SSH
CryptoAuditor 1.3.2

RSA SecurID Ready Implementation Guide

Last Modified: 7/17/2014

Partner Information

Product Information	
Partner Name	SSH
Web Site	www.ssh.com
Product Name	CryptoAuditor
Version & Platform	1.3.2.64
Product Description	CryptoAuditor is a transparent and centralized real-time privileged access monitoring and auditing solution that enables organizations to control trusted insider data transfer activities on the fly and without any impact on remote administrators. CryptoAuditor is designed to reduce potential security threats from trusted insiders, meet current and emerging compliance mandates and reduce costs associated with implementation and administration with a minimally invasive approach designed to work with your existing network architecture.

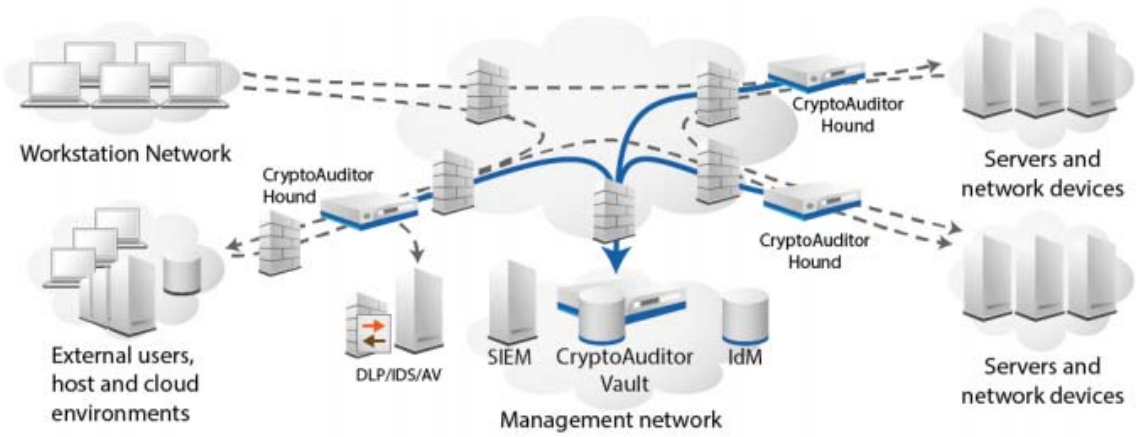
ssh
Securing the path to your information assets

Solution Summary

SSH CryptoAuditor utilizes RSA SecurID RADIUS authentication to increase security for SSH, TCP and RDP connections in either Gateway or Bastion configurations.

Note: SSH does not support RSA SecurID RADIUS challenge-response for RDP connections.

RSA Authentication Manager supported features	
CryptoAuditor 1.3.2.64	
RSA SecurID Authentication via Native RSA SecurID Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
On-Demand Authentication via Native SecurID Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	Yes
Risk-Based Authentication with Single Sign-On	No
RSA Authentication Manager Replica Support	No
Secondary RADIUS Server Support	No
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No



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 CryptoAuditor will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for CryptoAuditor 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.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the CryptoAuditor 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.

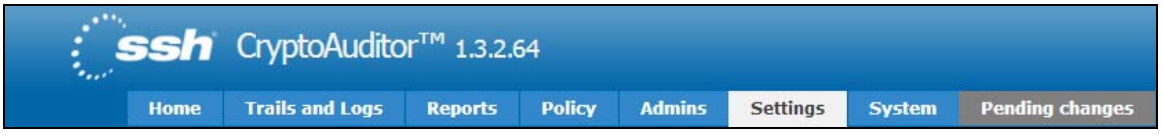
All CryptoAuditor components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring RSA SecurID/RADIUS for SSH CryptoAuditor

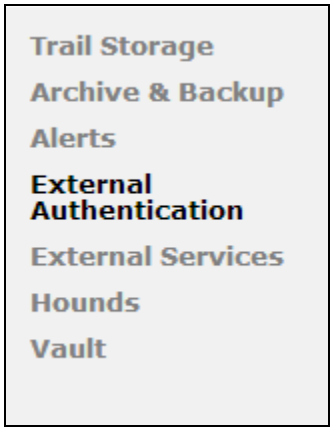
Adding a RADIUS Server for External Authentication

1. Login with the Administrators Username and Password set during the CryptoAuditor installation.

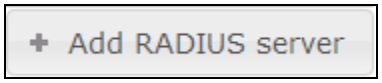
2. Select the **Settings** tab from the CryptoAuditor menu.



