Symantec
Encryption Management Server

RSA SecurID Ready Implementation Guide

Last Modified: September 5, 2014

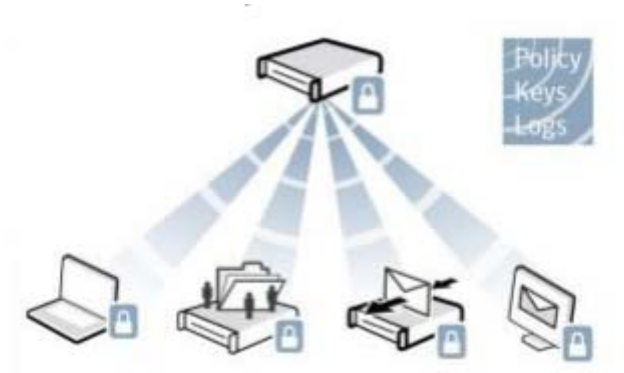
Partner Information

Product Information	
Partner Name	Symantec
Web Site	www.symantec.com
Product Name	Encryption Management Server
Version & Platform	3.3.2 MP3 (Build 15495)
Product Description	Encryption Management Server provides organizations with a single console to manage multiple Symantec encryption solutions. IT organizations can manage users, automate administrative activities and establish policies to defend sensitive data and avoid the financial loss, legal ramifications, and brand damage from a data breach.

Solution Summary

Symantec Encryption Management Server utilizes RSA SecurID for two factor authentication to protect the web server interface.

RSA Authentication Manager supported features	
Symantec Encryption Management Server 3.3.2	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	Yes
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	Yes
On-Demand Authentication via Native SecurID TCP Protocol	No
On-Demand Authentication via RADIUS Protocol	No
Risk-Based Authentication	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



Agent Host Configuration

To facilitate communication between the Symantec Encryption Management 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 Symantec Encryption Management Server and contains information about communication and encryption.

RSA Authentication Manager 8.0 introduced a new TCP-based authentication protocol and corresponding agent API. RSA Authentication Manager 8.0 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

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

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 Symantec Encryption Management Server will occur.

Partner Product Configuration

Before You Begin

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

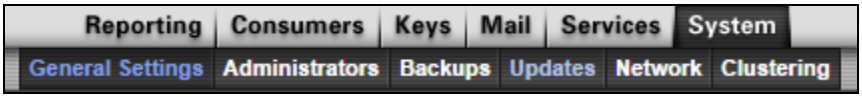
Configuration Summary

- Download a copy of the sdconf.rec.from the RSA Authentication Manager.
- Perform the Symantec Encryption Management Server RSA SecurID Configuration.
- Review and implement changes referenced in the Known Issues section of this guide.

Symantec Encryption Management Server RSA SecurID Configuration

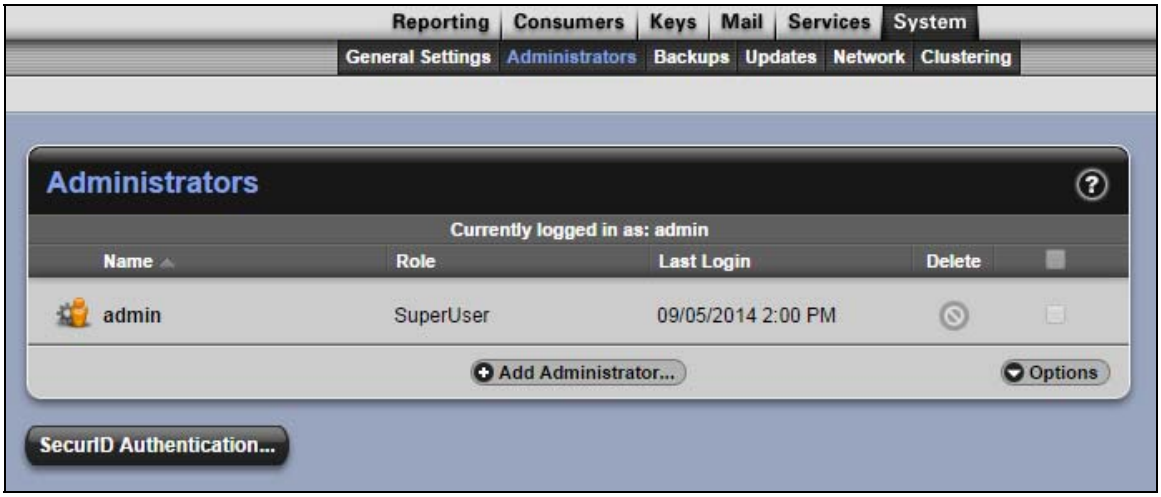
1. Login to the Symantec Encryption Management Server as Admin.

