RedSeal Installation and Administration Guide

Version 9.4.8

PATENTS:

Lloyd, Michael A., inventor; REDSEAL, INC., assignee. Method and system for evaluating access granted to users moving dynamically across endpoints in a network. US patent 9,325,719 filed October 27, 2014, and issued April 26, 2016.

Lloyd, Michael A., inventor; REDSEAL, INC., assignee. Method and system for evaluating access granted to dynamically provisioned virtual servers across endpoints in a network. US patent 9,325,741 filed February 27, 2015, and issued April 26, 2016.

Lloyd, Michael; Mayer, Alain Jules; Laing, Brian; inventors; REDSEAL, INC., assignee. Network security visualization methods, apparatus and graphical user interfaces. US patent 7,890,869 filed June 12, 2007, and issued February 15, 2011.

Lloyd, Michael; Mayer, Alain Jules; Laing, Brian; inventors; REDSEAL, INC., assignee. Methods and apparatus for prioritization of remediation techniques for network security risks. US patent 8,132,260 filed June 12, 2007, and issued March 6, 2012.

Lloyd, Michael; Mayer, Alain Jules; Laing, Brian; inventors; REDSEAL, INC., assignee. Methods and apparatus for determining network risk based upon incomplete network configuration data. US patent 8,307,444 filed June 12, 2007, and issued November 6, 2012.

Mayer, Alain Jules; Laing, Brian; Lloyd, Michael; inventors; REDSEAL, INC., assignee. US patent 8,321,944 filed June 12, 2007, and issued November 27, 2012.

Lloyd, Michael A.; Jackson, Cary D.; Durham, Jennifer Gates; Brenner, Ralph T.; inventors; REDSEAL, INC., assignee. Method and apparatus for assessing policy compliance of as-built data networks. US patent 8,479,257 filed August 7, 2009, and issued July 2, 2013.

Mayer, Alain Jules, inventor; REDSEAL, INC., assignee. Method and Apparatus for Network Wide Policy-Based Analysis of Configurations of Devices. US patent 7,003,562 filed September 17, 2001, and issued February 21, 2006.

Mayer, Alain Jules, inventor; REDSEAL, INC., assignee. Method and Apparatus for Network Wide Policy-Based Analysis of Configurations of Devices. US patent 8,135,815 filed November 8, 2005, and issued March 13, 2012.

DISCLAIMER: This publication (and any related software) is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This publication could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein, these changes will be incorporated in new editions of the publication. RedSeal, Inc., may make improvements and/or changes in the products and/or the programs described in this publication at any time.

In no event shall any portion of the software be disclosed (including posting and publishing) onto any public (i.e. non-private) software code sharing web sites or similar including, but not limited to, the following: GitHub, BitBucket, Google Code, Pastebin, Codeplex, LaunchPad, Unfuddle, JSFiddle, JSBin.

RedSeal, Inc.

Web:*http://www.redseal.net*

Email: info@redseal.net

Corporate Headquarters

1600 Technology Drive, 4th Floor

San Jose, CA 95110

Phone: 1-888-845-8169

1-408-641-2200

Contents

Chapter 1: Introduction

Chapter 2: RedSeal Appliance

Chapter 3: RedSeal Virtual Appliance

Chapter 4: Multiple network interfaces

Chapter 5: Client application

Chapter 8: Multi-Server Transport configuration

Chapter 9: Cluster configuration

Chapter 10: User accounts

Chapter 11: Security

Chapter 12: License administration

Chapter 13: Troubleshooting

Chapter 14: Command line interface

1

Introduction

The RedSeal system is a client-server enterprise application to manage the security profile of your networked assets. The application requires a valid RedSeal license. RedSeal software runs on a server and can also be deployed on supported virtual platforms.

Who needs this guide?

This guide is intended for experienced IT system administrators, network security officers and members of their organizations who will install and manage the RedSeal product. Knowledge of Linux or UNIX is helpful to manage the RedSeal appliance and virtual RedSeal instances.

RedSeal server

The server is a physical appliance that runs the application and stores the network database.

A variety of administrative tasks are performed on the RedSeal appliance through a command line interface (CLI) using a direct ethernet or VGA console connection or through an SSH session after the appliance has been configured and initialized through the console connection. See *Command line interface* on page 169 and *Administrative tasks* on page 63.

See *RedSeal Appliance* on page 19 for information about setting up the physical appliance.

See *RedSeal Virtual Appliance* on page 29 for information about deploying RedSeal on supported virtual appliance platforms.

Server Processes

The server processes are:

- admin server—provides administrative and infrastructure services to the several other processes that make up the RedSeal environment
- RedSeal server—manages the import of network device configurations, contains the analysis engine, and provides the database interface

RedSeal clients

Introduction

RedSeal data can be accessed two ways: (a) through a Java client application, and (b) through a legacy web application.

Open the user interface	From
Java client	`https://<redseal_server_IP>` Accept the license agreement, select a client option from the drop-down menu and click **Install Client (Recommended)**. This downloads an installation file that you run on your desktop. Follow the prompts. **Install Legacy Client** downloads the older version of the Java client installation, a Java Web Start-based client.
Web Legacy interface	`https://<redsealIPaddress>/redseal/a/login`, or select **Launch Web Legacy** from the Java client application launch page.

RedSeal documentation

RedSeal documentation is distributed in electronic format only. You can view PDFs from the Help menu in the client application. The online help in the client application is an HTML version of the user guide and is displayed in your system's default browser.

RedSeal may update documents at any time between software releases. You can obtain updated versions of documents on the support page: *https://www.redseal.net/services/#tech-suppport*.

For more information, contact *support@redseal.net*.

2

RedSeal Appliance

Introduction

RedSeal appliances are 1U devices and are configured with the same commands. Initial configuration involves passwords, network settings, and licenses.

Hardware specifications

You can view the data sheet for hardware specifications in the Resource Center at *http://www.redseal.net*.

Configure the appliance

Purpose

Use this procedure to perform the initial configuration of your RedSeal appliance.

Before you begin

If your appliance does not already have a valid license installed, obtain a valid license from support@redseal.net.

Procedure

1. Connect a VGA cable and USB keyboard to the back of the G5b appliance.
2. At the prompt, log in.

   ```
   cliadmin
   ```

   The cliadmin account:

- has access to the command line interface only
- does not appear in the **Manage user and accounts permissions** dialog in the Java client application

No password is required for the initial log in.

If your appliance does not already have a valid license installed, a message is displayed.

3. Set a password for the cliadmin user.

   ```
   set password cliadmin
   ```

   See *Passwords in the RedSeal environment* on page 63.

4. Set the date and timezone.

   ```
   set date ( MMddhhmm[[cc]yy][.ss]
   ```

   ```
   set timezone <REGION/CITY>
   ```

   See *set date* on page 198, *show date* on page 217, *set timezone* on page 212, and *show timezone* on page 223

5. Optionally configure the server to use one or two NTP time servers.

   ```
   set ntp primary <host_name|ip_addr>
   ```

   ```
   set ntp secondary <host_name|ip_addr>
   ```

   If you enable NTP, the time set by the NTP server overrides the time that is set manually.

6. If you want to configure a primary and secondary NTP server, you must configure a Key ID for both servers for sharing in the database. Key IDs can be 1 to 65534. Key values must conform to MD5 or SHA/SHA1 format.

   ```
   set ntp authentication symmetric add-key {MD5 | SHA | SHA1}
   <KEY_ID> <KEY_VALUE>
   ```

   See *set ntp authentication symmetric add-key* on page 206

7. Configure specific keys for the primary and secondary NTP servers.

   ```
   set ntp authentication symmetric configure-key trusted <KEY_ID>
   <IP_ADDR>
   ```

   See *set ntp authentication* on page 206 and *show ntp* on page 221.

8. Start the SSH process.

   ```
   enable autostart ssh
   ```

   You should start the SSH process even if you do not plan to leave it running on the appliance.

   Starting the process creates the DSA key required for SCP and SFTP used for moving log files and retrieving server images.

9. You can disable SSH access if it is not required.

   ```
   disable autostart ssh
   ```

10. If the appliance is connected to a device that is not set to auto-negotiate Ethernet speed and duplex, set the speed and duplex.

    ```
    set interface speed [ speed ( 10 | 100 ) ] [ duplex ( half |
    full ) ] [ autoneg ( on | off ) ]
    ```

    Auto-negotiation selects gigabit if available.

    See *set interface* on page 200

11. Set the appliance IP address manually or, if you use a DHCP server, enable DHCP.

    ```
    set ip dhcp
    ```

    This allows the server to obtain both an IPv4 and IPv6 address. RedSeal models IPv4 networks. An IPv6 address cannot be set using the CLI. Data collection from the IPv6 address of network devices is supported.

    To display the IPv6 address, select **View > System** in the Java client to display the **System Summary** window.

    See *set ip* on page 201 and *show ip* on page 219

12. If you want to use a DHCP reservation of a specific IP address, display the MAC address.

    ```
    show interface
    ```

    In the output, locate the MAC address on the line with the `ether` entry.

    ```
    ether 00:50:56:b3:34:42
    ```

    Give this address to your DHCP administrator, so they can configure the DHCP server to assign the appliance a static IP address, netmask, DNS server, and default gateway automatically.

    To configure multiple network interfaces on your RedSeal appliance, see *Configure the appliance with multiple interfaces* on page 23.

    Note The default hostname of a newly installed appliance is RedSeal. If the DHCP server assigns a hostname in addition to an IP address, the RedSeal server's hostname is set automatically and the `set hostname` command cannot be used to change it.

13. If you want to set a static IP address, DNS server, and default gateway instead of using DHCP.

    ```
    set ip <IP_ADDR> <NETMASK>
    ```

    ```
    set dns primary <IP_ADDR>
    ```

    ```
    set gateway <IP_ADDR>
    ```

See *set ip* on page 201, *show ip* on page 219, *set dns* on page 199, *show dns* on page 217, *set gateway* on page 199, and *show gateway* on page 217.

14. If your appliance does not already have a valid license installed, install it.

    a) On the machine being used as a console for configuring the appliance, use a text editor to open the file containing the license and copy the license text.

    b) On the RedSeal command line.

    ```
    set license
    ```

    When prompted, paste the contents of the license file into the command line and press `Ctrl+D` to install the license into the appliance. You can also upload the license from an FTP or HTTP server.

    See *set license* on page 201, *upload license* on page 230 and *Chapter 13, License Administration*.

15. Start the RedSeal server.

    ```
    startup server
    ```

    You are prompted to set the data password, which is used when encrypting data (such as for backups).

16. Enter the password you want to use for encrypting data. If you want to change this password after the server has started.

    ```
    set password data
    ```

    You are prompted to set the uiadmin password.

17. Enter the uiadmin user account password. This is the administrative account for the graphical user interface.

    See *Passwords in the RedSeal environment* on page 63

18. Optionally, you can restrict the Transport Layer Security (TLS) protocol version for browser-server communication to TLS 1.2. By default, the server allows TLS 1, 1.1, and 1.2. To restrict the server to TLS 1.2.

    ```
    set property server redseal.srm.nonfipsTLSVersions TLSv1.2
    ```

    See *set property* on page 209

    You are now finished with the initial configuration.

Configure the appliance with multiple interfaces

Introduction

Configuring RedSeal to use multiple interfaces allows you to isolate secure management networks from less secure data collection networks.

The RedSeal G5b physical appliance supports up to two Ethernet interfaces.

Dynamically adding or removing interfaces is not supported on virtual appliances. To add or remove interfaces on a virtual appliance, power off the appliance, make the changes through the virtual machine controller (for example VMware vCenter server) and then power the appliance back on.

RedSeal recommends using only static IP addressing to configure multiple interfaces. See *Chapter 4 Multiple Interfaces*.

Procedure

To configure RedSeal to use multiple interfaces, follow steps 1 to 10 as described in *Configure the appliance* on page 19 and then perform the steps in this procedure.

1. Configure the eth0 interface with a static IP address.

   ```
   set ip <IP_ADDRESS> <NETMASK_VALUE>
   ```

2. Set the IP address and enable each additional interface.

   ```
   set ip [INTERFACE] <IP_ADDRESS> <NETMASK_VALUE>
   ```

   For all commands where [INTERFACE] is an optional parameter, `<eth0>` is the default.

3. Set the DNS server.

   ```
   set dns primary <IP_ADDR>
   ```

4. Set the default gateway.

   ```
   set gateway [INTERFACE] <HOST_IP>
   ```

   INTERFACE is the interface being configured with the default gateway. For example, `<eth1>`.

5. If one of the interfaces needs to connect to a subnet that is not recognized by the default gateway, you must configure a static route for that interface.

```
add route <IP_ADDRESS> <NETMASK_VALUE> <GATEWAY> [INTERFACE]
```

A system can have only one default gateway. Since you cannot have a default gateway per interface, you must configure a static route for the interface you want to configure as a default gateway. For example, if you have two systems: 20.20.20.5 and 30.30.30.5 and you want all traffic for those systems to use gateway 10.10.2.1 on eth1, the route entries in the following routing table do not guarantee that traffic for 20.20.20.5 or 30.30.30.5 will take the 10.10.2.1 path:

Destination	Gateway	Genmask	Flags	Metric	Ref	Interface
0.0.0.0	192.168.1.1	0.0.0.0	UG	0	0	ETH0
0.0.0.0	10.10.2.1	0.0.0.0	UG	0	0	ETH1
10.10.2.0	0.0.0.0	255.255.255.0	U	0	0	ETH1
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	ETH0

Instead, you should configure static routes, as shown in the following routing table:

Destination	Gateway	Genmask	Flags	Metric	Ref	Interface
0.0.0.0	192.168.1.1	0.0.0.0	UG	0	0	ETH0
10.10.2.0	0.0.0.0	255.255.255.0	U	0	0	ETH1
20.20.20.0	10.10.2.1	255.255.255.0	U	0	0	ETH1
30.30.30.0	10.10.2.1	255.255.255.0	U	0	0	ETH1

192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	ETH0

When you are done, see steps 13 to 18 in *Configure the appliance* on page 19 to install a license and start up the server.

Ports required for access

Introduction

Certain ports are used on the RedSeal server by default. You must not block these ports on firewalls in the communication path.

Default ports

The table lists the default ports and their use.

Port	Use
22	SSH access to the CLI
3825 and 3826	RedSeal Java client-server communications using TLS
3835	Administrative tasks such as client and server logging using TLS
443	Installing the Java client, web-based reports, web-based API, and online help
10443	Certificate authentication
389	LDAP for data collection
636	LDAP over SSL (optional)
1812	RADIUS for user authentication

You can change the assignments to use different ports on the appliance using the `set port server` command. If you use non-default ports in your environment, unblock those ports instead.

See *set port server* on page 208 and *status* on page 226.

Troubleshoot the drive array

Purpose

Disk drive failure is indicated by a red Status LED on the on the front of the carrier and by the Overall Health Checks RAID status in the Java client application. Use this procedure to troubleshoot disk drives on the appliance.

Procedure

1. Verify the Status LED of the disk is red.
2. If the Status LED is indicates a failed disk, connect a VGA cable and USB keyboard to the appliance and reboot.

   ```
   reboot
   ```
3. Press `Ctrl+H` during boot-up to enter WebBIOS.
4. Press `Ctrl+N` to advance to a second screen which displays status of each drive.

   Possible statuses are:

   - Online—disk is operating normally
   - Rebuilding—hot-spare is copying information
   - Failed (or not listed)—call RedSeal technical support for a replacement

   If a drive is failed, replace it. If all disk drives are failed, contact *support@redseal.net*.

See *Replace a single disk drive* on page 26 and *Overall Health Checks* in the *RedSeal User Guide*.

Replace a single disk drive

Purpose

Replace a drive when there are indications it has failed. The appliance can be running when replacing a drive.

Details

Under normal conditions,the hard drive indicator light on the face of the appliance is green. If a single drive in the RAID array has failed, as indicated by a red Status LED or buzzing sound, replace it.

Procedure

1. Remove the failed drive and insert the replacement drive.

   The new drive is synchronized with the rest of the array. This rebuilding process might take more than an hour.
2. Verify the disk status is shown as `rebuilding` or `degraded`.

   ```
   status disk
   ```
3. After the disk completes rebuilding, verify the disk status is shown as `optimal`.

   ```
   status disk
   ```

   You can also verify disk status using the RAID controller utility.

See *Troubleshoot the drive array* on page 26.

3

RedSeal Virtual Appliance

Introduction

RedSeal software can be deployed on several virtual platforms.

Supported virtual platforms

RedSeal has verified the RedSeal Virtual Appliance installation on the following platforms.

- VMware ESXi™ Hypervisor version 6.0
- Microsoft Hyper-V Server 2016
- Oracle VM VirtualBox version 5.1
- KVM Virtual Machine Manager, libvirt, version 1.4.1
- Amazon EC2
- Microsoft Azure

Later versions of the supported platforms should work but have not been officially tested.

Virtual appliance sizing

The following is RedSeal's recommendation for provisioning virtual appliances for best performance and for minimum configurations. The recommendation that achieves best performance is based on the RedSeal G5b appliance. RedSeal suggests provisioning the same configuration or better for virtual deployments.

- Best performance—128 GB RAM and 8 processor cores

- Minimum configuration—64 GB RAM and 4 processor cores

Change disk space allocation on your virtual appliance

Purpose

Increase the allocated disk space on your virtual appliance after you install RedSeal and before you start the application.

Details

Before you start the RedSeal application on your virtual appliance, you can increase the allocated amount of disk space in the virtual appliance environment you are using. Although RedSeal software recognizes all the available CPU cores allocated to the virtual appliance, it is recommended to use 1–12 processor cores.

Procedure

1. In the virtual appliance environment, right click the RedSeal virtual instance, and adjust the hard disk entry and provisioned disk size.

   Note If you have less than 64 GB, RedSeal fails.

2. Start the RedSeal instance.

   When the virtual appliance starts, it detects the change in provisioned disk space and a prompt is displayed in the console asking if RedSeal should expand the file system to utilize the available space.

3. Choose **Yes**.

   RedSeal expands the file system to claim all the provisioned space and reboots.

4. Log in to the RedSeal CLI using the cliadmin account.

   At login, additional space is added to the data partition.

5. Verify that the additional space is added by running the `show support-summary | include data-data` command.

Deploy RedSeal on VMware ESXi

Purpose

To deploy RedSeal on VMware ESXi, follow these steps.

Before you begin

You must first install VMware ESXi™ Hypervisor software on the target host and obtain the .ova file from RedSeal.

Procedure

1. From the vSphere client, choose **File > Deploy OVF Template**.
2. Use the vSphere wizard to create the RedSeal appliance.
3. Locate the `.ova` file you obtained from RedSeal.

   The file should be in a location where the machine running the vSphere client can access it.

   Note When downloading the `.ova` file, the file might be identified as a `.tar` file. The operating system makes this change because the `.ova` file is a type of tar file. Let the download finish, then rename the `.tar` file using the `.ova` extension, and proceed.

4. Accept the RedSeal end user license agreement.
5. Name the VM instance that is being created.
6. Select a disk format.
7. Leave the **Power on** checkbox unselected so you can adjust the amount of disk space allocated to the virtual appliance after deployment but before the RedSeal server starts. See *Change disk space allocation on your virtual appliance* on page 30.
8. Start the appliance.

What happens next

Configure the appliance in vSphere. See *Configure the RedSeal appliance on vSphere* on page 32.

Configure the RedSeal appliance on vSphere

Purpose

You must configure the virtual appliance similar to how you would configure the physical appliance.

Details

When the RedSeal virtual machine is powered on in the vSphere console, a banner appears, followed by Linux start up messages, then an “rsva” login prompt. A series of “Press any key to continue” prompts display, which you can ignore. The process continues to the `rsva` prompt with user intervention.

Procedure

1. Log in as “cliadmin”.

   There is no password for this account at this stage of the configuration.

   The RedSeal appliance starts and automatically detects the difference between the default 64 GB disk and the new provision instructions you entered in the VM properties window. Advisory text displays that explains the consequences of expanding the file system, and a prompt asks if the expansion should proceed.
2. Answer `yes` to proceed.

   The file system expands, and the RedSeal appliance restarts. The `rsva` prompt reappears.
3. Log in again with as “cliadmin” without a password.

   Note If you did not expand the disk space when you deployed RedSeal as a virtual appliance, the `rsva` login prompt displays only once.

4. Set the cliadmin account password when you log in. For valid password naming, see *Passwords in the RedSeal environment* on page 63.
5. At the `RedSeal >` prompt, set a password.

   ```
   set password cliadmin
   ```
6. Assign an IP address to the appliance.

   ```
   set ip
   ```
7. Enable SSH on the appliance.

   ```
   enable autostart ssh
   ```
8. Close the vSphere console, and exit the vSphere client.

What happens next

Connect to the virtual appliance using SSH, and complete the configuration process. See *Configure the appliance* on page 19.

Deploy RedSeal on Hyper-V

Purpose

To deploy RedSeal as a Microsoft virtual appliance, follow these steps.

Before you begin

You must first install Microsoft Hyper-V software on the target host.

Procedure

1. Download the compressed RedSeal installer .zip file to a Hyper-V server and extract the files to obtain the`redseal_appliance.vdhx` file.
2. From the Hyper-V Manager **Actions** window, click **New** and choose **Virtual Machine** in the pop-up menu.

   The **New Virtual Machine** wizard displays.
3. Follow the wizard prompts.

   a) Name the appliance.
   The default is `New Virtual Machine`.

   b) Enable the **Generation 1** setting.

   c) Specify the amount of memory to allocate to the appliance. See *Change disk space allocation on your virtual appliance* on page 30.

   d) Specify the virtual switch to connect for networking, for example **Intel (R) Ethernet Connection (3) 12184M**.

   e) Enable the **Use an existing virtual hard drive** setting, and browse to locate the `redseal_appliance.vhdx` file you downloaded..

   f) Click to complete the new virtual appliance.

   A list of virtual appliance names displays.

   g) Start the appliance.

What happens next

Configure the appliance in Hyper-V Manager from the CLI. See *Configure the RedSeal appliance on Hyper-V* on page 34.

Configure the RedSeal appliance on Hyper-V

Purpose

You must configure the virtual appliance similar to how you would configure the physical appliance.

Procedure

1. Log in as “cliadmin”.

   There is no password for this account at this stage of the configuration.
2. Assign an IP address to the appliance.

   ```
   set ip
   ```
3. Set the default gateway.

   ```
   set gateway
   ```

What happens next

Complete the configuration process. See *Configure the appliance* on page 19.

Deploy RedSeal on VirtualBox

Purpose

To deploy RedSeal as a VirtualBox appliance, follow these steps.

Before you begin

You must first install Oracle VM VirtualBox software on the target host and obtain the `.ova` file from RedSeal.

Procedure

1. Use Oracle VirtualBox Manager to begin importing the appliance. You will need to locate the `.ova` file you obtained from RedSeal and open it.

The file should be in a location where the machine running the VirtualBox client can access it.

Note When downloading the `.ova` file, the file might be identified as a .tar file. The operating system makes this change because the .ova file is a type of tar file. Let the download finish, then rename the .tar file using the `.ova` extension, and proceed.

2. Reinitialize the MAC address of all network cards.
3. Import the appliance.
4. Start the appliance.

What happens next

Configure the appliance in VirtualBox similar to how you would configure the physical appliance. See *Configure the appliance* on page 19.

Deploy RedSeal on Red Hat KVM

Purpose

To deploy RedSeal as a Red Hat KVM virtual appliance, follow these steps.

Before you begin

Red Hat Enterprise Linux 7.6 or CentOS 1810 with Kernel-based Virtual Machine (KVM) 3.10.x, libvirt version 1.4.1 on the target host. You must also obtain a license key from RedSeal by contacting RedSeal Technical Support at *support@redseal.net*.

Procedure

1. Download the RedSeal .ova to the target host that is running KVM Virtual Machine Manager.
2. From the command line on the target host, unpack the `.ova` file.

   ```
   tar xvf <file_name>.ova
   ```

   Four additional files are created as part of the unpacking process:

   - `.ovf`
   - `.mf`
   - `.cert`

- `.vmdk` – this file is a virtual disk.

3. Convert the `.vmdk` file to a format compatible with Virtual Machine Manager.

```
qemu-img convert -f vmdk <file_name>.vmdk -O raw <file_name>.img
```

Note Use capital letter "O" for the `-O` option in the command.

The `.vmdk` file is converted and output to the `.img` file you specify.

4. Verify the `.img` file was created using `ls` to view a list of files.
5. Launch Virtual Machine Manager using your root password.

   The **New VM** window opens, which you use to create your new RedSeal Virtual Machine.
6. Choose the **Import existing disk image** option, and browse to the `.img` file you created with the `qemu-img` command.
7. Specify default setting **Generic** for both operating system type and version.
8. Choose RAM and processor cores.

   See recommendations for virtual appliance sizing in *System requirements* on page 241.
9. Type a name for the appliance, and set up networking for it either using the default, "NAT", or bridge the connection to the active interface.

   A RedSeal instance starts. When the boot process completes, the login prompt appears.

Configure the KVM appliance

Purpose

Use the short description to describe the purpose of the task.

Procedure

1. Log in as "cliadmin".
2. Assign an IP address to the appliance.

```
set ip dhcp
```

3. Verify the IP address the appliance is using.

```
show ip
```

4. Confirm connectivity between the appliance and the Red Hat host using `ping`.
5. Enable SSH on the appliance.

```
enable autostart ssh
```

6. Copy the contents of the license key text file you obtained in an email from RedSeal, and paste it at the prompt.
7. Verify the license was set.

   ```
   show license
   ```

   The RedSeal license properties are displayed.
8. Start the appliance.

   ```
   startup server
   ```

9. Open a web browser on the IP address of the RedSeal instance, and check the box in the client application launch page to accept the license.

Set up the Java environment on the target host

Purpose

If there are multiple Java applications running on the KVM target host, you must set up the RedSeal appliance to use the Java version RedSeal requires.

Details

More than one Java application running on the target host could interfere with the Java version the appliance requires.

Procedure

1. Download Java JDK version 8 to the `/opt` folder.

   ```
   curl -L -b "oraclelicense=a" -O http://download.oracle.com/otn-pub/java/jdk/8u191-b12/2787e4a523244c269598db4e85c51e0c/jdk-8u191-linux-x64.rpm
   ```

   Note Use capital letter “O” for the `-O` option in the command.

2. Unpack the Java installer .tar file using root privilege.

   ```
   tar xzf jdk-8u171-linux-x64.tar.gz
   ```

3. Change directories to the Java installer location.

   ```
   cd /opt/jdk1.8.0_171/
   ```

4. Verify the Java version that is currently running.

   ```
   java -version
   ```

5. If you will be switching between different Java versions, install Java using the `alternatives` command.

```
alternatives --install /usr/bin/java java
/opt/jdk1.8.0_171/bin/java 2
alternatives --install /usr/bin/javac javac
/opt/jdk1.8.0_171/bin/javac 2
```

6. Set up Java compiler and archive command paths.

```
alternatives –set jar /opt/jdk1.8.0_171/bin/jar
alternatives –set javac /opt/jdk1.8.0_171/bin/javac
```

7. Set up Java environment variables by adding the following commands to `/etc/bashrc`.

```
export JAVA_HOME=/opt/jdk1.8.0_171
export JRE_HOME=/opt/jdk1.8.0_171/jre
export PATH=$PATH:/opt/jdk1.8.0_171/bin:/opt/jdk1.8.0_171/jre/bin
```

Note If multiple versions of Java are installed on the KVM target, you must specify the absolute directory path for the Java version RedSeal requires.

8. Launch a browser to start the RedSeal appliance.

Deploy RedSeal AMI in Amazon EC2

Purpose

To deploy RedSeal Amazon Machine Image (AMI) in Amazon Elastic Compute Cloud (EC2), follow these steps. The Eastern Region is the only supported deployment region.

Before you begin

You must first generate an Amazon EC2 key pair, which you need to authenticate to your RedSeal instance. Refer to AWS documentation for information about how to generate key pairs for an Amazon EC2 instance.

Procedure

1. Log in to your AWS account, then select **EC2**.
2. In the search field at the top of the window, search for `RedSeal`.

   RedSeal Cloud Security Solution appears.
3. Click **Bring Your Own License**.

   The **Product Overview** page appears.
4. Click **Continue to Subscribe**.