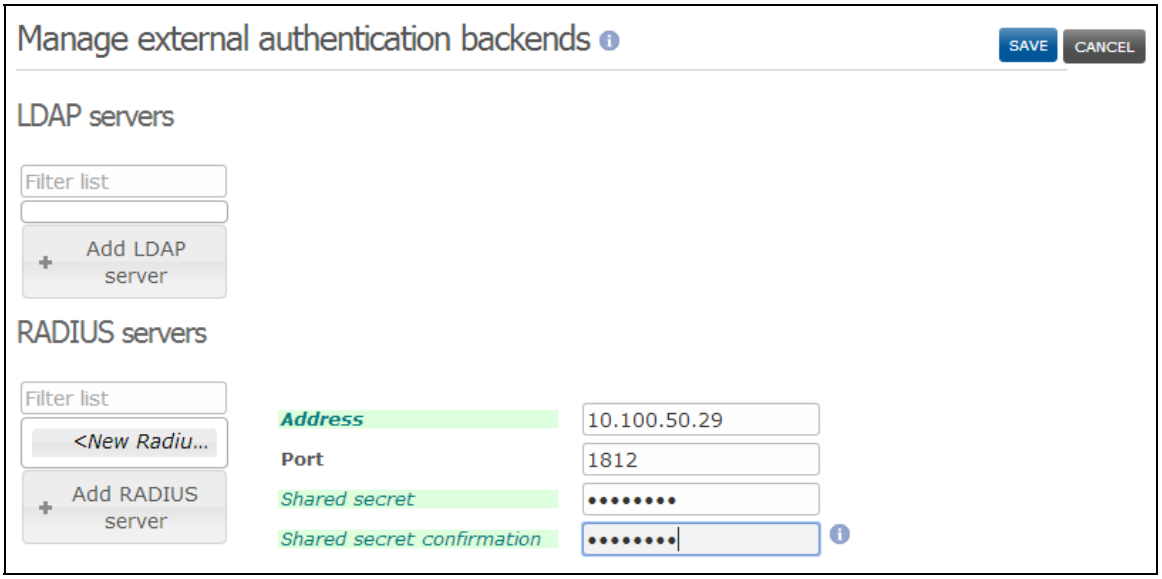
3. Select the **External Authentication** menu option from the left side of the page.



4. Select the **+ Add RADIUS server** button.

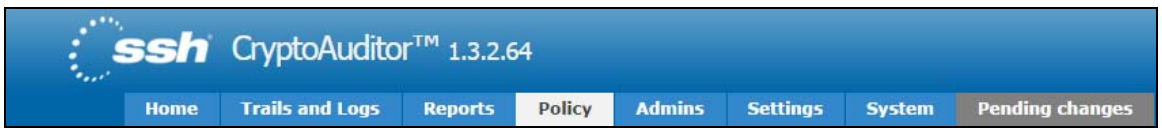


5. Enter the RADIUS server IP **Address**, **Port**, **Shared secret** and **confirmation** within the address fields provided, select **Save** to continue.

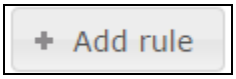


Creating the Authentication Rule

1. Select the **Policy** tab from the CryptoAuditor menu.



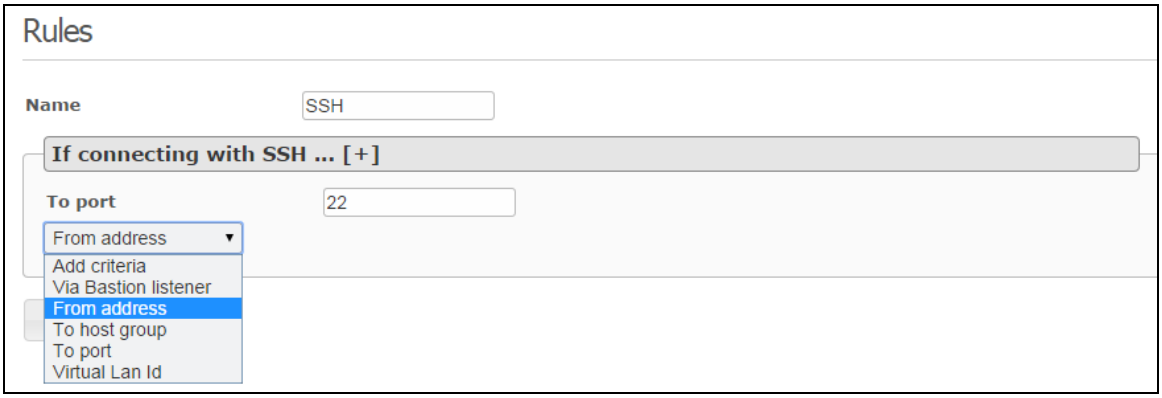
2. Select the **+ Add rule** button at the upper right hand side of the page.



