SolarWinds Cirrus Configuration Manager
Administrator Guide

About SolarWinds

SolarWinds, Inc develops and markets an array of network management, monitoring, and discovery tools to meet the diverse requirements of today's network management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in network management and discovery technology. The SolarWinds customer base includes over 45 percent of the Fortune 500 and customers from over 90 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Contacting SolarWinds

You can contact SolarWinds in a number of ways, including the following:

Team	Contact Information
Sales	1.866.530.8100 www.solarwinds.com
Technical Support	www.solarwinds.com/support
User Forums	www.thwack.com

Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

Convention	Specifying
Bold	Window items, including buttons and fields.
Italics	Book and CD titles, variable names, new terms
`Fixed font`	File and directory names, commands and code examples, text typed by you
Straight brackets, as in [*value*]	Optional command parameters
Curly braces, as in {*value*}	Required command parameters
Logical OR, as in *value1|value2*	Exclusive command parameters where only one of the options can be specified

Cirrus Configuration Manager Documentation Library

The following documents are included in the SolarWinds Cirrus Configuration Manager documentation library:

Document	Purpose
Administrator Guide	Provides detailed setup, configuration, and conceptual information.
Quick Start Guide	Provides installation, setup, and common scenarios for which Cirrus Configuration Manager provides a simple, yet powerful, solution.
Release Notes	Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at www.solarwinds.com.

<u>Contents</u>

Chapter 4

Chapter 1

Introduction

SolarWinds Cirrus Configuration Manager is a comprehensive, intuitive solution designed to streamline and automate network configuration management. Cirrus Configuration Manager increases availability, saves time, improves security, and ensures policy adherence. Cirrus Configuration Manager features automation capabilities that reduce the amount of time network engineers spend on mundane network tasks, allowing them to focus on business-critical network projects.

Why Install SolarWinds Cirrus Configuration Manager

Out of the box, SolarWinds Cirrus Configuration Manager offers numerous management features, including the ability to:

- Control access based on user roles

- Schedule device configuration backups

- Implement configuration changes in bulk (IOS and firmware updates)

- Generate detailed configuration reports for inventory, change, and policy management

- Receive notification of device configuration changes

- Identify configuration violations through policy management reporting

- View detailed change history and side-by-side comparison of configurations

- Perform detailed device inventory for each managed device

- Track and view configuration changes made by users

Cirrus Configuration Manager allows you to easily manage configurations on heterogeneous, multi-vendor networks. Cirrus supports routers, switches, firewalls, load balancers, and wireless access points from numerous vendors, including Cisco, Dell, Adtran, Arris, Aruba, Nortel, Nortel Alteon, Extreme, Marconi, Radware, Netscreen, Motorola, HP, Netscalar, Juniper and Foundry. You gain a single point of management. Whether you are faced with managing network configurations for 50 or 5,000 devices, Cirrus Configuration Manager provides you with an intuitive solution that immediately impacts the bottom line.

Key Features of Cirrus Configuration Manager

Considering the previously mentioned benefits of Cirrus Configuration Manager, coupled with the following features, Cirrus Configuration Manager is the clear choice to make:

Scheduled Configuration Backups

Using the scheduled job feature, you can schedule configuration downloads, configuration uploads, device reboots, command scripts execution, and more. In addition, configuration backups are stored both in a relational database for archival history and as flat files in an intuitive folder structure for easy viewing.

Policy Management

Allows you to ensure device compliance with federal regulations, as well as corporate standards. The Policy Reporting Manager comes with several out-of-the-box policy reports, including SOX, HIPAA, CISP, and Cisco Security.

Role-Based Access Control

Enables you to integrate your Windows Active Directory or local system user accounts with Cirrus Configuration Manager. You can manage users based on their role and establish individual device login credentials per user. Cirrus Configuration Manager logs all user activity allowing you to keep an archive of changes and activity.

Multivendor Support

Provides support for network devices from multiple hardware vendors. As a monitor and manager of routers, switches, firewalls, VPN concentrators, wireless access points and more, Cirrus is a robust solution that is fully capable of managing your hybrid vendor network.

Bulk Changes

Enables quick changes to community strings, passwords, and black lists. With Cirrus, you can execute bulk changes either in realtime or within a scheduled change window. Uploads, changes, and global command scripting can be scheduled by device type, physical location, by owner, or by any custom property you create.

Configuration Change History

Reports what devices have had configuration changes over any time period you specify. Configuration change reports can also compare current configurations with a baseline configuration alerting you whenever a change is discovered.

Chapter 2

Installing Cirrus Configuration Manager

Cirrus Configuration Manager provides a simple, wizard-driven installation process. For an enterprise-class product, the requirements are nominal.

Licensing Cirrus Configuration Manager

Cirrus Configuration Manager can manage almost any network device, including routers, switches, and firewalls. Any of your version 3 or earlier SNMP-enabled devices can provide configuration files to Cirrus Configuration Manager. You license Cirrus Configuration Manager by the number of *nodes*. A node is defined as an entire device, that is, a router, a switch, a server, an access point, or a modem.

The following list provides the different types of Cirrus Configuration Manager licenses available:

- Up to 50 devices (DL50)

- Up to 100 devices (DL100)

- Up to 200 devices (DL200)

- Up to 500 devices (DL500)

- Up to 1000 devices (DL1000)

- Up to 3000 devices (DL3000)

- Unlimited devices (DLX)

Requirements

The requirements for Cirrus Configuration Manager vary based upon the number of nodes, the frequency of configuration downloads, the length of time that configurations are maintained in the database, among other factors. The following table provides the minimal requirements for a Cirrus Configuration Manager installation:

Software/Hardware	Requirements
Operating System	Windows XP Pro Windows 2003 Server
CPU Speed	800 MHz
Memory	256 MB
Hard Drive Space	1GB
Windows account	Requires administrator permission on the target server
Database	SQL Server 2000 Standard or Enterprise -or- SQL Server 2005 Express, Standard, or Enterprise

About the Cirrus Configuration Manager Database

A copy of Microsoft SQL 2005 Express is distributed with each copy of Cirrus Configuration Manager. SQL 2005 Express supports a maximum database size of 4GB. For more information about SQL Server installation, see the Microsoft website at http://www.microsoft.com/sql.

SNMP Communication

Because Cirrus Configuration Manager takes advantage of SNMP communication to collect inventory information, ensure all devices from which you want to collect detailed information have SNMP properly configured.

Installing Cirrus Configuration Manager

Complete the following procedure to install Cirrus Configuration Manager.

To install Cirrus Configuration Manager:

1. Log on with an administrator account to the computer on which you want to install Cirrus Configuration Manager.

    Note: To ensure that Cirrus Configuration Manager runs properly, do not install Cirrus Configuration Manager on a domain controller.

2. *If you downloaded the product from the SolarWinds website,* navigate to your download location and launch the executable.

3. *If you received physical media,* browse to the executable file and launch it.

4. Review the Welcome text, and then click **Next**.

5. Agree to the license agreement on the End User License Agreement window, and then click **Next**.

6. Type the user name and organization in the fields provided.

7. Decide if you want to limit Cirrus Configuration Manager to the currently logged in account, and then click **Next**.

8. ***If you want to change the installation folder,*** click **Change**.

9. Click **Next**.

10. Click **Install**.

11. Click **Finish** on the InstallShield Wizard Completed window.

12. Provide the appropriate information on the Install Software License Key window, and then click **Continue**. You need a customer ID and password to successfully install the key. For more information, see "Software License Key" on page 5.

Software License Key

If you are prompted for your name, email address, phone number, customer ID, and password, complete the following procedure.

To license your product:

1. ***If the computer on which you are installing Cirrus Configuration Manager is connected to the Internet,*** complete the following procedure:

   a. Enter the required information on the Install Software License Key window.

   b. Click **Continue**. The SolarWinds license registration server will issue a license key that will allow Cirrus Configuration Manager to operate.

2. ***If the computer on which you are installing Cirrus Configuration Manager is not connected to the Internet,*** your system can not be authenticated by the SolarWinds license registration server. Complete the following procedure:

   a. Click **Skip This and Enter Software License Key Now** on the Install Software License Key window.

   b. Obtain a license using a computer that is connected to the Internet. Login to the customer area of the SolarWinds website at www.solarwinds.com/support, and then click **Software Keys** in the left navigation of the customer portal. Choose the product for which you need a key and follow the instructions on the page to obtain a key. The key can then be entered in the **Enter Software License Key** text box on the Install Software License Key window.

   c. Click **Continue** to complete your software license key installation.

Configuring Cirrus Configuration Manager

Complete the following procedure to configure Cirrus Configuration Manager.

To configure Cirrus Configuration Manager:

1. Click **Start > All Programs > SolarWinds Configuration Management > Cirrus Configuration Management**.

2. When logging into Cirrus Configuration Manager for the first time, leave the **Password** field blank, and then click **Login**.

3. Type a new password for the Administrator account, and then click **OK**.

4. Click **File > New/Open Database Wizard**.

5. Review the Welcome window, and then click **Next**

6. Click **Create a New Database**, and then click **Next**.

7. Click the appropriate authentication type.

8. *If you select SQL Authentication,* provide an account with sufficient rights to create new databases on that server. For example, you can use the SQL administrator account.

9. Select the name of the SQL instance from the SQL Server list. If your server is not listed, provide the instance. The default instance name for SQL Express is `Server-Name\SQLExpress` or `(local)\SQLExpress`.

10. Type a name for your database, and then click **OK**.

11. Navigate to the appropriate path to save your database, and then click **OK**.

12. Click **Next**.

13. Type the default read-only and read-write community strings for nodes on your network, and then click **Next**. This default string is tried first, before interactively requesting one.

14. *If your network devices use SNMPv3,* provide the appropriate values in the Default SNMPv3 Settings window, and then click **Next**.

15. Provide the default authentication settings for your network devices, and then click **Next**.

16. Select the default execute, request, and transfer protocols for your devices, and then click **Next**.

17. Select a grouping field, and then click **Next**.

    Note: This field is used to conveniently group nodes in the node tree. If grouping is not required, select `<none>`.

18. Type the Windows user account credentials you want to use to run scheduled jobs, and then click **Set Username and Password**. Use the following syntax: *domain\username*.

19. Click **Next**.

20. Select the appropriate device connectivity method for your network, and then click **Finished**.

21. *If the Manage Cirrus Users window appears,* configure at least one use account. For more information, see "Configuring User Access Control" on page 7.

After completing the wizard, populate the database with the network you want to manage by adding nodes. For more information, see "Adding Nodes" on page 13.

Configuring User Access Control

Cirrus Configuration Manager allows you to implement user access control to manage permissions for each user. Cirrus Configuration Manager integrates with Windows Active Directory and local system accounts to simplify the user management process.

To enable user access control:

1. Click **File > Settings > Security**.

2. Check **Require a login to use Cirrus Configuration Manager**.

3. *If you want to assign device login credentials to user accounts,* complete the following procedure:

    a. Click **Device Connectivity Method**.

    b. Click **Manage devices using a combination of individual login credentials per device and user account device login credentials**.

    c. Click **OK** in the Warning window

4. Click **OK** in the Cirrus Configuration Manager Settings window.

To add Windows Active Directory Account users:

1. Click **File > Manage Cirrus Users**.

2. Click **Add**.

3. Click **Locations**, browse to the domain that includes the user, and then click **OK**.

4. Type the user name including the domain, for example *domain\username*.

5. Click **Check Names** to ensure the user name is typed properly.

6. Click **OK**.

7. Select a role from the **Role** list on the Manage Cirrus Users window

   Administrator

   Access is granted to the entire Cirrus Configuration Manager application.