The **Subscribe to this software** page appears.

5. Click **Continue to Configuration**.

   The **Configure this software** page apears.

6. Choose the appropriate region from the Region menu, then click **Continue to Launch**.

   The **Launch this software** window displays.

7. Choose the action **Launch from Website**.

8. Select an EC2 instance type.

   When choosing an instance type, consider your network performance requirements. The table displays RedSeal's recommendation for best performance and for minimum configurations. The recommendation that achieves best performance is based on the RedSeal G5b appliance. RedSeal suggests provisioning the same configuration or better for virtual deployments.

Deployment	Package size
Best performance	r4.4xlarge
Minimum configuration	r4.2xlarge

Note You cannot set an IP address when deploying a RedSeal AMI. You must use DHCP to assign an IP address. For details about how to set an IP address or hostname for your virtual RedSeal appliance, refer to AWS documentation.

9. If you have multiple VPCs, choose a VPC from the **VPC Settings** menu.

10. Select a subnet from the **Subnet Settings** menu. The subnets are availability zones within the region you chose.

11. Configure instance details as needed.

    Add Storage and **Tag Instance** settings are optional.

12. Choose a security group from the **Security Group Settings** menu. If you have a pre-configured security group that meets RedSeal's requirements, you can choose that group. Or, you can choose **Create New Based on Seller Settings** and create a new security group, which has open only the minimum required ports (22, 443, 3825, 3826, 3835). If you need the other default RedSeal ports open, manually create a new security group; see AWS documentation for details.

    The table lists default ports and how RedSeal uses them.

Port	Use

22	SSH access to the CLI
3825 and 3826	RedSeal Java client-server communications using TLS
3835	Administrative tasks such as client and server logging using TLS
443	Installing the Java client, web-based reports, web-based API, and online help
10443	Certificate authentication
389	LDAP for data collection
636	LDAP over SSL (optional)
1812	RADIUS for user authentication

13. Select a key pair.

    Your Amazon EC2 key pair is required for authentication to connect to your RedSeal instance.

14. Launch the instance.

What happens next

Configure the appliance in EC2. See *Configure the RedSeal AMI in EC2* on page 40.

Configure the RedSeal AMI in EC2

Purpose

You must configure the RedSeal AMI similar to how you would configure the physical appliance. SSH and DHCP are already enabled on the RedSeal AMI.

Procedure

1. Log in as “cliadmin”.

   The default cliadmin account password is `ch@ngeM3`.

2. At the `RedSeal >` prompt, set a password.

   `set password cliadmin`

   See *Passwords in the RedSeal environment* on page 63.

What happens next

Connect to the virtual appliance using SSH, and complete the configuration process. See *Configure the appliance* on page 19.

RedSeal VMs on Microsoft Azure

Introduction

You can run RedSeal on Microsoft Azure as a VM.

Requirements

- Only VHD images are supported.
- RedSeal provides you with a VHD file.

See *Upload RedSeal VHD on Azure* on page 41

Upload RedSeal VHD on Azure

Purpose

To upload RedSeal VHD in Microsoft Azure, follow these steps.

Procedure

1. Log in to your Azure Portal account and select **Storage Accounts**.
2. Select the storage account where you want to upload the RedSeal VHD file, called `Redseal_appliance.vhd`. The location you choose determines where the image is created and deployed.
3. From **Blob Service**, select **Containers**.
4. Select a container to upload the VHD to.
5. Click **Upload** and select the RedSeal VHD file.

   Make sure that the Blob type is set to **Page Blob**.

What happens next

Create an image using the Azure Portal. See *Create an image using the Azure Portal* on page 42.

Create an image using the Azure Portal

Purpose

To create an image from RedSeal VHD in Microsoft Azure, follow these steps.

Before you begin

You must first upload the VHD file. See *Upload RedSeal VHD on Azure* on page 41.

Procedure

1. Log in to the Azure Portal and select **Images**.
2. Click **Add** to create a new image. Make sure that the location for the image is the same as the location for your storage account.
3. Enter a name for the image.
4. In the **OS Disk** section, select Linux and the OS type.
5. On the **Storage Blob** field, click **Browse** and find the RedSeal VHD.
6. Click **Create** to start the image creation process.

   The image creation process can take several minutes to complete.
7. When the process has finished, go back to the Images panel and verify that the image was successfully created.

What happens next

Deploy RedSeal virtual machines in Azure. See *Deploy RedSeal Image in Azure* on page 42.

Deploy RedSeal Image in Azure

Purpose

To deploy RedSeal image in Microsoft Azure, follow these steps.

Before you begin

Create a RedSeal image using the VHD. See *Create an image using the Azure Portal* on page 42.

Procedure

1. In the Azure Portal, select **Images**.
2. Select the RedSeal image.
3. On the Overview panel, click **Create VM**.
4. On the Basics page:
   a) Enter a name for the new virtual machine.
   b) Enter a username, then select the **Password Authentication** type and create a password. This username and password will be used to log in to RedSeal.
   c) Click **OK**.
5. On the **Choose a Size** page, select a size for the virtual machine, then click **Select**.

   The recommended minimum sizes are 64 GB of memory and 4 CPU cores.
6. On the **Settings** page, configure the network settings, then click **OK**.
7. On the summary page, review your settings, then click OK to create the RedSeal image.

What happens next

Configure the RedSeal virtual machine. See *Configure the RedSeal Image in Azure* on page 43.

Configure the RedSeal Image in Azure

Purpose

You must configure the RedSeal virtual machine similar to the way you would configure the physical appliance, except you must set the password the first time you log in. SSH should already be enabled. If it is not, you can enable it.

Procedure

1. In the RedSeal instance, start a Serial Console from **Support + Troubleshooting > Serial Console**.
2. At the `rsva>` prompt, log in as cliadmin, and wait for the `RedSeal>` prompt to display.

You will ***not*** be prompted for a password.

3. At the `RedSeal>` prompt, set the cliadmin password:

   ```
   set password cliadmin
   ```

   See *Passwords in the RedSeal environment* on page 63.

   If SSH is not already enabled, you can set it to start automatically:

   ```
   enable autostart ssh
   ```

   ```
   startup ssh
   ```

What happens next

Connect to the virtual appliance using SSH and complete the configuration process. See *Configure the appliance* on page 19.

4

Multiple network interfaces

Introduction

Multiple network interfaces (NICs) are used to segregate data plane traffic and management plane traffic on RedSeal physical or virtual appliances. RedSeal administrators can isolate secure management networks from less secure data collection networks using multiple interfaces.

Interface roles

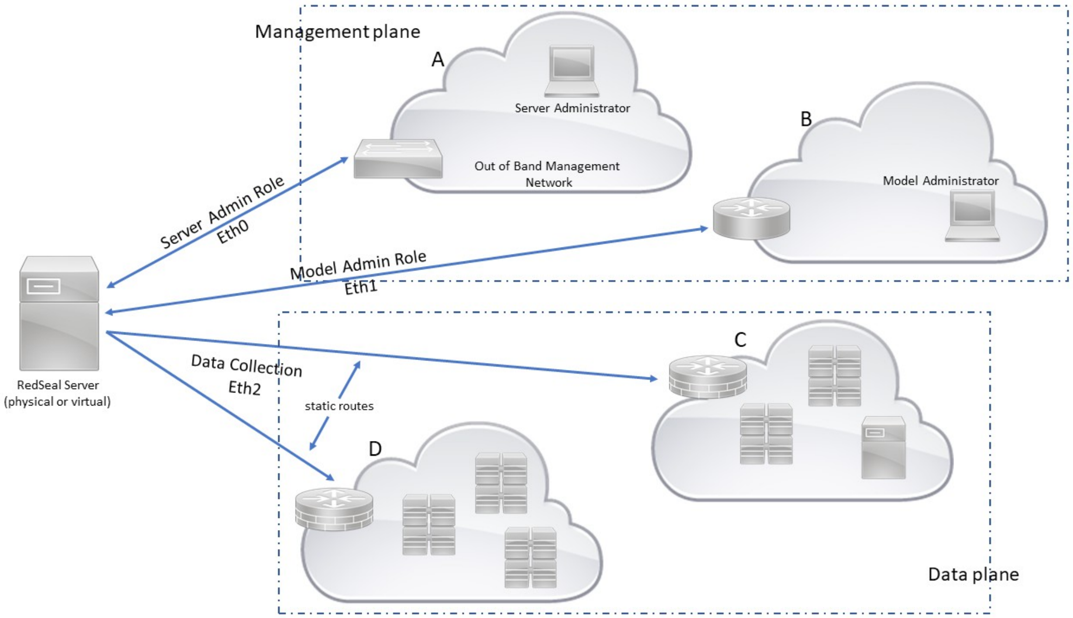
Interface Roles control which applications and services are allowed on each interface. Each network interface can have multiple roles. Interface roles are managed through the RedSeal CLI.

Each interface role supports different services. All roles are enabled on each interface by default.

Multiple interface example

In this example:

- the Server Admin role is configured on a dedicated eth0 interface to network A.
- the Model Admin role on the eth1 interface to network B.
- Data Collection is performed on networks C and D.



Multiple interface recommendations

Introduction

Consider the following recommendations before you configure multiple interfaces on a RedSeal appliance.

Use static routes

To ensure that your routes are not disrupted by system reboots or DHCP renewals, RedSeal recommends that you configure all interfaces with

- static gateway
- static IP addresses, and
- static routes for management and data collection.

Using a DHCP server to assign IP addresses for multiple interfaces and the default gateway could result in the following problems if a DHCP lease is renewed or if the system is rebooted,

- a default route is determined by the order in which each interface completes a DHCP transaction. The last DHCP transaction is the one that takes effect.
- a default route could change, which could result in some network segments becoming unreachable causing data collection tasks to fail.

Dedicate interfaces to Data Collection tasks

Data collection tasks communicate with devices configured in a data collection task profile to collect configuration and route information from a device. Whether an interface is used for data collection or not is determined by the routes to the devices contained in the various data collection tasks. If you do not want an interface to be used for data collection, you must ensure that routes configured in RedSeal to reach any of the devices in data collection tasks, point to different interfaces.

Important: It is essential that you configure routing to ensure that data collection traffic and data management plane traffic flow through the correct interfaces. RedSeal does reverse path forwarding checks, therefore only symmetric routing is supported.

At least one interface must have the Server Admin role

When adding and removing roles from interfaces, you must ensure that you do not remove the Server Admin role from all interfaces. Doing this locks you out of the SSH CLI session and you are no longer able to SSH into the appliance. However, you can still manage the appliance from the console through the CLI.

Add or remove an interface role

Purpose

Al interface roles are enabled on each interface by default. Add or remove roles as required.

Procedure

1. Log on the RedSeal appliance CLI.
2. Choose a command to use.

If you want to...	Then type the command...

Add a role to an interface	`add interface role <INTERFACE> (model-admin | server-admin)`
Remove a role from an interface	`remove interface role <INTERFACE> (model-admin | server-admin)`

3. View roles assigned to an interface.

```
show interface roles [INTERFACE]
```

Enable or disable an interface

Purpose

An interface is automatically enabled when you assign an IP address to that interface. You can then disable and re-enable that interface if required.

Procedure

1. Log on to the RedSeal appliance CLI.
2. Choose the command to use.

If you want to...	Then type the command...
Enable an interface.	`enable interface [INTERFACE]`
Disable an interface.	`disable interface [INTERFACE]`

3. View the status of an interface.

```
show interface
```

Add or remove a static route

Purpose

Add a static route to dedicate an interface to data collection tasks.

Procedure

1. Log on to the RedSeal appliance CLI.
2. Choose a command you want to use.

If you want to...	Then type the command...

Add a static route	`add route <IP_ADDRESS> <NETMASK_VALUE> <GATEWAY>`
	`[INTERFACE]`

Remove a static route	`delete route <IP_ADDRESS> <NETMASK_VALUE> <GATEWAY>`
	`[INTERFACE]`

3. View the status of the route you just configured.

```
show route
```

5

Client application

Introduction

Use the RedSeal client application to access and work with your RedSeal server. You can install and run the client application on Windows 32-bit or 64-bit, Mac OS X, or Linux. The client application is independent of the RedSeal server and is installed on a host through a web browser. To ensure security, the client application is packaged as a trusted application in a signed `.jar` file, signed with a class 3 code signing certificate from VeriSign or a Mac OS Developer ID with signing certificate.

Client installation requirements

To install the Java client

- the RedSeal server must be installed and running, and
- the web browser on the client host must have a direct, non-proxy, `http` or `https` connection to the server.

Client server connection requirements

To connect to and log in to the RedSeal server, the client and server versions must match.

Each user should have their own client install

Install individual clients for each user on the same client host.

Installing individual clients for each user identifies individual user activity in the RedSeal client application log. The client maintains separate properties and log files for each user.

Installing the client for individual user accounts requires logging into the host as each individual user and installing the client for that user account.

Install the client on Windows and Mac

Purpose

Install the client for each user on the host.

Before you begin

The RedSeal server must be installed and running.

The web browser on the client host must have a direct, non-proxy, HTTP or HTTPS connection to the server.

If you are using Mac OS, the Java (JNLP) client may not be able to read or write to files and folders on your local file system. You must grant Full Disk Access to the Java Web Start application. From System Preferences > Security & Privacy > Privacy > Full Disk Access, click Java Web Start. If Java Web Start does not appear in the list, you can add it from System > Library > CoreServices > Java Web Start.

Procedure

1. Log in to the client host as the user who will use the client.
2. Open a web browser and navigate to `http://<appliance_hostname_or_IP>` or `https://<appliance_hostname_or_IP>:443`

   When navigating to `http://<appliance_hostname_or_IP>`, the server automatically redirects to a Secure Socket Layer (SSL) `https` connection.

   If an untrusted connection warning appears, accept the server certificate. For information on addressing this condition, see SSL certificate.
3. Select and download the appropriate client installer.
4. Run the client installer file. A setup wizard appears.
5. Follow the prompts from the wizard to install the client.
6. On the Windows client installation page, use the default 1024 MB (1 GB) Java memory setting or select a different memory size option from the drop down. Skip this step for Mac installations.

3072 MB	64-bit
1024 MB	32-bit or 64-bit
512 MB	32-bit or 64-bit

7. When installation is complete, log out of the host.

Result

The RedSeal Java client is now installed for the selected user on the host.

What happens next

Log out of the host. If needed, log in as a different user and install the client for another user.

Install the client on Linux

Purpose

Install the client for each user on the host.

Before you begin

The RedSeal server must be installed and running.

The web browser on the client host must have a direct, non-proxy, HTTP or HTTPS connection to the server.

Procedure

1. Log in to the client host as the user who will use the client.
2. Open a web browser and navigate to `http://<appliance_hostname_or_IP>` or `https://<appliance_hostname_or_IP>:443`

   When navigating to `http://<appliance_hostname_or_IP>`, the server automatically redirects to a Secure Socket Layer (SSL) `https` connection.

   If an untrusted connection warning appears, accept the server certificate. For information on addressing this condition, see SSL certificate.
3. Select and download the Linux installer shell script.

4. Open a terminal and navigate to the directory where you downloaded the script; for example, `cd ~/Desktop/`.
5. Run the installation script, for example: `sh RedSeal_Client_Installer_\(unix\)_x_y_z.sh`.
6. Follow the installer instructions.
7. In the terminal, navigate to the directory where you installed the client, for example: `cd ~/RedSeal_Client/`.
8. Start the RedSeal client using the command `./RedSeal\ Client`.
9. When installation is complete, log out of the host.

Result

The RedSeal Java client is now installed for the selected user on the host.

What happens next

Log out of the host. If needed, log in as a different user and install the client for another user.

RedSeal and custom SSL certificates

Introduction

When you connect to the RedSeal server using HTTPS, an untrusted connection message may appear. This happens because the certificate on the RedSeal server is not signed by a Certificate Authority recognized by the browser.

Use the RedSeal certificate or set your own

You can

- have the browser accept the certificate provided by RedSeal, or
- install your own certificate in the RedSeal server.

For more information, see *SSL certificate* on page 144.

Set a custom Java memory size

Purpose

You can set a custom Java memory size, also called heap size.

Procedure

1. Find the location of the client `vmoptions.txt` file.

   For Linux and Windows, the file is in the RedSeal client installation directory.

   For Mac OS X, right-click on the client application and select **Show Package Contents**.

2. Edit the maximum memory usage as needed. Do not change any of the other attributes.

   ```
   # Enter one VM parameter per line
   # For example, to adjust the maximum memory usage to 512 MB,
   uncomment the following line:
   # -Xmx512m
   # To include another file, uncomment the following line:
   # -include-options [path to other .vmoption file]
   -Xms512m
   -Xmx1024m
   ```

3. Save and close the `vmoptions.txt` file.

Set network proxy connections

Purpose

The host on which the client is installed must have a direct network connection to the server. The RedSeal software will not work through a proxy. You can set network settings, including proxy settings, in the Java Control Panel or in the default web browser. By default, Java uses proxy settings obtained from the browser.

Procedure

1. Open your web browser.
2. Navigate to the network settings.

Refer to your browser's online help for instructions on finding the browser network settings.

3. Set the proxy connection to direct.

Uninstall the client

Purpose

Uninstall the client when you want to ensure that the client version is the same as the server version, for example when you have upgraded your server version.

Procedure

1. Delete the installed client.
2. Delete the directory where the client properties and logs are stored, for example `users/redseal`.

Using the client application

Introduction

You can use the same client software to connect to multiple servers as long as the client and server versions match.

Ensure the server is running

The client may not launch properly if the server is not running. If a Java error window displays on startup, ensure the server is running and try again.

Log in

When you launch the client, a log in window displays.

In the **Host Address** field, type the server's host name or IP address. Enter your user account ID and password.

Login messages

You can configure RedSeal to display an optional pre-login message whenever the client application starts. For more information, see “System Settings” in the *RedSeal User Guide*.

Client application timeout

You can configure the client to shut down after a specified period of inactivity. See “System Settings” in the *RedSeal User Guide*.

6

FIPS mode

Introduction

The RedSeal platform supports the Federal Information Processing Standards (FIPS). These standards ensure that all federal government agencies adhere to the same guidelines regarding security and communication.

In FIPS mode some encryption algorithms must be disabled, and certain others enabled. Once FIPS mode is enabled, certain functions may not be available on the Java Client. You must ensure that your browser supports FIPS cipher suites to be able to use RedSeal clients. When you enable FIPS mode on a RedSeal appliance

- the RedSeal server and client only use the RSA BSAFE library 6.1 for all cryptographic operations they initiate.
- all RedSeal client-server communication uses only FIPS-approved cipher suite SHA256.
- RedSeal allows TLS 1, 1.1 and 1.2 for browser-server communications and can be restricted to TLS 1.2 using the redseal.srm.nonfipsTLSVersions server property.
- the API and the reporting portal are restricted to a strong set of FIPS-approved cipher suites. Only browsers that support FIPS approved ciphers can be used.
- RedSeal uses FIPS-approved cipher suites and communication protocols to authenticate external users.
- RedSeal might not be able to communicate with products that do not support compatible protocol/cipher suites.

- SSH, SCP, and SFTP connections to SSH v1 servers and devices fail. Any data collection and backup tasks using these protocols fail in FIPS mode.

Protocols and cipher suites

Introduction

RedSeal uses TLS v1.2 for communication between the server and client processes. For browser-server communications, it allows TLS 1, 1.1 and 1.2, which can be restricted to TLS 1.2, see set property for details. All network access to the server is encrypted.

RedSeal client-server communication uses one of the following FIPS-approved ciphers:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

FIPS-approved ciphers for network-based access

Introduction

All network-based access with the server is encrypted through the use of Federal Information Processing Standards (FIPS)-approved ciphers.

Ciphers used in non-FIPS mode

In non-FIPS mode, RedSeal communication uses one of these FIPS-approved ciphers:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

Ciphers used in FIPS-mode

In FIPS mode, RedSeal communication uses one of these FIPS-approved ciphers:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

Enable or disable FIPS mode

Purpose

Enable FIPS mode on the RedSeal appliance to enforce the use of FIPS approved ciphers. Reboot the appliance after enabling ordisabling FIPS mode, restart alone is not enough to enable the feature.

Procedure

1. Log on the RedSeal appliance CLI.
2. Choose a command to use.

If you want to...	Then type the command...
enable FIPS mode	`set property server redseal.srm.fips140.mode true`
disable FIPS mode	`set property server redseal.srm.fips140.mode false`

3. Reboot the appliance.

7

Administrative tasks

Introduction

Administrative tasks on the RedSeal appliance are done by the default ***cliadmin*** user on the CLI and by the default client application user ***uiadmin*** on the Java client.

Administrative tasks in the RedSeal environment include:

- managing passwords
- importing or collection configuration data
- backing up and restoring data
- managing logs
- maintaining operating software
- enabling SNMP on your RedSeal server
- configuring smart card authentication for the ***cliadmin*** user

For more information about user management and permissions see *User accounts* on page 119.

Passwords in the RedSeal environment

Introduction

Password administration done from the CLI applies to the ***uiadmin***, ***cliadmin***, and ***data*** passwords. It does not apply to WEB user accounts created in the RedSeal Java client application.

RedSeal environments

RedSeal supports the NSS FIPS and DoDIN APL authentication approaches for three environments:

- client application administrative user ***uiadmin*** passwords.
- CLI administrative user ***cliadmin*** passwords
- encrypted data transfer ***data*** passwords

Change passwords

During the initial configuration of the RedSeal server, you create the ***cliadmin***, ***uiadmin***, and ***data*** passwords. To change these passwords, use:

- `set password cliadmin`
- `set password uiadmin`
- `set password data`

You are prompted for the current password, then the new password twice.

See *Enable password complexity* on page 65, *Enforce password history* on page 67, *Enable password expiration checking* on page 68, *Time limit to retry passwords* on page 67, and *Set password expiration interval* on page 68.

You can also reset the CLI password to the factory default state, see *Reset CLI password* on page 64.

Reset CLI password

Purpose

You can reset the CLI password to the factory default state.

Procedure

1. Power off your RedSeal server.
2. If your RedSeal server is a physical appliance, connect a VGA cable and USB keyboard to the back of the appliance. If your RedSeal server runs on a virtual machine, go to the next step.

3. Power on the server and monitor the startup messages that scroll up until you see the following message

   ```
   RedSeal O/S settings restore [OK]
   Type 'reset<enter>' to reset CLI password to factory default
   within 10 seconds
   ```

   You must type `reset` and press Enter within 10 seconds of this message displaying.

   The CLI password is reset and you can log in using the cliadmin user ID without a password as described in *Configure the appliance* on page 19. Resetting the CLI password to the factory default disables SSH. If you had enabled it, you need to re-enable it, see *enable autostart* on page 187.

Enable password complexity

Introduction

Password complexity refers to the set of rules enforced when setting a password. RedSeal supports password complexity for both the NSS FIPS and DoDIN APL protocols. RedSeal enforces NSS FIPS password requirements by default.You can also set a customized password length requirement.

Enable DoDIN APL password complexity

To set a valid password for ***uiadmin***, ***cliadmin***, and ***data***, your password string must conform to the applied rules.

To enable DoDIN APL password complexity.

```
set property server redseal.srm.strictPasswordCheck=true
```

To disable DoDIN APL password complexity.

```
set property server redseal.srm.strictPasswordCheck=false
```

To return to the default NSS FIPS password complexity rules, you may need also to reset the `min-password-length` command value.

Note These requirements only apply to passwords created since RedSeal 8.4.2 and do not apply to passwords established in earlier releases.

Enable custom password complexity

You can set a customized password length requirement of between 7 and 128 characters.

```
set min-password-length <value>
```

When the server property `redseal.srm.strictPasswordCheck` is enabled, you cannot set the `min-password-length` command to fewer than 15 characters.

Password requirements

The table lists password requirements for NSS FIPS and DoDIN APL passwords.

NSS FIPS	DoDIN APL
A minimum of seven characters	A minimum of fifteen characters
No spaces	No spaces
At least three of: • Numeric characters (0-9) that are not the last character of the password (for example, “PillinGton$4” is invalid) • ASCII lower case characters (a through z) • ASCII upper case characters (A through Z) that are not the first character of the password • Special ASCII characters, for example, punctuation marks • Non-ASCII characters, for example characters used in conjunction with pressing the `Alt` or `Ctrl` key	At least one: • Numeric characters (0-9) • ASCII lower case characters (a through z) • ASCII upper case characters (A through Z) • Special ASCII characters, for example, punctuation marks
The ***data*** password must not contain: + \ , : " < > #	The ***data*** password must not contain: + \ , : " < > #

See *Passwords in the RedSeal environment* on page 63.

Time limit to retry passwords

Introduction

By default, RedSeal allows three attempts to enter a valid password within a 15-minute period during login authentication.

Failed login attempts and remediation

After three failed attempts, RedSeal prevents you from logging in from the Java client, the Web-based GUI, and the cliadmin indefinitely. If a user exceeds the login retry limit, the cliadmin can unlock the account using the `enable user` command.

Enforce password history

Purpose

RedSeal provides password security by disallowing identical strings for several password generations for the ***uiadmin*** account. RedSeal does not enforce password history for the ***cliadmin*** and ***data*** passwords. You must set a different string for a definable number of password generations. RedSeal prevents you from setting a password that is identical to any of the strings you used within the defined number of password generations.

Procedure

1. To display the current password history policy.

   ```
   show property server redseal.srm.passwordCountUniqueInHistory
   redseal.srm.passwordCountUniqueInHistory = -1
   ```

   The default value for password history is inactive, indicated by the `-1` value.

2. To prevent a new password from being the same string as the current password.

   ```
   set property server redseal.srm.passwordCountUniqueInHistory = 0
   ```

3. To set the password history policy so that it enforces a number of unique passwords, set the value to an integer. For example, to enforce at least three unique passwords.

   ```
   set property server redseal.srm.passwordCountUniqueInHistory = 3
   ```

   See *Passwords in the RedSeal environment* on page 63.

Enable password expiration checking

Introduction

RedSeal enforces minimum and maximum intervals for passwords to remain valid. This applied to the ***cliadmin*** account, and to the uiadmin acccount only when logging into the Web user interface. By default, password expiration checking is not enabled.

Enable the check

To enable password expiration checking.

```
set property server redseal.srm.passwordExpiration=true
```

The password expiration checking feature:

- applies to both NSS FIPS and DoDIN APL when it is enabled.
- can only be enabled and disabled from the CLI.
- is not supported for data password and uiadmin-created users.
- applies to the uiadmin account when logging into the Web user interface, but does not apply when logging into the Java client.

See *Passwords in the RedSeal environment* on page 63 and *Set password expiration interval* on page 68.

Set password expiration interval

Introduction

When you create a password, RedSeal requires the password to be used for an amount of time you set in the minimum password expiration interval before you can change the password. Because of this requirement, exercise care when selecting a string for the password. You are not able to change it immediately.

Minimum and maximum password expiration intervals

A valid minimum password interval is one to 24 hours. The default is 24 hours.

To set the minimum password interval.

```
set property server redseal.srm.minPasswordLifetimeHours=hours
```

In addition, RedSeal enforces a limit to the maximum period a password is used. The maximum password interval is one to 365 days. The default is 365 days.

To set the maximum password interval.

```
set property server redseal.srm.maxPasswordLifetimeDays=days
```

If the maximum interval has elapsed, you are able to log in, but RedSeal requires you to change your password. RedSeal displays:

```
Password expired. 365-day maximum interval for password reached.
Please create a new password.
```

See *Passwords in the RedSeal environment* on page 63 and *Enable password expiration checking* on page 68,

Default password expiration settings

The table shows default values for password expiration.

Server Property	Description	Default
redseal.srm.minPasswordLifetimeHours	Minimum password interval	24
redseal.srm.maxPasswordLifetimeDays	Maximum password interval	365
redseal.srm.passwordExpiration	Password Expiration feature enabled	true

Note Do not set or change the cliadmin password and then enable password expiration (`redseal.srm.passwordExpiration=true`) within the minimum password interval (`redseal.srm.minPasswordLifetimeHours=hours`). If you do, you cannot log in using the cliadmin account until the minimum password interval has expired.

Data import

Introduction

RedSeal imports data from network devices to build a model of your network. Data is imported using manual file import or using a data collection task to import data from a device. RedSeal uses plug-ins to import device configurations and scanner data to build a model of your network. Refer to the ***RedSeal Data Import Plug-ins Guide*** for details about RedSeal plug-ins and how to use them.

