Opengear

SD/CM/IM/ACM Series Console Server

RSA SecurID Ready Implementation Guide

Last Modified: Jul 7, 2010

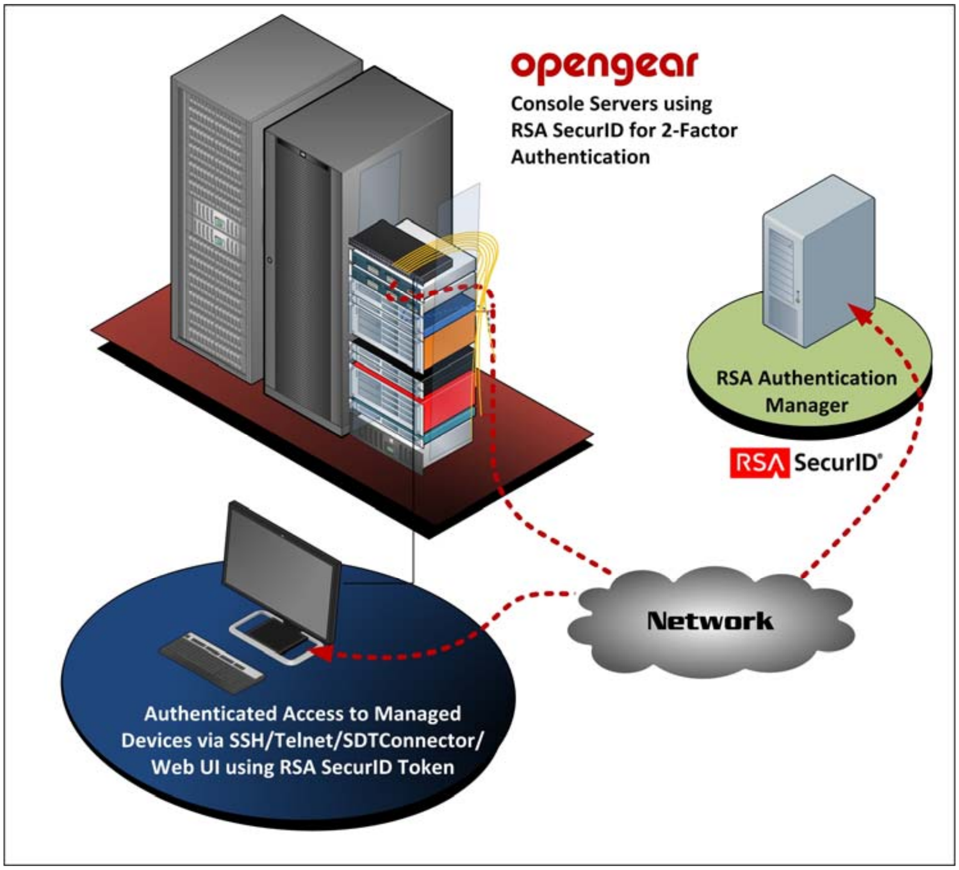
Partner Information

Product Information	
Partner Name	Opengear
Web Site	www.opengear.com
Product Name	Console Server
Version & Platform	3.2
Product Description	Opengear Console Servers provide Out-of-Band management of Serial/Network and USB Connected devices.
Product Category	Remote Access

Solution Summary

The Opengear Console Servers use RSA SecurID Authentication to allow seamless integration into enterprises already using RSA SecurID. User permissions can be centrally managed, allowing easy deployment of many console servers to remote sites.

RSA SecurID supported features Opengear Console Server 3.2	
RSA SecurID Authentication via Native RSA SecurID Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
RSA Authentication Manager Replica Support	No
Secondary RADIUS Server Support	Yes(2)
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 Opengear Console Server will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for Opengear Console Server 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