2. Once logged in click **System** within the Symantec Encryption Management Server menu.

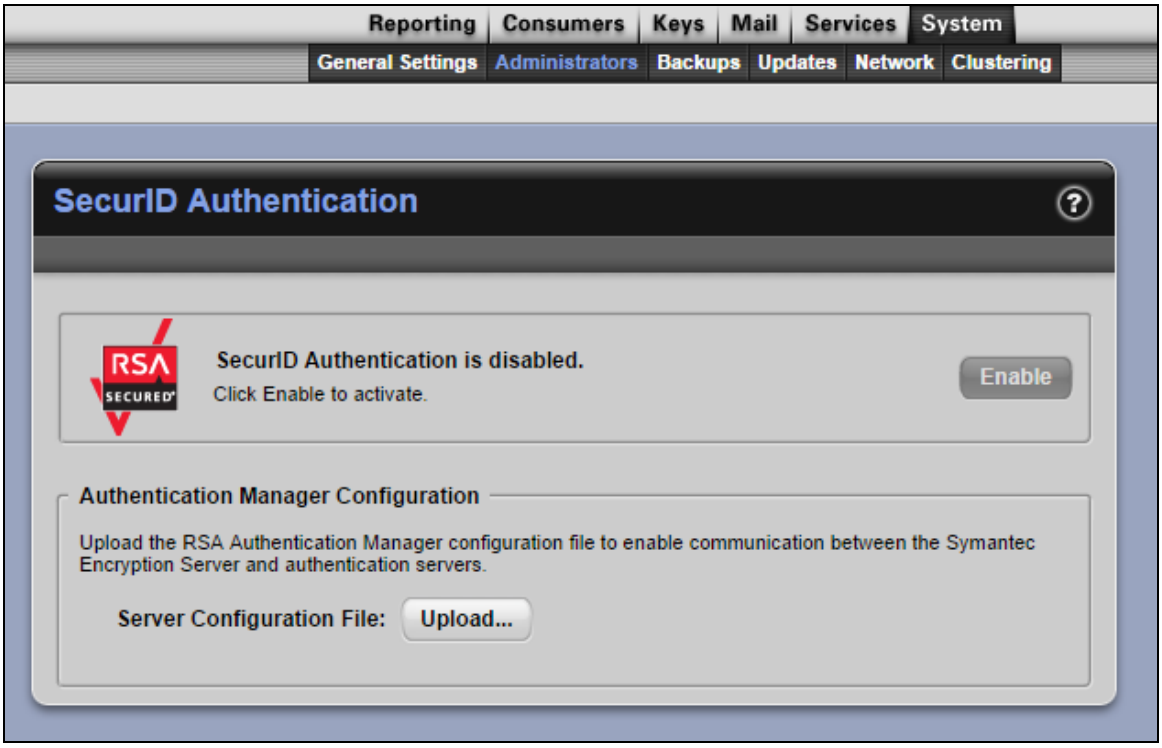


3. Click **Administrators** within the Symantec Encryption Management Server menu.

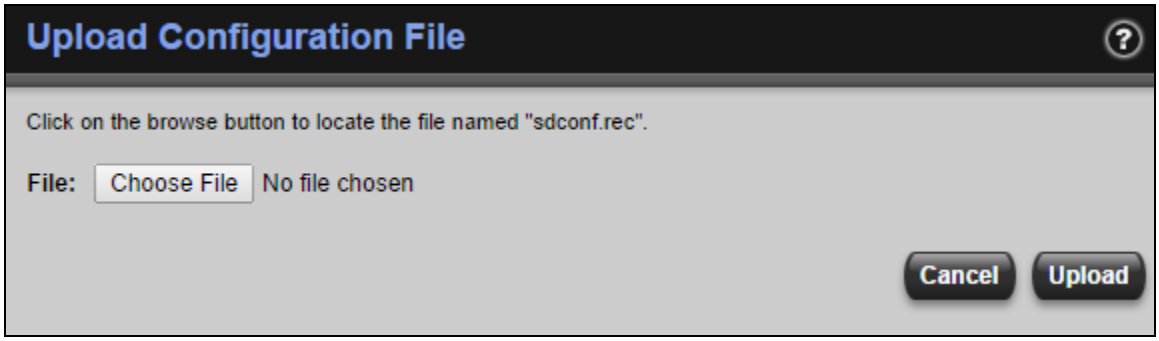
4. Within the Administrators window click **SecurID Authentication..**.



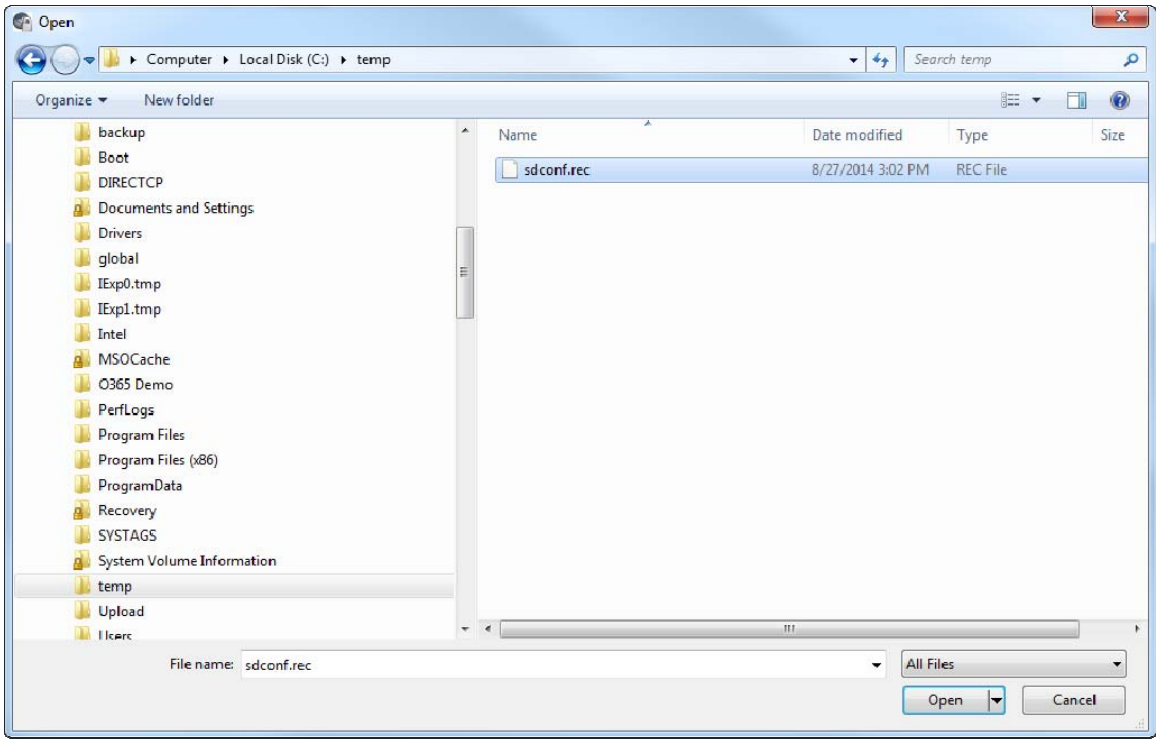
5. Click **Upload**….