   Engineer

   Access is granted to the Cirrus Configuration Manager application excluding the ability to create, modify, or delete user accounts, modify security settings, or alter device connectivity methods.

8. *If you are assigning device login credentials to user accounts,* type the user name and password used to access nodes for this user, and then type the enable level and enable password, if necessary.

9. *If you want to add another user,* click **Apply**, and then restart the procedure at **Step 2**.

10. Click **OK**.

To edit a user account:

1. Click **File > Manage Cirrus Users**.

2. *If you want to modify access or roles assigned to a Windows user account,* complete the following procedure.

   a. Select the Windows user account you want to modify in the **Users** list.

   b. In the Manage Cirrus Users window, select a role from the **Role** list.

   c. Type the user name and password used to access nodes for this user, and then type the enable level and enable password, if necessary.

   d. *If you want to modify another user account,* click **Apply**, and then repeat this procedure.

3. *If you want to modify a built-in Cirrus Configuration Manager user account,* complete the following procedure.

   a. Click the Built-In Cirrus Users tab.

   b. Select the user account you want to modify in the **Users** list.

   c. *If you want to change the password,* click **Change Password**, type and verify the new password, and then click **OK**.

    d. Type the user name and password used to access nodes for this user, and then type the enable level and enable password, if necessary.

    e. *If you want to modify another user account,* click **Apply**, and then repeat this procedure.

4. Click **OK**.

Configuring Event Logging

Logging events associated with a specific function of Cirrus Configuration Manager allows you to keep detailed record of events and helps you troubleshoot any anomalies you may encounter.

To enable logging for Cirrus Configuration Manager events:

1. Click **File > Settings**.

2. Click **Advanced > Logging**.

3. Check the Cirrus Configuration Manager events you wish to monitor, and then click **OK**.

Moving Cirrus Configuration Manager

The time necessary to move Cirrus Configuration Manager to a different computer depends on how long the database backup procedure takes. SolarWinds recommends scheduling an appropriate maintenance window to perform the migration procedure.

Requirements

To move your Cirrus Configuration Manager installation to a new server, you will need the following items.

- A computer meeting the minimum requirements for the new installation of Cirrus Configuration Manager. For more information on requirements, see "Requirements" on page 3.

- User accounts with administrative rights on both servers.

- You will need to reset your license to register Cirrus Configuration Manager on your new computer. Contact installation@solarwinds.com with your CustomerID number to request a license reset.

- A temporary storage area for custom scripts and reports. This can be any storage device able to hold the information and accessible from each Cirrus Configuration Manager computer, for example, a network drive accessible by each computer, a memory stick, or an external hard drive.

Migrating Cirrus Configuration Manager

Complete the following procedure to move Cirrus Configuration Manager.

To move Cirrus Configuration Manager to another computer:

1. Log on to the computer with an administrator account on which you installed the current Cirrus Configuration Manager.

2. Close Cirrus Configuration Manager and any other running applications.

3. Start Database Manager. Click **Start > All Programs > SolarWinds Configuration Management > SQL Database Manager**.

4. *If your SQL Server is not listed,* add your server to the list. For more information, see "Adding a Server" on page 69.

5. Click your Cirrus Configuration Manager database in the left pane of the Database Manager window, and then click **Database > Backup Database**.

6. Type a description of the database backup and specify a path and filename for the backup file. Save your database backup to a temporary storage area. This can be a network drive accessible from each Cirrus Configuration Manager computer, a memory stick, or an external hard drive.

   Note: Ensure the target location for the database backup has sufficient available disk space.

7. Click **OK**.

8. Log in to the new computer, and then install Cirrus Configuration Manager. For more information, see "About the Cirrus Configuration Manager Database" on page 4.

9. Click **Start > All Programs > SolarWinds Configuration Management > Cirrus Configuration Management**.

10. Click **File > New/Open Database Wizard**.

11. Review the Welcome window, and then click **Next**

12. Click **Open an Existing Database**, and then click **Next**.

13. *If you are using a SQL database,* complete the following procedure:

14. Click **SQL Server Database**.

15. Select the appropriate authentication method and, if necessary, provide your user login credentials.

16. Select your SQL Server from the list.

17. Select your database from the list, and then click **OK**.

18. Click **Finished**.

Migrating Jobs

If you are running any scheduled jobs, you will need to copy them to the new computer. Complete the following procedure to move your scheduled jobs.

To move jobs to new hardware:

1. Log in to the old computer.

2. Copy the files in the `Jobs` folder. By default, this folder is located at `C:\Program Files\SolarWinds\Configuration Management`.

3. Paste the files into the `Jobs` folder on the new server. By default, this folder is located at `C:\Program Files\SolarWinds\Configuration Management`.

4. Click **Start > All Programs > Accessories > Windows Explorer**.

5. Browse to **My Computer > Control Panel > Scheduled Tasks**.

6. Select all of your Cirrus Configuration Manager jobs, and then click **Edit > Copy**.

7. Paste the job files into the `Scheduled Tasks` folder on the new server.

Migrating Scripts

If you have created any custom scripts, it will be necessary to copy them to the new computer. Complete the following procedure to move your scripts.

To move scripts to new hardware:

1. Log in to the old computer.

2. Copy the files in the `Scripts` folder. By default, this folder is located at `C:\Program Files\SolarWinds\Configuration Management`.

3. Paste the files into the `Scripts` folder on the new server. By default, this folder is located at `C:\Program Files\SolarWinds\Configuration Management`.

Migrating Reports

If you have created any custom reports, it will be necessary to copy them to the new computer. Complete the following procedure to move your reports.

To move reports to new hardware:

1. Log in to the old computer.

2. Copy the files in the `Reports` folder. By default, this folder is located at `C:\Program Files\SolarWinds\Configuration Management`.

3. Paste the files into the `Reports` folder on the new server. By default, this folder is located at `C:\Program Files\SolarWinds\Configuration Management.`

Migrating Device Command Templates

If you have created any custom device command templates, it will be necessary to copy them to the new computer. Complete the following procedure to move your templates.

To move device command templates to new hardware:

1. Log in to the old computer.

2. Copy the files in the `DeviceTypes` folder. By default, this folder is located at `C:\Program Files\SolarWinds\Configuration Management.`

3. Paste the files into the `DeviceTypes` folder on the new server. By default, this folder is located at `C:\Program Files\SolarWinds\Configuration Management.`

Chapter 3

Managing Nodes

Cirrus Configuration Manager helps you manage, organize, and track changes to your network. To begin managing your nodes, review the following procedures:

- Adding Nodes
- Importing Nodes
- Editing Nodes
- Creating Custom Node Properties

Adding Nodes

You can add nodes individually, or import a list of nodes from a file. The following procedures guide you through both methods.

Adding Nodes

Complete the following procedure to add one of your network devices as a managed node.

To add individual nodes:

1. Click **Nodes > Add New Node**.
2. Type the hostname or IP address of the node.
3. Select the SNMP version of the node, and then type the SNMP read-only and read-write community strings.
4. *If the device uses SNMPv3,* expand the SNMPv3 category, and then provide the appropriate values needed to login to the device.
5. Click **Verify SNMP Community**.
6. Select the device template from the list.

    Note: Try **Auto Detect** first. If Cirrus Configuration Manager is unable to determine the appropriate device command template, or assigns the wrong template, then select the template from the list.

7. *If you want to add the node to a group,* type or select a node group from the list. If you do not select a group, your new node is grouped in the Unknown group.

8. ***If you are using individual device login credentials,*** set the **Login Credentials** field to `Device`, and then type the user name and password used to access the node. Type the enable level and enable password, if necessary.

    Notes:

    - Use the Telnet or Web Browse buttons to connect to the node and view node information.

    - When typing the login information, type values just as they would be typed during manual login. For example, if 15 represents enable level 15, then type `15` for the value.

9. If you want to use Cirrus user account device login credentials, set the **Login Credentials** field to `User`.

10. Select the protocol you want to use to run scripts in the **Execute scripts using** list.

    Note: Four options are available: TELNET, SSH1, SSH2, and SSH Auto. When selecting SSH Auto, **Error! Unknown document property name.** will first attempt to negotiate an SSH2 connection. If SSH2 is not supported, **Error! Unknown document property name.** defaults to SSH1.

11. Select the protocol you want to use to send requests for transfers to your device.

    Note: Five options are available: TELNET, SNMP, SSH1, SSH2, and SSH Auto. When selecting SSH Auto, Cirrus will first attempt to negotiate an SSH2 connection. If SSH2 is not supported, **Error! Unknown document property name.** defaults to SSH1. SNMP is only supported on Cisco devices.

12. Select the protocol you want to use to transfer configuration files to Cirrus Configuration Manager.

    Note: Five options are available for the command execute protocol and the config transfer protocol: TELNET, TFTP, SSH1, SSH2, and SSH Auto. When selecting SSH Auto, Cirrus will first attempt to negotiate an SSH2 connection. If SSH2 is not supported, **Error! Unknown document property name.** defaults to SSH1.

13. Click **Verify Login Information**.

14. ***If the node uses HTTPS to connect to the web interface,*** select `Yes` in the **Browse via HTTPS** field.

15. ***If the device uses an intermediary device to connect through,*** select `Yes` in the **Allow** field under the Intermediary Device Support category.

16. Click **OK** to add the node.

    Note: To keep the window open and add additional nodes, check **Keep this window open so I can add more nodes**.

Importing Nodes

You can import a list of nodes using several different file formats. Nodes can be imported from the following file formats:

- Text files

- Excel spreadsheets

- Access databases

- SQL databases

- SolarWinds Orion NPM databases

- SolarWinds Engineer's Edition NPM databases

- CiscoWorks database exports

- Kiwi CatTools database exports

To import nodes:

1. Click **File > Import Devices**.

2. Select the file type from the list, and then click **Next**.

3. Type or browse to the path and filename, and then click **Next**.

4. ***If you are importing a text file,*** check the column delimiters used to separate each field, and then click **Next**. Columns align based on the selections made.
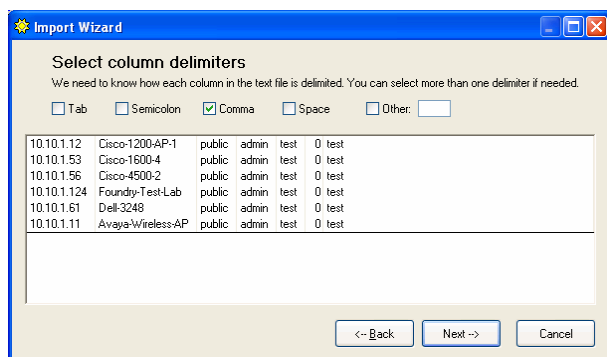
5. *If you are importing an Excel spreadsheet,* select the worksheet from the list, and then click **Next**.

6. *If you are importing a SQL database,* complete the following steps:

   a. Select the SQL server from the list, or type the server IP address

   b. Type or select the database name.

   c. Select the type of authentication required for the connection, and then click **Next**.

