network administrators, security staff and trusted third parties, have rights to access only the specific systems, devices and commands they require. In other words, it provides "least privilege" access.

Solution Summary

The Xceedium Xsuite integrates with the RSA Authentication Server to provide two factor authentication for all users required to use SecurID tokens for access to infrastructure resources.

RSA Authentication Manager supported features	
Xsuite 2.4	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	No
Risk-Based Authentication	No
Risk-Based Authentication with Single Sign-On	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	No
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	Yes



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 Xceedium Xsuite 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 documentation for additional information about creating, modifying and managing Authentication Agents.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	In Memory
Node Secret	In Memory
sdstatus.12	None Stored
sdopts.rec	In Memory

Partner Product Configuration

Before You Begin

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

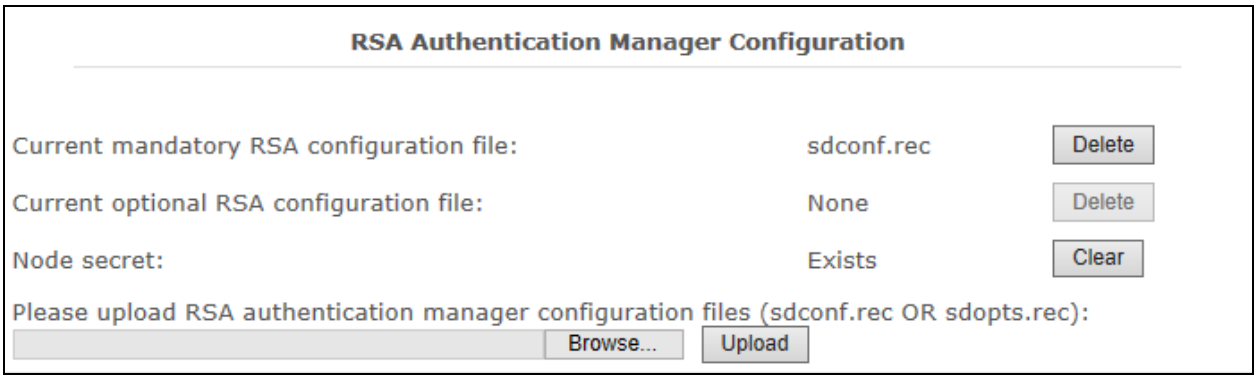
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

Xsuite SecurID Configuration

Importing the *sdconf.rec* file

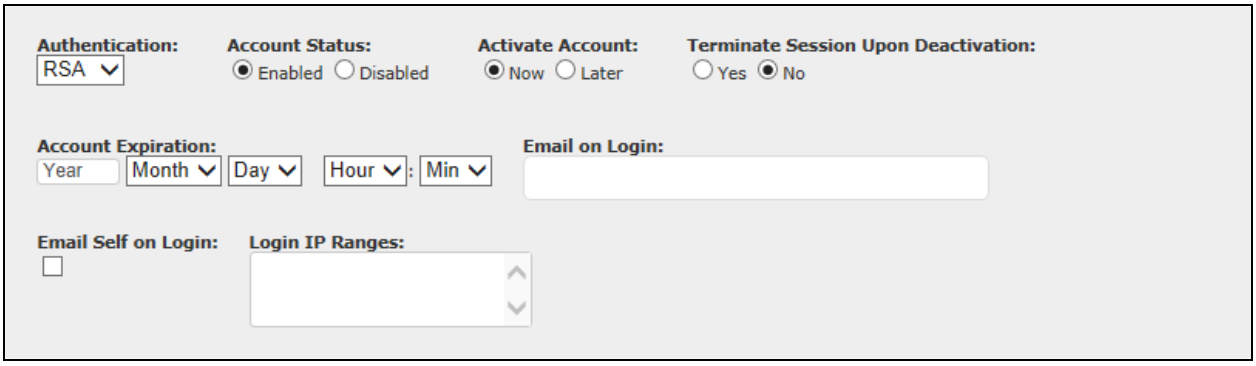
1. Login to the Xsuite config by browsing to **https://<XsuiteIP>/config/**.
2. Click on the **3rd Party** menu button.
3. Under the RSA Authentication Manager Configuration, import your **sdconf.rec** file that was generated from your RSA Authentication Manager server. Optionally, you can import your **sdopts.rec** if required.



Selecting Users

1. Login to the Xsuite as an administrator by going to **https://<XsuiteIP>.**
2. Click on the **Users** menu button.
3. Create a new user or edit an existing user and set the **Authentication** type to **RSA**.
4. Verify the **Account Status** is enabled.