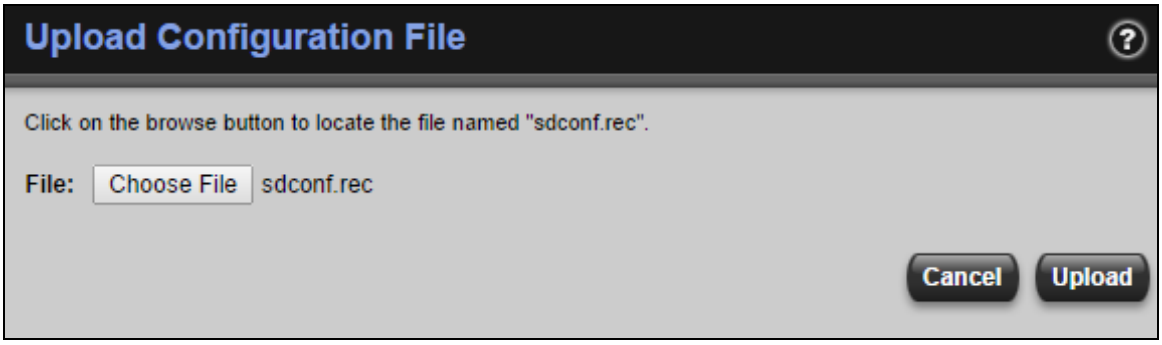
6. Click **Choose File**.



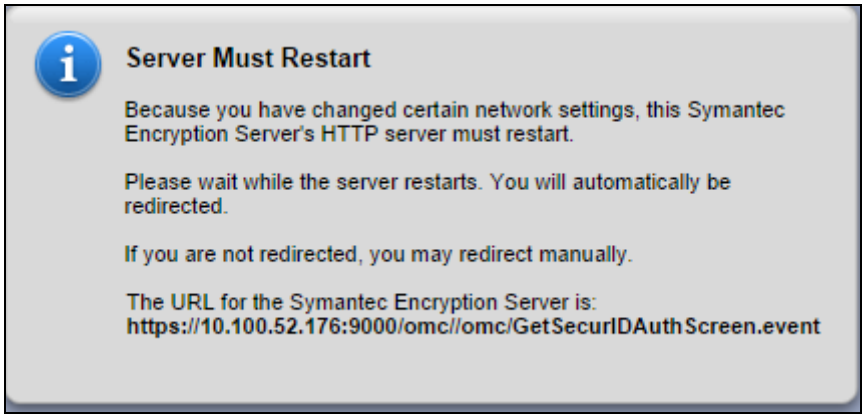
7. Select the **sdconf.rec** file downloaded from the RSA Authentication Manager and click **Open**.



8. Click the **Upload** button.



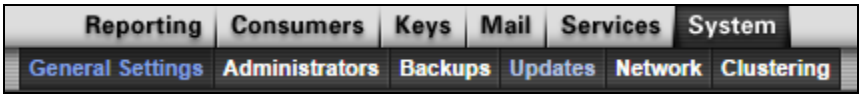
9. Allow the system to reboot as part of the configuration.



Important: Before proceeding review the Known Issues section of this guide and the Symantec Technical note to manually enable RSA SecurID.