7. Assign each column a field name. Click on the column header, and then select a field from the list. Selecting **<ignore>** allows you to bypass the column.
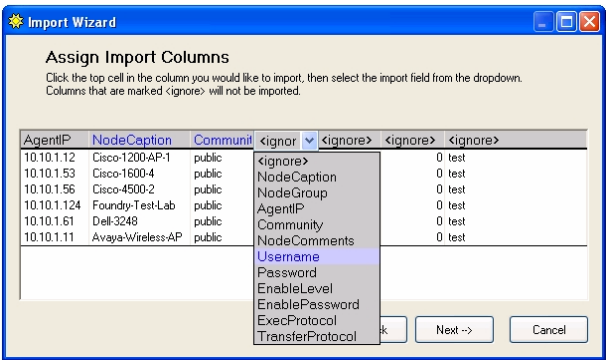
8. Ensure you are importing the appropriate data, and then click **Next**.

9. *If you want to exclude certain nodes,* clear the associated checkbox, and then click **Next**.

10. *If you want exclude previously added nodes,* check **Do not import nodes with IP addresses that already exist in the Configuration Management database**.

11. *If you are importing a large list of nodes,* uncheck **Discover device details immediately after Import**.

12. Click **Import**.

13. Click **Done** after the process completes.

Editing Nodes

You can easily edit the properties of a node after adding it to Cirrus Configuration Manager.

To edit node properties:

1. Click the node you want to modify in the node tree.

2. Click **Edit Selected Nodes**.

3. Click the Device Details tab

4. Modify the appropriate information, and then click anywhere else in the application to save the modifications.

   Note: Fields that appear in gray boxes can be edited by double-clicking the field.

Unmanaging Nodes

When you need to perform maintenance on nodes, such as upgrading firmware, installing new hardware, or updating security, you may want Cirrus Configuration Manager to discontinue downloading configurations and reporting information about the nodes while the devices are down. Unmanaging nodes while node maintenance is being performed helps maintain the accuracy of your data and prevents unnecessary and inaccurate reports.

Another reason to unmanage a node is if you want to keep configuration files for a decommissioned device. Configuration data for unmanaged nodes will remain in the Cirrus Configuration Manager database.

To unmanage nodes:

Select the nodes you want to unmanage in the nodes list, and then click **Nodes > Unmanage Selected Nodes**.

When nodes are unmanaged, Cirrus Configuration Manager will not perform actions on the nodes such as downloading configuration files, running scheduled jobs on the nodes, including the unmanaged nodes in reports.

To return nodes to a managed state:

Select the nodes you want to manage in the nodes list, and then click **Nodes > Manage Selected Nodes**.

Viewing Node Interface Details

You can view the following interface details about a node:

- Interface / Port Status

- Interface Traffic

- Interface / Port Configuration

- Time data was last transmitted / received

- Cisco Discovery Protocol (CDP)

- Cirrus user activity

- Realtime ARP cache

Complete the following procedure to view interface details.

To view the interface details of a specific node:

1. Click the Interfaces tab.

2. Select a category from the Interface Details list, and then click **Refresh** to view the selected statistics.

3. Check **Auto Refresh** to update statistics every 30 seconds.

4. To change the Auto Refresh time interval:

    a. Click **File > Settings**.

    b. Click **Interfaces** under **Node Details**.

    c. Adjust the slider to the appropriate interval.

    d. Click **OK** to save the changes.

Editing Multiple Nodes

Cirrus Configuration Manager allows you to change shared properties of multiple nodes.

To modify the properties of two or more nodes simultaneously:

1. Click the devices in the node tree while pressing the `Shift` or `Ctrl` key to select multiple devices.

2. Click **Nodes > Edit Multiple Nodes**.

3. Make the appropriate changes to the nodes, and then click **Done**.

    Note: To refresh the node tree and show the changes, click **Refresh** at the top of the node tree.

Adding Custom Node Properties

Cirrus Configuration Manager allows you to add custom properties to each node. You can define and store custom fields in the Cirrus Configuration Manager database. For example, you can define fields for country, physical location, asset tag, and serial number.

Cirrus Configuration Manager provides a collection of the most commonly used properties. New custom properties can also be defined. After creating a custom property, you can edit the property by editing node details. For more information, see "Importing Nodes" on page 15.

To define a custom property:

1. Click **File > Settings**.

2. Click **Custom Properties** in the left pane.

3. Select a property from the list or type a new property in the right pane.

4. Click **Add New Property**.

Searching for Network Addresses

Cirrus Configuration Manager provides the ability to search the entire database (nodes, configuration files, and inventory) for specific network addresses.

Finding IP Addresses

It can be important to find an IP address in Cirrus Configuration Manager. For example, you may need to search all of your nodes to see if a node you need to make changes to is managed by Cirrus Configuration Manager.

To find an IP address:

1. Click **Edit > Find IP Address**.
2. To ensure that the most complete results are available, click **Update Inventory** at the bottom of the Find Address tab to rescan all nodes in the database for any updated information. For more information on performing inventory scans, see "Managing Inventory" on page 45.
3. Type the address pattern you want to find in the **IP Address Pattern** field.
4. Click **Find**.

Finding MAC Addresses

It can be necessary to find an MAC address in Cirrus Configuration Manager. For example, you may need to search all of your configuration files to see if a MAC address is included in any black lists.

To find a MAC address:

1. Click **Edit > Find MAC Address**.
2. To ensure that the most complete results are available, click **Update Inventory** at the bottom of the Find Address tab to rescan all nodes in the database for any updated information. For more information on performing inventory scans, see "Managing Inventory" on page 45.
3. Type the address pattern you want to find in the **MAC Address Pattern** field.
4. Click **Find**.

Finding Hostnames

It can be vital to find a hostname in Cirrus Configuration Manager. For example, you may need to search all of your configuration files to see if a hostname is included in all of your allow lists.

To find a hostname:

1. Click **Edit > Find Hostname**.
2. To ensure that the most complete results are available, click **Update Inventory** at the bottom of the Find Address tab to rescan all nodes in the database for any updated information. For more information on performing inventory scans, see "Managing Inventory" on page 45.
3. Select Hostname from the Type of Address list.
4. Type the name pattern you want to find in the **Hostname** field.
5. Click **Find**.

Chapter 4

Managing Configuration Files

Configuration files can be downloaded, edited, compared, and uploaded using Cirrus Configuration Manager. The following procedures guide you through various tasks that simplify configuration file management.

Downloading Configuration Files

You can download configuration files to view the current configuration of your device, compare it to a previous configuration, or just to archive it for backup purposes. Cirrus Configuration Manager can transfer files using both direct and indirect transfers. Complete the following procedure to download configuration files from you devices.

To download a configuration file:

1. Right-click a node, group, or selection of nodes, and then click **Download Configs**.

    Note: Additional nodes can be added or removed from the list by using the associated buttons below the list of nodes.

2. Select the type of configuration file to download. For example, select **Startup**.

3. Check post download options. For example, you can select **View / Edit Downloaded Config** or **Compare to Last Config Downloaded**.

4. Click **Download**.

Once the download completes, the configuration files are written to the database and any post-download actions are performed.

Editing Configuration Files

When you need to update access lists, modify community strings, or adjust any other configuration changes, you will need to edit the configuration files you have already downloaded with Cirrus Configuration Manager. Complete the following procedure to edit a configuration file.

To edit an existing configuration file:

1. Click the configuration file in the left pane, and then click **Configs > Edit Configs**.

2. After making any changes to the configuration file, click **Save Changes.**

3. Type any details regarding the changes made to the configuration file.

4. Click **OK** to save the configuration file.

   Note: The revision is saved below the existing configuration file as a separate file with the revision comments as the name.

5. *If you have made all necessary changes,* upload your configuration. For more information, see "Uploading Configuration Changes" on page 28.

Decrypting Cisco Type 7 Passwords

When viewing a configuration file, all encrypted Cisco Type 7 passwords in the file can be decrypted. This is helpful when trying to recover lost passwords.

To decrypt Cisco Type 7 passwords:

1. Click on the configuration file in the left pane, and then clicking **Configs > Edit Configs**.

2. Click **Actions**, and then click **Decrypt Type 7 Passwords**.

   Notes:

   - All passwords that have been decrypted will appear in green text.

   - Decrypting Type 7 Passwords alters the text of the configuration file. If the configuration file is saved after decrypting the passwords, the passwords will be saved without encryption.

Comparing Configurations

Cirrus Configuration Manager provides the ability to compare configuration files. Configuration files can be compared between two nodes, or older configurations can be compared with the current configuration.

To compare two configurations, select the two configuration files in the left pane, and then click **Configs > Compare Selected Configs**.

   Notes:

   - Compared files are shown side-by-side.

     - Lines that have been changed are highlighted in yellow.

     - Missing lines are highlighted in red.

     - A green highlight indicates that the line has been added.

Using the Comparison Overview

A comparison overview is displayed to the left of the side-by-side comparison. This overview scales to fit the size of the window allowing for an overview of the entire comparison. Click anywhere on the comparison overview to jump to the associated sections of the configuration files.

Importing Configuration Files

You can import configuration files you have already downloaded from your devices into Cirrus Configuration Manager. Configuration files can be imported using the following file formats:

- SolarWinds Cirrus Configuration Manager Archive (.Config)

- SolarWinds Cisco Config Downloader (.CiscoConfig)

- Text File (.txt)

- Configuration File (.cfg)

- Any file in ASCII text

To import a configuration file to Cirrus Configuration Manager:

1. Select the node in the node list to which you want to import a configuration file.
2. Open the Windows Explorer file browser and browse to the folder containing your configuration file.
3. Drag the file from the Windows Explorer to the Cirrus Configuration Manager node list.
4. Type a name for the configuration file, and then click **OK**.

Understanding Baselines

A baseline is a configuration file that is known to be good for a particular application. When making node configuration changes, it is a good idea to establish a *known-good* configuration as a baseline.

Setting a Baseline Configuration

To set an existing configuration file as a baseline, click the configuration file in the left pane, and then click **Configs > Set/Clear Baseline Setting**.

Note: When downloading new configuration files, check **Compare to Last Baseline Config** in the Download Config window to automatically compare the new configuration file to the baseline.

Removing Baseline Status

To remove the baseline flag from a configuration file, click the configuration file in the left pane and then click **Configs > Set/Clear Baseline Setting**.

Baselining Your Entire Network

In some situations, it may be appropriate to establish a baseline configuration for every node managed by Cirrus Configuration Manager on your network. You can use either of the following options to create your baseline:

- Set to the last configuration file downloaded

- Set to the configuration files downloaded on a specific date

To create a baseline for your entire network:

1. Click **Configs > Baseline Entire Network**.

2. Select the appropriate option.

3. Click **Set Baseline**.

Clearing All Baselines

To remove all baselines from your database, click **Configs > Baseline Entire Network**, click **Clear all Baselines**, and then click **OK**.

Running Change Reports

A change report shows all modifications made to each configuration file over a specific time period. Change reports can show you changes made during a specific date range, or all differences between the latest downloaded configuration file and the baseline configuration file.

To run a config change report:

1. Click **Configs > Config Change Report**.

2. Select the type of change report to generate:

   Compare most recent download to the last baseline config

   Displays all differences between the most recent baseline and the latest downloaded configuration file.

   Compare the most recent download to the configuration on date

   Displays all differences between the most recent downloaded configuration file and a configuration file from the specified date.

> **Note:** If no configuration file was downloaded on the specified date, the configuration file following that date is used.

Show changes made over the past ## days

> Displays all changes made over the specified number of days.

Show changes made between dates

> Displays all the changes made through the specified date range.