Data collection is done from the **Data Import** dialog in the Java Client. Data can be collected directly from a device or scanner using a data collection task that includes the credentials required to log on to the device and retrieve the configuration information. Data can also be collected from an NCCM repository, an FTP server, or an HTTP server where the configuration files have been saved. You can use either method or a combination of both to collect data, depending on your network and operational requirements. RedSeal recommends that you run analysis after importing configuration data.

The method you choose depends on the network location of your RedSeal server. If you collect data from your network devices, RedSeal must be able to communicate with your network devices. If you collect data by importing configuration files, RedSeal must have access to your NCCM repository. See *Required ports for encrypted data exchanges* on page 143 for port access requirements.

Collection tasks can be scheduled to automatically collect the data on a regular basis, or they can be run on demand. You can increase the performance of data import tasks using the clustered import feature. See *Cluster configuration* on page 111 and *Enable or disable clustered import* on page 118 for information about configuring a cluster and enabling clustered import.

Data collection credentials

RedSeal uses authentication credentials to log into network devices to import data. The authentication credentials are created as independent objects that can be reused for multiple collection tasks if required. See

Import from devices

Importing data by connecting to individual devices provides an audit trail of collections and requires direct access to each device, including login credentials. Any collection exceptions must be resolved manually from the Java Client. The RedSeal administrator must add data collection tasks for any new devices that are added to the network and remove tasks for any decommissioned devices.

Import from repositories

Importing data from a repository requires the following criteria:

- The repository contains current configurations of all devices in your network including routers, firewalls, and load balancers.
- The repository is set up to ensure that collection exceptions, such as failure to collect a configuration, are handled.
- The repository is organized to allow per device type batch collections.

You must also set up an audit trail to satisfy operational and compliance requirements.

Set up a single data collection task to collect the same device configuration information from a directory that runs after the files in that folder have been updated.

If a collection task that imports multiple files encounters more than one file representing the same device, it imports only the most recent version of the device configuration file.

If multiple collection tasks gather data from a single directory at different times, only data collected by the last running task is imported.

If a collection task is delayed for some reason, you may not get the device configuration you want.

Force a data collection task

By default, RedSeal will not reimport a configuration if it has not changed since the last time it was imported into the RedSeal model. However, you may sometimes want to force an import operation even if the data has not changed. For example, you may have installed a plug-in update and you want the configuration to be parsed by the new plug-in. RedSeal's default behavior will not allow that unless you make some kind of a change to the configuration or, you modify the settings for data collection tasks to always update configurations. See *Data import system settings* on page 71 for more information.

Data import system settings

Introduction

The **System Settings > Data Import** page lets you configure general settings for data collection tasks such as omitting duplicate device configuration data, set how a timeout for device reponses, and which addresses to exclude from data collection. Each of the settings is described in the following sections.

Omit duplicates

The RedSeal server does not reimport device configurations if they are identical to the current RedSeal model and the plug-in version has not changed. The default setting is to omit any identical configurations.

There may be times when you want to force the import even when there is no change to the data. To force an update, select the **Always update configurations, even with no change in content or plugin** option.

Forcing a data import affects all plug-ins and devices for all every collection interval until the flag is reset. This can add to the time it takes to complete scheduled collections and this in turn could delay when analysis runs.

Device Response Wait Time

The device response time is the maximum amount of time RedSeal waits for a device to respond to a request sent during a data collection task when the communications method is either SSH or Telnet.

Some data import plug-ins require a two-way dialog with a device, which may require the user account represented by the credential to have administrative level privileges. Refer to the *Data Import Plug-ins Guide* for details about user authentication and communication requirements for specific devices.

Excluded Addresses

You can create lists of IP addresses to exclude as consideration as threat sources or to exclude from the network model entirely. You can exclude adresses individually or by range. Excluding adddresses may be useful in an organization where the same address range is used in multiple satellite locations, this allows RedSeal to model the entire network without triggering violations of RedSeal's Colliding IP Addresses model issue check. Refer to the *RedSeal User Guide* for more information about Model Issue checks.

RedSeal does not create objects for excluded addresses and they are not factored into the analysis of your network. After you add network addresses to the exclusion list, you must reimport the configurations for those devices.

If you exclude the address of a device that is the only device connected to a subnet, that subnet is removed from the model. If another device is also connected to the subnet, the subnet remains in the model.

If an excluded address is in a subnet that remains in the model, RedSeal continues to show access to and from the excluded address, since it is still a member of the subnet.

Multi Server Transport

Multi-Server Transport is used to transport all or some selected host data files from multiple data collecting servers to a central server. This feature is disabled by default. See *Multi-Server Transport configuration* on page 103 for how to enable and configure data import from multiple data collecting servers.

Manual data import

Introduction

Data about resources in your network can be imported manually from a repository to which device configurations have been written. This is done from the **Data Import** dialog in the Java Client.

The Java client must have access to the repository that contains your router and firewall configurations, and vulnerability assessment (VA) manager and scanner data files.

RedSeal reads the input files and and translates the data into objects defined by the RedSeal schema. ANy inconsistencies or unexpected data generates warning messages. These message are writtent o a log file and are displayed in the **Warnings** tab of the **Configuration Viewer**. Refer to the *RedSeal User Guide* for more information about the **Configuration Viewer**.

If errors occur during import, a status message is displayed in the lower right corner of the Java Client. After the import operation finishes, check the **Import Status** tab in the **Data Import** dialog for details. See *View data import status* on page 78.

Import a configuration file

Purpose

Import device configuration data from an NCCM repository, FTP server, or HTTP server.

Procedure

1. Select **File > Import** or click the **Network Devices** link in the RedSeal Model Status Panel on the **Home** tab on the Java Client.

The **Data Import** dialog displays with the **File Import** tab displayed.

2. Select a data type option to import the configuration file.

   The options are:

   - Auto-detect—select this option to allow RedSeal to determine the appropriate data type plug-in to use for importing the file based on the contents of the file.
   - L2 & L3 Devices—select this option to import configuration files from a specific type of device.
   - STIG/CIS—select this option to import a STIG or CIS module. For more information about RedSeal STIG modules refer to the *RedSeal STIG Modules* guide.
   - Scanner/Endpoint Details—select this option to import data from vulnerability scanners.
   - Other—select this option to import data other than device or vulnerability scanner files, for example TRL files.

3. Select a data type from the drop down menu below the data type options. If you selected auto-detect, the drop down menu does not contain any options as the RedSeal system determines which data type plug-in to use.
4. Locate the file directory in which to search for the files from the **Look In** drop down menu.
5. Select one or more files or use the **Get Multiple Files** options to find or exclude files in the designated directory and its subdirectories.
6. Click **Import**. Repeat this step for each data type as required.

   As each import operation completes, a status message is displayed in the lower right corner of the dialog. After the import operation completes, you can view details about each operation on the `Import Status` tab, see .*View data import status* on page 78.

Schedule data import

Introduction

You can create schedules for data collection tasks. Scheduling data collection tasks depends on various factors such as how you collect configuration information, either from a repository or directly from a device or vulnerability scanner and the amount of time it takes for RedSeal to analyze your network. The RedSeal server will not begin analysis while there are scheduled tasks underway or in the queue.

The following should be considered while scheduling data collection tasks.

Collection and analysis

You should set the interval between data collections at least long enough to allow for both collection and analysis to complete. You cannot calculate this interval in advance, you have to monitor the process and adjust your collection schedule accordingly.

Direct collection

If you collect directly from network devices and vulnerability scanners, the schedule should be based on the frequency at which changes are made to the device configurations. If your IT department implements a weekly change window, you should configure your collections to start just after the change window closes.

Indirect collection

If you collect configuration files from an NCCM repository, the data collection schedule should be set to coincide with the frequency and completion time of the repository's collection schedule.

Multiple collection tasks

If you have multiple collection tasks, schedule them to begin at the same time. The RedSeal server places all tasks in a queue to process them. The collected data is then parsed and processed. The processing time depends on the complexity of the configuration and the network.

Analysis is run when all tasks are completed and the task queue is empty.

Update the model

How and when collected data is integrated into the model depends on what the RedSeal analytical engine is doing when the collection task is run. The RedSeal server runs analysis automatically after each scheduled collection task completes, provided all queued tasks—either scheduled or manually triggered—have completed. If tasks are in the queue, analysis will be delayed until the queue is empty. The TRL collection task is not queued with other data collection tasks. Analysis runs whether or not the TRL collection task is complete.

If the network is small and the time interval between collection and analysis is sufficiently large to avoid overlap, the sequence of events is:

- data collection task runs
- newly gathered configurations and scanner results are imported into the network object model
- RedSeal analyzes the data

However, some networks are complex enough that collection and analysis each require hours to complete, and overlapping intervals make the sequence less clear.

If a collection task starts while analysis is in progress, new data will be gathered but it will not be included in the analysis currently underway. This newly acquired data is used to update the display of your network in the client interface. Devices appear on the topology and updated device configurations are accessible for such operations as calculating traffic vectors and detailed paths but the new data will not be used in the analysis.

If the TRL collection task starts while analysis is running, that task will fail.

As a consequence of running a collection task while analysis is underway, analysis is shown as outdated as soon as it completes.

Collect from a device or manager

Purpose

Use the Data Collection tab of the Data Import dialog to create and manage automated data collection tasks Create data collection tasks to collect configuration data directly from routers, firewalls, and vulnerability scanners, automatically at regularly scheduled intervals or on demand.

Procedure

1. Log on to the Java Client and select **Tools > Schedule Data Collection**.

   The **Data Import** dialog displays with the **Data Collection** tab selected.

2. Click **New** to create a new task.

   The **Data Collection Task** dialog displays with the Details tab open in the lower panel. This is empty until you select the data type for which to collect data.

3. Select a data type to determine which data import plug-in to use.

   The options are:

- Auto-detect—select this option to allow RedSeal to determine the appropriate data type plug-in to use for importing the file based on the contents of the file.
- L2 & L3 Devices—select this option to collect configuration from a router, firewall using a data type plug-in.
- Scanner/Endpoint Details—select this option to collect data from vulnerability scanners using scanner plug-ins.
- Other—select this option to collect data using plug-ins such as the TRL plug-in.

4. If you selected an option other than auto-detect, select a data type plug-in from the list to collect the data.
5. Select a communication method for selected data type plug-in. For details about which communication methods to use with a selected data type plug-in, refer to the *RedSeal Data Import Plug-ins Guide*.
6. Type the requisite information in the fields in the **Details** tab. The Details tab displays fields to create the data collection task once you select the communication method for the data type plug-in. These fields are unique to the selected data type and communication method. For information about these fields refer to the *RedSeal Data Import Plug-ins Guide*.
7. You can create a schedule for the task if you want it to run at specific intervals, or you can create the data collection task and run it on demand. To create a schedule click the **Schedule** tab and configure the settings per your requirements.
8. To configure a task to send an email to a predefined distribution list if the task fails. See *System Settings in the RedSeal User Guide* for details about configuring an email server.
9. Save the task. The task is added to the table on the **Data Collection** tab that lists all currently defined data collection tasks.

   Select a task and click on one of the buttons in the tool bar to edit, delete, or otherwise manage a data collection task.

Collect troubleshooting information

Introduction

It is now possible to run a data collection task in troubleshooting mode to collect logs and other relevant information to send to RedSeal Support to assist with troubleshooting data collection issues.

When you run a data collection ask in this mode, it sets log levels to DEBUG for the device and communication plugins used in the task. These logs and other relevant are bundled information into a ZIP file. This ZIP file can then be downloaded and sent to RedSeal Support to troubleshoot any problems that occur with data collection from that device or endpoint plug-in. See *Chapter 1* in the *RedSeal Data Plug-in Import Guide* for information about this feature.

View data import status

Purpose

You can check the status of data import tasks from the **Import Status** tab in the **Data Import** dialog.

Procedure

1. Log on to the Java Client and select **View > Data Import Status**.

   The **Data Import** dialog displays with the **Import Status** tab selected. The 50 most recent import operations are displayed. Each scheduled task is considered a single operation and is listed in the table only once. Each listing can be expanded to show user-defined number of records of previous collections.
2. Set the number of previous records to store in the Store [n] records per task field.
3. Use the Expand all or Collapse all buttons to expand or collapse nested records in the table.

   TRL upload is considered a single task with a single status regardless os how many times a new TRL is uploaded. There is only one TRL upload entry in the table.
4. To filter the contents of the table, click the filter icon on the upper right of the pane.
5. To export the table, click the green export arrow icon on the upper right of the pane. The table contents are exported as a tab delimited text file.
6. To see a list of computer systems affected by the collection, right-click a row and select **Affected Systems** from the menu. This menu item is disabled for manual collections through the **File Import** tab or device configuration import through the REST API.
7. To re-run a specific data collection task, select a row and click **Rerun**. You cannot re-run file imports.

Configuration import parser warnings

Introduction

When you open a device's configuration file to view **Model Issue** violations, the **Warnings** subtab shows errors that occurred when the device plug-in parsed the file. These warnings now provide the **Data Type**, the name of the plug-in; **Classification**, what part of the parser is generating the warning; and **Context**, which provides the cause and the remediation for the warning. You can control some of the types of warnings displayed using the `include_parser_warning_display` server property.

Parser warning types controlled by the server property

To choose parser warning types to display:

```
set property server include_parserwarning_display=none|
import,review,informational|all
```

You can use the server property to choose whether to display these warning types:

- REVIEW
- INFORMATIONAL
- IMPORT

Parser warning types that always appear

These parser warning types always appear, even if the server property is set to `none`:

- DEPENDENCY_MISSING
- EXTERNAL_ISSUE
- INCONSISTENCY
- UNSUPPORTED
- ERROR

Data accumulation

Introduction

The RedSeal server can accumulate a substantial amount of data in a relatively short period of time. The larger the network, and the more you use RedSeal's query tracking and modeling features, the faster the growth. RedSeal provides a data-purge facility to manage this growth.

RedSeal stores three different types of data:

- Data derived from device configurations—Each time you import configurations for network devices, either manually or by data collection tasks, network configuration data, such as NAT rules or access lists, are extracted and saved to the database as individual data objects (in addition to the configurations themselves, which are also stored as part of computer system network model objects).
- Query details—Access and threat queries flagged to be tracked in the Security Intelligence Manager are run each time you run analysis. Results are stored for later use in trend reports (in addition to trend data objects, consisting of data derived from these query results, stored as network model data objects).
- Network model data—Data objects are created for each computer system modeled in the RedSeal object model. In addition, when data is imported or analysis is run, new data objects are created for the results.

As this data ages, it becomes less significant and therefore can, and should, be purged on a regular schedule. The frequency of that schedule is dependent on how far back in time you want your trend reports to go; how large your network is (and therefore how fast you accumulate data); and the impact of your database size on RedSeal performance, especially related to the amount of time it takes to run analysis. See *Purge Data in the RedSeal User Guide* for more information on purging data.

Manual purge

You control when query and network model data becomes stale by setting age-out time periods in the System Settings dialog. This data is purged during the system's automatic purge process, or you can trigger the purge manually.

Automatic purge

Only current data is kept for data derived from device configurations. Data objects obtained from collections earlier than the most recent is purged daily, during an automatic purge. Purging the database removes data structures built by the RedSeal server for purposes of modeling the devices internally, not the actual device configurations.

Timing of the automatic purge is configurable by setting the frequency and time of day to run the task from the **Admin > Database > Configure Auto Database Purge** dialog. By default, this automatic purge occurs at 11 p.m. RedSeal servers running on machines that get turned off at the end of the day are presumed unlikely to be managing large, complex networks prone to the type of list growth the automatic purge is designed to control. However, if you notice persistently degraded performance whenever analysis runs, try leaving the computer on overnight periodically to allow this internal purge to take place.

Automatic purge will not run if analysis is running at the time the purge is scheduled. Coordinate your purge and collection schedules; analysis runs automatically after all queued data collection tasks have completed.

Stale hosts and devices

Stale data is data that has been in the system without being updated longer than a userdefined threshold. You can set different stale-data time periods for hosts and network devices. See *Stale Data and Purge Data in System Settings in the RedSeal User Guide* for more information.

These time periods should be synchronized with your data collection schedule. Data that has been marked stale should be purged regularly. Purging not only ensures that analysis results, and the reports that use these results, are based on the most current state of your network, it also is your only means of managing the size of the database.

The time span for devices should be set at three times the collection interval; for hosts, three times the scanning interval. If you collect configurations weekly, a device would be flagged as stale if its configuration were not seen again after three weeks, a host if it was not seen in a manager report after three weeks from the last time it was seen.

Log management

Introduction

The RedSeal system maintains multiple log files. All log files, except UI logs and Event logs are written to the appliance's hard drive.

Log types

- User interface log—Contains messages generated by the client application and is located on the host where the client is installed. If the client is used to connect to different RedSeal servers, the logs are maintained in individual client instance folders named after the server to which the client connected. For example, `C:\<user_home>\<redseal server name>/logs`. When the current client log file grows to 1 MB, a new log file is started, and the current log file is saved with a sequence number appended to its name. The sequence numbers indicate the chronological order of the rotated log files with 1 the most recent and 4 the oldest. RedSeal maintains four log files in addition to the current active file for a maximum size of 5 MB.
- Audit log—Contains messages recording all system configuration changes made in the client user interface and the CLI.
- Analyzer—Contains messages recording date, time, and details of each analysis event, including when the event started, when it finished, and whether it finished successfully or failed and why. The Analyzer log also records details of each data collection event, including date, time, name of the event, name of the credential used, the communication method used, method of execution (manual or scheduled), and detailed results.
- Server—Contains all log messages generated by a RedSeal server and database processes, including messages contained in the audit, analyzer and system logs.
- System—Contains detailed information about all system events, including server starts, stops, restorations, and license errors.

Configuration settings for all RedSeal logs, except the UI log, can be set in the Java Client or the CLI. See *set log* on page 202 for how to configure log settings from the CLI.

Log messages can also be sent to an external syslog server. Individual snapshots of logs can be saved to an SFTP, SCP, or FTP server from the CLI, see *save logfile* on page 196.

Configure log settings

Purpose

Use the Java Client to configure settings for all RedSeal logs, except the UI log. Log messages can also be sent to an external syslog server. Individual snapshots of logs can be saved to an SFTP, SCP, or FTP server.

Procedure

1. Navigate to **Edit > System Settings** and select the **Logging** tab.

   The **Logging** page displays.
2. In the **Configure Server Logs** panel, select one of the following log types, Audit, Analyzer, System, or Server. To configure Event logs see *Configure event log settings* on page 83.
3. Set the following options:
   - Log level—the default is INFO, you can change this per your requirements. Note that logs levels that generate a lot of messages consume disk space and could lead to your disk running out of memory.
   - Rotation size and frequency—the default is a rotation size of 50 MB. Rotation size must be between 1000 bytes and 1000 MB, if specifying in bytes, do not use the 'bytes' modifier, the system will add bytes. The frequency and size parameters are mutually exclusive. Logs are rotated on a set schedule or when the log file reaches a specified size.
   - Number of logs—this is the total number of log files to maintain before the first one is rolled over. The default is 5, including the current active log file.
   - Primary and Secondary Syslog Host—enter a valid IP address or a resolvable host name.
     - To change the default syslog port add ':port' to the end of the syslog server IP address or hostname.
     - To change the protocol from UDP to TCP, you must add the @ symbol in front of the IP address or hostname.
   - Syslog Facility—facility represents the part of the system sending the message. Refer to your syslog documentation for more information about syslog facility settings.
4. Click **Apply** to save your settings.

Configure event log settings

Purpose

Use the Java Client to configure settings for RedSeal event logs. Event logging is disabled by default, and if enabled, event logs must be saved to an external syslog server.

Procedure

1. Navigate to **Edit > System Settings** and select the **Logging** tab.

   The **Logging** page displays.
2. In the **Configure Server Logs** panel, select the Events log type. To configure other RedSeal logs see *Configure log settings* on page 82.
3. Add a syslog server, you can configure more than one if required. Enter a valid IP address of a resolvable host name.
   - To change the default syslog port add `:port` to the end of the syslog server IP address or hostname.
   - To change the protocol from UDP to TCP, you must add the `@` symbol in front of the IP address or hostname.
4. Set the syslog facility per your requirements. Refer to your syslog documentation for more information about syslog facility settings.
5. In the **External Syslog Events** panel, under **Event Messages** select the format to log events.
   - No events logged—default selection, no events are logged.
   - Use ArcSight CEF format—events are generated in ArcSight Common Event Format (CEF) format. The ArcSight CEF defines a syslog-based event format to be used by other vendors.
   - Use RedSeal format—events are generated as RedSeal log messages.
   - Use ArcSight LEEF format—events are generated in Log Event Extended Format (LEEF). LEEF is a customized event format for IBM Security QRadar.
6. Select one or more event types to be logged. The different Event types are:
   - **BestPracticesCheckEvent**—an event message sent for each Best Practice Check violation found during data import. The message identifies the device, the check, and date/time of violation, and severity:
     - HIGH—severity level is 5
     - MEDIUM—severity level is 3
     - LOW—severity level is 1
   - **HostMetricsEvent**—event message sent for each host found during analysis. The status message contains risk metrics and identifies whether the host is accessible from an untrusted subnet or has access to critical assets.

  - If RedSeal's risk value for the host is 0, severity level is 0
  - If RedSeal's risk value is greater than 0, severity level is risk/10
  - If RedSeal's downstream risk is greater than 0, severity is risk/10 plus 1 (to a maximum value of 10)
  - If RedSeal's downstream risk is greater than 0 and the host has access to resources in the Critical Assets group, severity is 10

- **ModelIssuesEvent**—event message sent for each model issue detected. A message identifies subnet, name of model issue, and the date/timestamp when the issue was detected. Severity levels are the same as for BestPracticeCheckEvents.
- **PolicyEvent**—event message sent when RedSeal analysis finds access between policy zones that is forbidden by policy rules; message identifies the policy, source and destination zones, and details of the rule.

  - If RedSeal shows policy compliance as Pass, severity is 0
  - If RedSeal shows policy compliance as Warning, severity is 5
  - If RedSeal shows policy compliance as Fail, severity is 10, except when Fail status is because of an overlap, severity is 5

7. Click **Apply** to save your settings.

View or download logs

Purpose

View or download logs from the Java Client or the CLI. The UI logs cannot be viewed from the CLI.

Procedure

1. In the Java Client, navigate to **View > Logs**.

   The **View/Download Log** dialog displays.
2. Select a type of log to view or download.
3. If there are more than one files available for that log type, select the one you want to view or download.

Delete logs

Purpose

Use the Java Client to delete all log files.

Procedure

1. Navigate to **Edit > System Settings**and select the **Logging** tab.

   The **Logging** page displays.
2. Click **Clear All Logs** to clear all UI, Audit, Analyzer, Server, and System logs.

Back up a RedSeal server

Introduction

RedSeal server data can be backed up from the Java client or the CLI. Data can be backed up manually or scheduled to run automatically. Backups can be scheduled only from the Java client.

Backup file data

The backup file includes the following:

- Analysis results
- custom Best Practices
- custom report definitions
- customized topology layouts
- data collection task definitions and credentials
- group definitions
- detailed path queries
- device deletion status
- imported device configurations
- imported VA scan data
- policy definitions (including approvals)
- report definitions

- results of all previous Analysis runs
- suppressions (Best Practices and vulnerabilities)
- topology layouts
- trouble tickets
- user accounts

The following are not included in the backup file:

- client-application configurable settings
- currently loaded TRL
- Java properties settings
- plug-ins

Analysis data

Network analysis data can be included or excluded from a backup file. Large complex networks can generate enormous volumes of data during analysis, which considerably increases the time to complete a backup operation. In such a scenario, it may be more efficient to exclude the analysis data from a backup file and then run analysis again after restoring the backup.

External data repositories

You can save your backup file to your local file system or an external FTP, SFTP, or SCP server. If backup files are saved to an external repository, RedSeal recommends SFTP instead of SCP or FTP, especially for files larger than 2 GB.

RedSeal cannot be configured to use a proxy server. The external repository where a backup file is to be saved must be directly accessible from the RedSeal appliance.

Backup from the Java Client

Purpose

Create a backup of your RedSeal appliance from the Java client.

Procedure

1. On the Java client, navigate to **Admin > Database**, select **Backup**.

The **Back Up Database** window displays.

2. Select the Local File or URL option to save the backup file.
3. Type a data password. Do not lose this password, which is required when you restore the file. For valid password naming conventions see *Enable password complexity* on page 65
4. The **Omit Analysis Data** checkbox is selected by default. Clear this option to include analysis data in the backup.

Backup from the CLI

Purpose

Create a backup of your RedSeal appliance from the CLI.

Procedure

1. Log on to the RedSeal appliance CLI.
2. On the appliance, back up your server data and provide a location to save the file. You can also choose to include or exclude analysis data in the backup. If your external repository requires authentication, include your credentials in the URL. You can specify a name for the back file otherwise the file is saved with a default name, which consists of the host name and a timestamp. See *backup* on page 178 for details about using this command.

   ```
   backup no-analysis ftp://<user_id>:<pwd>@<host>[:<port>]/<path>
   ```

3. If the external repository where the backup is to be saved does not have enough space, a message displays informing you about space requirements and any actions required to proceed with the backup.
4. Type a data password when prompted. The password is used to encrypt the file. Do not lose this password, which is required when you restore the file.

   The backup file is encrypted and saved to the specified location. If the external repository where the backup is to be saved does not have enough space, a message displays about space requirements and any actions required to proceed with the backup.

5. A SHA-512 checksum value is generated and displayed on the command prompt, once the backup file is saved to the external repository. Record this checksum value as it is required if you restore this backup file.

Scheduled backups

Introduction

Backups can be scheduled to run at a specified interval or to run after successful completion of data collection tasks. You can schedule automatic backups from the Java client but not the CLI.

Scheduled backups and Data Collection

When you schedule a backup to run after a data collection task, the backup schedule depends on the data collection schedule.

- If you schedule collection tasks to run daily and backups to run weekly, then the scheduled backup task runs once a week following the data collection task on that day.
- If you schedule collections to run weekly and backups to run daily, backups run once a week because the data collection tasks that trigger the backup occur only once a week.

Scheduled backups and Analysis data

Including or excluding analysis data determines when a backup starts.

- If backup includes analysis data, the backup starts after the analysis that follows a successful collection task.
- If backup excludes analysis data, the backup runs simultaneously with the post-data-collection analysis.

Schedule a backup

Purpose

Schedule a backup from the Java client.

Procedure

1. On the Java client navigate to **Admin > Database**, select **Configure Scheduled Backup**.

   The **Configure Scheduled Backup** window displays.

2. Select a frequency for the backup, then set the details appropriate for that frequency.
3. Type a URL destination to save the backup file. Backup files are saved as ENC files with a timestamp included in the file name. You can change the default file name if required.
4. Type a password for the backup file. Do not lose this password, which is required when you restore the file.
5. The **Omit Analysis Data** checkbox is selected by default. Clear this option to include analysis data in the backup. When you include analysis data, the backup starts after the analysis completes.
6. Save your schedule.

Schedule a backup after data collection

Purpose

Schedule a backup to run after data collection.

Procedure

1. On the Java client navigate to **Admin > Database**, select **Configure Data Collection Driven Backup**.

   The **Configure Data Collection Driven Backup** window displays.
2. Type a URL of the location where the backup file is to be saved.
3. Type a password for the backup file. Do not lose this password, it is required when you restore the file.
4. The **Omit Analysis Data** checkbox is selected by default, clear this option to include analysis data in the backup. When you include analysis data, the backup starts after the analysis completes.
5. Save your schedule.

View backup file details

Purpose

View details about the ten most recent backups including, file location, type of backup (manual or scheduled), the SHA-512 checksum associated with a backup file, and a timestamp of when the backup file was made.

Procedure

1. On the Java client navigate to **Admin > Database**, select **Show Recent Backups**.

The **Show Recent Backups** window displays.

2. Click the export icon to export the table to a tab delimited file.

Restore a backup to a RedSeal server

Introduction

RedSeal data can be restored from the Java client or the CLI. The RedSeal server process is automatically shut down during a restore operation. Any users logged on to the server are automatically logged off when the operation begins.