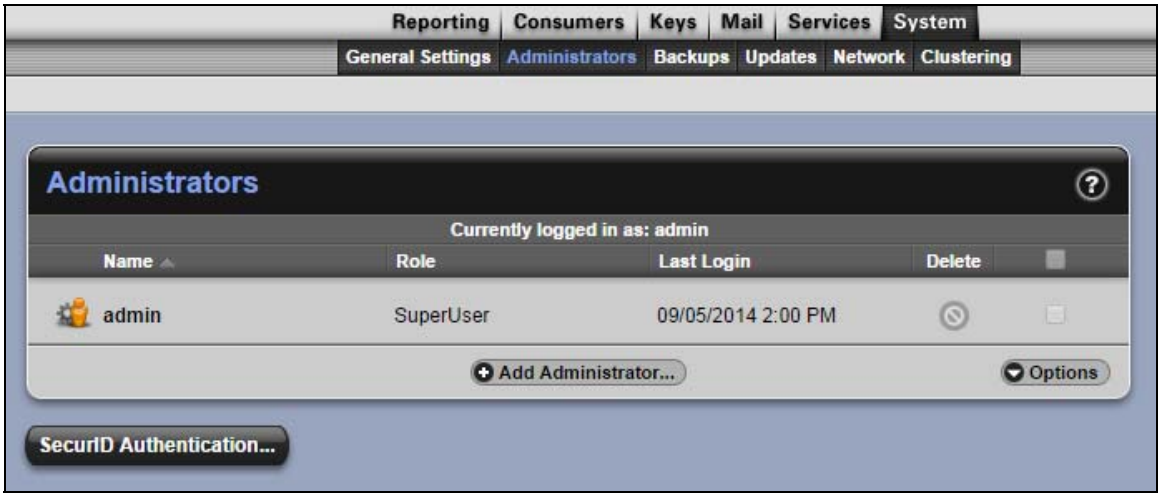
10. After the reboot has completed log in as the admin.