3. *If you want the config change report to ignore specific changes,* complete the following procedure:

   a. Click **Edit Comparison Criteria**.

   b. Check the appropriate exclusions.

   c. *If you want to create a new exclusion,* see "Creating New Config Change Report Exclusions" on page 27.

   d. Click **Done**.

4. *If you want to see detailed changes between each configuration file,* click , and then check **Show detailed changes**. This shows each change from one configuration file to the next. For example, if there were 14 configuration changes made during a specific date range, the report will show the differences in the first configuration file as compared to the second configuration, and then show the differences in the second configuration file as compared to the third, and so on.

5. Click **Generate Report**.

Creating New Config Change Report Exclusions

When viewing config change reports, some changes can be ignored. For example, the `!Last Configuration change` line in Cisco configuration files can safely be ignored.

To specify sections of configuration files that can be ignored, Cirrus Configuration Manager uses regular expression patterns. The following are some of the regular expression pattern combinations Cirrus Configuration Manager recognizes:

```
^! Last
```

> Ignores the `!Last Configuration change` line in Cisco configurations.

`^ntp clock-period`

Ignores the `ntp clock-period` line in Cisco configurations.

`^wlccp ap username cisco`

Ignores the `wlccp` line in Cisco access point configurations.

Exclusions specified with regular expressions are global, and used for all comparison operations throughout Cirrus, including scheduled jobs. For more information about regular expression patterns, see "Regular Expression Pattern Matching" on page 91.

To create a new exclusion:

1. Click **Add Pattern**.

2. Type a name for the new comparison criteria in the **Title** field.

3. Type the regular expression pattern you want Cirrus Configuration Manager to ignore when running change reports in the **RegEx Pattern** field.

4. Type any comments you have in the **Comment** field.

Creating Config Snippets

A config snippet is a string of text that can be saved to a file, allowing you to easily merge sections of configuration files easily. For example, a config snippet is created from a router with the string `snmp-server community 123@dm1n RO`. When editing another router configuration, the config snippet can be reused. Config snippets can be used to edit an existing configuration file, or they can be uploaded directly to a node or group of nodes. For more information, see "Uploading a Config Snippet" on page 30.

To create a new Config snippet:

1. Click **Configs > Config Snippets**.

2. Click **New Snippet**.

3. Type a name in the **Snippet** field.

4. Type configuration lines for the new config snippet in the large text box provided, and then click **Save Changes**.

Uploading Configuration Changes

After editing your configuration files, you can easily upload changes to a node or group of nodes. There are three different ways to upload configuration changes:

• Upload an entire configuration

- Upload selected lines

- Upload a config snippet.

Uploading an Entire Configuration

Complete the following procedure to upload an entire configuration file.

To upload an entire configuration file:

1. Click the configuration file in the left pane, and then click **Configs > Upload Entire Config**.

    Note: Additional nodes can be added or removed from the list by using the associated buttons below the list of nodes.

2. *If you want to write the configuration to memory,* check **Write Config to NVRAM**.

3. *If your device needs to be rebooted following the upload,* check **Reboot Device**.

    Warning: Rebooting a device may cause momentary connectivity outages.

4. Click **Create Upload Script**.

5. Click **Execute Command Script**.

6. *If you want to save the results of the script when the upload finishes,* click **Save Results**.

Uploading Selected Lines

There are times when you only need to upload part of a configuration file. Cirrus Configuration Manager includes the ability to upload specific configuration lines.

To upload specific lines:

1. Click a configuration file in the left pane, and then click **Configs > Edit Configs**.

2. Select the lines you want to upload, and then click **Actions > Upload Selected Lines**.

    Note: Additional nodes can be added or removed from the list by using the associated buttons below the list of nodes.

3. *If you want to write the configuration to memory,* check **Write Config to NVRAM**.

4. *If you need to reboot your device following the upload,* check **Reboot Device**.

    Warning: Rebooting a device may cause momentary connectivity outages.

5. Click **Create Upload Script**.

6. Click **Execute Command Script**.

7. *If you want to save the results of the script when the upload finishes,* click **Save Results**.

Uploading a Config Snippet

Complete the following procedure to upload a config snippet. For information on how to create config snippets, see "Creating Config Snippets" on page 28.

To upload a Config Snippet:

1. Click **Configs > Config Snippets**.

2. Right-click the snippet in the Config Snippets window, and then click **Upload to Devices**.

    Note: Additional nodes can be added or removed from the list by using the associated buttons below the list of nodes.

3. *If you want to write the configuration to memory,* check **Write Config to NVRAM**.

4. *If you need to reboot your device following the upload,* check **Reboot Device**.

    Warning: Rebooting a device may cause momentary connectivity outages.

5. Click **Create Upload Script**.

6. Click **Execute Command Script**.

7. *If you want to save the results of the script when the upload finishes,* click **Save Results**.

Configuring a Config Archive

Cirrus Configuration Manager can copy every configuration file downloaded to an archive location for backup purposes.

To configure a configuration archive:

1. Click **File > Settings**.

2. Click **Configs > Config Archive**.

3. Check **Save a copy of each Config to the Config-Archive directory when it is downloaded**.

4. Type or browse to the folder you want to store the configuration files using the **Config-Archive directory** field.

5. Type the template you want to use when naming the configuration files. For more information, see "Configuration Archive Variables" on page 87.

6. If you want to archive your existing configuration files, click **Export all Configs to the Config-Archive directory now**.

7. Click **OK**.

Enabling Realtime Configuration Change Detection

When Cirrus Configuration Manager is installed on the same computer as SolarWinds Orion Network Performance Monitor, you can enable realtime configuration change detection. This feature notifies you via email whenever a change in any of your device configurations is detected.

Requirements

To utilize realtime configuration change detection you will need the following items.

- A Windows user accounts with administrative rights.

- A copy of Orion Network Performance Monitor or another Syslog or SNMP Trap receiver that can execute a third-party application installed on the same computer as Cirrus Configuration Manager.

- Network devices configured to send Syslog or SNMP Trap messages upon configuration changes.

Configuring Realtime Configuration Change Detection

Complete the following procedure to enable realtime configuration change detection using SolarWinds Orion Network Performance Monitor.

To enable realtime configuration change detection:

1. Configure your network devices to send syslog or SNMP trap messages to your server when configuration changes are detected. The IP address the device uses to send messages must be the same IP address used to manage the device in Cirrus Configuration Manager. For more information, see the vendor documentation for each network device.

2. Start Cirrus Configuration Manager. Click **Start > All Programs > SolarWinds Configuration Management > Cirrus Configuration Manager**.

3. Click **File > Settings**.

4. Click **Realtime Change Detection** in the left pane.

5. Check **Enable Realtime Config Change Notifications**.

6. Click **Config Change Settings** in the left pane.

7. *If you want to login to all devices with a single set of account credentials,* check **Use a single set of device login credentials to login to all of your devices**, and then type the appropriate login credentials.

8. Type the Windows account credentials you want to use to execute the job.

   Note: To use the Windows account you are currently logged in as, leave the **User Name** and **Password** fields blank.

9. *If you want to save the log file in another location,* browse to the new location.

10. Click **Download Options** in the left pane.

11. Select the configuration type you want to download.

12. *If you want to be notified if the new configuration is different than the previously downloaded configuration,* select **Last Config**.

13. *If you want to be notified if the new configuration is different than the baseline configuration,* select **Baseline Config**.

14. Click **Email Addresses** in the left pane, and then provide the appropriate email address information. To suppress email notification, leave the email address fields blank.

    Note: You can use a custom property as an email address allowing you to assign different email addresses for each of your devices.

15. Click **Email Server Details** in the left pane, and then provide the appropriate email server information.

16. Click **OK**.

17. ***If your device sends change notifications to Orion using Syslog messages,*** complete the following procedure:

   a. Click **Start > All Programs > SolarWinds Orion Network Performance Monitor > Syslog Viewer**.

   b. Click **View > Alerts/Filter Rules**.

   c. Click **Add New Rule**.

   d. Provide the appropriate information on the General tab and DNS Hostname tab.

   e. Click the Message tab, and then type the message pattern to look for in the **Message Type Pattern** field. The message pattern will vary by device type. For example, when a change is made to a Cisco router, a syslog message containing `%SYS-5-CONFIG_I:` is sent. For more information about what messages are sent, see the documentation provided by the vendor of your device.

   f. Click the Alert Actions tab, and then click **Add New Action**.

   g. Select **Execute an external program**, and then click **OK**.

   h. Type the following in the **Program to execute** field:

   `Path\Configuration Management\ConfigAutoDownload.exe ${IP}`

   Where `Path` is the location of the `Configuration Management` folder. For example, "`C:\Program Files\SolarWinds`". If the path contains spaces, enclose the path section of the statement in quotation marks (`"`).

   i. Click **OK**.

   j. Ensure the new rule is checked in the Alerts / Filter Rules tab of the Syslog Server Settings window, and then click **OK**.

18. ***If your device sends change notifications to Orion using SNMP Trap messages,*** complete the following procedure:

    a. Click **Start > All Programs > SolarWinds Orion Network Performance Monitor > Trap Viewer**.

    b. Click **View > Alerts/Filter Rules**.

    c. Click **Add New Rule**.

    d. Provide the appropriate information on the General tab and DNS Hostname tab.

    e. Click the Conditions tab, and then click **Add a condition**.

    f. Click **SNMPv2-MIB:snmpTrapOID**, and then browse to the MIB that contains the trap message.

    g. Click the asterisk, and then type the message pattern to look for. The message pattern will vary by device type. For example, when a change is made to a Cisco router, a syslog message containing `%SYS-5-CONFIG_I:` is sent. For more information about what messages are sent, see the documentation provided by the vendor of your device.

    h. Click the Alert Actions tab, and then click **Add Action**.

    i. Select **Execute an external program**, and then click **OK**.

    j. Type the following in the **Program to execute** field:

```
"Path\Configuration Management\ConfigAutoDownload.exe"
${IP}
```

    Where `Path` is the location of the `Configuration Management` folder. For example, `"C:\Program Files\SolarWinds"`. If the path contains spaces, enclose the path section of the statement in quotation marks (").

    k. Click **OK**.

    l. Ensure the new rule is checked in the Alerts / Filter Rules tab of the Trap Server Settings window, and then click **OK**.

19. ***If your device sends change notifications to a system other than Orion,*** complete the following procedure:

    a. Start your third-party Syslog or SNMP Trap receiver.

    b. Setup an alert that executes an external program.

    c. Type the following in the program to execute field:

```
Path\Configuration Management\ConfigAutoDownload.exe ${IP}
```

Where *Path* is the location of the `Configuration Management` folder. For example, `"C:\Program Files\SolarWinds"`. If the path contains spaces, enclose the path section of the statement in quotation marks (").

d. Save the alert and ensure it is enabled.

Searching for Configuration Files

Complete the following procedure to search for specific strings of text within the configuration files stored in the Cirrus Configuration Manager database. If you want to complete detailed searches using Regular Expression pattern matching or if you want to ensure your configurations follow appropriate configuration standards, use the Cirrus Policy Manager. For more information, see "Using Policy Reports" on page 55.

To search for text within configuration files:

1. Click **Edit > Search Configs**.

2. *If you want to select which nodes to search,* complete the following procedure:

    a. Click **Add Devices**.

    b. Select the devices you want to search.

    c. Click **OK**.

3. *If you want to search all nodes,* click **Select Nodes Directly**, and then click **All Nodes in the Database**.