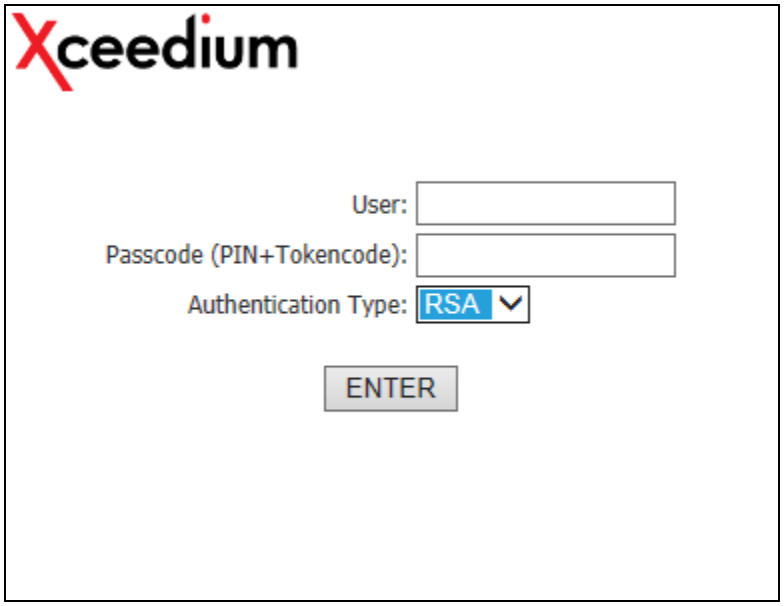
> **Note: The users that are created MUST match the users that reside within RSA Authentication Manager Server. IE: user = *dpintal_rsa* in Xsuite must equate to *dpintal_rsa* in Authentication Manager.**
>
> **The user accounts can also be imported into the Xsuite via a CSV file. Please refer to the Xsuite documentation in reference to importing user accounts.**



5. Once you have performed the configuration steps above, RSA authentication for your selected users is now enabled and they can now login to the Xsuite using their SecurID pin and token.

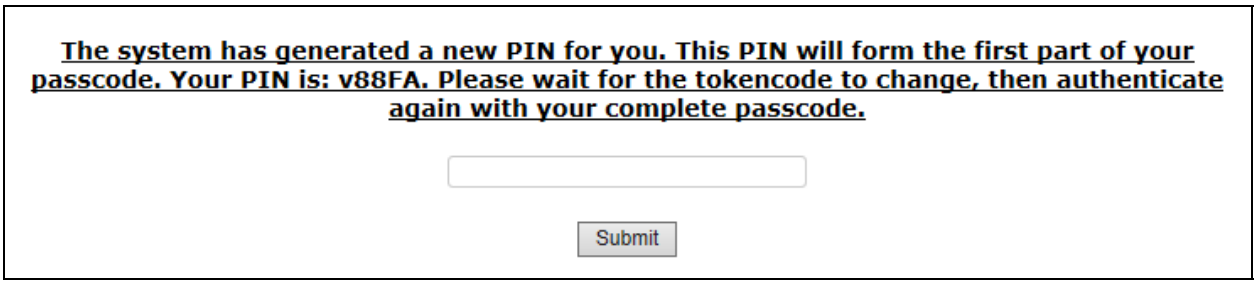
RSA SecurID Login Screens

Login screen:

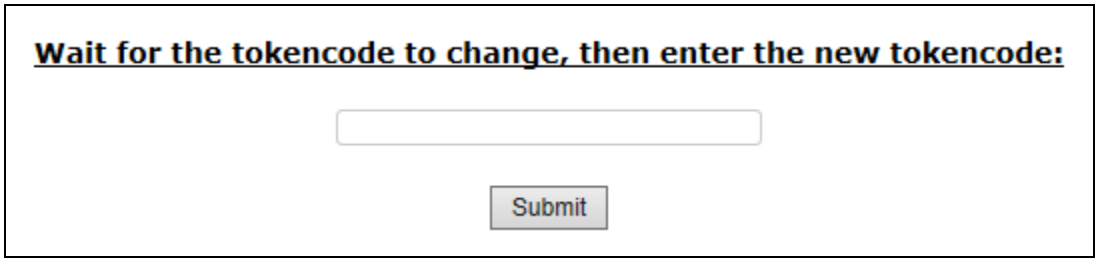


User-defined New PIN:

System-generated New PIN:



Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: January 23, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
Xceedium Xsuite	2.4	Proprietary (Linux)

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

DRP

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

Appendix

Partner Integration Details	
RSA SecurID API	6.1
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	No

Adding/removing the sdconf.rec or the optional sdopts.rec and clearing the Node secret can be performed through the RSA Authentication Manager Configuration screen.

1. Login to the Xsuite config by browsing to **https://<XsuiteIP>/config/**.
2. Click on the **3rd Party** menu button.
3. Under the RSA Authentication Manager Configuration, **Delete** your **sdconf.rec** file, sdopts.rec or clear the node secret as needed.