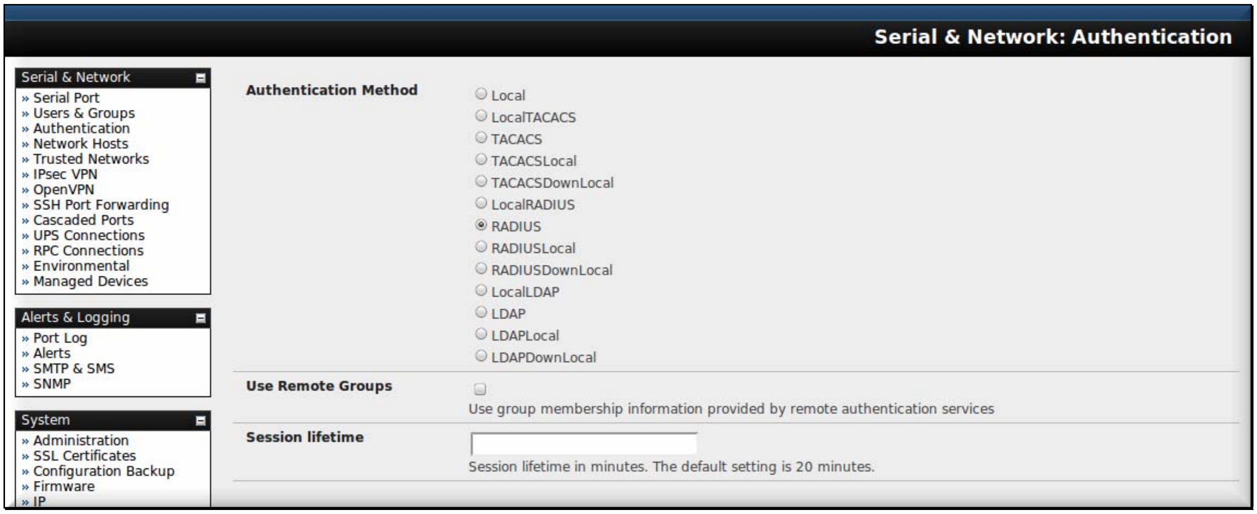
This section provides instructions for integrating the partners' product with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

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.

Opengear Console Server

Connect to the Web UI of the Opengear Console Server, and then click on the **Authentication** link in the navigation bar.



Serial & Network: Authentication

Authentication Method

○ Local
○ LocalTACACS
○ TACACS
○ TACACSLocal
○ TACACSDownLocal
○ LocalRADIUS
● RADIUS
○ RADIUSLocal
○ RADIUSDownLocal
○ LocalLDAP
○ LDAP
○ LDAPLocal
○ LDAPDownLocal

Use Remote Groups

□
Use group membership information provided by remote authentication services

Session lifetime

Session lifetime in minutes. The default setting is 20 minutes.

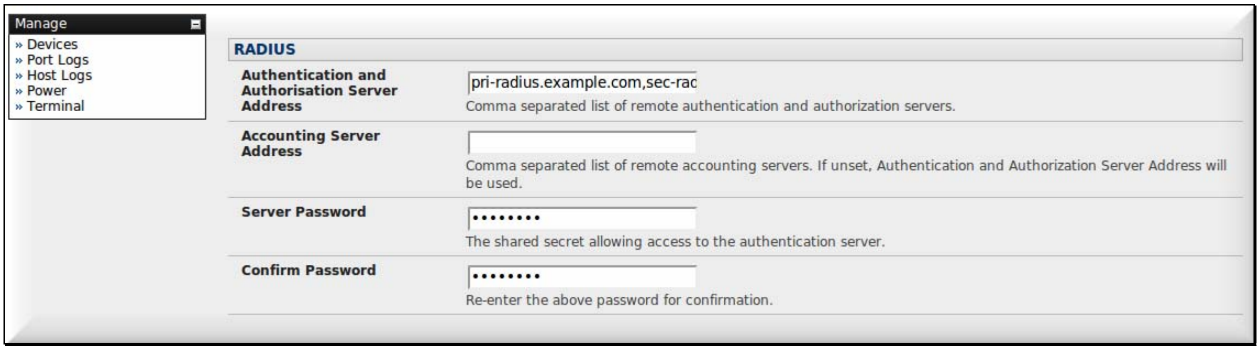
Select the **RADIUS** authentication method.

If remote group support is required, tick **Use Remote Groups**

Note: By default, only local permissions are used, so each RSA SecurID user must have a corresponding local user with the relevant permissions.

If you wish to use the RSA RADIUS server to provide Group Membership details, some of the RSA RADIUS server settings need to be modified. Please see Appendix.

Scroll down to the **RADIUS** section, and enter the RADIUS server details.



RADIUS

Authentication and Authorisation Server Address: pri-radius.example.com,sec-rac
Comma separated list of remote authentication and authorization servers.

Accounting Server Address:
Comma separated list of remote accounting servers. If unset, Authentication and Authorization Server Address will be used.

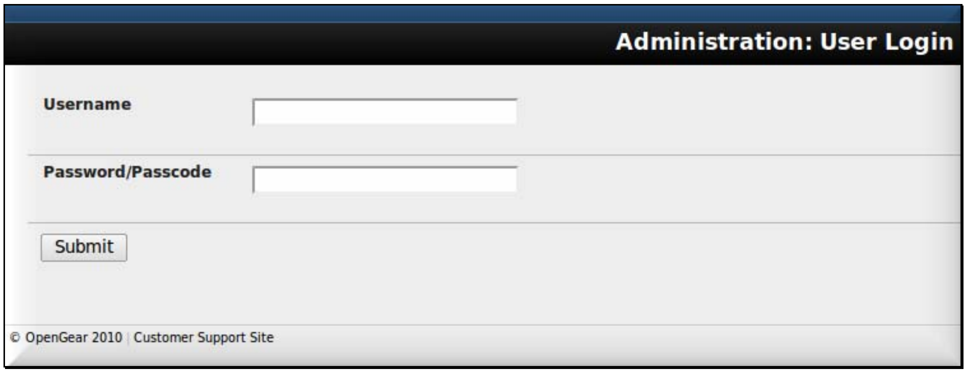
Server Password: ••••••••
The shared secret allowing access to the authentication server.