Access external repositories

Backup files can be restored from your local file system or an external repository such as an FTP, SFTP, HTTP, HTTPS, or SCP server. If files are retrieved from an external repository, RedSeal recommends using SFTP instead of SCP or FTP, especially for files larger than 2 GB.

RedSeal cannot be configured to use a proxy server. The external repository from where the backup file is to be retrieved must be directly accessible from the RedSeal appliance.

Restore from the Java client

Purpose

Restore a backup from the Java client.

Before you begin

Restoring the a backup file replaces all data on the RedSeal server to the state at which that backup file was created.

Procedure

1. On the Java client navigate to **Admin > Database**, select Restore.

   The **Restore** window displays.
2. Select Local File or URL to retrieve the backup file.
3. Type the data password associated with this file when prompted. This is the same password you typed when creating the backup file.

4. Optionally, you can type the checksum for the backup file that you are restoring. This is the checksum that was generated when this backup was created. The **Show Recent Backups** dialog contains a list of the ten most recent backups and the associated checksums for each backup. See *View backup file details* on page 90 to find the checksum for the backup file to be restored. If the checksum is not valid the data is not restored.
5. Click **Restore**. After the restore is complete, close and restart the Java Client.

Restore from the CLI

Purpose

Restore a backup from the CLI.

Before you begin

Restoring the a backup file replaces all data on the RedSeal server to the state at which that backup file was created.

Procedure

1. Log in to the CLI.
2. On the appliance, provide a URL location for the backup file to be restored and type the restore command.

   ```
   restore sftp://<user>[:<pwd>]@<host>/<dir>/<file>
   ```
3. When prompted, type the data password associated with this file. This is the same password you typed when creating the backup file.
4. Verify the checksum, type `yes`, then enter the checksum when prompted. This is the checksum that was generated when this backup was created. The **Show Recent Backups** window contains a list of the ten most recent backups and the associated checksums for each backup. See *View backup file details* on page 90 to find the checksum for the backup file to be restored. If the checksum is not valid, the data is not restored.
5. Restart the server when the restore operation is complete.

   ```
   startup server
   ```

Software updates and upgrades

Introduction

RedSeal periodically releases new versions of the RedSeal software, plug-in updates, and TRL updates. New releases of the RedSeal server software contain current versions of the plug-ins and the TRL current at the time of the release.

RedSeal server software upgrade

When you upgrade RedSeal software, the following information persists from one image to the next:

- Passwords and data for the ***cliadmin*** and ***uiadmin*** user accounts.
- The following appliance configuration settings
    - IP address
    - host name
    - DNS servers
    - default gateway
    - NTP server
    - time zone
- The following miscellaneous settings
    - ssh autostart status
    - syslog host
    - log levels

The RedSeal appliance can hold a total of two images. If you attempt to upload a third, an error message advises you that you cannot proceed. Delete one or more of the stored images before uploading the new one. See *delete image* on page 181 for information about how to use this command.

Upgrade RedSeal server from the Java Client

Purpose

Upgrade the RedSeal server using the Java client.

Before you begin

- Save the new RedSeal server image that you received from RedSeal Support to an SFTP, FTP, HTTP, HTTPS, or SCP server that is accessible from your RedSeal server or Java client.
- Back up your data before you upgrade or update RedSeal software.

Procedure

1. On the Java client navigate to **Admin > Server**, select **Upload Image**.

   The **Upload Image** window displays.
2. Select Local File or URL to locate the RedSeal image file.
3. Optionally, you can type the checksum for the image file you received from RedSeal. If the checksum is valid, a confirmation message displays, and the image uploads.
4. Click **Upload Image**.
5. Reboot the appliance to install the uploaded image.

Upgrade RedSeal server from the CLI

Purpose

Upgrade the RedSeal server from the CLI.

Before you begin

- Save the new RedSeal server image that you received from RedSeal Support to an SFTP, FTP, HTTP, HTTPS, or SCP server that is accessible from your RedSeal server or Java client.
- Back up your data before you upgrade or update RedSeal software.

Procedure

1. Log in to the CLI.
2. Upload the RedSeal image file from the location it was saved.

```
upload image
sftp://username:password@server//home/image<version>.enc
```

3. Reboot the appliance to install the uploaded image. See *upload image* on page 230 for details about using this command.

```
reboot
```

Rollback to a previous image

Purpose

To roll back to an earlier version of the software than the one currently installed on a RedSeal appliance, RedSeal recommends that you restore the network blueprint and configuration data appropriate to that version of the system software.

Before you begin

Make sure you have a backup of your server data for the version of the software to which you want to rollback. You need to restore this backup file after you roll back to the earlier version.

Procedure

1. View a list of the images available on the RedSeal server.

```
show images
```

2. Set the RedSeal server to use a specific image to install.

```
set next image <image_name>
```

3. Reboot the appliance to install the selected image.

```
reboot
```

4. Restore the backup file (consistent with the software version you rolled back to), after you reboot but ***before*** you start the server.

```
restore <filename>.enc
```

5. Start the RedSeal server.

```
startup server
```

Plug-in updates

Introduction

RedSeal periodically releases new or updated plug-ins. Plug-ins can be uploaded using the Java client or the CLI.

Plug-in versions

Plug-ins are implemented for specific versions of RedSeal software. A plug-in with a version number ***N.n.x*** should be used in an ***N.n*** version of the RedSeal software, where the ***N*** and ***n*** match in both server and plug-in version strings. For example, if you import an interim release of a plug-in versioned 9.0.x, when you upgrade the server to 9.1 you should also upgrade the plug-in to an 9.1.x version.

Plug-ins contained in new releases of the server software are the most current plug-in versions. Maintenance releases do not always contain the latest versions of the plug-ins. For example, plug-ins get updated when the release version increments from N.0 to N.1, but not when the software increments from N.n.0 to N.n.1.

Plug-in version IDs are included in the filename of the .jar file distributed by RedSeal and in the manifest file contained in the .jar file as ***Implementation-Version***. File names are subject to change, so the ID in the manifest file is the definitive identifier.

Always read the release notes carefully to determine plug-in status.

Update plug-ins from the Java client

Purpose

Use the Java client to update a plug-in file. A server restart is not required after a plug-in update.

Before you begin

- Save the new plug-in file to an SFTP, FTP, HTTP, HTTPS, or SCP server accessible from the Java client.
- Back up your data before you update the plug-in.

Procedure

1. On the Java client navigate to **Admin > Plugin**, select **Upload Plugin**.

   The **Upload Plugin** window displays.
2. Select Local File or URL to locate the plug-in and upload the file.

Update plug-ins from the CLI

Purpose

Use the RedSeal CLI to update a plug-in file. A server restart is not required after a plug-in update.

Before you begin

- Save the new plug-in file to an SFTP, FTP, HTTP, HTTPS, or SCP server that is accessible from the RedSeal server.
- Back up your data before you update the plug-in.

Procedure

1. Log in to the CLI.
2. Upload the plug-in file from the location it was saved.

```
upload plugin ( <SFTP_URL> | <SCP_URL> | <HTTP_URL> | <HTTPS_URL>
| <FTP_URL> )
```

TRL update

Introduction

RedSeal's Threat Reference Library (TRL), which maps known vulnerabilities to specific devices and applications is updated and published every week. Update the TRL from the Java client Home page.

New releases of RedSeal software contain the version of the TRL that was current at the time of that release. If you update the TRL on the server weekly, your current installation may contain a later version of the TRL than the new software you are installing. This could produce unexpected results when you run analysis again.

RedSeal recommends that you always update the TRL after upgrading your server.

Use SNMP with RedSeal

Introduction

You can access your RedSeal server from a remote host using Simple Network

Management Protocol (SNMP) v3 in an IPv4 or IPv6 network. SNMP is disabled by default.

Enabling or disabling SNMP

When you install RedSeal the first time or migrate to a new RedSeal version, you must create at least one SNMP user before SNMP can be enabled, see *Create an SNMP user* on page 98. With SNMP enabled, you can access objects stored in a Management Information Base II (MIB II) database. SNMP uses UDP port 161, which is closed when SNMP is not running.

Deleting all SNMP users disables the service, see *Delete an SNMP user* on page 99. You can also stop the SNMP service even when you have existing users, see *shutdown snmp* on page 233.

You can also set SNMP to start automatically when the system reboots, see *enable autostart snmp* on page 232 and *disable autostart snmp* on page 232.

Create an SNMP user

Purpose

SNMP is disabled by default on RedSeal systems. To use it, you must create at least one SNMP user to connect from your host. SNMP monitoring requires one or more SNMP users. Creating a user and starting the service enables SNMP. The service is disabled if there are no users. If you try to start SNMP without first having created an SNMP user, you are prompted to create one.

Procedure

1. Log on to your RedSeal server CLI console.
2. Type the following command and follow the prompts to create an authPRIV user. Authentication (MD5/SHA) and privacy (AES/DES) protocols are case sensitive.

   ```
   create user snmp
   ```

   Most of the profile information you provide when creating the user is also used with the `snmpwalk` command. See*SNMP commands* on page 231 for parameter descriptions for `snmpwalk` and other SNMP commands.
3. Type the following command at the prompt to start the service.

   ```
   startup snmp
   ```

   When SNMP is enabled and you want to create another user, you are prompted to stop the service. After you create the user, the SNMP service resumes.

4. To view a list of SNMP users, type the following command at the prompt

   ```
   show users snmp
   ```

5. To verufy that the SNMP service is running, type the following command at the prompt

   ```
   status snmp
   ```

Delete an SNMP user

Purpose

You can delete users when they are no longer needed. To modify SNMP user settings, you must first delete the user, then recreate the user with new settings. SNMP is disabled on the RedSeal system when all users are deleted.

Procedure

1. Log on to your RedSeal server CLI.
2. To view a list of existing users, type the following command at the prompt

   ```
   show users snmp
   ```

3. Identify the user to delete, type the following command at the prompt

   ```
   delete user snmp <user_name>
   ```

   Confirm the deletion. If there are no other SNMP users after the deletion, you are informed that SNMP is disabled.

Access RedSeal from your host

Purpose

After you enable SNMP, you can use a MIB browser or the command line to log into your RedSeal server to access network objects stored in the MIB.

Procedure

1. To connect using a MIB browser:
   a) Specify SNMP v3 in your MOB browser.
   b) Specify your RedSeal server as the target host.
   c) Provide the same credentials and authentication and privacy protocols as for the SNMP user you created on your RedSeal server.
2. To connect from the command line:
   a) Log on to your host.

b) Use the same credentials and authentication and privacy protocols as for the SNMP user you created on your RedSeal server. Type the following command:

On Windows:

```
snmpwalk -v3 -u <user_name> -A <auth_passphrase> -X
<priv_passphrase> -a { MD5 | SHA } -x { AES | DES } -l authPriv
<RedSeal_server_name>
```

On a Mac:

```
snmpwalk -v 3 -u <user_name> -l authPriv -a { MD5 | SHA } -A
<auth_passphrase> -x { AES | DES } -X <priv_passphrase>
<RedSeal_server_name>
```

Smart card authentication for cliadmin account

Introduction

CLI administrators can also log in using smart cards rather than the cliadmin password. Using smart cards for CLI authentication means you can revoke access for a single CLI user without having to change the shared cliadmin account password. RedSeal suppports CAC smart cards.

There is only one ***cliadmin*** account, which means everyone who uses the CLI must share the account and the account password. To revoke access for one user of a shared account, you must reset the cliadmin password. To avoid having to give the cliadmin password to all CLI users, you can associate each user's smart card certificate with the cliadmin account, so that each person uses their own smart card to authenticate to the CLI. Then, if you want to revoke a user's access, you only need to disassociate that one smart card from the cliadmin account.

Associate smart card certificate with cliadmin account

Purpose

Associate a smart card certificate with the cliadmin account to enable smart card authentication.

Procedure

1. Copy the SSH keystring from the smart card, or have the card user copy the SSH keystring and send it to the RedSeal administrator. See below for details.

a) On the computer where the RedSeal client application or web application will run, save the smart card certificate's SSH key string.

- On Windows, use PuTTY-CAC.
- On Mac OS X, have opensc installed and find the keystring using a terminal window.

2. Add the SSH keystring to the cliadmin account. See below for details.

a) Log on to the RedSeal CLI.

b) From the CLI, use the command

```
add credential cliadmin
```

c) Paste the user's SSH keystring at the prompt.

8

Multi-Server Transport configuration

Introduction

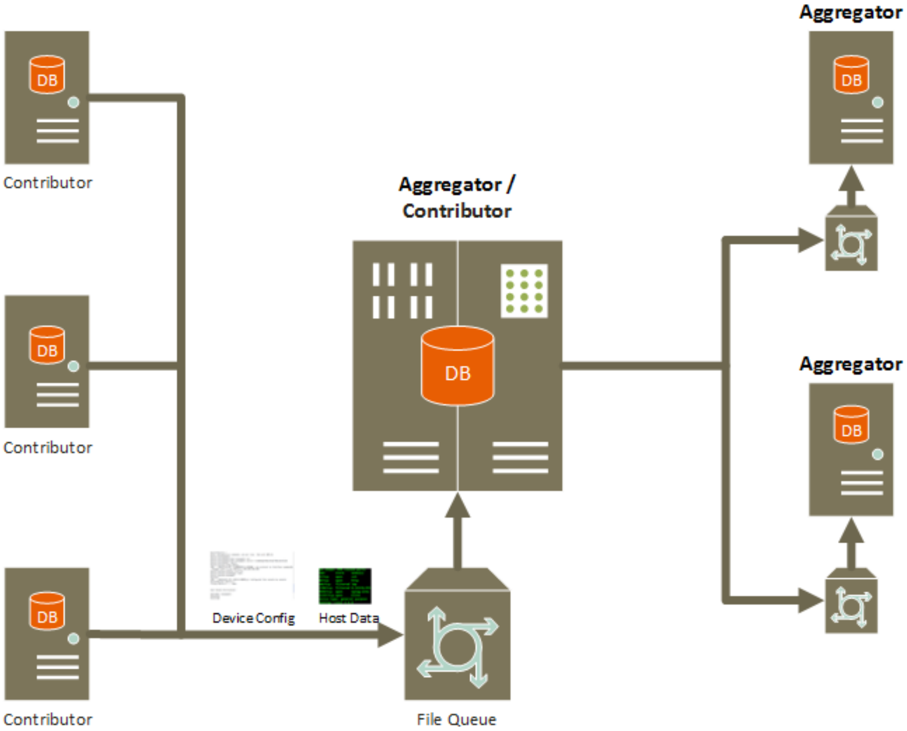
Multi-Server Transport (MST) is used to perform distributed data collection in a segmented network. It allows configuration data and host data files imported by one or more RedSeal servers, each with their own database, to be replicated on a remote RedSeal server. Remote in an MST environment means the server is inaccessible in the network. It does not refer to geographic location.

Server roles in MST

In the MST environment, data collecting servers are called Contributors, and remote servers to which data is transported are called Aggregators.

An Aggregator's role can change to Contributor, or it can serve as both if it is configured to transport data to other remote servers.

The diagram shows the data flow between servers in an MST configuration. (1) Contributors transport data to an Aggregator using a data collection task. (2) Transported files are queued on the Aggregator. (3) A Multi-Server Transport collection task created on the Aggregator imports queued files to the server's database. (4) This model can be extended to transport data from Aggregators to other remote servers, where the Aggregator then acts as a Contributor.



Data transport using the API

Data can also be transported using the `data/multi_server_transport` API. For more information, see the *RedSeal API Guide*.

Aggregating data using Multi-Server Transport

Purpose

Use MST when you want to export configuration and host data files to a remote server.

Details

“Remote” does not necessarily refer to the geographic location of a server. “Remote” in the MST environment means access to a server is blocked within a segmented network. Configure MST on the Contributor and Aggregator using the RedSeal client application.

On the	set the	in
Contributor	transport option	**System Settings > Data Import** **Transport all collection task data** transports all imported device data to the Aggregator. **Transport data from selected collection tasks** transports imported data from selected tasks to the Aggregator. When selected, you must enable transport settings on individual transport tasks.
	remote server IP address and credentials	**System Settings > Data Import > Add** Credentials must have Model or Admin privileges.
Aggregator	Data Collection Task	**Tools > Schedule Data Collection > New** Set **Data Type** to **Auto-detect** and select the **Multi-Server Transport** communication method. This task imports queued files to the Aggregator’s database.

Set up the Contributor to transport data

Purpose

Set up the Contributor to transport configuration data and host files to a remote server.

Procedure

1. From **System Settings > Data Import**, choose a transport setting in the **Multi-Server Transport** pane.

   Transport all collection task data transports all imported data to a specified server.

   Transport data from selected collection tasks transports imported data from collection task(s) you specify. When selected, you must enable the transport setting for individual tasks.

   Choosing either option enables Multi-Server Transport.

2. Click **Add** to specify the remote server.

   The **Add Remote RedSeal Server** window opens.

3. Type the remote server IP address or host name, and choose a credential.

   Credentials must have Model or Admin privilege. To add a new credential, click the **Add** icon next to the **Credential** field.

4. Click **Add** in the **Add Remote RedSeal Server** window to save remote server information.

   The remote server IP address appears in the table with credential privilege. When a collection task runs, the transported data is added to the queue on the Aggregator.

What happens next

1. If you enabled **Transport data from selected collection tasks** option, edit individual collection tasks to enable transport. See *Enable transport for only selected collection tasks* on page 107.

2. Set up the remote server, or Aggregator, to import queued data to its database. See *Set up the Aggregator to import queued files* on page 108.

Enable transport for only selected collection tasks

Purpose

Edit a collection task on the Contributor to transport its data to an Aggregator.

Details

You only need to edit individual collection tasks if you enable the **System Setting > Data Import > Transport data from selected collection tasks** setting.

Procedure

1. From **System Settings > Data Import**, choose **Transport data from selected collection tasks**.
2. Choose **Tools > Schedule Data Collection**.

   The **Data Import** window opens.
3. Select the collection task with the device data you want to transport, and click the **Edit** icon.

   The **Data Collection Task** window opens
4. Open the **Transport** tab and enable the setting labeled **Transport configuration data associated with this task to remote RedSeal servers**.

   When you save the setting, the collection task in the table is marked **Yes** in the **Transport** column in the **Data Import** window.

What happens next

Set up the Aggregator to import queued data to its database. See *Set up the Aggregator to import queued files* on page 108.

Set up the Aggregator to import queued files

Purpose

When device configuration data or host files are transported, they are queued internally on the Aggregator. You must create an MST data collection task on the Aggregator to import queued files to its database.

Procedure

1. From **Tools > Schedule Data Collection**, click **New**.

   The **Data Collection Task** window opens.
2. Set Data Type to **Auto-detect**, select **Multi-Server Transport** as the communication method, and set the schedule.

   The collection task appears in **Data Import** window.

Result

When the task runs, configuration data and host files are imported into the Aggregator's database.

Clear files queued on the Aggregator

Purpose

On the Aggregator, clear queued files when data exported by a Contributor is not needed, such as data sent to test the MST setup.

Procedure

1. From **System Settings > Data Import**, in the **Multi-Server Transport** pane, click **Clear File Queue**.

Disable Multi-Server Transport

Procedure

1. From **System Settings > Data Import**, choose **Disabled** in the Multi-Server Transport pane.

9

Cluster configuration

Introduction

In a cluster configuration, a single RedSeal server, called a datahub, can distribute its tasks to multiple RedSeal servers, called spokes, to add processing power for such tasks such as network modeling, data collection, and analysis. Servers in a cluster configuration share one database, which resides on the datahub.

Cluster configuration recommendations

When configuring a cluster datahub, RedSeal recommends that you have

- all servers belong to the same subnet, and
- a 1 GB full-duplex on a local switch.

Minimum hard disk space requirements

Ensure you have the minimum hard disk space requirements before deploying a RedSeal server cluster.

- Datahub—1 TB (for example, a G5b appliance)

- Each spoke—64 GB

Requirements for cluster datahub and spoke ports

Statement

For the specified ports, ensure that they are open in the hub and spokes and that environmental network access controls (firewalls and routers) permit communication between the hub and spokes over the ports (all TCP).

Specified ports

Port	Use
5432 — JDBC/TLS	Encrypted data channel used by a spoke to read and write to the central database at the datahub.
3826 — JMS/TLS	Encrypted channel used to distribute work items. A spoke connects to the datahub over that port for work orchestration.
3835 — RMI/TLS	Encrypted channel used by the datahub and spokes for cluster administration, such as health and status monitoring, and upgrades.

Change the data password in the cluster setup

Purpose

Before configuring a cluster, you must set the data password on the datahub and each spoke.

Details

If you do not set the datahub password on each spoke, the password change on the datahub results in disconnected spokes.

When you start up a disconnected spoke, you are prompted to enter the new data password and verify that it matches that of the datahub.

Procedure

1. Set the data password on the datahub.

   ```
   set passsword data
   ```

Configure a cluster datahub and spokes

Purpose

Use the cluster feature to increase the performance of RedSeal's analysis and clustered import tools.

Details

Configure the cluster datahub and spokes using the command line interface (CLI) of each RedSeal server, but use the RedSeal Multi-Server Manager (RSMM) for overall RedSeal cluster visualization, management, and monitoring. See the *RedSeal Multi-Server Manager User Guide* for details related to server operations including software updates, server inventory management, logging, and security monitoring.

Before you begin

Before configuring a cluster datahub, you must

- set your data password
- ensure all RedSeal servers in the cluster are running the same software image, and
- ensure all RedSeal servers are configured for the same time zone and date.

If you need to set or change your data password, see *Change the data password in the cluster setup* on page 112.

Procedure

1. Log in to a RedSeal server that you want to configure as a datahub in a cluster.

   Only one server can be configured as a datahub.
2. On the datahub, add the spokes.

   ```
   add spoke <IP ADDR>
   ```

   Adding the first spoke converts a standalone server to operate in Cluster mode.
3. On each spoke, set up the datahub of the cluster.

   ```
   set datahub <IP_ADDR>
   ```

   If your data password was not set up on the spoke or if it does not match that of the datahub, you will be prompted to enter and verify the data password of the datahub.

   CAUTION When setting up datahub spokes, a warning message displays and the local database will be disabled. Any local data will be unrecoverable.

   This command shuts down the server.
4. From separate sessions on each spoke of the cluster, start the server.

   ```
   startup server
   ```

Verify the datahub from the spoke

Purpose

To verify that the datahub is enabled and running, check the datahub identity and the spoke status.

Details

If you are logged in to a spoke, you cannot view the identity of other spokes configured in the cluster.

Procedure

1. Log in to the server spoke.
2. View the identity of the datahub.

   ```
   show datahub
   ```
3. Verify the datahub is enabled and running.

   ```
   status all
   ```

   This example shows a server configured in Datahub mode:

```
admin                auto enabled    tcp 3835    running
server (datahub)     auto enabled    tcp 3825    running
server-jms           auto enabled    tcp 3826    running
server-http          auto enabled    tcp 80      running
server-https         auto enabled    tcp 443     running
server-https-cert    auto disabled   tcp 10443   not running
db                   auto enabled    tcp 5432    running
ssh                  auto enabled    tcp 22      running
snmp                 auto disabled   udp 161     not running
```

Add a spoke to an existing cluster

Purpose

Add a RedSeal server spoke to a cluster to share processing power with other spokes in the cluster.

Procedure

1. Log in to the RedSeal server that you specified as a datahub.
2. Add a spoke.

   ```
   add spoke <IP_ADDR>
   ```
3. From the newly added spoke, set up the datahub.

   ```
   set datahub <IP_ADDR>
   ```

   CAUTION When setting up datahub spokes a warning message will be displayed and the local database will be disabled. Any local data will be unrecoverable.

   This command shuts down the server.
4. Start the server.

   ```
   startup server
   ```

Manage the cluster

Purpose

View information about the cluster, including a list of connected spokes and processes that are currently running on them.

Details

You can view all connected spokes only from the datahub.

Procedure

1. Log in to the datahub.
2. Display the status of the datahub.

   ```
   show datahub
   ```

3. View a list of IP addresses of all the spokes in the cluster.

   ```
   show spokes
   ```

4. Display the status of the datahub. The datahub should be enabled, running, and communicating with its spokes.

   ```
   status all
   ```

   This example shows a server configured in Datahub mode:

   ```
   admin                 auto enabled    tcp 3835    running
   server (datahub)      auto enabled    tcp 3825    running
   server-jms            auto enabled    tcp 3826    running
   server-http           auto enabled    tcp 80      running
   server-https          auto enabled    tcp 443     running
   server-https-cert     auto disabled   tcp 10443   not running
   db                    auto enabled    tcp 5432    running
   ssh                   auto enabled    tcp 22      running
   snmp                  auto disabled   udp 161     not running
   ```

5. Display the status of a spoke. The spoke should be enabled, running, and communicating with the Datahub.

   ```
   status all
   ```

   This example shows a server configured in Spoke mode:

   ```
   admin              auto enabled    tcp 3835   running
   server (spoke)     auto enabled    tcp        running
   ssh                auto enabled    tcp 22     running
   snmp               auto disabled   udp 161    not running
   ```

Remove a spoke from an existing cluster

Purpose

To return a RedSeal server configured as a spoke on an existing cluster to a standalone server with default settings, remove the spoke from the existing cluster.

Procedure

1. Log in to the datahub.
2. Delete a spoke.

   ```
   delete spoke <IP_ADDR>
   ```

3. Log in to the RedSeal server spoke that you deleted.
4. Restore the spoke to its default standalone RedSeal appliance settings.

   ```
   unset datahub
   ```

5. Verify that the former RedSeal server operating as a spoke is now a standalone server.

   ```
   status all
   ```

   This example shows a server configured in Standalone mode:

   ```
   admin                auto enabled    tcp 3835    running
   server               auto enabled    tcp 3825    running
   server-jms           auto enabled    tcp 3826    running
   server-http          auto enabled    tcp 80      running
   server-https         auto enabled    tcp 443     running
   server-https-cert    auto enabled    tcp 10443   running
   db                   auto enabled    tcp 5432    running
   ssh                  auto enabled    tcp 22      running
   snmp                 auto disabled   udp 161     not running
   ```

Remove a cluster

Purpose

Removing a cluster allows you to return RedSeal servers configured as a datahub and spokes to standalone servers with default settings.

Procedure

1. Log in to the datahub.
2. Identify all spokes connected to the datahub.

   ```
   show spokes
   ```

3. Restore all spokes to their default standalone RedSeal appliance settings.
   a) Delete a connected spoke.

      ```
      delete spoke <IP_ADDR>
      ```

   b) Log in to the RedSeal server spoke that you deleted.
   c) Restore the spoke to its former standalone RedSeal appliance settings.

      ```
      unset datahub
      ```

4. Confirm that the cluster configuration settings were removed on former datahub and spoke servers.

   ```
   show datahub
   show spokes
   status all
   ```

   For detailed information about these commands, see the *Command Line Interface* chapter of the *RedSeal Multi-Server Manager User Guide*.

Enable or disable clustered import

Purpose

Enable the clustered import feature to increase data collection performance by allowing the datahub to distribute its tasks across the cluster.

Details

Clustered import is disabled by default. To turn on this feature, you must enable it from the RedSeal server operating as a datahub.

Procedure

1. Log in to the datahub.
2. Determine the command you want to enter.

If you want to...	Then type the command...
enable clustered import	`set property server clustered_import true`
disable clustered import	`set property server clustered_import false`

3. Shut down the datahub.

   ```
   shutdown server
   ```

4. Restart the datahub.

   ```
   startup server
   ```

10

User accounts

Introduction

Use the **Users** tab of the **System Settings** window to create and manage RedSeal user accounts. You can create as many user accounts with administrative privileges as you need. You can also create new, non-admin users with a variety of different permissions and authentication methods.

User accounts for the web-based interface

You can create user accounts for use in the web-based and Java interface. You can only create user accounts in the Java client version of RedSeal.

Supported authentication methods

There are three supported authentication methods.

Local authentication

Users authenticate directly to the RedSeal server using a password created by you and stored on the server.

External authentication servers

You can configure RedSeal to use your LDAP or RADIUS server for authenticating RedSeal users. For information about creating additional user accounts and using your LDAP or RADIUS server, see *Add or edit user accounts* on page 123, *Configure LDAP* on page 128, and *Configure RADIUS* on page 130.