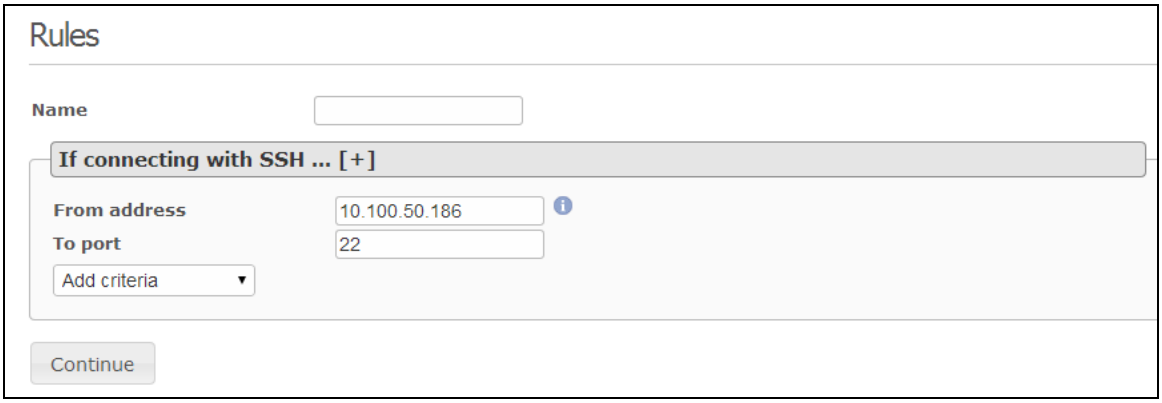
3. Enter the Rule Name.

4. Select the ▼ and choose **SSH** within the Connecting with options.

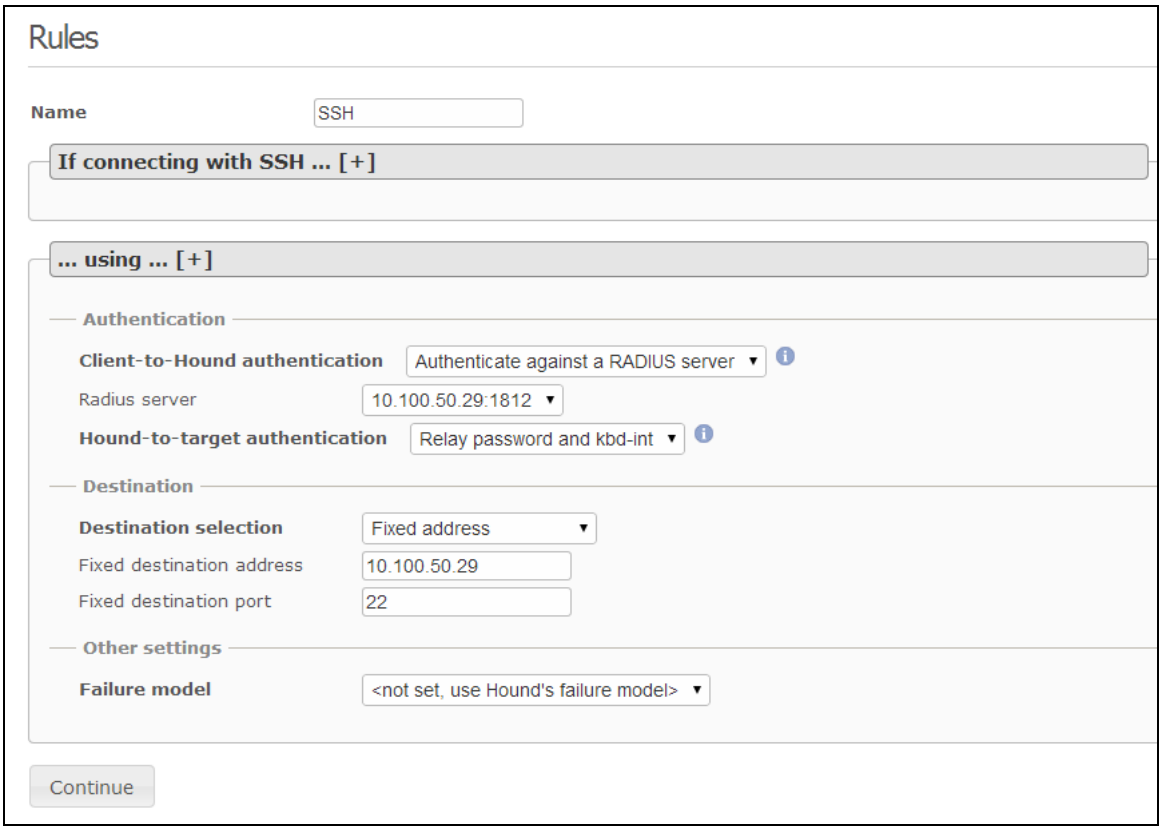
5. Select the ▼ and choose **From address** within the To port options.