4. *If you want to search a group of nodes that meet specific criteria,* complete the following procedure:

    a. Click **Select Nodes Directly**

    b. Click **Specify a Selection Criteria**.

    c. Click **Browse**, and then click **Add a Simple Condition**.

    d. Click the first asterisk, and then click the appropriate field.

    e. *If you want to change the comparison operator,* click **is equal to**, and then select the comparison operator you want to use.

    f. Click the second asterisk, and then type the value or select it from the list.

    Note: All values currently in the database for the field are displayed when you browse the list.

5. Type the string of text you want to find in the **Find** field.

6. ***If you want to specify a date range for your search,*** complete the following procedure:

    a. Click ⊗ to expand the search criteria pane.

    b. Set the date range for your search.

7. ***If you want to specify the type of configuration files to search,*** complete the following procedure:

    a. Click ⊗ to expand the search criteria pane.

    b. Check the configuration types you want to search.

8. Click **Start Search**.

9. ***If you want to save the results of the search,*** click **Save Results**.

Deleting Configuration Files from the Database

As the Cirrus database grows in size, you can delete existing configuration files from the database. If there is any chance you may need information you want to delete, back up your database. For more information, see "Creating Database Backups" on page 70.

To purge the database:

1. Click **Configs > Purge Old Configs**.

2. ***If you want to delete configuration files from selected nodes,*** complete the following procedure:

    a. Click **Add Devices**.

    b. Select the devices you want to add to the list.

    c. Click **OK**.

3. ***If you want to delete configuration files from all nodes,*** click **Select Nodes Directly**, and then click **All Nodes in the database**.

4. *If you want to delete configuration files from a group of nodes that meet specific criteria,* complete the following procedure:

   a. Click **Select Nodes Directly**

   b. Click **Specify a Selection Criteria**.

   c. Click **Browse**, and then click **Add a Simple Condition**.

   d. Click the first asterisk and then click the appropriate field.

   e. *If you want to change the comparison operator,* click **is equal to**, and then click the comparison operator you want to use.

   f. Click the second asterisk, and then type the value or select it from the list.

      Note: All values currently in the database for the field are displayed when you browse the list.

5. Click the Select Purge Method tab.

6. *If you want to remove configuration files older than a specific date,* complete the following procedure:

   a. Click **Purge all Configs downloaded before**.

   b. Type the date or click the arrow to browse.

   c. *If you want to specify the time of day,* check **Include Time**, and then type or select a time from the list.

7. *If you want to specify the number of configuration files to keep,* complete the following procedure:

   a. Click **Purge all Configs except the last 10**.

   b. Adjust the slider to adjust the number of configuration files that should be kept in the database.

8. Click **Purge**.

9. When the purge completes, click **Purge More Configs** to delete more files, or click **Done** to close the window.

Chapter 5

Working with Command Scripts

Cirrus Configuration Manager allows you to accomplish several tasks through the creation and execution of command scripts. Consider the following tasks you can simplify by using command scripts.

- Downloading configuration files

- Uploading configuration files

- Uploading IOS images

- Updating login banners

- Updating access control lists (ACLs)

With the appropriate use of variables, a single script can be executed on several different devices, without concern for syntax differences.

Executing Command Scripts

Complete the following procedure to create and execute a command script.

To create and execute a command script:

1. Click **Nodes > Execute Command**.

2. *If you want to select the nodes on which to run the script,* complete the following procedure:

   a. Click **Add Devices**.

   b. Select the devices on which you want to run your command script.

   c. Click **OK**.

3. *If you want to run the script on all nodes,* click **Select Nodes Directly**, and then click **All Nodes in the Database**.

4. *If you want to run the script on a group of nodes that meet specific criteria,* complete the following procedure:

   a. Click **Select Nodes Directly**.

   b. Click **Specify a Selection Criteria**.

   c. Click **Browse**, and then click **Add a Simple Condition**.

    d. Click the first asterisk, and then click the appropriate field.

    e. *If you want to change the comparison operator,* click **is equal to**, and then select the comparison operator you want to use.

    f. Click the second asterisk, and then type the value or select it from the list.

    Note: All values currently in the database for the field are displayed when you browse the list.

5. *If you want to type a new script,* type the script in the **Command Script to Execute** field.

Note: Scripts can consist of a single command or list of commands to be executed sequentially. Scripts should mirror commands entered when manually typing instructions from the command prompt. For example, when sending the `show version` command to a router via a TELNET session, the prompt requires the user to type `sh version`. The command script must mimic this entry. For example, type `sh version` with a carriage return at the end of the line.

6. *If you want to load a previously saved script,* complete the following procedure:

    a. Click **Load Script**.

    b. Browse to the script you want to load, and then click **Open**.

    Note: To view sample scripts, browse to the `\Sample Scripts` folder.

7. *If you want to see results that meet specific criteria,* complete the following procedure:

    a. Click ⌃.

    b. Check **Filter Results that Match a Pattern**.

    c. Type the string you want Cirrus Configuration Manager to use for filtering. For example, adding the word `Serial` to the filter displays lines that start with the word Serial. For more information on pattern matching, see "Regular Expression Pattern Matching" on page 91.

    Note: The example script `Get Serial Number from each Device.txt` demonstrates this feature.

8. ***If you want to write the results of a script to a file,*** complete the following procedure:

    a. Click ⊗.

    b. Check **Save Results to a File**.

    c. Type or browse to the path and filename for the log file.

9. ***If you want to hide script commands when the script is executed,*** complete the following procedure:

    a. Click ⊗.

    b. Uncheck **Show Commands in Output**.

10. Click **Execute Command Script**.

11. ***If you want to save the results of the script,*** click **Save Results**.

    Note: Unchecking **Outline View** displays results without formatting.

12. ***If you want to save the script for later use,*** complete the following procedure:

    a. Click the Execute Script tab.

    b. Click **Save Script**.

    c. Type a filename, and then click **Save**.

Using Variables within Scripts

The power of the Cirrus Configuration Manager scripting engine is highlighted by the ability to use variables within scripts. Variables always begin with a dollar sign and a curly brace (${) and end with a curly brace (}).

Script variables substitute the appropriate commands based on the device type. For example, the variable ${EnterConfigMode} parses as "config terminal" when communicating with Cisco IOS devices, but parses as "configure" when communicating with an HP Procurve Switch.

For a list of variables that can be used in command scripts and device command templates, see "Variables" on page 85.

Example Variable Script

The following script contains commands with variables to remove the public read-only community string.

```
${EnterConfigMode}

no snmp-server community public RO

${ExitConfigMode}

${SaveConfig}

${Reboot}
```

Parsed for Cisco IOS devices:

```
config terminal

no snmp-server community public RO

end

write memory

reload${CRLF}y${CRLF}y
```

Parsed for a Dell PowerConnect Switch:

```
config

no snmp-server community public RO

end

copy running-config startup-config${CRLF}${CRLF}

reload${CRLF}Yes
```

Note: The *${CRLF}* variable equals a carriage return line feed for all devices.

Script variables are defined in device command templates. Templates are located in the `Configuration Management\DeviceTypes` folder. Each `.ConfigMgmt-Commands` file contains a System OID that is used to uniquely identify a device. A list of command names and the corresponding commands to be sent to the device when the command name is called are also included in the templates. These command names are the variables used when creating a script.

For example, consider the following line taken from the Cisco IOS device command template:

```
<Command Name="EnterConfigMode" Value="config terminal"/>
```

When a script is run on a Cisco IOS device, the variable `${EnterConfigMode}` parses as `config terminal`. New command names can be added and existing command names can be modified within these files.

Note: Altering device command templates changes the way that Cirrus Configuration Manager communicates with network devices. SolarWinds does not recommend altering a device command template file unless you have advanced knowledge and experience with device commands and variables.

Managing Inventory

The robust inventory engine of Cirrus Configuration Manager compliments the configuration management functions of the product. Inventory can be performed on all of your nodes, on node groups, or on single nodes. You can view collected inventory statistics in the detail view of each device.

Running a Complete Inventory Scan

To perform an inventory of all nodes managed by Cirrus Configuration Manager, click **Inventory > Start Full Inventory**.

Note: A full inventory scan can take anywhere from a few minutes to several hours to complete. The time period varies based on the number of nodes and the type of statistics you want to collect. For more information on how to establish which statistics are collected, see "Adjusting Inventory Settings" on page 48.

Running Inventory Scans

Complete the following procedure to run an individual inventory scan.

To complete an individual inventory scan:

1. Click a node or a group of nodes in the left pane.
2. Click **Inventory > Inventory Selected Nodes**.

Scheduling an Inventory Scan

A full inventory scan can be set to run on a schedule. Scheduled inventory scans are referred to as inventory jobs.

To create a new inventory job:

1. Click **Inventory > Schedule Inventory**.
2. Type a name for the job, and then click **Continue**.
3. Select the frequency of your job from the **Schedule Job** list.
4. Type or select a time in the **Start Time** field.
5. Type or select a date in the **Starting On** field.

6. Type or select a date in the **Ending On** field. To assign a job to run with no end date, leave this field blank.

7. *If you want to run the job daily,* type a number in the **Every days** field to set the daily frequency.

8. *If you want to run the job weekly,* complete the following procedure:

   a. Type a number in the **Every weeks on** field to set the frequency.

   b. Check the days of the week on which you want to run your job.

9. *If you are running your job monthly,* complete the following procedure:

   a. Type a number in the **Every months on** field to set the frequency.

   b. Check each month in which you want to run your job.

10. Click **Continue**.

11. Type the Windows account name used to run the job.

12. Type the password for the Windows account in the appropriate password fields.

13. Click **Finish**.

14. Type any comments in the **Comments** field.

15. Click the Nodes tab.

16. *If you want to select the nodes on which the job will be run,* complete the following procedure:

   a. Click **All Nodes in the Database**.

   b. Click **Select Nodes Directly**.

   c. Click **Add Devices**.

   d. Select the devices you want to add to the list.

   e. Click **OK**.

17. *If you want to run the job on a group of nodes that meet specific criteria,* complete the following procedure:

   a. Click **Select All Nodes in the Database**.

   b. Click **Specify a Selection Criteria**.

   c. Click **Browse**, and then click **Add a Simple Condition**.

   d. Click the first asterisk, and then click the appropriate field.

    e. *If you want to change the comparison operator,* click **is equal to**, and then click the comparison operator you want to use.

    f. Click the second asterisk, and then type the value or select it from the list.

    Note: All values currently in the database for the field are displayed when you browse the list.

18. Click the Notifications tab.

19. *If you want to print the results,* complete the following procedure:

    a. Check **Print Results**.

    b. Select a printer from the **Printer** list on the Printer Settings tab.

20. *If you want to write the results to a file,* do the following

    a. Check **Save Results To File**.

    b. Click the File Settings tab.

    c. Type or browse to the file in which you want to write the results in the **Path and Filename** field.

    d. *If you want to ignore results that do not contain errors,* check **Only save results if this job encounters an error during execution**.

21. *If you want to email the results,* complete the following procedure:

    a. Check **E-Mail Results**.

    b. Click the Email Settings tab.

    c. Type the email addresses to which you want to send the results in the **To**, **CC** and **BCC** fields. Use a semicolon to separate multiple email addresses.

    d. Type the subject of the email in the **Subject** field.

22. *If you want to log the job steps to a log file,* check **Log job steps to JOB-#####.log**.

23. *If you want to ensure that all Notification settings are configured properly,* click **Test Notifications**.