Smart card authentication

RedSeal supports two-factor authentication using CAC smart cards. CAC (Common Access Card) is a smart card used by the U.S. military for identification and authentication. For information on smart card authentication, see *Smart card authentication* on page 134.

Default client application login account

Introduction

After you install RedSeal, the default client application login account is the uiadmin user. This account is in the Admin permissions group and provides administrative-level access to the user interface. You cannot rename or disable the uiadmin account, though you can disable it once you have created at least one other account with administrative privileges.

Default account password

The password for this account is created during the first-time initialization of the server and database. You can change this password from the CLI: `set password uiadmin`.

User accounts and permission levels

Introduction

RedSeal supports two user types: a Java client and a web client.

RedSeal user access summary

This table summarizes which user interfaces each user can access.

User type	Java Client	Web interface
Java client • View user • Model user • Admin user	Yes	Yes

Web Interface	No	Yes

Java client user

Introduction

You can assign Java Client users one of the following permission levels: (a) View permissions, (b) Model permissions, and (c) Administrator permissions.

View permissions

Users whose accounts are in the View group are able to

- modify the layout of devices and subnets on the topology display
- modify user preferences
- choose settings for the risk map display
- generate queries in the Detailed Paths
- run reports using built-in report templates
- have read-only access to documents in the **Public** folder on the **Reporting** tab, and
- access the web UI.

Model permissions

Users in the Model group can do everything View users can do, plus

- update the RedSeal Threat Reference Library (TRL)
- manage credentials for accessing network devices
- manage data collection tasks
- import data manually
- manage devices, subnets, device groups, and applications
- run the RedSeal analysis engine
- use the API to retrieve and update data

- read and edit report and document files in folders named for the user account ID on the **Reporting** tab
- read report and document files in public folders on the **Reporting** tab, and
- access report design tools to create custom report templates on the **Reporting** tab.

Administrator permissions

Users in the Admin group can do everything Model and View users can do, plus

- create and manage user accounts
- manage certificates
- manage logging data
- read and edit all users' report design files and documents
- read and edit report templates
- configure data backup and restore tasks using the client application interface
- upload plug-ins and new server installation images using the client application interface, and
- restart the appliance using the client application interface.

Web interface user

The web interface user has access to a subset of the same functions as the Java client application. You can specify which parts of the web application interface this user can access.

Refer to the *RedSeal User Guide* for details about each of the available applications.

Access to menu commands

Introduction

Commands on the RedSeal client application's menus are enabled or disabled according to the permission level of the currently logged in user.

Access to the Admin menu

Only Admin user accounts will see the **Admin** menu displayed in the user interface if the server is running on a RedSeal appliance.

User account management

Introduction

There are two ways to create accounts depending on how you want to control user permissions. You can (a) create accounts to authenticate through the server, or (b) create accounts to authenticate through LDAP or RADIUS.

Add or edit user accounts

Purpose

You can add a new account or edit an existing user account for any of the three user types from the Java client.

Procedure

1. Click **System Settings > Users > Add User**.
2. Type a username.

   If the user authenticates through LDAP, the username can be any common name (cn) associated with a user object in your LDAP database.
3. Select an authentication type.

If you have selected...	Then...
Smart Card authentication	choose or add a Subject DN. For more information, see *Smart card authentication* on page 134.
Local (RedSeal-managed) authentication	assign a password.
LDAP authentication	see *Configure LDAP* on page 128 for more information, if necessary.

RADIUS authentication	see *Configure RADIUS* on page 130 for more information, if necessary.

4. Select the authorization type and then assign either permissions, applications, or Topology Groups depending on the user type.

User type	Action
Java client	Assign a user type to the Java client and assign one of the three permissions types (Admin, Model, View). For more information, see *User Accounts and Permission Levels* in the *User Guide*.
Web Interface	Set desired Web applications the user can access. You can remove and change the Web applications assigned to this user.

5. To prevent the user account from logging in, click **Disabled**.

   The user account will not be deleted.

Add a backup authentication method for smart card users

Purpose

Add a backup authentication method for smart card user so that they can log in if smart card authentication is unavailable.

Procedure

1. Click **System Settings > Users > Add User**.
2. Type a username.

   If the user authenticates through LDAP, the username can be any common name (cn) associated with a user object in your LDAP database.
3. Select the smart card authentication type.
4. Click **Enable backup auth**.

5. Select a backup type and add any necessary backup information.

   You cannot edit a smart card user account. To change smart card user account settings, for example to give the user a password backup, you must delete the user account and re-create it.

Assign permissions through LDAP or RADIUS

Purpose

Assign permissions by associating a RedSeal permissions level with a group of user accounts in your LDAP or RADIUS database.

Before you begin

You must already have LDAP or RADIUS server information configured on RedSeal. See *External authentication* on page 128.

Procedure

1. Click **Edit > System Settings**.
2. On the **Users** tab, click **Remote Authorization**.

If using...	Then...
client application remote authorization	1. On the **SRM** tab of the **Remote Authorization Settings** dialog, enter comma-separated lists of names of the LDAP or RADIUS groups you want to associate with the RedSeal permission types. 2. Add a group attribute. 3. Click **Save**.
web interface remote authorization	Go to the **Web** tab of the **Remote Authorization Settings** dialog.

3. Click **Add** for either LDAP or RADIUS groups.

   The **Add Groups** dialog displays.

4. Enter a comma-separated list of names of the LDAP or RADIUS groups you want to associate with the Web permission type.
5. Add the web UI features you want the groups to be able to use.
6. Click **Save**.

   The dialog closes.
7. On the **SRM** tab, click **Save**.

Example

If your LDAP directory tree contains an ou=Admin organizational unit object which contains a people object for an individual user account cn=usr1, enter the value `Admin` in the **Admin** field of the **SRM** tab or the **Group(s)** field in the **Add Groups** dialog.

This enables a RedSeal user account with Admin permissions for usr1.

The user object in the LDAP directory must have a `<memberOf>` attribute set to the ou=Admin group's DN.

In Active Directory, the user object will likely be associated with a Security Group object rather than be contained in an Admin OU.

In Active Directory, user objects are associated with groups in the **Propertie**s dialog of the user object. Right-click on a user object in the directory tree. On the **Member Of** tab, click **Add**.

User account deletion rule

Statement

Before deleting a user, delete any reports scheduled by that user.

Results of deleting a user

Deleting a user account also deletes

- report definitions created by the account being deleted
- any customizations created for reports by the account being deleted
- the user account home directory in the reports repository, and

- all topology records saved by the user.

Change password with administrator privileges

Purpose

If your RedSeal user account has administrative privileges, you can change the password for any locally defined account.

LDAP and RADIUS account passwords

You cannot modify passwords for LDAP and RADIUS accounts from the RedSeal interface.

Procedure

1. Click **Edit > System Settings**.
2. On the **Users** tab of the **System Settings** dialog, select the account whose password should be changed.
3. Click **Edit User**.
4. Enter the new password twice.

Change password without administrative privileges

Purpose

If you do not have administrative privileges, you can change the password only for your account.

LDAP and RADIUS account passwords

You cannot modify passwords for LDAP and RADIUS accounts from the RedSeal interface.

Procedure

1. From **System Settings > Password**, enter your current password.
2. Enter the password twice.

External authentication

Introduction

RedSeal supports external two-factor authentication when integrated with LDAP or RADIUS.

LDAP and RADIUS combined authentication

RedSeal does not support LDAP and RADIUS combined authentication.

Choose a configuration method

Configure external authentication either from **System Settings > Users** or from within a single user's **Add/Edit** window. It does not matter which you choose. Setting up external authentication from within a single user's account window applies to more than that one user. You only need to set up LDAP or RADIUS once.

Configure LDAP

Purpose

Integrate RedSeal with LDAP to support external two-factor authentication.

Procedure

1. In the **LDAP Configuration** dialog, enter the host names or IP addresses of the servers on which your primary and, optionally, secondary LDAP servers are installed, and the ports on which the LDAP servers are listening.
2. To connect to LDAP over SSL, click **Enable SSL**.

   SSL must also be enabled on the LDAP server.
3. In the **Base DN** field, enter the value of the entry level of your LDAP directory tree, `dc=docs,dc=redsealnetworks,dc=com`.

   The entry level is the top level that contains all RedSeal user accounts.

   For Active Directory, use Microsoft's ADSI Edit tool to obtain distinguished names in LDAP syntax. The Active Directory Users and Computers tool does not show object names in the syntax required by RedSeal. Examples of the syntax are DN=, OU=, and CN=.
4. In the **Unique attribute** field, enter the attribute name.

If...	Then...
your LDAP database identifies users by a unique attribute	enter the attribute name in the **Unique attribute** field.
you use Active Directory	set the **Unique attribute** field to `sAMAccountName`. See *RedSeal user ID requirements when using an Active Directory server* on page 129.

5. In the Admin User DN field, enter the distinguished name (dn) of the LDAP database root user, such as `cn=admin,dc=docs,dc=redseal,dc=com`.

   If you use Active Directory, the **Admin User DN** can be the DN of any account that has rights to view the OU that contains the users to be given RedSeal user accounts.
6. In the **RedSeal LDAP Configuration** dialog, enter and confirm the admin user's password if your LDAP installation requires one.
7. If you use Microsoft's Active Directory, click **Active Directory**.
8. To make sure you have accurately configured the LDAP connection, click **Test Connection**.

RedSeal user ID requirements when using an Active Directory server

Statement

When the LDAP implementation is an Active Directory server, set the **Unique Attribute** field in the **LDAP Configuration** dialog to the user's `<sAMAccountName>`.

- For RedSeal accounts, use the AD value of the `<sAMAccountName>` parameter as the login ID.

Outcome

If the `<sAMAccountName>` parameter is not specified, RedSeal user accounts will be accessible only by the user's full name (first and last names), and this log in identifier will be case sensitive.

Example

If a user account exists in AD for the user John Doe, with a `<sAMAccountName>` of "jdoe", the RedSeal user account ID will be "jdoe" if the **Unique Attribute** field is set to `<sAMAccountName>`.

If the **Unique Attribute** field is not used, then the RedSeal user account ID would be "John Doe", case sensitive.

Find users in the LDAP database

Purpose

To look up a user in the LDAP database, follow these steps.

Procedure

1. Click **System Settings**.
2. On the **Users** tab, click **LDAP Lookup** to see if a user ID is present in the LDAP database.

   The **LDAP Query Tool** dialog displays.
3. Enter search text, and then click **Search**.

   Use an asterisk to do a wildcard search.

   Results display in the table at the bottom of the dialog.

Configure RADIUS

Purpose

Integrate RedSeal with RADIUS to support external 2-factor authentication.

Procedure

1. In the **RADIUS Configuration** dialog, enter the host names or IP addresses of your primary, and optionally, secondary RADIUS servers and the ports on which they listen.
2. Enter and confirm a **Shared Secret** password and the number of times RedSeal should attempt to authenticate.

   RedSeal user passwords cannot exceed the maximum number of characters allowed by RADIUS.

3. To ensure you have accurately configured the RADIUS connection, click **Test Connection**.

Single sign-on

Introduction

RedSeal supports single sign-on (SSO) using OAuth with Azure Active Directory (Azure AD), or Active Directory Federation Services (AD FS).

To set up SSO using OAuth on RedSeal, configure the following settings on your Identity Provider (IdP) and on RedSeal.

Identity Provider settings

1. **Create and register an application for RedSeal on the IdP to obtain the discovery endpoint and client ID**: To allow the IdP to manage identity and access functions for RedSeal, you must first create and register an application for the RedSeal OAuth client under your tenant account in Azure AD. Registering the application allows it to integrate with Azure AD. Select **App registrations > New registrations** and provide display name and account details to register the RedSeal application. Make a note of the client ID. Refer to Microsoft Azure documentation for details about how to register an application. The registered application communicates with the Azure platform by sending requests to an endpoint, for the RedSeal OAuth client, this is the OpenID Connect (OIDC) endpoint. RedSeal OAuth requires the OIDC endpoint and the client ID.
2. **Create a client secret**: Use the **Certificates & Secrets** page to add a new client secret. Make a note of the client secret. Refer to Microsoft Azure documentation for details about this step.
3. **Create users and add them to Security Groups**: Add users to the group whose group type is “Security Group”.
4. **Add Security Group information to ID token**: The Security Group information must be included in the ID token.

   If using Azure AD, add a groups claim to the ID token and select the security groups and corresponding attributes. Refer to Azure AD documentation for more information.

5. **Redirect URI**: A redirect URI must be added to your RedSeal server. If you use more than one server, each server requires a URI. You must provide a redirect URI otherwise authentication will fail.

   The URI must be in the format:

   ```
   https://<host_name>:<port_number>/oauth/callback
   ```

   where,

   host_name = Fully qualified domain name (FQDN) of your RedSeal server

   port_number = HTTPS port number to connect to RedSeal, see *Ports required for access* on page 25 for details.

   On ADFS, the ADFS server certificate must be imported into RedSeal if that certificate has been signed by a private Certificate Authority (CA). Use the `upload certificate` command on the CLI to import the ADFS certificate to RedSeal, see *upload certificate* on page 229 for details.

RedSeal settings

1. Configure OAuth on RedSeal.
2. Add the Security Groups that contain users who will log on to RedSeal and authenticate using OAuth.

Configure OAuth

Purpose

Configure OAuth on RedSeal to set up single sign-on.

Procedure

1. On the Java client, navigate to **Edit > System Settings > Users**.
2. Click **Configure OAuth**.

   The **OAuth Configuration** dialog displays.
3. Type the following information:
   - **Federated Identity Provider**: OAuth identity provider's URL. This URL is the same OIDC endpoint obtained in step 1 of the Identity Provider settings. You can obtain the OIDC endpoints for the different identity and access management services as follows:

  - Azure AD: From the Azure Active Directory portal select **App Registration > Select Your Application > Overview tab > Endpoints > OpenID Connect metadata document** .
  - For AD FS use the power shell command Get-AdfsEndpoint > OpenID Connect Discovery

  These are just a few examples of the ways to obtain the endpoints. Refer to your specific Identity Provider service documentation for more information.

- **Client Id**: the ID used to identify RedSeal with the Identity Provider.
- **Client Secret**: the password associated with the ID used to identify RedSeal with the Identity Provider.

4. Click **Test Connection** to confirm that RedSeal can connect with the Identity Provider.
5. If the test succeeds, you are redirected to your Identity Provider server. Enter your credentials to authenticate with your Identity Provider. If your credentials are accepted, a connection succeeded message is displayed.

Configure Remote Authorization

Purpose

These steps apply to all Identity Providers that RedSeal supports: Azure AD and AD FS.

Procedure

1. On the Java client, navigate to **Edit > System Settings > Users**.
2. Click **Remote Authorization**.

   The **Remote Authorization Settings** dialog displays.
3. Type the names of the security groups to which users who will log on to RedSeal belong, in the correct user type field. Save your settings.

   A user's access to RedSeal features depends on the user type to which their Security Group has been added, see *User accounts and permission levels* on page 120.
4. The next time you start the Java client, the log in screen displays a new radio button option: **SSO**. Select **SSO** to log on to RedSeal using OAuth.
5. Type your username and click **Login**. You are redirected to your Identity Provider login page.
6. Enter your credentials and follow any instructions to authenticate with your Identity Provider.

7. If you are successfully authenticated, the browser displays a confirmation message, and you are logged into the RedSeal client.

Note When a user clicks context sensitive help, online help, or a guide from the **Help** menu, it displays in a new browser window. To access the page in the browser window, users will have to re-authenticate.

Disable OAuth

Purpose

OAuth on RedSeal is enabled by default. You can disable it using the server property command. When you disable OAuth, the next time the client starts up, the SSO option is hidden. If you re-enable OAuth, the option will be available again, provided OAuth is configured.

Procedure

1. Log on the RedSeal appliance CLI.
2. Choose a command to use.

If you want to...	Then type the command...
disable OAuth	`set property server redseal.srm.https.oauth.enabled=false`
enable OAuth	`set property server redseal.srm.https.oauth.enabled=true`

Smart card authentication

Introduction

To improve security, RedSeal supports two-factor authentication using CAC (common access cards), also known as smart cards. Smart card users authenticate using a Subject DN (Distinguished Name) instead of a user name. The US Military uses smart cards for identification and authentication.

Smart card use for CLI administrators

CLI administrators can log in using smart cards rather than the cliadmin password. Using CAC for CLI authentication means you can revoke access for a single administrator without having to change the shared cliadmin account. For more information, see *Reset CLI password* on page 64

Smart card commands

For all smart card-related commands see *Smart card commands* on page 235.

Enabling smart card authentication

To enable smart card authentication, the administrator

1. Enables certificate authentication. See *Enable certificate authentication* on page 135.
2. Adds the root CA certificate to the RedSeal server. See *Add the root certificate to RedSeal* on page 136.
3. Adds the OCSP (Online Certificate Status Protocol) responder URL. See *Configure OCSP* on page 136.
4. Adds the Subject DNs to the RedSeal server. See *Add a user Subject DN to RedSeal* on page 137.
5. Create smart card user accounts. See *Add or edit user accounts* on page 123.

Enable certificate authentication

Purpose

To make smart card authentication available for user accounts, you must enable certificate authentication.

Procedure

1. Log in to the RedSeal Command Line Interface.
2. Enable certicate authentication.

```
enable authentication certificate
```

Add the root certificate to RedSeal

Purpose

You must add a root CA certificate to RedSeal that all smart card users will authenticate against.

Before you begin

Before adding the root certificate to RedSeal, you must have a root CA certificate. The browser root certificate must be installed and available to the browser on any device used to access the RedSeal client application or web interface.

Procedure

1. Log in to the RedSeal Command Line Interface.
2. Upload the root CA certificate to the Trust Store.

   ```
   upload ca-certificate
   ```

   For example: `upload ca-certificate http://my.root.certificate.example.com/example.cac`

Configure OCSP

Purpose

RedSeal uses the Online Certificate Status Protocol (OCSP) URL to validate user certificates and make sure they have not been revoked. The OCSP validates user certificates every time they are used to log in. You must configure the OCSP to enable certificate verification.

Details

Checking for revoked certificates requires a live connection to the OCSP Responder.

Procedure

1. Click **System Settings > Users**.
2. Click **Configure OCSP**.
3. In the **OCSP** dialog, type the OCSP responder URL.
4. To enable certificate verification, click **Verify User using OCSP**.

Add a user Subject DN to RedSeal

Purpose

Before you can create a user account that allows smart card access, you must add the user's Subject DN to the RedSeal server.

Procedure

1. Determine if the user has their Subject DN readily available.

If the user...	Then have the user...
has their Subject DN readily available	send their Subject DN to you.
does not have their Subject DN readily available	attempt to log in to RedSeal through the web interface at `https://<server>:10443/redseal/`. The login dialog available on this port offers certificate authentication. The authentication fails and the user's Subject DN is automatically added to the RedSeal server.

2. When you create the user's account, enter the Subject DN to RedSeal obtained from the user, or select the stored Subject DN from the Subject DN drop down menu that was automatically added.

Log in to the client application as a smart card user

Purpose

U.S. military personnel authenticate to the RedSeal application using a smart card.

Before you begin

The card reader and card enabler software must already be installed on the device used to access the RedSeal client application.

Procedure

1. Insert the smart card in to the card reader.

2. At the RedSeal client application login dialog, select **Certificate**.

   You are redirected to a browser.
3. If necessary, enter the card reader PIN to access the smart card certificate.
4. Select the correct user certificate from the browser dialog.

Log in to the web interface as a smart card user

Purpose

To log in to RedSeal using a smart card, follow these steps.

Before you begin

The card reader and card enabler software must already be installed on the device used to access the RedSeal web interface.

Procedure

1. Insert the smart card into the card reader.
2. Access the web interface through port 10443.

   Example: `https://<server>:10443/redseal/`
3. If necessary, enter the card reader PIN to access the smart card certificate.
4. Select the correct user certificate from the browser dialog.

11

Security

Introduction

The RedSeal application provides virtual penetration analysis of the network and hosts to identify threat vectors and vulnerabilities that may be exploited by an attacker. Both physical and network access to the RedSeal server must be protected. The RedSeal server requires user name and password validation for access.

TLS protocol version

Introduction

RedSeal client-server communication uses Transport Layer Security (TLS) protocol version 1.2. For browser-server communications, it allows TLS 1, 1.1, and 1.2, which you can restrict to 1.2 and also reset using the `<redseal.srm.nonfipsTLSVersions>` server property.

Set the `<redseal.srm.nonfipsTLSVersions>` server property

For details about how to set `<redseal.srm.nonfipsTLSVersions>` server property, see *set property* on page 209.

TLS and HTTPS certificate validation

Introduction

To meet Common Criteria requirements, enable validation of all TLS and HTTPS certificates using the `<strict_server_cert_check>` server property to `true`. When validation is enabled, RedSeal evaluates all TLS and HTTPS certificates for a valid certificate path, valid expiration date, revocation status, and reference identifier. The connection fails if the certificate is invalid.

Set the `<strict_server_cert_check>` server property

For details about how to set `<strict_server_cert_check>` server property, see *set property* on page 209.

FIPS-approved ciphers for network-based access

Introduction

All network-based access with the server is encrypted through the use of Federal Information Processing Standards (FIPS)-approved ciphers.

Ciphers used in non-FIPS mode

In non-FIPS mode, RedSeal communication uses one of these FIPS-approved ciphers:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

Ciphers used in FIPS-mode

In FIPS mode, RedSeal communication uses one of these FIPS-approved ciphers:

- TLS_RSA_WITH_AES_128_CBC_SHA256

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

Disable cipher suites and MAC algorithms

Purpose

To conform to your organization's internal policies, you might need to disable cipher suites you do not want to be used by the server and SSH process. You might also need to disable message authentication code (MAC) algorithms used by the SSH process. This example procedure shows how to disable, verify, and enable specified cipher suites and MAC algorithms for both the server and the SSH process.

Procedure

1. Disable the cipher suite with the name `TLS_RSA_WITH_AES_128_CBC_SHA` for the server.

```
disable cipher-suites server TLS_RSA_WITH_AES_128_CBC_SHA
Disabling cipher suites will restart the server and admin server
process.
Do you want to proceed? [(Y)es or (N)o] y
Restarting admin server...
Command succeeded.
```

2. Disable the cipher suite with the name `aes128-ctr` for the SSH process.

```
disable cipher-suites ssh ciphers aes128-ctr
Command succeeded.
```

3. Disable the MAC algorithm with the name `umac-64@openssh.com` for the SSH process.

```
disable cipher-suites ssh macs umac-64@openssh.com
Command succeeded.
```

4. Verify which cipher suites are enabled and disabled for the server.

```
show cipher-suites server
Enabled Ciphers:
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
     TLS_RSA_WITH_AES_256_CBC_SHA
     TLS_RSA_WITH_AES_128_CBC_SHA256
     TLS_RSA_WITH_AES_128_GCM_SHA256
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
     TLS_RSA_WITH_AES_256_CBC_SHA256
     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
     TLS_RSA_WITH_AES_256_GCM_SHA384
     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Disabled Ciphers:
     TLS_RSA_WITH_AES_128_CBC_SHA
```

5. Verify which cipher suites and MAC algorithms are enabled and disabled for the SSH process.

```
show cipher-suites ssh
Enabled Ciphers:
     aes192-ctr
     aes256-ctr
     aes128-cbc
     aes192-cbc
     aes256-cbc
Enabled MACs:
     hmac-sha1
     hmac-sha2-256
     hmac-sha2-512
     hmac-md5

Disabled Ciphers:
     aes128-ctr
Disabled MACs:
     umac-64@openssh.com
```

6. Enable the cipher suite with the name `TLS_RSA_WITH_AES_128_CBC_SHA` for the server.

```
enable cipher-suites server TLS_RSA_WITH_AES_128_CBC_SHA
Enabling cipher suites will restart the server and admin server
process.
Do you want to proceed? [(Y)es or (N)o] y
Restarting admin server...
Command succeeded.
```

7. Enable the cipher suite with the name `aes128-ctr` for the SSH process.

```
enable cipher-suites ssh ciphers aes128-ctr
Command succeeded.
```

8. Enable the MAC algorithm with the name `umac-64@openssh.com` for the SSH process.

```
enable cipher-suites ssh macs umac-64@openssh.com
```

```
Command succeeded.
```

See *show cipher-suites* on page 213, *disable cipher-suites server* on page 184, *disable cipher-suites ssh* on page 185, *enable cipher-suites server* on page 188, *enable cipher-suites ssh* on page 188.

Required ports for encrypted data exchanges

Port numbers and descriptions

Several ports are required for access to the RedSeal server when operating in a secure environment requiring encrypted data exchanges.

Port	Use
22	SSH access to the CLI
3825 and 3826	RedSeal Java client-server communications using TLS
3835	Administrative tasks such as client and server logging using TLS
443	Installing the Java client, web-based reports, web-based API, and online help
10443	Certificate authentication
389	LDAP for data collection
636	LDAP over SSL (optional)
1812	RADIUS for user authentication

RedSeal client download requirements

Statement

Before downloading the RedSeal client to a remote host, install a custom SSL certificate.

- Use HTTPS port 443 to download the RedSeal client to a remote host.

Outcome

If you attempt to download the client using HTTPS without a custom certificate, you will be asked to accept the default RedSeal certificate for every `.jar` that is downloaded.

SSL certificate

Introduction

The SSL certificate installed in the server by default is a self-signed certificate generated by RedSeal. The certificate has a 2,000-day lifespan, and is used for HTTPS communication between the server and the user interface or web browser.

Supported certificate formats

The product supports these certificate formats:

- .der
- .cer
- .crt
- .pem, and
- X.509 SSL/TLS.

Prerequisites for use of the SSL certificate

Use of an SSL certificate requires familiarity with the SSL trust model and certificate train.

Change the default common name

The certificate has a default common name (CN) of “redseal”. To avoid web browser SSL challenges, change the default CN value to the hostname of your server.

To change the CN value, either install a self-signed certificate or obtain a certificate from a third-party Certificate Authority (CA). Third-party providers may require the CN to identify a fully qualified domain name (FQDN). If the CA from which you obtain your certificate is not one of the CAs known to Java, import the CA’s public certificate. An example is if you are acting as your own CA.

Create a certificate or certificate request

A signed certificate provides additional security. Create a certificate or certificate request using the client interface or through the CLI. When you use the certificate commands in the CLI to create a new self-signed certificate, the server CN is set to the host name of the server on which it is created, and it has a new 2,000-day lifespan.

Install a certificate

Install a certificate using the client interface or through the CLI.

Initially specify your custom attributes for a certificate

To initially specify your custom attributes for the certificate, use the CLI to create a self-signed certificate.

Verify the root certificate is in the Java store

Verify if the root certificate is in the Java store, and that the authority is listed in the output.

```
show certificates
```

Add a self-signed certificate to the server using the CLI

Purpose

To specify your custom attributes for the certificate, you must use the CLI to create a self-signed certificate.

Procedure

1. Create the self-signed SSL certificate. You are prompted to enter your custom attributes.

```
create self-certificate
    Hostname (CN) (<server_name.your_org.net>):
    Keysize (2048):
    Organization Unit (OU) (RedSeal):
    Organization (O) (RedSeal Networks):
    City (L) (Santa Clara):
    State (ST) (CA):
    Country (C) (US):
    Subject Alternate Names (SAN)
    (redseal.co,redsealnetworks.com,redseal.net):
```

2. Shut down the server.

```
shutdown server
```

3. Verify the server is shut down.

```
status server
```

4. Restart the server.

```
startup server
```

5. Create a certificate signing request (CSR).

   When you create a self-certificate, it creates a file on the server of the URL you specify. See *create cert-request* on page 180.

```
create cert-request scp://username:password@10.0.0.0:
    Exporting certificate request to scp://10.0.0.0:/
    redseal_cert_request_20181125134405.csr ...
    Command succeeded. Certificate request copied to
    scp://10.0.0.0:/redseal_cert_request_20181125134405.csr
```

6. Submit the CSR to the Certificate Authority (CA) for approval.

   The CA sends a file back that you need to upload.

7. After the certificate is approved, upload the certificate in to the server.

   The URL should point to a digital certificate obtained from the CA.

```
upload certificate <URL>
```

   See *upload certificate* on page 229.

Add the certificate to the server using the CLI and a fully qualified domain name

Purpose

Create a certificate signing request (CSR) that includes your fully qualified domain name (FQDN) instead of only a hostname.