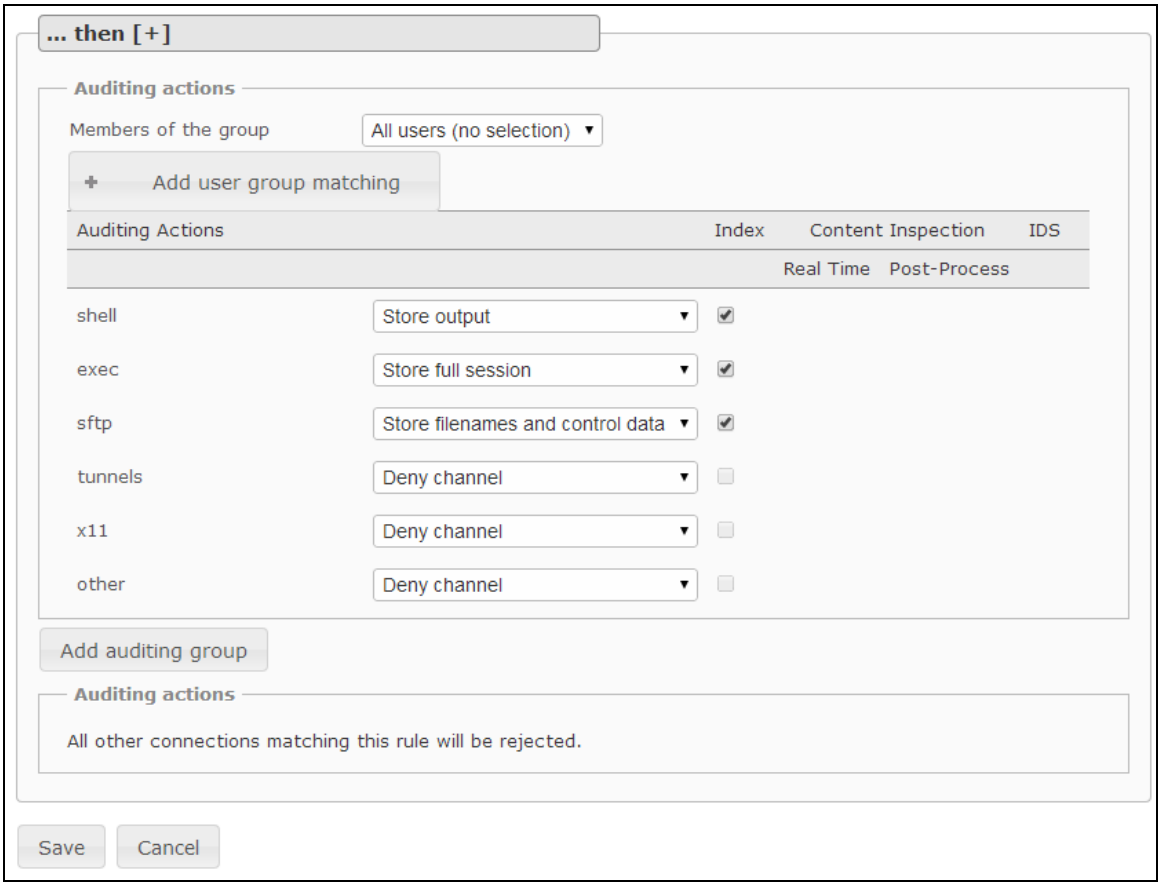
6. Select the **Continue** button.