11. Once logged in click **System** within the Symantec Encryption Management Server menu.

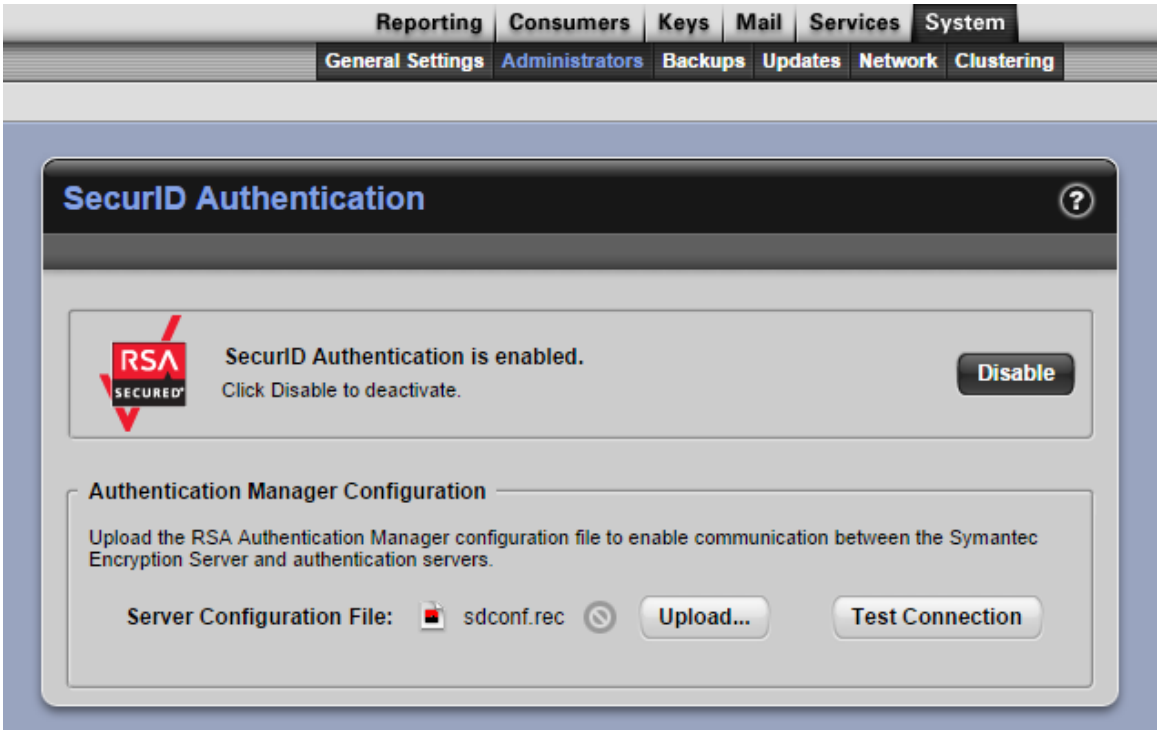


12. Click **Administrators** within the Symantec Encryption Management Server menu.