24. ***If you need to change the Windows account information,*** complete the following procedure:

   a. Click the Security tab.

   b. Type the Windows account name that will be used to run the job.

   c. Click **Set Password**.

   d. Type the password for the Windows account in the appropriate password fields, and then click **OK**.

Adjusting Inventory Settings

Complete the following procedure to change your inventory settings.

To change the statistics to collect during an inventory scan:

1. Click **Inventory > Inventory Settings**.
2. Check the statistics you want to collect, and then click **OK**.
3. Click **Inventory Engine Settings** in the left pane.
4. Adjust the slider to set the number of devices you want Cirrus Configuration Manager to scan concurrently.

   Note: Increasing the number of devices Cirrus Configuration Manager can scan concurrently increases the amount of system resources need during a scan.

Viewing Inventory

Complete the following procedure to view your inventory statistics. For more information, see "Running Inventory Scans" on page 45.

To view your inventory statistics:

1. Click a node in the left pane, and then click **Nodes > Edit Selected Node**.
2. Click the Inventory tab.
3. Click **Inventory Details**, and then click an inventory category.

Chapter 7

Managing Reports

Cirrus Configuration Manager includes several standard reports. These reports display configuration information for each node and statistics collected by the inventory engine.

Viewing Reports

Complete the following task to view a report.

To view a report:

1. Click **Reports > View Report**.

2. Click the report you want to view, and then click **OK**.

Creating and Editing Reports

If the report you are looking for is not included with Cirrus Configuration Manager, new reports can be created. Complete the following procedure to create and modify your reports.

To create a new report or edit an existing report:

1. *If you want to create a new report,* complete the following procedure:

   a. Click **Reports > New Report**.

   b. Click Browse next to the **Filename** field

   c. Browse to a folder, and then type a filename.

   d. Click **Save**.

      Note: For a report to be included with the list of existing reports, it must be saved in the default folder (`\Reports`).

2. *If you want to edit an existing report,* complete the following procedure:

   a. Click **Reports > View Report.**

   b. Click the report you want to view, and then click **OK**.

   c. Click **Modify Report**.

3. Type a name for the report in the **Report Title** field.

4. *If you want a subtitle for your report,* type the subtitle it in the **Sub Title** field.

5. Type the name of the category into which you want to group the report in the **Category** field.

6. *If you want to add a description of the report,* type a description and any other comments in the **Description** field.

7. Click **Portrait** or **Landscape** to set the print orientation.

8. *If you want to include device status in your report,* click **Display current device Up/Down Status**

9. *If you want to group rows containing like values,* click **Group/Merge similar rows**.

10. Click **Horizontal Lines**, and then click the option you want to use in your report.

11. Click the Select Fields tab.

12. Click **Type of Report**, and then click the type of report you want to run.

13. Click **Group the Routers/Switches by**, and then click a category by which to group your devices. You can use custom node properties when grouping nodes. For more information on how to create custom properties, see "Adding Custom Node Properties" on page 19.

14. Select the properties you want to add in the **All Properties** list, and then click the **Right Arrow** to add them to the **Selected Properties** list.

15. *If you want to filter the results of your report,* complete the following procedure:

    a. Click the Filter Results tab.

    b. Click **Add Condition**, and then click **Add a Simple Condition**.

    c. Click the first asterisk, and then click the appropriate field.

    d. *If you want to change the comparison operator,* click **is equal to**, and then click the comparison operator you want to use.

    e. Click the second asterisk, and then type the value or select it from the list.

       Note: All values currently in the database for the field are displayed when you browse the list.

    f. *If you want to see the list of filtered nodes,* click **View Selected Nodes**.

g. *If you want to limit the number of records by count,* click **Show only the Top XX Records**, and then type the number of records you want to display.

h. *If you want to limit the number of records by percentage,* click **Show the Top ##% of Records to display**, and then type the percentage of records you want to display.

16. Click **OK**.

17. *If you want to save the report,* click **Save Changes**.

Scheduling Reports

Cirrus Configuration Manager allows you to schedule reports enabling you to send/receive email reports regularly. Complete the following task to schedule a report.

To schedule a report:

1. Click **Reports > Schedule Report**.

2. Type a name for the job, and then click **Next**.

3. Select the frequency of your job from the **Schedule Job** list.

4. Type or select a time in the **Start Time** field.

5. Type or select a date in the **Starting On** field.

6. Type or select a date in the **Ending On** field. To assign a job to run with no end date, leave this field blank.

7. *If you want to run the job daily,* type a number in the **Every days** field to set the daily frequency.

8. *If you want to run the job weekly,* complete the following procedure:

   a. Type a number in the **Every weeks on** field to set the frequency.

   b. Check the days of the week on which you want to run your job.

9. *If you are running your job monthly,* complete the following procedure:

   a. Type a number in the **Every months on** field to set the frequency.

   b. Check each month in which you want to run your job.

10. Click **Next**.

11. Type the Windows account name that will be used to run the job.

12. Type the password for the Windows account in the appropriate password fields.

13. Click **Finish**.

14. Type any comments in the **Comments** field.

15. Click the Report tab.

16. Select the appropriate report. Only one report can be executed at a time. To execute more than one report, create a job for each additional report.

17. Click the Report Destinations tab.

18. *If you want to print the results,* complete the following procedure:

    a. Check **Print Results**.

    b. Select a printer from the **Printer** list on the Printer Settings tab.

19. *If you want to write the results to a file,* complete the following procedure:

    a. Check **Save Results To File**.

    b. Click the File Settings tab.

    c. Type or browse to the file in which you want to write the results in the **Path and Filename** field.

    d. *If you want to ignore results that do not contain errors,* check **Only save results if this job encounters an error during execution**.

20. *If you want to email the results,* complete the following procedure:

    a. Check **E-Mail Results**.

    b. Click the Email Settings tab.

    c. Type the email addresses to which you want to send the results in the **To**, **CC** and **BCC** fields. Use a semicolon to separate multiple email addresses.

    d. Type the subject of the email in the **Subject** field.

21. *If you want to log the job steps to a log file,* check **Log job steps to JOB-#####.log**.

22. *If you want to ensure that all notification settings are configured properly,* click **Test Notifications**.

23. ***If you need to change the Windows account information,*** complete the following procedure:

   a. Click the Security tab.

   b. Type the Windows account name that will be used to run the job.

   c. Click **Set Password**.

   d. Type the password for the Windows account in the appropriate password fields.

24. Click **OK**.

Deleting Reports

Complete the following procedure to delete a report.

To delete an existing report:

1. Click **Reports > View Report.**

2. Click the report you want to delete, and then click **Delete Selected Reports**.

Chapter 8

Using Policy Reports

Policy reports help ensure device configurations conform to both internal business practices and federal regulations, such as Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability (HIPAA), and Computer Inventory of Survey Plans (CISP). Policy reports scan configuration files and report any discovered rule violations. For example, a rule requires configurations do not include the read-only community string `public`. You can run a report on your configuration files, and then display any configurations that violate the rule. Your policy report lists violations, including the line number where the violation occurred if applicable. Several example reports, policies, and rules are included with Cirrus Configuration Manager.

A policy report is a report that includes a collection of policies. A policy is a collection of rules. A report can contain several policies which, in turn, can contain several rules.
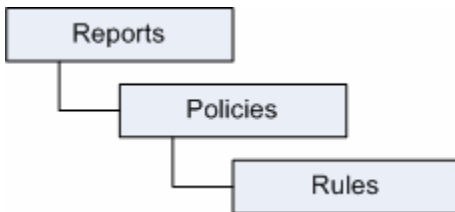
Launching Policy Reporting

The Cirrus Configuration Manager Policy Reporting application is launched by clicking **Reports > Cirrus Policy Reporter** from the Cirrus Configuration Manager application.

Using the Policy Creation Wizard

The Policy Creation wizard allows you to create a complete policy report, including the creation of rules and policies. Complete the following procedure to create a policy report using the Policy Creation wizard.

To create a policy report:

1. Click **File > Policy Creation Wizard**.

2. Review the welcome text, and then click **Next**.

3. Review the introduction to rules, and then click **Next**.

4. Click **Walk me through creating a new Rule**, and then click **Next**.

5. Type a name for your new rule, and then click **Next**.

6. Type any comments in the **Comment** field.

7. *If you want to assign this rule to a group,* type a new group name in the **Grouping** field or select an existing group from the list.

8. Click **Next**.

9. *If you want to use a regular expression for your search pattern,* complete the following procedure:

    a. Set the **Search Pattern Type** to **RegEx Expression**.

    b. Type the expression in the **Search Pattern** field. For more information see "Regular Expression Pattern Matching" on page 91.

        Note: To view examples, click **Example Search Patterns**.

10. *If you want to use a simple expression for your search pattern,* complete the following procedure:

    a. Select **Simple Find** for the search pattern type. The simple find expressions allow you to use the asterisk and question mark (?) characters as wildcard characters.

    b. Type the expression in the **Search Pattern** field.

11. Click **Found** or **Not Found** to determine how violation is defined, and then click **Next**.

12. Click **Informational**, **Warning**, or **Critical** to set the severity of your rule, and then click **Next**.

13. Review the Rule Details, check **Save This Rule**, and then click **Next**.

14. Review the introduction to policies, and then click **Next**.

15. Click **Yes, Let's Create a New Policy**, and then click **Next**.

16. Type a name for your new policy.

17. Type any comments in the **Comment** field.

18. *If you want to assign this policy to a group,* type a new group name in the **Grouping** field or select an existing group from the list.

19. Click **Next**.

20. ***If you want to select which devices the policy applies to,*** complete the following procedure:

   a. Click **Add Devices**.

   b. Select the devices you want to add to the list.

   c. Click **OK**.

21. ***If you want your policy to apply to all devices,*** click **Select Nodes Directly**, and then click **All Nodes in the Database**.

22. ***If you want your policy to apply to a specific group of nodes,*** complete the following procedure:

   a. Click **Select Nodes Directly**

   b. Click **Specify Selection Criteria**.

   c. Click **Browse**, and then click **Add a Simple Condition**.

   d. Click the first asterisk, and then click the appropriate field.

   e. ***If you want to change the comparison operator,*** click **is equal to**, and then click the comparison operator you want to use.

   f. Click the second asterisk, and then type the value or select it from the list.

      Note: All values currently in the database for the field are displayed when you browse the list.

23. Click **Next**, and then check the configuration file types you want to search when executing this policy. **Any** searches the last downloaded configuration file, regardless of type.

24. Click **Next**, and then select the rules in the **All Rules** list you want to add to your policy, and then click the **Right Arrow** to add the rules to the **Assigned Rules** list.

25. Click **Next**, and then click **Yes** to save the new policy.

26. Click **Next**, and then click **Yes, Let's Create a New Report**, and then click **Next**.

27. Type a name for your new report.

28. Type any comments in the **Comment** field.

29. ***If you want to assign this report to a group,*** type a new group name in the **Grouping** field or select an existing group from the list.

30. Click **Next**, and then select the policies in the **All Policies** list you want to add to your report, and then click the **Right Arrow** to add your selection to the **Assigned Policies** list.

31. Click **Next**, and then click **Yes** to save the new report.

32. Click **Exit**.

Executing a Policy Report

A policy report shows rule violations contained within the policies of the report.

To execute a policy report:

1. Select the policy report you want to execute in the Policy Reports list.

2. Click **Reports > Execute Selected Reports**.

   Note: When viewing a report, mouse over any rule or violation icon to display a description of the item.