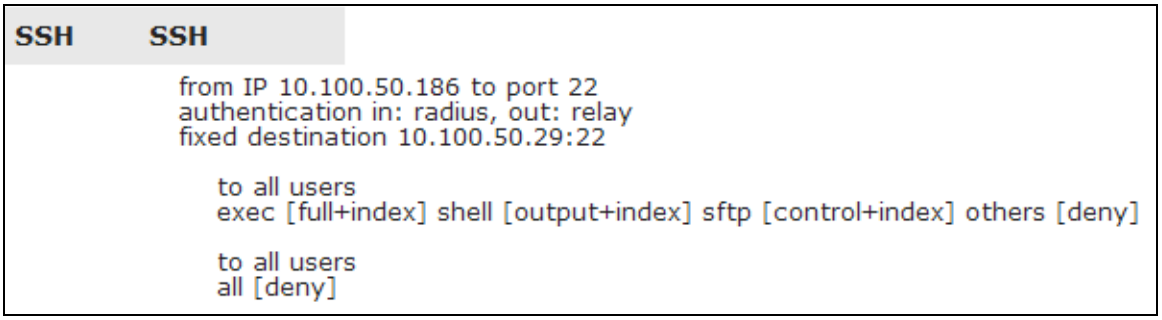
7. Within the Client-to-Hound authentication drop down, select **Authenticate against a RADIUS Server.** Within the Radius Server drop down, select the IP address and port of the External Authentication server previously configured. Within the Hound-to-target authentication drop down, select **Relay password and kbd-int,** select **Continue.**



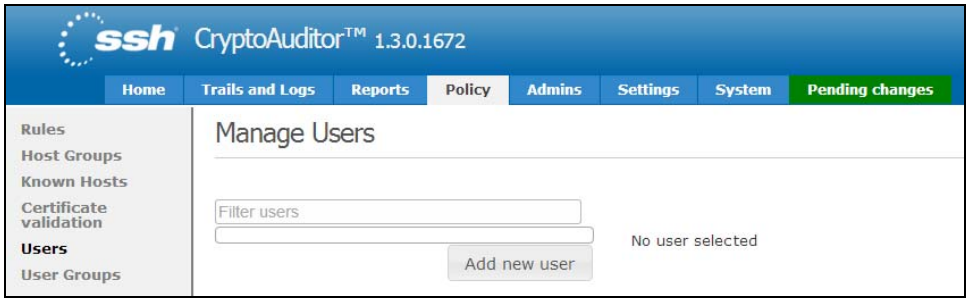
8. Choose the defaults from the … then [+] screen and select **Save**.