Confirm Password: ••••••••
Re-enter the above password for confirmation.

If more than one RADIUS server is entered, separate them with a single comma, with no spaces.

Scroll to the bottom of the page, and then click **Apply**.

Click the **Log Out** shortcut on the top of the page, and you should now be able to log in using an RSA SecurID token. Make sure that the user has Administration privileges, or they will not be able to access the Web UI.



Administration: User Login

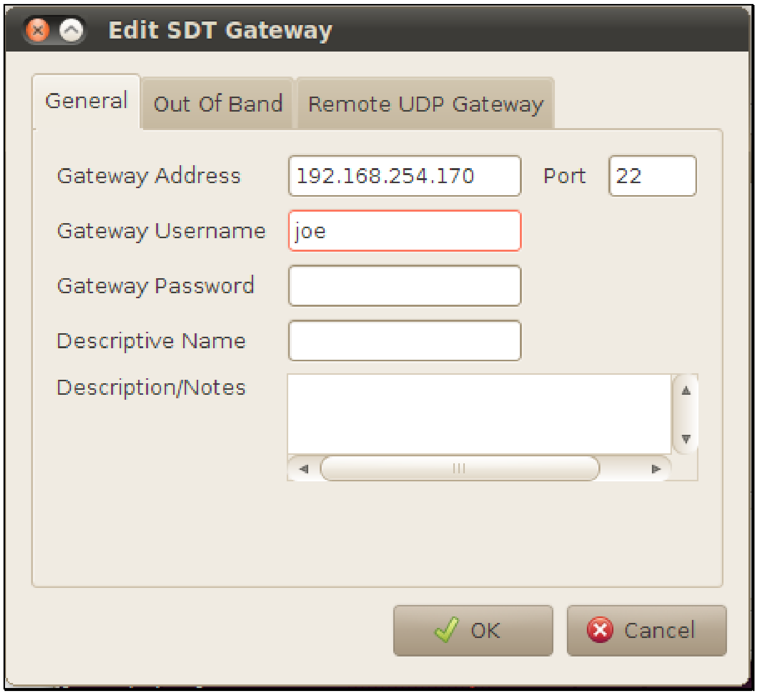
Username

Password/Passcode

© OpenGear 2010 | Customer Support Site

RSA SecurID Authentication can also be used for SSH and Telnet connections to the device.

If you choose to use SDTConnector, the only change to the usual setup you need to make is to not fill in a password in the SDT Gateway configuration. When you bring up a connection to a managed device, SDTConnector will prompt you for your token code.



Edit SDT Gateway

Gateway Address: 192.168.254.170
Port: 22
Gateway Username: joe
Gateway Password:
Descriptive Name:
Description/Notes:

Certification Checklist for RSA Authentication Manager 7.x

Date Tested: June 8, 2010

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1 SP2	Windows 2003
Opengear Console Server	3.2	Opengear µCLinux

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	✓
PIN Reuse	N/A	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	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A

BSD / PAR

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

Note: To enable the use of System Generated PINs via RADIUS, the RSA RADIUS server configuration needs to be modified. The following must be added to securid.ini in the [Configuration] section

AllowSystemPins=1

Appendix

Configuring RSA RADIUS Server for provisioning of remote groups

The Opengear Console Servers can receive a list of group memberships for a particular RADIUS user via the **Framed-Filter-Id** RADIUS attribute.

To enable sending these attributes, the RSA RADIUS server configuration must be modified to allow these attributes on Authenticate-Only requests.

In the **[Configuration]** section of **radius.ini**, add

```
AuthenticateOnly=0
```

For more information on this setting, see the RSA Authentication Manager RADIUS Reference Guide

Configuring RSA Authentication Manager for provisioning of remote groups

The Opengear Console Server expects the list of group names to be in the following format

```
:group_name=group1,group2,group3:
```

group1, **group2**, and **group3** are the names of local groups configured on the Console Server. The group list must be set as the contents of the **Framed-Filter-Id** attribute. If other devices require the attribute to have other values, append the group list to the end of the exiting content. For example:

```
other_content:group_name=group1,group2,group3:
```

See the Administering RSA RADIUS chapter of the RSA Authentication Manager Administrators Guide for information on assigning RADIUS user attributes.