Procedure

1. Reset the host name to the FQDN. See *set hostname* on page 200.
2. Create and upload a self-signed SSL certificate.

   See *Add a self-signed certificate to the server using the CLI* on page 145, *create self-certificate* on page 180, and *upload certificate* on page 229.

   When you create the self-signed SSL certificate, you will be prompted for your custom properties. The properties you specify are then used in the CSR.
3. Shut down and restart the server so the new certificate is in effect.

   See *shutdown* on page 223 and *startup* on page 226.
4. After installing the self-signed certificate, generate a CSR.

   See*Add a self-signed certificate to the server using the CLI* on page 145, and *create cert-request* on page 180.

   The CSR automatically contains the custom properties from the self-signed certificate.
5. Upload the new server certificate you received from the Certificate Authority.

   ```
   upload certificate
   ```

   See *upload certificate* on page 229.
6. To ensure the new certificate is in effect, shut down and restart the server.

   See *shutdown* on page 223 and *startup* on page 226.

Add an intermediate certificate to the server using the CLI

Purpose

For the server to accept any certificates that are signed by an intermediate certificate authority, you need to combine both the root certificates and the intermediate certificates into one text file before uploading it to the server.

Details

In this task, you are working with two types of certificate files: root certificates and intermediate certificates.

This task uses the filename `combine_certs.cer` as an example.

Procedure

1. Open the intermediate and root certificates in a text editor, such as Notepad++.
2. Select all of the characters in each certificate, including the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- tags.
3. Copy and paste the selected text into a new file.
4. Save the results to `combine_certs.cer`.

   The file should have the intermediate certificate at the top of the file and the root certificate at the bottom of the file.
5. Upload `combine_certs.cer` into the server.

   ```
   upload ca-certificate <URL>
   ```
6. After the upload completes, you might need to install the server certificate. If your signed server certificate from the Certificate Authority is not in the Java store, you must also upload a server certificate after you upload the combined intermediate and root certificates and before restarting the server.

   ```
   upload ca-certificate <URL>
   ```
7. After the server certificate is installed, shut down the server.

   ```
   shutdown server
   ```
8. Verify the server is shut down.

   ```
   status server
   ```
9. Restart the server.

   ```
   startup server
   ```

Adding the certificate to the RedSeal server using the client interface

Purpose

The administrator uploads a Certificate Authority (CA)-created SSL certificate to the RedSeal server before creating a certificate signing request (CSR).

Details

The administrator has the option to create a self-signed SSL certificate instead of using a CA. As a best practice, the administrator should use a CA as they are more secure.

Process

1. The administrator

    a) generates and saves a certificate request in the RedSeal server, and

    b) sends the certificate request to the CA.

2. The CA

    a) creates an intermediate CA certificate, and

    b) sends it to the administrator.

3. The administrator installs the CA certificate on the RedSeal server.

Data collection task communications

Introduction

The server can be configured to use credential-based tasks to automatically retrieve network device configurations and vulnerability scan data. The data collection tasks are configured with a device/server address, communication protocol, and credential.

Target device or server types

The target device or server can be one of several types, such as a router, scanner or a database such as FTP or Cisco Prime. Each task may be configured to use a secure protocol like SSH and HTTPS, or in many cases a vendor specific protocol such as the Check Point OPSEC interface, for gathering data.

Supported communication protocols

For details on supported communication protocols, see the *RedSeal Data Import Plugins Guide*.

Credentials

Credential objects containing authentication information required to log in to the devices or databases are stored in the RedSeal database as encrypted objects using a FIPS certified 128-bit AES algorithm. Passwords are never shown by the server but are indicated as **** and do not indicate length of the password.

Store SSH authentication keys locally

Purpose

To meet Common Criteria requirements, create, enable, and populate a local database of public keys used to authenticate all SSH communications, including SSH data collection tasks and software uploads using SCP or SFTP. When this setting is enabled, if the server tries to connect with a server that does not have a locally stored key, the communication fails.

Procedure

1. Enable the local SSH key database using the server property `strict_host_key_checking`.

```
RedSeal> show property server strict_host_key_checking
strict_host_key_checking                          =true
```

2. Restart the RedSeal server.

```
startup server
```

3. From the CLI, retrieve and save each required public key using the `set ssh public-key <IP|Hostname>` command.

   The command fetches the server's public key and stores it in the local database. See *set ssh public-key* on page 211.

4. Use the `set ssh public-key <IP|Hostname>` command for every server communicated with using SSH.

How network device passwords are screened

Purpose

The RedSeal server performs a best practices check on network devices to find and remove weak or absent encryption.

Process

1. The RedSeal server gathers network device configurations containing sensitive data such as ***enable*** passwords.

2. The import process performs a best practices check to screen ***root*** or ***enable*** passwords on most network devices.

   This process compares configured passwords against vendor defaults and looks for weak or no encryption.

3. The RedSeal server

   a) strips the password information, and

   b) the device configuration is written to the database.

   These passwords cannot be retrieved using either the client or reporting interfaces.

Password and database encryption

Introduction

Both the data password and the database .enc backup file are encrypted using RSA BSAFE to ensure compliance with Federal Information Processing Standards (FIPS 140-2).

Generate an encrypted backup

Generate an encrypted backup by using a user-defined password and 128-bit AES key.

Access restrictions when running postgres database

The appliance does not allow direct access to the running postgres database.

Additional information

For more information about FIPS 140-2, see *http://www.nist.gov*.

For more information about database management, see *Data management strategies* on page 152.

For more information on passwords, see *Passwords in the RedSeal environment* on page 63.

Data password standards

Introduction

The NSS FIPS and DoDIN APL standards apply to RedSeal Data passwords.

Password complexity

You can enable and disable password complexity for each standard.

Syntax rules

You must follow syntax rules for both protocols when

- establishing a valid RedSeal Data password, and
- making multiple attempts at establishing or changing a Data password.

  See *Passwords in the RedSeal environment* on page 63.

Data management strategies

Statement

To maintain separation of duties, Network Operations and Security Operations staff may need to share use of the RedSeal application. To ensure these two groups can work together without exposing critical data such as device authentication information

- establish ownership of your RedSeal installation

- set the data password, and
- import data manually from files provided by a network operations engineer, or data sent to secondary databases, such as FTP or Check Point.

Applicability

In all cases, the working methods need to be structured in such a way that the network blueprint data does not become stale or inaccurate.

Example

If Security Operations owns your RedSeal installation, then

- a security engineer
    - configures the database password, and
    - creates the data collection credential objects and tasks retrieving vulnerability scan data, and
- a Network Operations engineer independently manages data collection credential objects and tasks for importing networking device configurations.

Because of the password protections maintained by RedSeal, separation of duty is maintained.

Reversed roles

Reverse the roles if Network Operations owns the RedSeal installation.

Appliance OS hardening

Introduction

The RedSeal appliance runs an CentOS operating system, which has been hardened a number of ways.

Hardening

The appliance OS has been hardened as follows:

- the firewall (iptables) has been configured to allow only traffic required by RedSeal
- port numbers are user configurable
- RPM packages deemed unnecessary for RedSeal operations have been removed
- all known security updates are applied to RPMs installed on the appliance for each release
- services not needed by RedSeal but installed as part of a needed package have been turned off
- ICMP redirects have been disabled
- the ssh login banner warns against unauthorized use
- core dumps have been disabled

12

License administration

Introduction

Operation of the RedSeal software requires a valid RedSeal license. A Redseal license is encrypted and delivered as an ASCII text file that must be installed on the RedSeal server.

Server license requirements

You must have a valid RedSeal license installed before you can start the server process. If your license was not installed by RedSeal prior to shipping, you must install the license during the initial configuration of the server.

To obtain a license, contact *support@redseal.net*.

Install the RedSeal license by uploading

Purpose

You can upload the license from an FTP or HTTP repository that the RedSeal server can access.

Procedure

1. From the CLI on the RedSeal server, upload the license.

   ```
   upload license <url_to_license>
   ```

2. Verify the license is installed.

   ```
   show license
   ```

Install the RedSeal license by copying

Purpose

You can copy the contents of a text file that contains the license and paste it in the RedSeal CLI to install it.

Procedure

1. In a text editor, open the text file containing the license and copy the contents, including `--begin` and `end--` markers.
2. In a terminal window, SSH to the RedSeal server.
3. Shut down the server if it is running.

   ```
   shutdown <server>
   ```
4. Install the license.

   ```
   set license
   ```
5. When prompted, paste the copied license text into the CLI, and press `Ctrl-D`.
6. Start the server.

   ```
   startup <server>
   ```
7. Verify the license is installed.

   ```
   show license
   ```

View STIG module status

Purpose

Review the status of your license. If you have purchased STIGs for specific vendor platforms, you can check that they are enabled.

Details

RedSeal enforces STIG checks on a per-vendor basis. Existing STIG license holders now have Cisco and Juniper STIG checks in their implementation. For details on Palo Alto Networks and F5 checks, contact your account team. RedSeal currently enforces STIG checks for the following vendors:

- Cisco

- Juniper
- F5
- Palo Alto Networks

Procedure

1. Choose **View > License**.

   The License Status window displays.
2. Under **STIG Module** confirm that modules you have selected for your implementations, are Enabled..

Import the STIG ENC file

Purpose

RedSeal enforces STIG checks on a per-vendor basis. Import the vendor-specific STIG ENC file to apply and view the STIG checks.

Procedure

1. Choose **File > Import**.

   The **Data Import** window displays.
2. From the **File Import** tab, choose **STIG/CIS** data type.

   The available STIG ENC files appear in a list.
3. Select the STIG ENC file you want to import, and click **Import**.

   The **Import Status** tab shows the status of the file imports.

13

Troubleshooting

Introduction

You can perform troubleshooting tasks when file transfers fail or performance is slow. It is also important to understand why the inventory and map might not match and how to interpret disk space alerts. You can also collect troubleshooting information for data collection tasks.

Failed file transfers

Introduction

File transfers can fail with a generic ***bad syntax*** error message if your URL contains invalid characters in the user ID or password included for authentication.

Reserved characters

Reserved characters must be encoded, with the percent sign (%) followed by the character's hex equivalent. The table identifies some character encodings (search the Internet for URL encodings):

Character	Symbol	Hex Value
'at' symbol	@	40
ampersand	&	26
bracket (left)	[	5B

bracket (right)	]	5D
colon	:	3A
comma	,	2C
cross hatch	#	23
dollar sign	$	24
equals sign	=	3D
forward slash	/	2F
plus sign	+	2B
question-mark	?	3F
semi-colon	;	3B

For example, if your user name is ***jsmith***, your password is ***p@ssword***, and your FTP server's hostname is ***example.com***, enter the URL:

See *URL path rule* on page 172.

Performance issues

Introduction

There are tasks you can perform to address when analysis performance is very slow.

Analysis Information in the System Summary

If analysis performance is very slow, examine the server logs or select **View > System** to display the System Summary to help diagnose the cause. For help in diagnosing the issue, contact RedSeal Support.

The Analysis Information section of the System Summary shows how long each phase takes. The stage called Netmap BPC's in the System Summary is also called

NETMAP_NCC in the server logs. If this stage of analysis is the cause of the problem, you can improve performance by turning it off using the `netmap_ncc_enabled` server property.

NETMAP_NCC is the name for the set of Best Practice Checks from RS-62 through RS70:

- Untrusted Remote Login Access to Network Device (RS-62)
- Untrusted Network Device Access (RS-63)
- Untrusted Netbios Access (RS-64)
- Untrusted Access to ANY Service (RS-65)
- Untrusted Remote Login Access (RS-66)
- Untrusted Miscellaneous Service Access (RS-67)
- Untrusted SNMP Access (RS-68)
- Untrusted Traceroute and Ping Access (RS-69)
- Bogon/Private Address as External Source (RS-70)

NETMAP_NCC checks examine access from untrusted sources to the entire network. In large networks, each failure means hundreds or thousands of results showing access from a single untrusted source to exposed network devices.

How turning off NETMAP_NCC affects security

Turning off these checks lowers your Best Practice Check count. Other scores, like your Risk Analysis score, are not affected. The overall Digital Resilience Score is not affected by this change unless access from untrusted sources is one of the most common and most severe problems in your environment.

Most Best Practice Checks uncover misconfigurations on individual devices and are addressed by fixing those specific devices. The NETMAP_NCC checks show larger systemic problems that are more difficult to investigate and fix.

If you do not want to turn off these checks permanently, you can disable them while you are building your model and addressing the simpler configuration issues uncovered by most checks. Re-enable the NETMAP_NCC checks after you have corrected the majority of basic configuration issues found.

Turn off NetNCC Best Practice Checks

If the server logs indicate that the NETMAP_NCC stage of analysis is causing performance issues, you can turn off that stage using the `set property server netmap_ncc_enabled false` command. To turn the checks back on, use the `set property server netmap_ncc_enabled true` command

Size, complexity, and performance

Introduction

As the size and complexity of the object model of your network increases, so does the amount of computing resources required by the RedSeal server. Network size is defined by number of hosts referenced in the VA scan data. Complexity is a factor of such things as the number of access rules, which are equivalent to lines in an access control list.

Analysis and file import performance

It is not possible to define the exact nature of network performance and differing tolerance thresholds among users. There may be some tradeoffs. For example, if the number of hosts is smaller, then the number of access rules can be larger and non-contiguous rules have a larger impact on complexity than contiguous rules. They are unique to each network environment.

The most important variable appears to be the amount of RAM available to the server when it analyzes the network. See *Hardware specifications*

The RedSeal server should be able to work at acceptable performance levels with networks of up to 5,000 hosts and up to 50,000 ACL rules.

As you approach or exceed these metrics, you can expect the RedSeal software to require more time to import VA scan data, and more time to analyze network vulnerabilities. At the upper limits, these operations can take several hours to complete.

Alerts

Introduction

It is important to identify Low Disk Space and Low Log Partitions Space alerts.

Low Disk Space Alerts

When the available disk space is less than 10 percent, a red icon is displayed in the **Overall Health** pane of the **Home** tab in the client interface. The disk space is checked every 10 minutes.

Low Log Partition Space Alerts

When the available log partition space is less than 10 percent, a red icon is displayed in the **Overall Health** pane of the **Home** tab in the client interface. The log partition space is checked every 15 minutes.

Database maintenance tasks

Introduction

On rare occasions, very large enterprises may have to run vacuum and indexing operations on the Postgres database.

Vacuum and indexing

The vacuum and indexing tasks on the Postgres database are manual operations. The Vacuum Full option can also be scheduled to run automatically however, this is not recommended, see following section *Configure an automatic database maintenance task*.

To perform these operations, select **Admin > DB Maintenance Tasks** in the RedSeal client application. Options are:

- **Vacuum Analyze**—performs a vacuum operation (reclaims storage space) on the selected tables and analyzes the tables to help make queries more efficient. This operation may improve query performance. You can continue to work while this process runs in the background.
- **Vacuum Full**—performs a full vacuum operation (rewrites the entire table) on selected tables. This operation frees up disk space but must be used with caution. You must ensure no other tasks run concurrently with this task. Treat the system as down for maintenance.
- **Re-Index Tables**—rebuilds corrupted indexes, but should never be used unless you see significant performance degradation. Blocks other user activity while it runs. Only brings performance improvements in unusual situations.

Select the tables to be vacuumed or indexed in the drop-down targets menu.

Use the **verbose** check box to determine the quantity of status message text. If you select verbose, the status pane at the bottom of the dialog shows detailed progress through the chosen task. If verbose is not selected, the status pane shows the start and completion of the task.

Note Postgres cautions against frequent use of vacuuming and indexing operations. An ***autovacuum*** process that runs periodically without user intervention is intended to keep the database properly maintained. However, RedSeal has seen some databases in large, network-intensive enterprises stop working until vacuum and indexing operations were performed. Use these tools sparingly. Postgres advises that overuse can degrade, rather than enhance, database performance.

Configure an automatic database maintenance task

RedSeal allows you to configure an automatic database maintenance task to perform a Vacuum Full operation on the Postgres database. The Database maintenance task is a time-based operation scheduled to take place at regular intervals. However, it important to note that it ***not recommended*** to schedule a Vacuum Full maintenance task. Instead run this task manually when required. Use a schedule only if the window for this task is at a time when there is nobody available to run it manually. You must ensure no other tasks run concurrently with this task. Treat the system as down for maintenance.

To schedule an automatic database maintenance task:

1. In the RedSeal client application, select **Admin > Database > Configure Auto Database Maintenance**
2. Select a frequency for the database maintenance schedule task, then set the details as appropriate for that frequency:
   - **Weekly**—set the time of day as described for daily (only one allowed), then use the check boxes to select one or more days of the week to configure the weekly database maintenance task.

  - **Monthly**—set the time of day as described for daily (only one allowed), then select the day of the month to configure the monthly database maintenance task.

3. Select **Save**.
4. To cancel the configured automatic database maintenance task, select **Delete**.

Data collection troubleshooting bundle

Introduction

It is now possible to run a data collection task in troubleshooting mode to collect logs and other relevant information. When you run a data collection task in this mode, it sets log levels to DEBUG for the device and communication plug-ins used in the task. These logs and other relevant information are bundled into a ZIP file, which can be downloaded and sent to RedSeal Support, to troubleshoot problems that occur with data collection from a device or endpoint plug-in.

It is important to note this utility is to be used for focused troubleshooting. RedSeal recommends that you do not import a large number of devices when running a data collection task in troubleshooting mode. Use filters to narrow down the device to be imported in troubleshooting mode. Running a data collection task in this mode is available on demand for one task at a time and cannot be scheduled. When a task in this mode completes, logs are reset to their previous levels.

If a data collection task running in troubleshooting mode fails, or is canceled, all relevant data up to the point of failure or cancellation, is collected and bundled into a ZIP file.

The following data is collected in troubleshooting mode:

- Logs in DEBUG mode
- RSXML
- SSH transcripts
- Data collection task profile, which includes,
  - plug-in type and version
  - task details
  - live data collection information, if the option is selected

  - proxy information, if one is configured

- Import Status
- System details

This first version of the data collection troubleshooting feature has certain limitations.

- Only one data collection task at a time can run in troubleshooting mode.
- The current version of this utility covers all SSH based plug-ins but may not be as comprehensive for others such as REST API plug-ins.
- The Auto-detect data type is not supported at this time.

Run a data collection task in troubleshooting mode

1. To run a data collection task in troubleshooting mode, choose **File > Import** in the RedSeal client application, the **Data Import** window displays.
2. Navigate to the **Data Collection** tab and select a data collection task.
3. Right-click the task and select **Run in Troubleshooting Mode** from the menu. A warning displays about the information collected in this mode, click **Yes** to proceed.
4. When the task completes, navigate to the **Import Status** tab and select the task. The **Details** pane contains the status of the task and a URL to download the troubleshooting bundle.
5. Copy the URL and paste it in your browser, replacing the ***<your server here>*** placeholder text with the FQDN or IP address of your RedSeal Server. The ZIP file is downloaded to the default location set in your browser.

   The messages in the **Details** pane also include instructions to download the file using the RedSeal API.

When the download completes, the ZIP file is deleted from RedSeal. The file is deleted after 72 hours during the nightly purge. This can be changed using the server property `ts_bundle_purge_after_in_days`.

You can choose not to delete the file by setting the URL flag to false as follows: `?deleteFromServerAfterDownload=false`

A maximum of five ZIP files can be saved on the RedSeal server. If you already have five of these troubleshooting bundles saved on RedSeal, and you run another task in troubleshooting mode, an error is displayed on the **Import Status** tab.

You can change the number of files that can be stored using the server property `ts_bundle_max_number _of_bundles`.

See *set property* for how to set server properties.

14

Command line interface

Introduction

The operating system includes a command line interface (CLI) that is similar in structure and operation to the CLI on a typical routing device.

Management tasks

Using the CLI, you can perform these management tasks on an appliance:

- configure and maintain the operating system
- manage the database
- manage the model of your network, and
- check the health of your server.

Set and show commands

Similar to a router CLI, this CLI includes numerous `set` and `show` commands for setting various values and viewing their current settings.

Requirement for access

To use the CLI, you must have console or SSH access to the appliance.

Log in to the CLI

Purpose

You need to access the CLI to complete many of the administrative tasks.

Details

The console CLI session does not time out. You can enable an SSH CLI session timeout. Note, that third-party emulation software, which you might use for both SSH and Ethernet or VGA access, might have their own timeout periods.

Procedure

1. Enter the user name `cliadmin`.
2. Enter the CLI administrator password.

   If you followed the appliance installation and configuration instructions, this password was set when you initially configured the appliance.
3. Log out of the CLI when you are finished.

   ```
   exit
   ```

CLI session restrictions

Statement

Only operate one CLI session at a time.

Applicability

On occasion you may need to open a second session. For example, in order to restart the server or to enable access for RedSeal Technical Support.

Outcome

Nothing currently prevents multiple sessions, but having multiple sessions open is not recommended because it may cause unpredictable behavior on the appliance. See *set max-concurrent-session-per-user* on page 203.

CLI syntax

Introduction

The CLI follows a specific syntax to clarify the relationships between commands and arguments. Several commands take one or more arguments, where some of them are required and some of them are optional.

Curly braces and square brackets

Curly braces ({ }) or parenthesis (( )) indicate that an argument is required; square brackets ([ ]) indicate the argument is optional.

Curly braces nested inside square brackets

Curly braces or parenthesis nested inside square brackets means that if you use the optional argument, one of the entries inside the curly braces or parenthesis is required.

Optional argument example

```
set interface [INTERFACE] [ speed { 10 | 100 } ] [ duplex { half |
full } ] [ autoneg { on | off } ]
```

The `set interface` command takes either speed and duplex arguments or the autoneg argument:

- `speed`
  - if you configure `speed`, you must specify either 10 or 100
- `duplex`
  - if you configure `duplex`, you must specify either `half` or `full`
- `autoneg`
  - if you use `autoneg`, you must specify `on` or `off`

Required argument example

```
set dns { primary | secondary } <IP_ADDR>
```

In this example, you must specify either primary or secondary in the `set dns` command. The command also requires an IP address, as indicated by the `<IP_ADDR>` placeholder .

Vertical pipe

The vertical pipe symbol (|) separates possible valid values.

Angle brackets

Angle brackets (< >) indicate a placeholder value where you need to enter user-specific data. If an argument is not enclosed in brackets, that argument is required.

Case-sensitivity

The CLI is case-sensitive.

SCP and SFTP use prerequisite

Statement

Before you can use SCP or SFTP, you must first generate a DSA key on the appliance by starting the SSH daemon with the `enable autostart ssh` command.

Disable SSH daemon

After the process has created the DSA key, you can disable the process using the `disable autostart ssh` command if you do not want SSH running on the appliance.

See *enable autostart* on page 187 and *disable autostart* on page 184.

URL path rule

Statement

When transferring files using SCP, FTP, or SFTP, be sure the URL contains the correct path to the file.

Reserved characters

Reserved characters must be encoded, with the percent sign (%) followed by the character's hex equivalent. The table identifies some character encodings (search the Internet for URL encodings):

Character	Symbol	Hex Value
'at' symbol	@	40
ampersand	&	26
bracket (left)	[	5B
bracket (right)	]	5D
colon	:	3A
comma	,	2C
cross hatch	#	23
dollar sign	$	24
equals sign	=	3D
forward slash	/	2F
plus sign	+	2B
question-mark	?	3F
semi-colon	;	3B

Single slash

A single slash between the hostname and the path denotes a location relative to the home directory of the logged in user.

Example

The `plugin.jar` being uploaded should be in the `tmp` folder in the home directory of the user specified in the command.

```
upload plugin scp://user:pass@server/tmp/plugin.jar
```

Double slash

A double slash between the hostname and the path denotes an absolute path.

Example

The `plugin.jar` being uploaded should be in the `/tmp` directory:

```
upload plugin scp://user:pass@server//tmp/plugin.jar
```

Find a command using the CLI online help

Purpose

Use the CLI online help to determine the appropriate command to use.

Procedure

1. Access the online help.

   `help`

   A list of command names and brief descriptions displays. This list does not include the syntax for each command.
2. Scroll down the list to find the command you want to use.
3. To see the syntax for the command.

   `help <command>` OR

   `<command> ?`

   For example, to see the syntax for the `set date` command enter `help set date`.

   Note If you enter part of a command, such as only the word `set`, you see a list of the possible `set` commands along with a description, but not the syntax.

Output filtering

Introduction

Output filtering is available for any CLI command, but you typically use it for `show` commands.

Filter types

There are five filter types:

Filter type	Description
include	Shows only lines that contain the value string.
exclude	Shows only lines that do not contain the value string.
begin	Shows only lines that begin with the value string. When filtering output from the `show logfile` command by date, use the YYYY-MM-DD format: `show logfile server | begin 2018-08-09`
glob	Same as `include`. Shows only lines that contain the value string, except the value string may contain these globbing characters: • asterisk (*), meaning any number of valid characters • question mark (?), meaning one valid character • character classes, such as [a-z]
regexp	Filter based on the regular expression in the value string, using Java regular expression syntax (pattern).

Filter the output

To filter the output, add a pipe character (|), the filtering type, and a value string to the end of the command.

Quotation marks in the value string

You do not need quotation marks for the value string. The CLI assumes all characters after the filter type and the first space following it constitute the entire value string. If you enter quotation marks at the start and end of the value string, the CLI strips them off silently. The CLI treats quotation marks at any place else in the value string as literals and leaves them in.

Example

This example uses the `show support-summary` command and the filter type `include` to output only lines that contain the string “File not found”.

```
show support-summary | include File not found
```

Alphabetical list of commands

Introduction

This section provides command syntax, descriptions, and examples. SNMP commands used to check server health and Smart Card commands are in their own sections.

add interface role

Introduction

Adds a role to an interface.

```
add interface role <INTERFACE> { model-admin | server-
admin }
```

Example

This example shows the model-admin role being added to the eth1 interface.

```
add interface role eth1 model-admin
```

Description

An interface role is a set of application services allowed on a specific interface. A role can be enabled on an interface to control the type of traffic allowed on that interface. All roles are enabled by default on all interfaces. A role controls which applications or services are allowed on that interface. There are three interface roles available:

Interface role	Description
Data Collection	Data collection tasks and MST data collection tasks. This role cannot be added or removed from an interface.
Server Admin	SSH, SNMP for basic administration using the CLI
Model Admin	Java client, R2/R3 Web Interface, REST APIs, cluster communication, and RSMM management

See *show interface roles* on page 219 and *remove interface role* on page 194.

add route

Introduction

Adds a static route to the routing table.

```
add route <IP_ADDRESS> <NETMASK_VALUE> <GATEWAY> [
INTERFACE ]
```

Example

This example shows the specified static route being added to the routing table.

```
add route 192.168.234.0 255.255.255.0 192.168.152.1
```

Description

Use this command to add routes to networks from where data collection tasks need to run. If `INTERFACE` is not provided, the interface for the route is determined by the gateway.

See also *delete route* on page 183.

add spoke

Introduction

Adds a spoke to a datahub.

```
add spoke <ADDRESS>
```

Example

To add a spoke server on the datahub.

```
add spoke 172.16.0.68
```

Description

Converts a standalone server to a datahub. Use this command on the server that is functioning as the datahub.

See also *delete spoke* on page 183.

backup

Introduction

Backs up and encrypts customer-specific data to a location other than the appliance.

```
backup [ with-analysis | no-analysis ] <URL>
```

with-analysis	Analysis data is included in the backup file. This keyword is optional; if omitted, analysis data is not included.
no-analysis	Analysis data is not included in the backup file. This keyword is optional; if omitted, analysis data is not included.

Description

Use the command to store the backup on an external device; specify an FTP, SFTP, or SCP URL. See *URL path rule* on page 172.

Since very large, complex networks can generate enormous volumes of data during analysis, you have the option to include or exclude analytical data when performing a backup. Having to process very large (multi-gigabyte) files can add considerably to the time it takes the server to complete a backup.

If the URL specifies a file name that does not end with `.enc`, it is added.

If the URL specifies a directory, not a complete file path, a file name is generated automatically in the form: `rs_data_<yyyymmddhhss>.enc`, where "<yyyymmddhhss>" represents the date-time stamp.

If you have a choice, RedSeal recommends SFTP rather than FTP or SCP as the most reliable, especially with files larger than 2GB.