9. The rule will be displayed as follows.

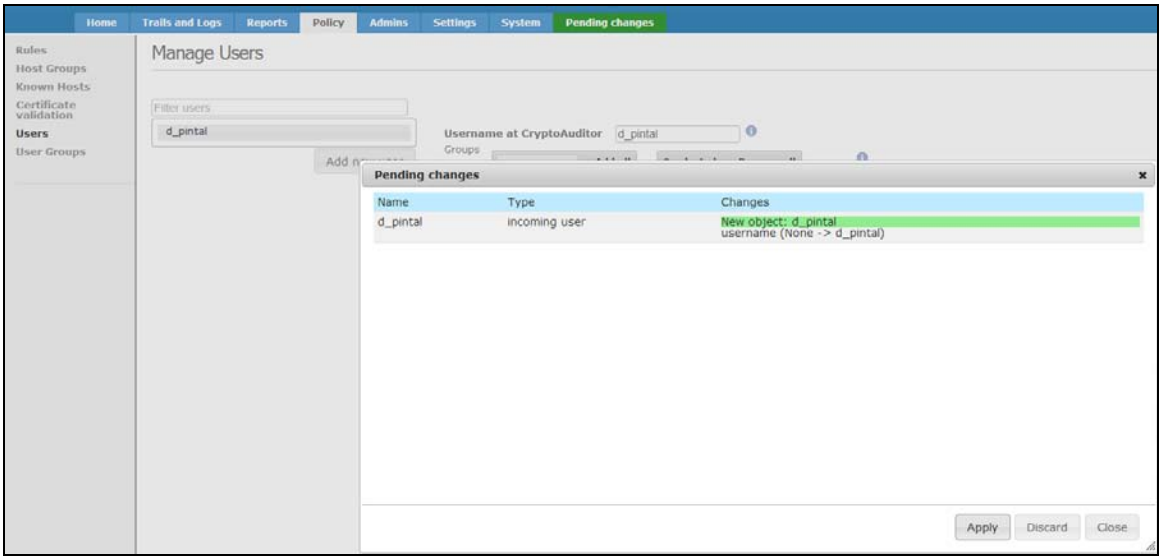


10. Select **Users** from the sidebar menu.



11. Select the **Add new user** button and within the Username at CryptoAuditor field enter the **username of the client** and select **Save**.

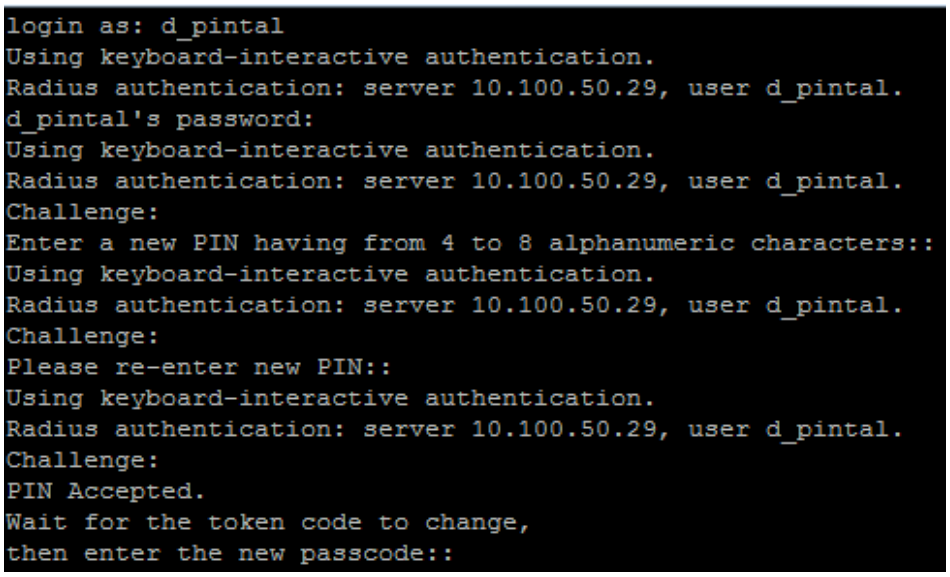
12. Select the **Pending changes** tab and click **Apply**.



RSA SecurID Login Screens

Login screen:

User-defined New PIN:



System-generated New PIN:

```
login as: d_pintal
Using keyboard-interactive authentication.
Radius authentication: server 10.100.50.29, user d_pintal.
d_pintal's password:
Using keyboard-interactive authentication.
Radius authentication: server 10.100.50.29, user d_pintal.
Challenge:
ARE YOU PREPARED TO HAVE THE SYSTEM GENERATE YOUR PIN? (y/n)::
Using keyboard-interactive authentication.
Radius authentication: server 10.100.50.29, user d_pintal.
Challenge:
Are you satisfied with system generated PIN dIumW ? (y/n)::
Using keyboard-interactive authentication.
Radius authentication: server 10.100.50.29, user d_pintal.
Challenge:
PIN Accepted.
Wait for the token code to change,
then enter the new passcode::
```

Next Tokencode:

```
login as: d_pintal
Using keyboard-interactive authentication.
Radius authentication: server 10.100.50.29, user d_pintal.
d_pintal's password:
Using keyboard-interactive authentication.
Radius authentication: server 10.100.50.29, user d_pintal.
Challenge:
Wait for token to change,
then enter the new tokencode::
```

Certification Checklist for RSA Authentication Manager

Date Tested: July 17, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.1	Virtual Appliance
SSH CryptoAuditor	1.3.2.64	Linux

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 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	✓

DRP

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