3. To display and make changes to a configuration file that has violated a rule, right-click the violation icon, and then click **View / Edit Config**.

4. *If you find a violation and want to execute a script on the device to make a change,* right-click the device name, and then click **Remediate Rule Violation**. For more information, see "Executing Command Scripts" on page 39.

Rules

Rules describe what is to be found (or not found) in device configuration files. Rules contain the following properties:

Property	Description
Name	How the rule will be shown in display lists and Reports
Comment	Description of the rule
Grouping	Category to which the rule belongs
Pattern	Regular expression or find string that defines the search object
Pattern Type	Type of search expression (regular expression or find string)
Pattern Must Exist	Whether the pattern should be found or not

Editing Rules

If you need to modify a rule to update a change in your policies, you will need to edit the rule. Complete the following procedure to modify your rule.

To edit a rule:

1. Click **Rules > View All Rules**.

2. Click the rule you want to edit.

3. Edit the appropriate values.

4. Review the rule details, and then click **Save Changes**.

Deleting Rules

Complete the following procedure to delete a rule.

To delete an existing rule:

1. Click **Rules > View All Rules**.

2. Click the rule you want to delete, and then click **Delete Selected Reports**.

3. Click **Yes**.

Policies

A policy is a collection of one or more rules. These rules define the type of configuration file to search and the nodes that are included in the search.

Editing Policies

If you need to modify a policy, complete the following procedure.

To edit a policy:

1. Click **Policies > View All Policies**.

2. Click the policy you want to edit.

3. Edit the appropriate values.

4. Review the policy details, and then click **Save Changes**.

Deleting Policies

Complete the following procedure to delete a policy.

To delete a policy:

1. Click **Policies > View All Policies**.

2. Click the policy you want to delete, and then click **Delete Selected Policy**.

3. Click **Yes**.

Reports

Reports provide a way to group policies, either by the devices that they will be executed against or by the type of report in which they are used. Report properties include Name, Comment, Grouping, and the policies included in the Report.

Editing Reports

If you need to modify a report to update a change in your policies, complete the following procedure.

To edit a report:

1. Click **Report > View All Reports**.

2. Click the report you want to edit in the list of reports, and then click **Reports > Edit Selected Reports**.

3. Edit the appropriate values.

4. Review the report details, and then click **Save Changes**.

   Note: When viewing a report, mouse over any rule or violation icon to display a description of the item.

5. To display and make changes to a configuration file that has violated a rule, right-click the violation icon, and then click **View / Edit Config**.

Deleting Reports

Complete the following procedure to delete a report.

To delete an existing report:

1. Click **Reports > View All Reports**.

2. Click the policy you want to delete, and then click **Delete Selected Policy**.

3. Click **Yes**.

Scheduling a Policy Report

A policy report can be scheduled to run at any time.

To schedule a policy report:

1. Click **Schedule > Schedule a Policy Report**.

2. Type a name for the job, and then click **Next**.

3. Select the frequency of the job from the **Schedule Job** list.

4. Type or select a time in the **Start Time** field.

5. Type or select a date in the **Starting On** field.

6. Type or select a date in the **Ending On** field. To assign a job to run with no end date, leave this field blank.

7. *If you want to run the job daily,* type a number in the **Every days** field to set the daily frequency.

8. *If you want to run the job weekly,* complete the following procedure:

   a. Type a number in the **Every weeks on** field to set the frequency.

   b. Check the days of the week you want to run your job.

9. *If you are running your job monthly,* complete the following procedure:

   a. Type a number in the **Every months on** field to set the frequency.

   b. Check each month you want to run your job.

10. Click **Next**.

11. Type the Windows user account name for the job.

12. Type the password for the user account in the appropriate password fields.

13. Click **Finish**.

14. Type any comments in the **Comments** field.

15. Click the Policy Report tab.

16. Select the policy report that is to be executed when the job is run.

17. *If you want to suppress notifications if violations are not found,* check **Send Notification only when Policy Violations are present**.

18. *If you want to launch the Policy Reporting application,* click **Edit Policy Reports**.

19. Click the Notifications tab.

20. *If you want to print the results,* complete the following procedure:

    a. Check **Print Results**.

    b. Select a printer from the Printer list on the Printer Settings tab.

21. *If you want to write the results to a file,* complete the following procedure:

    a. Check **Save Results To File**.

    b. Click the File Settings tab.

    c. Type or browse to the file in which you want to write the results in the **Path and Filename** field.

    d. If you want to ignore results that do not contain errors**,** check **Only save results if this job encounters an error during execution**.

22. *If you want to email the results,* complete the following procedure:

    a. Check **E-Mail Results**.

    b. Click the Email Settings tab.

    c. Type the email addresses to which you want to send the results in the **To**, **CC** and **BCC** fields. Use a semicolon to separate multiple email addresses.

    d. Type the subject of the email in the **Subject** field.

23. *If you want to log the job steps to a log file,* check **Log job steps to JOB-#####.log**.

24. *If you want to ensure that all Notification settings are configured properly,* click **Test Notifications**.

25. *If you need to change the Windows account information,* complete the following procedure:

    a. Click the Security tab.

    b. Type the Windows account name that will be used to run the job.

    c. Click **Set Password**.

    d. Type the password for the Windows account in the appropriate password fields.

26. Click **OK**.

Modifying Policy Reporting Settings

Complete the following procedure to modify the Cirrus Configuration Manager Policy Reporting settings.

To adjust policy reporting settings:

1. Click **File > Settings**.

2. Check the tabs you want to display on startup in the **Startup Options** group.

3. *If you want to group reports by the report group,* check **Use Grouping on Report List**.

4. Check the report display options you want to enable in the **Report Options** group.

Chapter 9

Scheduling Jobs

Cirrus Configuration Manager provides configuration management job scheduling to help automate the management of network devices.

You can schedule numerous operations, including configuration file uploads and downloads, node reboots, and command script execution.

Creating a New Job

Complete the following procedure to create a new job. Cirrus Configuration Manager takes advantage of proven Microsoft task scheduling technology and leverages it for the management of scheduled jobs.

To create a new job:

1. Click **Schedule > Create New Job**.

2. Click the type of job you want to create, and then click **Continue**.

3. Type a name for the job, and then click **Continue**.

4. Select the frequency of the job from the **Schedule Job** list.

5. Type or select a time in the **Start Time** field.

6. Type or select a date in the **Starting On** field.

7. Type or select a date in the **Ending On** field.

    Note: To assign a job to run with no end date, leave the **Ending On** field blank.

8. *If you want to run the job daily,* type a number in the **Every days** field to set the daily frequency.

9. *If you want to run the job weekly,* complete the following procedure:

    a. Type a number in the **Every weeks on** field to set the frequency.

    b. Check the days of the week on which you want to run your job.

10. *If you are running your job monthly,* complete the following procedure:

    a. Type a number in the **Every months on** field to set the monthly-frequency.

    b. Check each month in which you want to run your job.

11. Click **Continue**.

12. Type the Windows account name that will be used to run the job.

13. Type the password for the Windows account in the appropriate password fields.

14. Click **Finish**.

15. Type any comments in the **Comments** field.

16. *If the job you are editing does not have a Nodes tab,* skip to step 20.

17. Click the Nodes tab.

18. *If you want to select the nodes on which the job will run,* complete the following procedure:

    a. Click **All Nodes in the Database**.

    b. Click **Select Nodes Directly**.

    c. Click **Add Devices**.

    d. Select the devices you want to add to the list.

    e. Click **OK**.

19. *If you want to run the job on a group of nodes that meet specific criteria,* complete the following procedure:

    a. Click **Select All Nodes in the Database**.

    b. Click **Specify Selection Criteria**.

    c. Click Browse, and then click **Add a Simple Condition**.

    d. Click the first asterisk, and then click the appropriate field.

    e. *If you want to change the comparison operator,* click **is equal to**, and then click the comparison operator you want to use.

    f. Click the second asterisk, and then type the value or select it from the list.

    Note: All values currently in the database for the field are displayed when you browse the list.

20. *If the job you are editing does not have a Download Config tab,* skip to step 27.

21. Click the Download Config tab.

22. Check the configuration types you want to download.

23. *If you want to be notified when the downloaded configuration file is different from the last configuration,* check **Last Config**.

24. ***If you want to be notified when the downloaded configuration file is
    different from the baseline configuration,*** check **Baseline Config**.

25. ***If you want the notification to ignore specific changes,*** complete the
    following procedure:

    a. Click **Edit Comparison Criteria**.

    b. Check the exclusions you want to enable.

    c. ***If you want to create a new exclusion,*** see "Creating New Config
       Change Report Exclusions" on page 27.

    d. Click **Done**.

26. ***If you only want to save the configuration file when changes are found,***
    check **Only save Configs that have changed**.

27. ***If the job you are editing does not have a Command Script tab,*** skip to
    step 31.

28. Click the Command Script tab.

29. ***If you want to type a new script,*** type the command script that is to be
    executed in the text box provided.

30. ***If you want to load an existing command script,*** complete the following
    procedure:

    a. Click **Load Script From File**.

    b. Browse to your command script file, and then click **Open**.

31. ***If the job you are editing does not have a Reports tab,*** skip to step 34.

32. Click the Reports tab.

33. Select the report that is to be executed.

    Note: Only one report can be executed at a time. To execute more than one
    report, a new job will have to be created for each additional report.

34. ***If the job you are editing does not have a Config Archive tab,*** skip to
    step 40.

35. Click the Config Archive tab.

36. Type a path for exporting the configuration files.

37. Set the template for the filename structure.

38. Select the types of configuration file to export.

39. Choose whether to export all configurations, or only the last downloaded for
    each node.

40. ***If the job you are editing does not have a Program tab,*** skip to step 43.

41. Click the Program tab.

42. Click Browse, browse to the application that must be executed, and then click **Open**.

43. *If the job you are editing does not have a Config Change Report tab,* skip to step 48.

44. Click the Config Change Report tab.

45. Select the type of config change report to generate. The choices are as follows:

- Compare most recent Download to the last Baseline Config: This will display all the differences between the most recent baseline configuration, and the last downloaded configuration file.

- Compare the most recent Download to the Configuration on: This will show you all differences between the most recent downloaded configuration file and a configuration file from the specified date.

  Note: If no configuration file was downloaded on the specified date, the next configuration file downloaded after that date will be used.

- Show changes made over the past ## days: Shows you all changes that were made over the specified amount of days.

- Show changes made between: Shows you all changes that were made over the specified date range.

46. *If you want the config change report to ignore specific changes,* complete the following procedure:

a. Click **Edit Comparison Criteria**.

b. Check the exclusions you want to enable.

c. *If you want to create a new exclusion,* see "Creating New Config Change Report Exclusions" on page 27.

d. Click **Done**.

47. *If you want to see detailed changes between each configuration file,* check **Show detailed changes**.

Note: This will show each change from one configuration file to the next. For example, if there were 4 configuration changes made within a specific date range, the report will show the differences in the first configuration file as compared to the second configuration, and then show the differences in the second configuration file as compared to the third, and so on.

48. *If the job you are editing does not have a Policy Report tab,* skip to step 53.

49. Click the Policy Report tab.

50. Select the policy report that is to be executed when the job is run.

51. *If you want to suppress notifications when no violations are found,* check **Send Notification only when Policy Violations are present**.

52. *If you want to launch the Policy Reporting application,* click **Edit Policy Reports**.