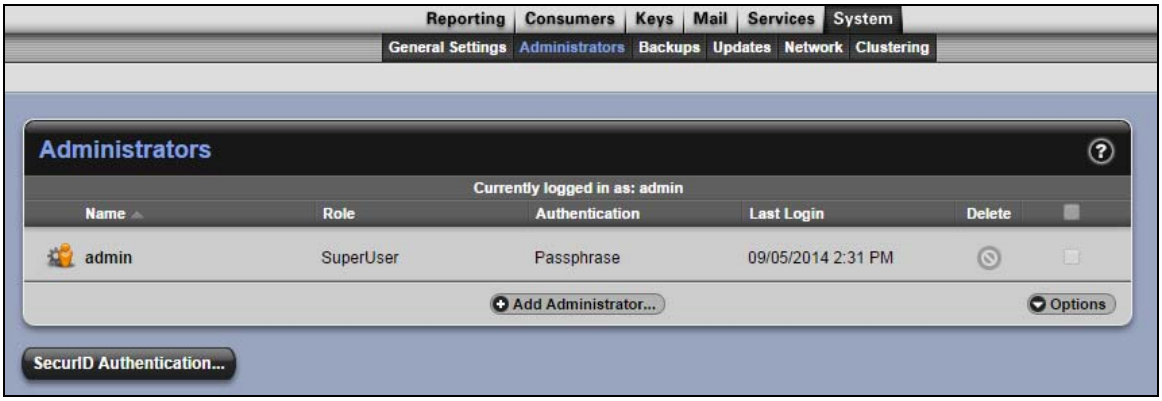
13. Within the Administrators window click **SecurID Authentication..**.



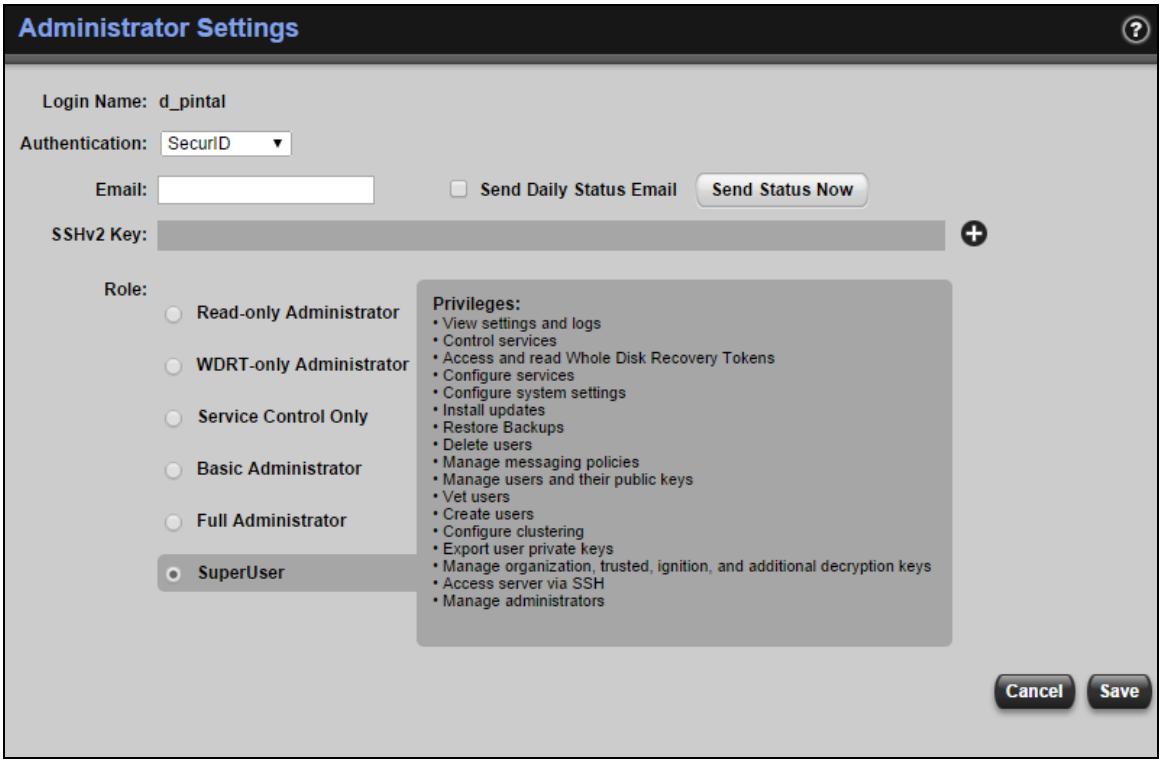
14. Verify that SecurID Authentication is enabled.