The <pwd> argument is optional for SFTP or SCP, provided the target device is configured correctly with a DSA credential generated on the appliance. If this credential is properly installed on the targeted host, you can use either SFTP or SCP without having to enter a password in the command. If SSH is not set up correctly, the connection attempt fails. You are not prompted for a password. See *save credential* on page 196.

You are prompted to supply the data password that was set by using the set password command. See *set password* on page 207.

See *show backups* on page 212.

clear

Introduction

Clears the screen.

```
clear
```

cls

Introduction

Clears the screen.

```
cls
```

create cert-request

Introduction

Generates a request for an SSL certificate which you can then use to obtain a digital certificate from a certificate authority (CA) that can be imported into your server.

```
create cert-request <URL>
```

Description

In the command, `URL` should point to the location where you want the request file to be written.

See also *upload certificate* on page 229.

For information about URL syntax, see *backup* on page 178.

create self-certificate

Introduction

Generates a self-signed SSL certificate which is installed the next time the server is restarted.

```
create self-certificate
```

Description

This certificate is used for communication between the server and the user interface, and also with web browsers. When you create a self-signed SSL, you specify these items:

Item	Description
CN	Hostname (the fully qualified domain name of your server)
Keysize	2048 **Note** You cannot create a self-certificate with a key size less than 2048 bits.

OU	Organization unit
O	Organization
L	City
ST	State
C	Country

Shut down and restart the server

For the new certificate to take effect, shut down and restart the server using the `shutdown server` and `startup server` commands.

delete gateway

Introduction

Deletes the default gateway from the server configuration.

```
delete gateway
```

See *set gateway* on page 199.

delete image

Introduction

Deletes a specific image.

```
delete image { <FULL_NAME> | <SHORT_NAME> }
```

Example

This example deletes the image with the short name “Build-2319”.

```
show images

Current Next         RedSeal 9.2.0 (Build-20484)
```

```
                    RedSeal 9.1.2 (Build-2319)
delete image Build-2319
```

Description

You can enter the image's full or short name as shown by the `show images` command. In the example, the short name is the information in parenthesis.

For example, in this CLI output the full name of the image is "RedSeal N.N (Build-nnn)" and the short name is "Build-nnn" (where "N.N" and "nnn" are replaced by version and build numbers).

See *show images* on page 218.

delete ntp

Introduction

Deletes an NTP server.

```
delete ntp { <NTP_SERVER_NAME_OR_IP_LIST> }
```

Example

This example deletes the NTP server 172.16.0.66.

```
delete ntp 172.16.0.66
```

Description

Provide a comma-seperated list of up to 5 servers. Deletes all listed NTP servers.

Use `set ntp off` to clear all NTP servers and shut down the NTP process.

Specify either the fully qualified domain name or the IP address of the NTP server.

See *set ntp* on page 205.

delete property

Introduction

Deletes the value for the specified property for the specified server process.

```
delete property server <PROPERTY_NAME>
```

See *show property* on page 221 and *set property* on page 209.

delete route

Introduction

Deletes a static route from the routing table.

```
delete route <IP_ADDRESS> <NETMASK_VALUE> <GATEWAY> [
INTERFACE ]
```

Example

This example shows the route to 192.168.234.0 being deleted.

```
delete route 192.168.234.0 255.255.255.0 192.168.152.1
```

See *add route* on page 177 and *show route* on page 222

delete spoke

Introduction

Unregisters a spoke from the datahub of a cluster.

```
Delete spoke <IP_ADDRESS>
```

Example

This example unregisters spoke 172.16.0.68 from the datahub of the cluster.

```
delete spoke 172.16.0.68
```

Description

After unregistering the spoke from the datahub of the cluster, you must then log in to the spoke that was deleted and enter the `unset datahub` command to revert the spoke to a standalone RedSeal appliance.

See *add spoke* on page 178 and *unset datahub* on page 229.

delete ssh public-key

Introduction

Deletes public keys stored in a local database for SSH authentication.

```
delete ssh public-key ( IP | hostname | all )
```

See *Store SSH authentication keys locally* on page 150.

See *set ssh public-key* on page 211.

See *show ssh public-key*.

disable autostart

Introduction

Disables autostart for the specified process and stops the process.

```
disable autostart ( ssh | snmp )
```

Description

By default, autostart is disabled for both SNMP and SSH.

See *enable autostart* on page 187 and *status autostart* on page 227.

disable cipher-suites server

Introduction

Disables cipher suites used by the server.

```
disable cipher-suites server <CIPHER_SUITES>
```

Example

This example disables the cipher suite named `TLS_RSA_WITH_AES_128_CBC_SHA`.

```
disable cipher-suites server TLS_RSA_WITH_AES_128_CBC_SHA
Disabling cipher suites will restart the server and admin server
process.
Do you want to proceed? [(Y)es or (N)o] y
Restarting admin server...
```

```
Command succeeded.
```

Description

To conform to your organization's internal policies, use this command to disable cipher suites you do not want to be used by the server. You are prompted to confirm the disable. After the command is executed, the admin server and server are restarted. To disable multiple cipher suites with one command, type a comma-separated list of cipher-suite names.

See *show cipher-suites* on page 213 and *enable cipher-suites server* on page 188.

disable cipher-suites ssh

Introduction

Disables cipher suites and message authentication code (MAC) algorithms used by the SSH process.

```
disable cipher-suites ssh (ciphers|macs) <CIPHERS>
```

Example

The first example disables the cipher suite named `aes128-ctr`. The second example disables the MAC algorithm named `umac-64@openssh.com`.

```
disable cipher-suites ssh ciphers aes128-ctr
Command succeeded.


disable cipher-suites ssh macs umac-64@openssh.com
Command succeeded.
```

Description

To conform to your organization's internal policies, use this command to disable cipher suites and MAC algorithms you do not want to be used by the SSH process. To disable multiple cipher suites or MAC algorithms with one command, type a comma-separated list of cipher-suite or MAC-algorithm names.

See *enable cipher-suites ssh* on page 188 and *show cipher-suites* on page 213.

disable common-criteria

Introduction

Disables all commands and settings required for Common Criteria compliance.

```
disable common-criteria
```

Description

Use this option to disable all the commands and settings required for Common Criteria compliance.

See *enable common-criteria* on page 189.

disable interface

Introduction

Disables an interface.

```
disable interface [ INTERFACE ]
```

Description

If you are using multiple interfaces, use the `INTERFACE` argument to specify the interface to be disabled. If it is not specified, eth0 is used by default.

See *enable interface* on page 189 and *show interface* on page 218.

disable outbound ssh

Introduction

Disables the SSH client communications protocol from creating SSH sessions with your server.

```
disable outbound ssh
```

Description

By default, the state of SSH is disabled.

See *enable outbound ssh* on page 190.

disable paging

Introduction

Disables CLI output paging.

```
disable paging
```

Description

All output from a CLI command is displayed without pause.

See *enable paging* on page 190.

disable support access

Introduction

Disables special access for RedSeal Technical Support.

```
disable support-access
```

Description

By default, support access is disabled.

See *enable support-access* on page 191 and *status support-access* on page 227.

enable autostart

Introduction

Enables autostart and starts the process.

```
enable autostart ( ssh | snmp )
```

Description

When enabled, the process is automatically restarted following a reboot of the appliance.

The process is automatically disabled if you reset the `cliadmin` password to its default condition.

See *disable autostart* on page 184, *Reset CLI password* on page 64, and *status autostart* on page 227.

enable cipher-suites server

Introduction

Enables cipher suites used by the server.

```
enable cipher-suites server <CIPHER_SUITES>
```

Example

This example enables the cipher suite named `TLS_RSA_WITH_AES_128_CBC_SHA`.

```
enable cipher-suites server TLS_RSA_WITH_AES_128_CBC_SHA
Enabling cipher suites will restart the server and admin server
process.
Do you want to proceed? [(Y)es or (N)o] y
Restarting admin server...
Command succeeded.
```

Description

Use this command to enable cipher suites you previously disabled on the server. You are prompted to confirm the enable. After the command is executed, the server and admin server are restarted. To enable multiple cipher suites with one command, type a comma-separated list of cipher-suite names.

See *show cipher-suites* on page 213 and *disable cipher-suites server* on page 184.

enable cipher-suites ssh

Introduction

Enables cipher suites and message authentication code (MAC) algorithms used by the SSH process.

```
enable cipher-suites ssh (ciphers|macs) <CIPHERS>
```

Example

The first example enables the cipher suite named `aes128-ctr`. The second example enables the MAC algorithm with the name `umac-64@openssh.com`.

```
enable cipher-suites ssh ciphers aes128-ctr
Command succeeded.


enable cipher-suites ssh macs umac-64@openssh.com
Command succeeded.
```

Description

Use this command to enable cipher suites and MAC algorithms you previously disabled for the SSH process. To enable multiple cipher suites or MAC algorithms with one command, type a comma-separated list of cipher-suite or MAC-algorithm names.

See *show cipher-suites* on page 213 and *disable cipher-suites ssh* on page 185.

enable common-criteria

Introduction

Enables all commands and settings required for Common Criteria compliance.

```
enable common-criteria
```

Description

Use this option to enable all the commands and settings required for Common Criteria compliance.

See *disable common-criteria* on page 186.

enable interface

Introduction

Enables an interface.

```
enable interface [INTERFACE ]
```

Example

This example shows interface eth1 being enabled.

```
enable interface eth1
```

Description

Use the `INTERFACE` argument to specify the interface to be enabled. If it is not specified, eth0 is used by default.

See *disable interface* on page 186 and *show interface* on page 218.

enable outbound ssh

Introduction

Enables the SSH client communications protocol to create SSH sessions with your servers.

```
enable outbound ssh
```

Description

By default, the state of ssh is disabled.

See *disable outbound ssh* on page 186.

enable paging

Introduction

Enables CLI output paging.

```
enable paging
```

Description

Output is shown a page at a time rather than all output being displayed at once, without pause. By default, paging is enabled.

See *disable paging* on page 187.

enable support-access

Introduction

Enables special access for RedSeal Technical Support.

```
enable support-access
```

Description

Use this option after consulting with RedSeal Technical Support. When a new image is uploaded to the system, support access is disabled after the appliance is rebooted with the new image regardless of its state before the upload.

See *disable support access* on page 187 and *status support-access* on page 227.

export user-inputs

Introduction

Exports data entered by users into the user interface, such as the unnumbered interfaces from your network blueprint, to an XML file, in native RedSeal XML format.

```
export user-inputs <URL>
```

Example

This example shows the command format used to export the user input to an FTP server and provide the username and password.

```
export user-inputs ftp://<usr>:<pwd>@<host>/<dest>
```

Description

The FTP, SFTP or SCP URL specifies a directory, not a complete file path. The file name is generated automatically and is in the form: `rs_user_inputs_yyyymmddhhss.xml`, where “yyyymmddhhss” represents the date and timestamp.

For information about the URL syntax, see *backup* on page 178.

For information about relative and absolute paths when using SCP, see *URL path rule* on page 172.

For information about reserved characters in URLs, see *Failed file transfers* on page 159.

Use this command if, for example, you have manually linked the devices with unnumbered interfaces, which are originally listed in the `Unlinked` folder on the **Maps & Views** Tab of the RedSeal Java client application.

When you install a new image and re-import configuration files for these devices, you need to relink these unnumbered interfaces. To avoid having to link them manually, use the `export user-inputs` command to save your inputs to an XML file before you install a new image.

After you install the new image and re-import the configuration files, import the RedSeal Native XML file generated by the `export user-inputs` command to restore the links.

netstat

Introduction

Displays network statistics.

```
netstat
```

obliterate

Introduction

Overwrites all bytes on the appliance's hard disk drive, meeting specifications of the United States Department of Defense National Industrial Security Program Operating Manual (DoD NISPOM) section 5220.22-M.

```
obliterate
```

Description

Three passes are made, overwriting every data byte with 0, 1 and a randomly selected byte.

The `obliterate` command cannot be executed from a remote session. You must be logged in through the appliance's console port.

Because of the damage that can be done by misusing this command, it is hidden from view, which means it is not listed in the CLI online help, nor can you use TAB completion on a partial entry (`obli<TAB>`) to run the command.

The `reset` command with the `all` option clears the database and all logs from the appliance, without requiring a reload from a boot CD. See *reset* on page 194

CAUTION Do not use `obliterate` command unless you are absolutely certain you are finished using the appliance. After the command executes, your appliance's hard drive is wiped clean and the appliance is not usable. There is no confirmation that the command was executed, and, although there may be a message telling you to reboot, you are not able to log in to the device. After you have executed the command, there is no recovery.

ping

Introduction

Sends a UNIX ping datagram to the address identified by `dest_addr` and displays the response time on the command line.

```
ping [ ( count <COUNT> ) | (tcp [port <DESTINATION_PORT>]
) ] <DESTINATION>
```

Description

The number of packets sent is set by the count argument value (count). Include the keyword `tcp` to send a TCP packet. Specify the keyword `port` with a port number as the `dest_port` value to direct the TCP packet to a specific port.

ps

Introduction

Displays a list of all currently running processes.

```
ps
```

pstree

Introduction

Displays the current process tree.

```
pstree
```

reboot

Introduction

Reboots the appliance immediately.

```
reboot
```

remove interface role

Introduction

Removes a role from an interface.

```
remove interface role <INTERFACE> { model-admin | server
admin }
```

Example

This example shows the model-admin role being removed from the eth1 interface.

```
remove interface role eth1 model-admin
```

Description

All roles are enabled by default on all interfaces. The Data Collection role cannot be removed from an interface.

See *show interface roles* on page 219 and *add interface role* on page 176.

reset

Introduction

Resets the specified information to factory defaults.

```
reset { all | data }
```

all	Resets database tables, all Java properties, appliance configuration, and the TRL to factory defaults; clears all log files; deletes NTP keys, SSH known fingerprints, and user-added CA certificates in the key store; and resets the cliadmin, data, and uiadmin passwords; does not clear the currently installed license.

data Clears out and re-initializes the database; also resets the data and uiadmin passwords (but not the cliadmin password); log files remain in place; the server's Java properties and appliance configurations remain as currently set.

Description

After running `reset all`, you must run `set ip` to set a valid IP address before starting your servers. See *set ip* on page 201.

Clearing the database results in loss of network blueprint, threat analysis, and user-associated data (including such things as user accounts, topology layouts and scheduled tasks, for example).

When you use the `all` option, the currently loaded Threat Reference Library is deleted and the appliance returns to using the TRL that was originally installed.

When you use the `data` option, the currently loaded TRL is retained.

The `all` option is valid only when logged in directly to the console. Once executed, network connectivity is lost until reconfigured. You cannot enter `reset all` remotely.

restore

Introduction

Drops the current database tables and performs a restore of customer-specific data.

```
restore <URL>
```

Example

This examples show the command format used to restore the database from an FTP, SFTP, or SCP server and provide the username, password, hostname, and file path..

```
restore ftp://<user>:<pwd>@<host>/<dir>/<file>
restore sftp://<user>[:<pwd>]@<host>/<dir>/<file>
restore scp://<user>[:<pwd>]@<host>/<dir>/<file>
```

Description

You are prompted to supply the data password that was set by using the `set password` command. See *set password* on page 207.

Use an FTP, SFTP or SCP URL. For URL syntax, see *backup* on page 178.

See *SCP and SFTP use prerequisite* on page 172 and *URL path rule* on page 172.

save credential

Introduction

Saves a DSA public key to the specified FTP, SFTP, or SCP URL.

```
save credential dsa <url>
```

Description

When properly stored (using Open SSH's `ssh-agent`, for example) on the host where you want to keep your database backups, this DSA key allows SSH connections between the server and the remote host without having to enter a password each time.

See *show credential* on page 216.

save logfile

Introduction

Saves the named log to a remote host.

```
save logfile ( audit | analyzer | system | server )
( <SFTP_URL> | <SCP_URL> | <FTP_URL> )
```

Example

This example saves the log file to the remote `host1.acme.com` FTP server in the `temp/` directory.

```
save logfile server ftp://host1.acme.com/temp/
```

Description

You can use this command when you plan to e-mail the log to RedSeal Technical Support. The URL specifies a directory, not a complete file path. The file name is generated automatically and is in the form: `redseal_yyyymmddhhss.xml`, where "yyyymmddhhss" represents the date and timestamp.

set banner

Introduction

Sets a message that displays on the server. The server prompt you to type the message and then type **Ctrl+D** on a separate line to complete the command.

```
set banner { pre-authentication | post-authentication }
```

pre-authentication A message that is set to display after a user enters their username in but before entering their password.

post-authentication A message that can be set to display after the user authenticates.

Example

These examples set the pre-authentication message and the post-authentication message.

```
set banner pre-authentication
Type the pre-authentication banner message
Hit Control-D after typing the banner message.

set banner post-authentication
Type the post-authentication banner message
Hit Control-D after typing the banner message.
```

Description

To clear a banner so that nothing displays, run the set banner command using a series of spaces to replace the text.

See *show banner* on page 213.

set datahub

Introduction

Sets a datahub on a spoke and shuts down the server.

```
set datahub <IP_ADDR>
```

Example

This example sets the datahub 172.16.0.68 on the spoke.

```
set datahub 172.16.0.68
```

Description

This command should be followed by a `startup server` command.

See *show datahub* on page 216.

set date

Introduction

Sets the system date and time to the values specified.

```
set date <MM> <dd> <hh> <mm> [ [ <cc> ] | <yy> ] [ <.ss>
]
```

MM	month
dd	day of the month
hh	hour of the day
mm	minute
cc	century
yy	year
ss	second

Example

This example sets the system date to 15 August 2018 and the time to 13:50:55.

```
set date 081513502018.55
```

Description

After setting the date, reboot the appliance. This forces all processes to acquire the new date. Failure to reboot may cause system failures some time in the future.

Analysis does not run if any object in the database shows a time that is in the future. If the system is set to a future time prior to the `set date` reset, analysis cannot able to run until the interval between the current and future time has elapsed. Analysis is sensitive to date/timestamps associated with data in the database. Date and timestamps on existing objects are not affected by the `set date` command.

See *show date* on page 217.

set dns

Introduction

Sets which primary or secondary DNS server to use on the appliance. The IP_ADDR is the IP address of the DNS server.

```
set dns { primary | secondary } <IP_ADDR>
```

Example

This example sets the appliance to use the primary DNS server with the IP address 172.16.0.66.

```
set dns primary 172.16.0.66
```

Description

You must restart after setting a new DNS address.

See *show dns* on page 217.

set gateway

Introduction

Sets the default gateway for the server to use.

```
set gateway [ INTERFACE ] <GATEWAY_IP>
```

Example

This example sets the appliance to use 172.16.33.203 as the default gateway server on the eth1 interface.

```
set gateway eth1 172.16.33.203
```

Description

Specify the IP address of the gateway. Use the `INTERFACE` argument to identify the interface for which the gateway is being set when multiple network interfaces (NICs) are configured. If it is not specified, the eth0 interface is used by default.

See *delete gateway* on page 181.

set hostname

Introduction

Sets the fully qualified domain name of the appliance.

```
set hostname <HOST_NAME>
```

See *show hostname* on page 217.

set interface

Introduction

Sets the speed, duplex, or auto-negotiation state of the appliance's default network interface.

```
set interface [ speed { 10 | 100} ] [ duplex { half |
full } ] [ autoneg { on | off } ]
```

Example

This example sets the auto-negotiation state to `off`.

```
set interface autoneg off
```

Description

If you set the speed or duplex, auto-negotiation is turned off. The default is to use auto-negotiation, which can accommodate up to 1 Gb/s.

This is the interface line rate, not a guaranteed file transfer rate. File transfer speed can be affected by numerous variables beyond the reach of the appliance, including cable rating, the capabilities of the switch to which the appliance is connected, as well as the capabilities of the other device with which data is being transferred.

See *show interface* on page 218.

set ip

Introduction

Sets the IP address and subnet mask of interfaces on the appliance, or sets the appliance to use DHCP settings.

```
set ip [INTERFACE ]{ <IP_ADDR> <NETMASK> | dhcp }
```

Example

The first example sets the IP address and netmask of the default eth0 interface. The second example set the IP address and netmask of the specified eth1 interface. The third example enables DHCP.

```
set ip 172.16.0.66 255.255.255.0
```

```
set ip eth1 172.16.33.203 255.255.255.0
```

```
set ip dhcp
```

Description

Use the `INTERFACE` argument to set an IP address for a specific interface when using multiple NICs. If it is not specified, eth0 is the default. RedSeal recommends setting static IP addresses when using multiple network interfaces rather than using DHCP settings.

See *show ip* on page 219.

set license

Introduction

Installs a license on the server.

```
set license
```

Description

Obtain a license from support@redseal.net.

When you enter `set license` on the command line, instructions are displayed on the screen. When prompted, copy and paste the contents of the license file which you obtained from RedSeal onto the command line, then press **Ctrl+D**.

The license is installed into the appliance.

See *show license* on page 219.

set log

Introduction

Defines log rotation parameters for the named log. The log can be for the events, audit, analyzer, system, or server .

```
set log ( events | audit | analyzer | system | server )
[facility ( daemon | local0 | local1 | local2 | local3 |
local4 | local5 | local6 | local7 | user )] [level
( trace | debug | info | warn | error | fatal )]
[(frequency ( daily | weekly | monthly )) | (size <1-
1000> (KB|MB))] [number <positive number of logs>]
[remotehost ( primary | secondary ) ( <IP> | <IP:port> |
<hostname> | <hostname:port> | reset )] [connection-type
( none | TLS | SSL )]
```

Description

Log messages generated by the Postgres database are included in the server log.

The client log is maintained on the host on which the client is installed, in the directory `C:\Documents and Settings\<userID>\redseal`. "C:" is the installation directory, and "<userID"> is a Windows user account name.

Set `<num_logs>` to the number of files to be kept on the appliance at any one time, for the named log type. If `num_logs` is 5 (the default), the five most recently created log files are kept on the system, for each of the four log types.

The `frequency` and `size` parameters are mutually exclusive. Logs are rotated either on a set schedule or when the log file reaches a specified size. If you try to set both arguments in the same command, the command fails.

The `level`, `frequency`, and `number` parameters are not applicable when using the `events` parameter.

Size must be in the range of 1000 KB to 1000 MB. Maximum amount of space available on an appliance for all logs is 2 GB.

The `remotehost` parameters `IP` or `hostname` must point to a syslog server. Messages continue to be logged locally on the appliance. You must specify either primary or secondary, followed by an IP address or hostname for the log server, or the `reset` command argument .

The `reset` argument restores user-defined settings for the specified server to their default values:

- facility—different for each log:
  - server—local0
  - audit—local2
  - analyzer—local1
  - system—local3
  - events—local4
- level—info
- frequency—none (size is set instead)
- size—50MB
- number—5

See *show log* on page 219.

set max-concurrent-session-per-user

Introduction

Sets a limit on the number of concurrent user interface sessions per user across all interfaces.

```
set max-concurrent-session-per-user { <NUMBER> |
unlimited }
```

NUMBER	A non zero positive number.
unlimited	Sets no limit to the number of concurrent user interface sessions. The default is unlimited.

Example

This example sets a limit of 5.

```
set max-concurrent-session-per-user 5
```

Description

If a user attempts to open more sessions than the allowed limit, an error message is displayed informing the user that the maximum limit of concurrent sessions has been reached.

See *show max-concurrent-session-per-user* on page 220.

set min-password-length

Introduction

Sets the minumum required password length. If this value is not set, the default password length is 7-128 characters, as required by NSS FIPS. When the server property `redseal.srm.strictPasswordCheck` is enabled, the minimum character length is 15.

```
set min-password-length <VALUE FROM 7 to 128>
```

See *show min-password-length* on page 220.

set next image

Introduction

Sets a pointer to the image to be used after a reboot.

```
set next image { <FULL_NAME> | <SHORT_NAME> }
```

FULL_NAME	The complete name of the image as displayed by the show images command.
SHORT_NAME	The text shown in the parenthesis of the full name.

Example of full and short names

If the full name is “RedSeal N.N (Build-nnn)”, the short name is “Build-nnn”.

```
show images
```

```
Current Next         RedSeal 9.2.0 (Build-20484)
                     RedSeal 9.1.2 (Build-2319)
```

Description

The image must already be available on the appliance. Use the `set next image` command to rollback to an older version.

See *upload image* on page 230 and *show images* on page 218.

set ntp

Introduction

Sets the NTP servers to use for the appliance.

```
set ntp { off | { {servers}
<NTP_SERVER_NAME_OR_IP_LIST> } }
```

Example

This example sets the appliance to use NTP server 172.16.0.66.

```
set ntp servers 172.16.0.66
```

Description

Provide a comma-seperated list of up to 5 servers. If multiple servers are configured, both are contacted and the system clock is set according to the NTP assessment of reliability between the two sources.

Use the `off` keyword to clear all NTP servers and shut down the NTP process. After executing `set ntp off`, the `show ntp` command returns the message “There are no NTP servers (the local ntpd is not running).”

Specify either the fully qualified domain name or the IP address of the NTP server.

See *show ntp* on page 221.

See *set ntp* on page 205.

set ntp authentication symmetric add-key

Introduction

Configures a set of keys in the appliance database to authenticate a source of time.

```
set ntp authentication symmetric add-key { MD5 | SHA |
SHA1 } <KEY_ID> <KEY_VALUE>
```

Example

This example configures a key in the appliance database to authenticate a source of time.

```
set ntp authentication symmetric add-key MD5 12 qMiaJLkk(Z7iSovN>cK1
```

Description

Symmetric key authentication requires both the NTP client and server to share the same set of keys.

Key IDs can be from 1 to 65534. Key values for

- MD5 can be a 20-character printable ASCII string, and
- SHA/SHA1 can be a 40-character hex string.

set ntp authentication

Introduction

Sets the Key ID used to authenticate the specified server as a source of time and enables authentication.

```
set ntp authentication { off | { symmetric configure-key
trusted <KEY_ID> <NTP_SERVER> } }
```

Example

This example specifies key 12 to be used to authenticate server 172.16.0.66 as a source of time and enables authentication.

```
set ntp authentication symmetric configure-key trusted 12 172.16.0.66
```

Description

If primary and secondary servers are configured, use the `set ntp authentication` command to configure Key IDs for both servers.

Key IDs can be 1 to 65534 and must first be set for sharing in the appliance database using the `set ntp authentication symmetric add-key` command.

To disable NTP server authentication, use the `set ntp authentication off` command.

set password

Introduction

Sets a password.

```
set password { cliadmin | data | uiadmin }
```

cliadmin The password for the CLI administrative user account; for logging in to the CLI.

data This password is used for encrypting credentials and backups. The data password must be FIPS (Federal Information Processing Standards) compliant. See *https://www.nist.gov*.

uiadmin This password is for the uiadmin user account for logging in to the client user interface. After this password is set, the first person who logs in from the client application needs to log in as `uiadmin` and enter this password.

Description

After you enter this command, you are prompted to enter a password of at least seven characters, and then you are prompted to enter it again to confirm it.

Password syntax

Passwords for `cliadmin`, `uiadmin`, and other users, can contain any printable ASCII character except the space character.

The `data` password can contain any printable ASCII character except + \ , : " < > # and the space character.

Passwords for data collection credentials can contain any characters supported by the device targeted by the collection task.

set port server

Introduction

Changes the default port numbers used for processes.

```
set port server <server_port_number> <JMS_port_number>
<admin_port_number> <http_port_number>
<https_port_number> <https_certauth_port_number>
```

server The port used by the client to connect to the server. Default: 3825 . Required argument but not configurable.

JMS The port used by the client to connect to the JMS server. Default: 3826

admin The port used by the client to connect to the administrative server process. Default: 3835,

http The port used to connect to the HTTP server. Default: 80

https The port used to connect to the HTTPS server. Default: 443

https_certauth The port used to connect to the https certificate authentication server. This port must be open to enable certificate authentication. Default: 10443

Example

This example sets the `server_port_number` , `JMS_port_number`, `admin_port_number`, `http_port_number`, `https_port_number`, and `https_certauth_port_number`. The status all command shows the results.

```
set port server 3921 3922 3923 3924 3925 3926
Command succeeded.

RedSeal> status all
admin                 auto enabled     tcp 3923   running
server                auto enabled     tcp 3825   running
server-jms            auto enabled     tcp 3922   running
server-http           auto enabled     tcp 3924   running
server-https          auto enabled     tcp 3925   running
server-https-cert     auto disabled    tcp 3926   not running
server-elasticsearch auto enabled     tcp 9200   not listening
```

```
db                      auto enabled     tcp 5432    running
ssh                     auto enabled     tcp 22      running
snmp                    auto disabled    udp 161     not running
```

Description

When changing any one port, you must enter all six values. Use the `status all` command to show current port numbers.