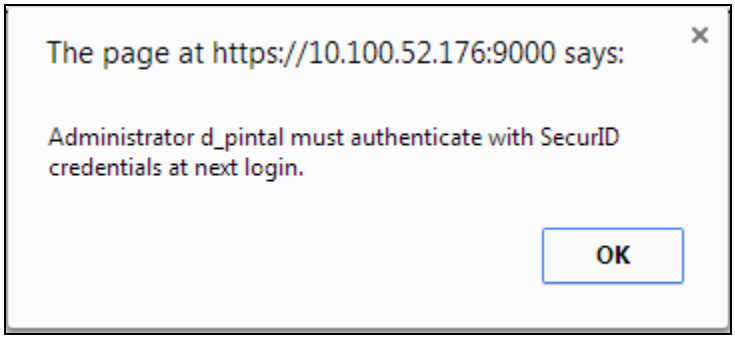
15. Once verified, return to the Administrators menu and click Add Administrator…



16. Enter a **Login Name** and change the **Authentication** method by using the drop down menu, select **SecurID** and click **Save**..



17. The administrator is then presented with a notification that the administrator must authenticate with SecurID at next login.



RSA SecurID Login Screens

Login screen:

User-defined New PIN:

System-generated New PIN:

Next Tokencode:

Certification Test Checklist for RSA Authentication Manager

Certification Environment

Product Name	Version Information	Operating System
RSA Authentication Manager	8.1	Virtual Appliance
Symantec Encryption Mgmt Srvr	3.3.2 MP3 (Build 15495)	Virtual Appliance

RSA SecurID Authentication

Date Tested: September 5, 2014

Mandatory Functionality	RSA Native UDP Agent	RSA Native TCP Agent	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

DRP / PAR

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

Known Issues

RSA had identified and reported an issue with enabling SecurID authentication within the Symantec Encryption Management Server. The issue is being addressed by Symantec with a workaround and will be available within a future release of the product. Reference the Symantec KB article.

Use the following link to find the workaround for this known issue on the Symantec website;

http://www.symantec.com/docs/TECH224283

Appendix

RSA SecurID Authentication Files

RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	**/etc/ovid**
sdopts.rec	**/etc/ovid (not tested)**
Node secret	**/etc/ovid**
sdstatus.12 / jastatus.12	**/etc/ovid**

Partner Integration Details

Partner Integration Details	
RSA SecurID UDP API	5.03
RSA SecurID TCP API	N/A
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Administrators
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	No

Node Secret:

The Node Secret (securid file) is stored in /etc/ovid and can be deleted from the server by connecting to the server using SSH. Symantec instructions for setting up SSH access can be found at the following link. **http://www.symantec.com/docs/TECH149673**

sdconf.rec:

The SDconf.rec is managed through the Administrators web interface however it can be also managed through an SSH connection. Symantec instructions for setting up SSH access can be found at the following link. **http://www.symantec.com/docs/TECH149673**

sdopts.rec:

The sdopts.rec is managed through an SSH console. Symantec instructions for setting up SSH access can be found at the following link. **http://www.symantec.com/docs/TECH149673**

sdstatus.12:

The sdstatus.12 file can be viewed through an SSH console. Symantec instructions for setting up SSH access can be found at the following link. **http://www.symantec.com/docs/TECH149673**