See *status* on page 226.

set property

Introduction

Sets a property related to either the server or the admin server process.

```
set property { server | admin_server } <PROPERTY_NAME>
[=|:| ] <PROPERTY_VALUE>
```

Description

After you set or delete the property, restart the server process by using the `shutdown server` and `startup server` commands. To see a list of all properties that can be set, use the `show property` command.

Server properties

This is a table of server properties that you might need to set.

RedSeal server property	Description
`<redseal.srm.vulnerability.rollup>`	Determines whether the server can create rollup vulnerabilities. This is a roll-up of all the inferred vulnerabilities related to all versions of an application or OS. By default, this property is set to `true`. Set it to `false` if you want to infer vulnerabilities only when the specific version of the application is known.

`<redseal.srm.nonfipsTLSVersions>`	Sets the Transport Layer Security (TLS) protocol version for browser-server communication. By default, the server allows TLS 1, 1.1 and 1.2. You can restrict the server to TLS 1.2 or reset it to use the default. • To set the protocol to a specific version, enter `set property server redseal.srm.nonfipsTLSVersions = TLSv1.2` • To reset the protocol to the default, enter `set property server redseal.srm.nonfipsTLSVersions = TLSv1,TLSv1.1,TLSv1.2`
`<redseal.srm.https.sessionTimeout>`	Set or disable the session idle timeouts for the web applications interface sessions. Set the timeout in minutes. To disable, the timeout, set to 0. See *set session-timeout* on page 211
`<analysis_after_data_collection>`	Determines the automatic start of analysis after a data collection. By default, this property is set to `true`. Set it to `false` if you want to stop analysis from running automatically after data collection.

See *show property* on page 221.

set respond-to-ping

Introduction

Configures the appliance to respond or ignore ping requests from remote systems.

```
set respond-to-ping { on | off }
```

set session-timeout

Introduction

Sets the session idle timeout for cliadmin and root SSH sessions in minutes.

```
set session-timeout { <MINUTES> | infinite }
```

Description

By default, the SSH session idle timeout is infinite.

See *show session-timeout* on page 222.

set ssh public-key

Introduction

Fetches public keys and stores them in a local database for SSH authentication.

```
set ssh public-key ( IP | hostname )
```

Description

To meet Common Criteria requirements, create, enable, and populate a local database of public keys used to authenticate all SSH communications, including SSH data collection tasks and software uploads using SCP or SFTP.

Use the server property `strict_host_key_checking` to enable the local key database. When this setting is enabled, if you try to connect with a remote server that does not have a locally stored key, the communication fails.

Use the `set ssh public-key` commmand to populate the local key database.

See *Store SSH authentication keys locally* on page 150.

See *show ssh public-key* on page 223.

See *delete ssh public-key* on page 184.

set timezone

Introduction

Sets the time zone of the appliance. The default time zone is Universal Time Code (UTC).

```
set timezone <REGION/CITY>
```

Example

Below is an example of the syntax setting the time zone for Detroit.

```
set timezone America/Detroit
```

Display valid values for REGION/CITY

To display a list of valid values for `REGION/CITY`

1. Type the `set timezone` command.
2. Press the **Tab** key .
3. The system prompts **Display all 422 possibilities? (y or n)**.
4. Type `y`.

Best practice for changing time zone

After changing the time zone setting, reboot to ensure the change migrates to all server-related processes.

See *show timezone* on page 223.

show backups

Introduction

Displays a table itemizing recent backups.

```
show backups
```

Description

The table of recent backups includes the checksum, type (with or without analysis), backup timestamp, and location where the backup was written.

See *backup* on page 178.

show banner

Introduction

Displays the banner messages that appear on the server at login or authentication.

```
show banner
```

Description

The pre-authentication message displays after the username is entered and before the password is entered. The post-authentication message displays after the user authenticates.

See *set banner* on page 197.

show cipher-suites

Introduction

Displays enabled and disabled cipher suites and message authentication code (MAC) algorithms used by the server or the SSH process, or displays the cipher suites used when the RedSeal server acts as an SSH client.

```
show cipher-suites (server | ssh | ssh client <java> |
<openssh>)
```

Example

The first example displays the cipher suites enabled and disabled for the server. The second example shows the cipher suites and MAC algorithms enabled and disabled for the SSH process. The third example displays cipher suites used when RedSeal acts as an SSH client and using the `java` parameter. The fourth example displays the cipher suites used when RedSeal acts an SSH client and using the `openssh` parameter.

```
show cipher-suites server
```

```
Enabled Ciphers:
     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
     TLS_RSA_WITH_AES_256_CBC_SHA
     TLS_RSA_WITH_AES_128_CBC_SHA256
     TLS_RSA_WITH_AES_128_GCM_SHA256
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
     TLS_RSA_WITH_AES_256_CBC_SHA256
     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
     TLS_RSA_WITH_AES_256_GCM_SHA384
     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Disabled Ciphers:
     TLS_RSA_WITH_AES_128_CBC_SHA
     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA


show cipher-suites ssh

Enabled Ciphers:
     aes192-ctr
     aes256-ctr
     aes128-cbc
     aes192-cbc
     aes256-cbc
Enabled MACs:
     hmac-sha1
     hmac-sha2-256
     hmac-sha2-512
     hmac-md5

Disabled Ciphers:
     aes128-ctr
Disabled MACs:
     umac-64@openssh.com


show cipher-suites ssh-client java

Enabled Ciphers:
     blowfish-cbc
     aes128-cbc
     aes192-cbc
     aes256-cbc
     aes128-ctr
     aes192-ctr
     aes256-ctr
     3des-ctr
     arcfour
     arcfour256
     none
Enabled MACs:
     hmac-md5-96
```

```
Disabled Ciphers:
     3des-cbc
     arcfour128
Disabled MACs:
     hmac-md5
     hmac-sha1
     hmac-sha2-256
     hmac-sha1-96

show cipher-suites ssh-client openssh

Enabled Ciphers:
     aes128-ctr
     aes192-ctr
     aes256-ctr
     aes128-cbc
     aes192-cbc
     aes256-cbc
Enabled MACs:
     hmac-sha1
     hmac-sha2-256
     hmac-sha2-512
     hmac-md5
     umac-64@openssh.com

Disabled Ciphers:
Disabled MACs:
```

Description

Use this command to display which server cipher suites are enabled and disabled or, to display which SSH process cipher suites and MAC algorithms are enabled and disabled.

Also use this command to display the cipher suites used when the product acts as an SSH client. There are two different SSH modules:

- `openssh`—use this option to control outbound SSH traffic.
- `java`—use this option for all other actions when using the product as an SSH client for example, data collection, backup, or restore.

See *enable cipher-suites server* on page 188, *disable cipher-suites server* on page 184, *enable cipher-suites ssh* on page 188, and *disable cipher-suites ssh* on page 185.

show config

Introduction

Displays details of the current appliance configuration.

```
show config
```

show credential

Introduction

Displays the authorization keys for the cliadmin account or DSA public key.

```
show credential ( cliadmin | dsa )
```

Description

The DSA credential can be transferred to a host on which you intend to store data. Use the `save credential` command to write the credential to an external location. However, you must first remove any line breaks that get added to the text by your terminal. The host can store database backups or user data.

See *save credential* on page 196.

show datahub

Introduction

Displays the IP address of the datahub if the command is entered on a spoke.

```
show datahub
```

Example

When entered on the datahub, this message is displayed:

```
This system is the datahub.
```

See *set datahub* on page 197.

show date

Introduction

Displays the system date, time, and time zone.

```
show date
```

See *set date* on page 198 and *set timezone* on page 212.

show dns

Introduction

Displays the IP address of the DNS server or servers being used.

```
show dns
```

See *set dns* on page 199.

show gateway

Introduction

Displays the interface, IP address, and fully qualified domain name of the default gateway that the server uses.

```
show gateway
```

set gateway on page 199.

show hostname

Introduction

Displays the fully qualified domain name of the appliance.

```
show hostname
```

See *set hostname* on page 200.

show images

Introduction

Lists all RedSeal images currently saved in the file system, identifies which image is currently being used, and identifies the next image to be used at reboot.

```
show images
```

Example

This example shows the full name is “RedSeal N.N (Build-nnn)” and the short name is “Build-nnn” for the current and next images.

```
show images

Current Next          RedSeal 9.2.0 (Build-20484)
                      RedSeal 9.1.2 (Build-2319)
```

Description

Normally, the image currently being used and the image used at reboot are the same. They are different when performing an upgrade. Use the `set next image` command to set the image used after the `reboot` command.

See *set next image* on page 204 and *delete image* on page 181.

show interface

Introduction

Displays all information about the network interfaces of the appliance.

```
show interface
```

Description

Displays the interface name, IP address, subnet mask, broadcast address, MAC address, speed, duplex, and other settings. Use the `set interface` command to set the speed, duplex, or auto-negotiation state of the default network interface. Use the `enable interface` or `disable interface` command to enable or disable an interface.

See *set interface* on page 200.

show interface roles

Introduction

Displays the roles available on each interface of the appliance.

```
show interface roles [ INTERFACE ]
```

See *add interface role* on page 176 and *remove interface role* on page 194.

show ip

Introduction

Shows the IP address and subnet mask of the appliance and indicates whether the addresses come from DHCP.

```
show ip [ INTERFACE ]
```

INTERFACE Use the `INTERFACE` argument to display the IP address of a specific interface if using multiple NICs. If `INTERFACE` is not specified, eth0 is the default.

See *set ip* on page 201.

show license

Introduction

Displays the current status of your license.

```
show license
```

See *set license* on page 201.

show log

Introduction

Displays data about the specified log.

```
show log ( events | audit | analyzer | system | server )
```

See *set log* on page 202.

show logfile

Introduction

Displays the contents of the specified log.

```
show logfile ( audit | analyzer | system | server )
```

Description

You can filter the output to display specific information, such as messages generated on a specific date. For more information, see *Output filtering*.

See *set log* on page 202.

show logged-in users

Introduction

Lists users currently logged in.

```
show logged-in users
```

show max-concurrent-session-per-user

Introduction

Displays the maximum number of concurrent user sessions that can be opened on that RedSeal appliance.

```
show max-concurrent-session-per-user
```

See *set max-concurrent-session-per-user* on page 203.

show min-password-length

Introduction

Shows the minumum required password length value set through the `set_min_password_length` command.

```
show min-password-length
```

See *set min-password-length* on page 204.

show ntp

Introduction

Lists the NTP servers being used, if there are any.

```
show ntp
```

See *set ntp* on page 205.

show property

Introduction

Displays the value currently set for a property related to the specified process.

```
show property [ * | all | <PROPERTY_NAME> ]
```

Description

Currently, there are no properties for the `admin_server` process.

Display non-null server properties

To see a list of non-null server properties and their values, use the `show property server` command.

Note The `*` and `all` options are identical to the no argument form of the command, and are implemented as a convenience to users who expect them.

Display all server properties

To see a list of all server properties, enter the `show property server` command and then press **Ctrl+I** or **Tab**. A list of all server properties without assigned values is displayed.

To see which value is set for a specific property, use the `show property server <PROPERTY_NAME>` syntax. Many of the properties might show null for the value or the string `not explicitly set` because a default is set in the code.

See *set property* on page 209.

show respond-to-ping

Introduction

Displays whether or not the server responds to ping requests from remote hosts.

```
show respond-to-ping
```

See *set respond-to-ping* on page 210.

show route

Introduction

Displays the routing table for all interfaces on the server.

```
show route
```

See *add route* on page 177.

show session-timeout

Introduction

Displays the session idle timeout for cliadmin and root SSH sessions.

```
show session-timeout
```

See *set session-timeout* on page 211.

show spokes

Introduction

Displays the IP address of all spokes set up on a datahub cluster.

```
show spokes
```

Description

This command is available on the datahub only.

See *add spoke* on page 178.

show ssh public-key

Introduction

Shows public keys stored in a local database for SSH authentication.

```
show ssh public-key ( IP | hostname | all )
```

See *Store SSH authentication keys locally* on page 150.

See *set ssh public-key* on page 211.

See *delete ssh public-key*.

show support-summary

Introduction

Displays a summary of information useful to RedSeal Technical Support.

```
show support-summary
```

Description

You can filter the output to display specific information. For more information, see *Output filtering* on page 175.

show timezone

Introduction

Displays the time zone used by the appliance.

```
show timezone
```

See *set timezone* on page 212.

shutdown

Introduction

Stops the specified process.

```
shutdown [ server | db | ssh | snmp | machine ]
```

server	The server process.
db	The database process.
ssh	SSH process.
snmp	The SNMP process.
machine	The virtual machine or physical appliance the server is running on. The machine powers down after shutting down the server and database.

Note If you are logged in remotely, you cannot reconnect after shutting down the machine.

Description

For the `shutdown ssh` command, you are prompted to specify whether you want the shutdown to be immediate even if there is an open SSH connection.

For the other options, shutdown is immediate.

If autostart has been enabled for a process prior to a shutdown, the process is restarted following a reboot. If you do not want the process to run, you must explicitly disable autostart for that process.

Use the `status`, `startup`, and `reboot` commands to manage the autostart and reboot processes.

See *status* on page 226, *startup* on page 226, and *reboot* on page 194.

ssh

Introduction

Provides a secure login connection to execute CLI commands on the remote host machine.

```
ssh [-1246AaCfgKkMNnqsTtVvXxYy] [-L
[bind_address:]port:host:hostport] [-l [login_name]
[user@]]host
```

-1	Protocol version 1 only.

-2 Protocol version 2 only.

-4 IPv4 addresses only.

-6 IPv6 addresses only.

-A Enables forwarding of the authentication agent connection.

-a Disables forwarding of the authentication agent connection.

-C Runs data compression.

-f Requests ssh to run in the background.

-g Allows remote hosts to connect to local forwarded ports.

-K Enables GSSAPI-based authentication and forwarding (delegation of Generic Security Services Application Program Interface (GSSAPI) credentials to the server.

-k Disables forwarding (delegation) of GSSAPI credentials to the server.

-M Puts the ssh client into master mode for connection sharing.

-N Disallows execution of a remote command.

-n Redirects stdin from /dev/null. Must be used when ssh is run in the background.

-q Quiet mode. All warning and diagnostic messages are suppressed.

-s Specifies the location of a control socket for connection sharing.

-T Disables pseudo-tty allocation.

-t Forces pseudo-tty allocation.

-V Displays the version number.

-v Enters verbose mode.

-X Enables X11 forwarding.

-x Disables X11 forwarding.

-Y Enables trusted X11 forwarding.

-y Sends log information using the syslog system module.

-L [bind_address:]port:host:hostport]	Specifies that the given port on the local (client) host is to be forwarded to the given host and port on the remote side. This works by allocating a socket to listen to a port on the local side, optionally bound to the specified bind_address.
-l [login_name] [user@]	Connects and logs into the specified host (with optional user name). The user must prove identity to the remote machine.

startup

Introduction

Starts the specified process.

```
startup { server | db | ssh | snmp }
```

server	Required keyword.
db	The database process.
ssh	SSH process.
snmp	SNMP process.

Description

Servers started up with the `startup` command are not automatically restarted following a reboot. Use the `enable autostart` command to enable automatic restart.

See *shutdown* on page 223 and *status* on page 226.

status

Introduction

Displays the status of the specified process, the port it uses, the protocol, and the autostart status.

```
status { server | db | ssh | disk | all }
```

server	The server.
db	The database.
ssh	SSH process.

`disk`	RAID array (4000 and 4100 only).
`all`	All processes.

status autostart

Introduction

Displays the enabled or disabled status of autostart for SSH and SNMP processes.

```
status autostart ( ssh|snmp )
```

status support-access

Introduction

Displays the enabled or disabled status of special access for RedSeal Technical Support.

```
status support-access
```

See *enable support-access* on page 191.

tail

Introduction

Displays the end of the server log.

```
tail [ -n | -c | -f | -q | -s ] [serverlog ]
```

`-n`	Number of lines.
`-c`	Number of bytes.
`-f`	Output data appended as the file grows. Use `Ctrl+c` to exit the display.
`-q`	Never output headers giving file names.
`-s`	Number of seconds. Used with -f, sleep for N seconds between iterations. Default is 1.0
`serverlog`	Required argument.

Example

This example sets the server log to append new data to the display every two seconds as the file grows.

```
tail -f -s 2 serverlog
```

test connection

Introduction

Writes a test file to the FTP or SFTP server or SCP host specified by the URL.

```
test connection <URL>
```

Example

This is an example of a test file name.

```
rs_connection_test_<timestamp>.txt
```

See *SCP and SFTP use prerequisite* on page 172, and *URL path rule* on page 172.

top

Introduction

Displays the top CPU-consuming processes.

```
top
```

traceroute

Introduction

Displays in the command line the route taken by packets from the source host to the address specified as dest_addr.

```
traceroute [tcp [port<dest_port>] ] <dest_addr>
```

tcp	Specify the keyword to use a TCP packet rather than the default ICMP packet.
port	Specify the keyword to send the TCP packet to a specific port.

<dest_port>	The port number that is the destination of the TCP packet.
<dest_addr>	The IP address that is the destination of the packet.

unset datahub

Introduction

Restores the server that was removed from the datahub cluster to factory-default settings.

```
unset datahub
```

See *delete spoke* on page 183.

upload certificate

Introduction

Upload a SSL digital certificate to the appliance.

```
upload certificate <URL>
```

<URL>	URL points to a digital certificate obtained from a certificate authority (CA).

Description

The digital certificate is used for SSL communication with the client application and with web browsers when installing the client. The certificate must be an approved certificate generated from a request produced by the `create cert-request` command.

If the CA that signs your certificate is unknown to Java, you must first upload a public certificate obtained from the CA, using the `ca-certificate` keyword. Use the `create cert-request` command to generate a request for an SSL certificate. For information about certificate authorities, A server restart is not necessary when importing the CA's public certificate, but it is required after the subsequent import of your own certificate.

See *SSL certificate* on page 144, *Add a self-signed certificate to the server using the CLI* on page 145, *Add an intermediate certificate to the server using the CLI* on page 147, and *Add the certificate to the server using the CLI and a fully qualified domain name* on page 147.

upload image

Introduction

Upload an image to the appliance.

```
upload image <URL>
```

Description

You can upload up to two images on the appliance. The most recently uploaded image is designated as the image to use after a reboot. Use the `show images` and `set next image` commands to manage the uploaded images.

The image to be uploaded can be an earlier version or a later version of the image currently being used. However, if there were schema changes introduced in the later version, you may not be able to use a later version database with an earlier-version server image.

After the appliance is rebooted with the newly uploaded image, support access is always disabled regardless of its state before the upload. Use the `enable support-access` command to enable support access.

You should always update your TRL after uploading a new image to your appliance. See *TRL update* on page 97

Image upload restrictions

If two images are already installed on the appliance and you attempt to upload an additional image, you receive an error message. Use the `delete image` command to delete an image.

If you attempt to upload an image whose version matches the version of an image already installed on the appliance, you are prompted to specify whether you want the installed image to be overwritten.

See *show images* on page 218, *set next image* on page 204, *delete image* on page 181.

upload license

Introduction

Upload a license to the server.

```
upload license <URL>
```

upload plugin

Introduction

Move a plug-in file from your HTTP or FTP server to the server file system.

```
upload plugin <URL>
```

Description

RedSeal occasionally releases new plug-ins or updates to existing plug-ins. The plug-ins affect importing device configurations and vulnerability scan data.

SNMP commands

Introduction

This section provides command syntax and descriptions for SNMP commands.

create user snmp

Introduction

Creates a new SNMP user.

```
create user snmp
```

Description

By default, SNMP is disabled and requires you to create one or more SNMP users before starting the service the first time or when migrating to a new software version.

You are prompted to provide the user name, pass phrase, encryption pass phrase, authentication protocol, and privacy protocol.

If SNMP is already running when you enter the `create user snmp` command, you are prompted to stop the SNMP process while you create the user. Type `y` to stop the SNMP process. The SNMP service restarts automatically when you are done creating the user.

UDP port 161 is open when SNMP is running and shuts down when the service is stopped.

delete user snmp

Introduction

Deletes the specified SNMP user.

```
delete user snmp <user_name>
```

`<user_name>`	SNMP user on the server

Description

If you want to modify user settings, you must delete and then re-create the user with different settings.

disable autostart snmp

Introduction

Prevents SNMP from starting automatically after the system reboots.

```
disable autostart snmp
```

enable autostart snmp

Introduction

Sets SNMP to start automatically when the system reboots.

```
enable autostart snmp
```

show users snmp

Introduction

Lists SNMP users.

```
show users snmp
```

shutdown snmp

Introduction

Stops the SNMP process from running and shuts down UDP port 161.

```
shutdown snmp
```

snmpwalk for Mac

Introduction

Allows you to use the command line from your Macintosh host to monitor objects stored in the Management Interface Base (MIB).

```
snmpwalk -v 3 -u <user_name> -l authPriv -a { MD5 | SHA }
-A <auth_passphrase> -x { AES | DES } -X
<priv_passphrase> <server_name>
```

<user_name>	SNMP user on the server
authPriv	The allowable security level for creating SNMP users.
<-a MD5 | SHA>	Choose Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)
<-A <auth_passphrase>>	The SNMP user password.
<-x AES | DES>	Choose Advanced Encryption Standard (AES) or Data Encryption Standard (DES)
<priv_passphrase>	SNMP privilege access user password
<server_name>	A name using a .net extension or IP address.

Example

This example initiates an snmpwalk on a Macintosh.

```
snmpwalk -v 3 -u bob -l authPriv -a SHA -A MyAuthPassphrase
-x DES -X MyPrivPassphrase RSserver.net
```

Description

The `snmpwalk` command uses much of the same information provided when the SNMP user is created. This includes the username, pass phrases, and authentication and privacy protocols.

snmpwalk for Windows

Introduction

Allows you to use the command line from your Windows host to monitor objects stored in the Management Interface Base (MIB).

```
snmpwalk -v3 -u <user_name> -A <auth_passphrase> -X
<priv_passphrase> -a { MD5 | SHA } -x { AES | DES } -1
authPriv <server_name>
```

<user_name>	SNMP user on the server
<auth_passphrase>	SNMP user password
<priv_passphrase>	SNMP privilege access user password
<-a MD5 | SHA>	Choose Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)
<-x AES | DES>	Choose Advanced Encryption Standard (AES) or Data Encryption Standard (DES)
authPriv	The allowable security level for creating SNMP users.
<server_name>	A hostname using a .net extension or an IP address.

Example

This example initiates an snmpwalk on a Windows PC.

```
snmpwalk -v3 -u bob -A MyAuthPassphrase
-X MyPrivPassphrase -a SHA -x DES -l authPriv RSserver.net
```

Description

The `snmpwalk` command uses much of the same information provided when the SNMP user is created. This includes the username, pass phrases, and authentication and privacy protocols.

startup snmp

Introduction

Starts the SNMP process and opens UDP port 161.

```
startup snmp
```

Description

Before you enable SNMP the first time, you must create at least one SNMP user.

status snmp

Introduction

Shows if the SNMP process is running or not, the port it uses, and if it is set to start when the server reboots.

```
status snmp
```

Smart card commands

Introduction

This section provides command syntax, descriptions, and examples for Smart Card commands. CLI commands used to configure the appliance and SNMP commands are in their own sections.

enable authentication certificate

Introduction

Enables certificate authentication.

```
enable authentication certificate
```

Description

Users can authenticate using a certificate on a smart card. By default, certificate authentication is disabled.

enable authentication password

Introduction

Enables password authentication.

```
enable authentication password
```

Description

Users with passwords can authenticate locally. Certificate users can have a local password backup. By default, password authentication is enabled.

disable authentication certificate

Introduction

Disables certificate authentication.

```
disable authentication certificate
```

Description

Users cannot authenticate using a certificate.

disable authentication password

Introduction

Disables password authentication for smart card certificate users.

```
disable authentication password
```

Description

No users can use local password authentication. Certificate users cannot have a local password backup. Non-certificate CLI users can still authenticate with a password.

set port server

Introduction

Changes the default port numbers used for RedSeal processes.

Description

The default port used to connect to the RedSeal HTTPS certificate authentication server is 10443. This port must be open to enable certificate authentication. If certificate authentication is enabled, all users login through this port. For command syntax see *set port server* on page 208.

status all

Introduction

Displays the processes that are running, the port and protocol used, and the autostart status. To get the status of the smart card process, use the argument `all`.

```
status all
```

Example

This is an example of the output of the status all command. See *status* on page 226.

```
server-https-cert auto disabled TCP 10443 not running
```

show property server

Introduction

Shows the value currently set for the property related to the process.

```
show property server <PROPERTY_NAME>
```

Description

To see which value is set for a specific property, you need to enter the complete property name in the show command.

Example

The example shows the property names and default value for the certificate authentication processes.

```
show property server redseal.srm.https.certauth.enabled
redseal.srm.https.certauth.enabled        = false

show property server redseal.srm.https.passwordauth.enabled
redseal.srm.https.passwordauth.enabled    = true
```

See *show property* on page 221.

add credential cliadmin

Introduction

Associates a smart card SSH key string with the `cliadmin` account. The smart card user uses the smart card to access the CLI.

```
add credential cliadmin <keystring>
```

Description

The credential must be stored on the computer where the RedSeal client application or web application runs:

- On Windows, use PuTTY-CAC
- On Mac OS X, use opensc

delete credential cliamin

Introduction

Deletes a smart card SSH key string used for authentication to the `cliadmin` account. This revokes the smart card user's access to the CLI.

```
delete credential cliadmin <keystring>
```

show credential cliadmin

Introduction

Lists the SSH key strings associated with the `cliadmin` account.

```
show credential cliadmin
```

A

System requirements

Introduction

Client and server hosts must meet operating system, browser, disk space, and RAM requirements. Client hosts also require network access to the RedSeal server. Virtual deployments have requirements for minimal configuration and best performance.

Client operating system requirements

The client host must have one of these operating systems.

- Linux CentOS 7.
- Ubuntu 18.04.2 LTS.
- Microsoft Windows 8 and 10.
- Microsoft Windows 8 Enterprise, 64-bit.
- Microsoft Windows Server 2012, Standard Edition.
- Apple Mac OS X, all versions.

Note The latest version of Apple Mac OS X version 10.15 (Catalina) introduces new security features that require you to adjust some settings to run the RedSeal Client. Refer to https://support.apple.com/en-us/HT202491 for more information about updating your settings.

Client storage requirements

The client host must have sufficient disk space and memory to run the RedSeal application.

Storage space	RAM
150 MB	1 GB minimum

Client network access requirements

The client host must have network access to the RedSeal server as follows.

- If the server is running on a physical appliance, the workstation must have https access through port 443 to install the client application. Port 80 http connections redirect to port 443.
- To set up two factor authentication, the RedSeal server must have TCP access through port 10443.
- To run the client application after it is installed, the workstation must have TCP access to the RedSeal server. The server can be either a physical or virtual appliance with client host connections through ports 3825, 3826, and 3835.

Client browser requirements

Browser requirements for the client host vary depending on what you want to view.

If you want to	You must have one of these browsers
View reports	• Internet Explorer, version 11.0 and higher (all platforms) • Microsoft Edge 44.18362.449.0 • Firefox 56.0.1 or higher • Safari 10.0 or higher • Chrome version 61 and higher

View the web interface	• Internet Explorer, version 11.0 and higher (all platforms) • Microsoft Edge 44.18362.449.0 • FireFox, version 83 and higher • Safari, version 10.0 and higher • Chrome, version 87 and higher

Virtual appliance sizing

The following is RedSeal's recommendation for provisioning virtual appliances for best performance and for minimum configurations. The recommendation that achieves best performance is based on the RedSeal G5b appliance. RedSeal suggests provisioning the same configuration or better for virtual deployments.

- Best performance—128 GB RAM and 8 processor cores
- Minimum configuration—64 GB RAM and 4 processor cores