53. Click the Notifications tab.

54. *If you want to print the results,* complete the following procedure:

    a. Check **Print Results**.

    b. Select a printer from the **Printer** list on the Printer Settings tab.

55. *If you want to write the results to a file,* complete the following procedure:

    a. Check **Save Results To File**.

    b. Click the File Settings tab.

    c. Type or browse to the file in which you want to write the results in the **Path and Filename** field.

    d. *If you do not want to write the results when no changes are found,* check **Only save results if this job encounters an error during execution**.

56. *If you want to email the results,* complete the following procedure:

    a. Check **E-Mail Results**.

    b. Click the Email Settings tab.

    c. Type the email addresses to which you want to send the results in the **To**, **CC** and **BCC** fields. Use a semicolon to separate multiple email addresses.

    d. Type the subject of the email in the **Subject** field.

57. *If you want to log the job steps to a log file,* check **Log job steps to JOB-#####.log**.

58. *If you want to ensure that all Notification settings are configured properly,* click **Test Notifications**.

59. *If you need to change the Windows account information,* complete the following procedure:

    a. Click the Security tab.

    b. Type the Windows account name that will be used to run the job.

    c. Click **Set Password**.

    d. Type the password for the Windows account in the appropriate password fields.

60. *If you want to change the Windows user account used to run this job,* click the Security tab, type the new user account, and then set the password.

61. Click **OK**.

Viewing Job Logs

If you ever need to verify that a job was run as scheduled, or to view the history of the job, view the job log.

To view a job log:

1. Click **Schedule > Display/Edit Jobs**.

2. Click the job, and then click **Schedule > View Selected Job's Log**.

Viewing and Modifying Scheduled Jobs

Any job created with Cirrus Configuration Manager can be viewed and modified with the Windows Task Scheduler. You can launch the Windows Task Scheduler from the Control panel. For more information, see your Windows documentation.

Chapter 10

Using the Database Manager

The Database Manager can be used to perform queries, view database and table details, export data, and edit database values. The Database Manager can also be used to repair, compact, restore, or back up the database.

Starting Database Manager

To perform any maintenance on your database, the Database Manager must be used. Complete the following procedure to start the Database Manager.

To open Database Manager, click **Start > All Programs > SolarWinds Configuration Management > SQL Database Manager**.

Adding a Server

The following procedure adds a SQL server to the Cirrus Database Manager.

To add a SQL server:

1. Start Database Manager. For more information, see "Starting Database Manager" on page 69.

2. Click **File > Add Server**.

3. Select the SQL server from the list or enter the IP address of the SQL Server machine.

4. Provide the appropriate login type:

    - Windows NT Integrated Security automatically passes Windows account credentials to the SQL server

    - SQL Server user ID and password

5. Click **Connect to Database Server**. The left pane navigation tree populates with your database server information.

Creating Database Backups

It is very important you periodically back up your Cirrus Configuration Manager database. Regular backups enable you to recover your Cirrus Configuration Manager data in case of hardware failure. For more information about scheduling a maintenance plan, see "Creating a Database Maintenance Plan" on page 73.

To create a database backup:

1. Start Database Manager. For more information, see "Starting Database Manager" on page 69.

2. Click the database in the left pane of the Database Manager window, and then click **Database > Backup Database**.

3. Type a description of the database backup and specify a path and filename for the backup file.

    Note: Ensure the target location for the database backup has sufficient available disk space.

Restoring a Database

If you need to restore a database due to corruption, disaster recovery, or some other unexpected occurrence, Cirrus Configuration Manager allows you to do so with the Database Manager. Complete the following procedure to restore a database from a backup.

To restore a database from backup:

1. Start Database Manager. For more information, see "Starting Database Manager" on page 69.

2. Click **Database > Restore Database**.

3. Browse to the location of the appropriate database, or type a valid SQL backup database name and path in the text box. Typically the default is `SolarWinds\Data\ConfigurationManagement.BAK`.

    Note: Databases that are currently in use can not be restored.

4. Click **Verify** to ensure you have specified a valid SQL backup database name.

5. Click **OK** to restore the selected database.

Compacting your Database

Run the database compact procedure to remove whitespace, reindex, and shrink your database. SolarWinds recommends you compact your database as it approaches capacity. If you are using SQL Express, the maximum database size is 4GB.

To compact your database:

1. Start Database Manager. For more information, see "Starting Database Manager" on page 69.

2. Select a database to compact.

3. Click **Database > Compact Database**.

4. *If the before and after sizes are the same value,* compact tables within your database. For more information, see "Compacting Individual Tables" on page 71.

5. You can review the details of the compacting by viewing the log. By default, the log is stored in `\SolarWinds\Cirrus Configuration Manager\NetPerfMon-Compact-`*YYYYMMDD*`.log`.

Compacting Individual Tables

You can use the Database Manager to compact individual tables. You can use this functionality when compacting the database does not shrink the database enough.

To compact a table:

1. Start Database Manager. For more information, see "Starting Database Manager" on page 69.

2. Drill into your database to display the tables.

3. Click the appropriate table in the left pane, and then click **Table > Compact/Rebuild Indexes**.

Viewing Database Details

Details about your database can be viewed in Database Manager. To maintain peak performance, monitor the value in the **Total Space Used** field. SolarWinds recommends you compact your database as it approaches capacity. If you are using SQL Express, the maximum database size is 4GB. For more information, see "Compacting your Database" on page 71.

The **Last Backup** field should also be noted to ensure you are adhering to a regular database maintenance plan. If this field is blank, you do not have a backup of your database. For details on how to schedule a regular database backup, see "Creating a Database Maintenance Plan" on page 73.

To view database details:

1. Start Database Manager. For more information, see "Starting Database Manager" on page 69.

2. Select your database from the Database Manager.

3. Click **Database > Database Details**

4. Review the Properties tab.

Viewing Table Details

Details about a table in a selected database can be viewed in Database Manager. The Properties tab includes general statistics pertaining to table size and creation date. The Columns tab describes table columns, keys, and field types. The Indexes tab provides a list of indexes used within the table.

To view table details:

1. Start Database Manager. For more information, see "Starting Database Manager" on page 69.

2. Select your table from the Database Manager.

3. Click **Table > Table Details**.

4. Click the Properties, Columns, or Indexes tabs to view details about respective aspects of your table.

Creating a Database Maintenance Plan

You can create a database maintenance plan to compact and back up the database on a schedule. To create a database maintenance plan for the Cirrus Configuration Manager database, complete the following procedure.

Note: SQL Server Agent must be running in order to execute your database maintenance plan.

To create a database maintenance plan:

1. Start Database Manager. For more information, see "Starting Database Manager" on page 69.

2. Click the database you want to create a maintenance plan for, and then click **Database > Database Backup Schedule**.

3. Select the frequency with which to run the backup.

4. Set the time for the backup to run, and then click **Next**.

5. Check **Compact and Shrink the database before the backup**.

6. Specify the database backup file and backup report locations.

7. Click **Finish**.

Using MS Enterprise Manager with Cirrus Databases

If you have a licensed copy of SQL Server, you can use Enterprise Manager to maintain your Cirrus Configuration Manager database instead of the SolarWinds Database Manager.

To use Enterprise Manager to set up a maintenance plan for your Cirrus Configuration Manager database:

1. Open Enterprise Manager.

2. Select the SQL Server group in the left pane.

3. Select **Action > New SQL Server Registration**.

4. Click **Next** to begin the SQL Server Register Wizard.

5. Select your Cirrus Configuration Manager Server/Instance Name in the field, and then click **Add**.

6. Choose the appropriate type of authentication to use when connecting to the SQL server.

7. Select the Server Group to which the SQL Server should be added.

8. Click **Finish**.

9. Navigate to your Cirrus Configuration Manager database.

10. Click the database you want to set a maintenance plan for, and then click **All Tasks > Maintenance Plan**.

11. Complete the Maintenance Plan Wizard.

For additional help with using Microsoft Enterprise Manager, visit the Microsoft Support Website at http://support.microsoft.com.

Chapter 11

Example Scenarios

The following sections present example scenarios to help demonstrate how you can use Cirrus Configuration Manager in different network environments.

Customizing the Login Banner of a Device

You can easily change the login banner for a router, switch, or firewall using Cirrus Configuration Manager. This customization can be rolled out to a single or multiple devices. The following procedure references other sections of the guide:

- "Downloading Configuration Files" on page 23

- "Comparing Configurations" on page 24

- "Executing Command Scripts" on page 39

To update a login banner:

1. Back up your running configuration prior to making changes.

2. Click the node or group of nodes you want to update, and then click **Nodes > Download Configs**.

3. Click **Download**.

4. Click the node or group of nodes you want to update, and then click **Nodes > Execute Command Script**.

5. Type the following command script:

   ```
   config t
   no banner login
   banner login ^Unauthorized use of these systems is punishable
   by law^
   exit
   wr mem
   ```

   Where *Unauthorized use of these systems is punishable by law* is the new banner.

6. Click **Execute Command Script**.

7. To verify the script executed successfully using a Telnet session, complete the following procedure:

   a. Select the nodes from the node tree.

   b. Click **Nodes > Tools > Telnet**. A new window with a Telnet session command prompt will open, displaying the new login banner.

8. To verify the script executed successfully by comparing the current configuration to the previous configuration, complete the following procedure:

   a. Select the nodes from the node tree.

   b. Click the node or group of nodes you updated, and then click **Nodes > Download Configs**.

   c. Check **Compare to last Config Downloaded**.

   d. Click **Download**. When the download completes, a comparison window opens. Changes to the login banner are highlighted in yellow if the banner is different from a previous login banner. If no login banner was previously specified, changes are highlighted in red and green.

Configuring Automated Nightly Backups

A powerful feature of Cirrus Configuration Manager is the ability to schedule daily configuration file backups. Cirrus Configuration Manager ships with an example job which downloads the configuration files nightly for all nodes in the database. You can modify the example for your specific needs, or you can create a new job. The following procedure creates a new nightly configuration backup job. For more information on creating jobs, see "Creating a New Job" on page 63.

To setup nightly configuration backups for all nodes:

1. Click **Schedule > Create New Job**.

2. Click **Download Configs from Devices**, and then click **Next**.

3. Type a name for the job, and then click **Continue**.

4. Select **Daily** in the **Schedule Job** list.

5. Type or select a time in **Start Time**.

6. Type or select a date in **Starting On**.

7. Type or select a date in **Ending On**. To assign a job to run with no end date, leave this field blank.

8. Click **Continue**.

9. Type the Windows account name that will be used to run the job.

10. Type the password for the Windows account in the appropriate password fields.

11. Click **Finish**.

12. Type any comments in the **Comments** field.

13. Click the Download Config tab.

14. Check the configuration types you want to download.

15. Check **Last Config** to be notified when the downloaded configuration file is different from the last configuration.

16. Check **Baseline Config** to be notified when the downloaded configuration file is different from the baseline configuration.

17. Click **OK**.

Changing the Community String on Multiple Nodes

The following procedure replaces the `public` read-only community string with a new read-only community string on several network nodes at the same time. The procedure references other sections of the guide:

- "Downloading Configuration Files" on page 23

- "Comparing Configurations" on page 24

- "Executing Command Scripts" on page 39

To update the community string for a group of nodes:

1. Back up the running configuration prior to making any changes.

2. Click the node or group of nodes you want to update, and then click **Nodes > Download Configs**.

3. Click **Download**.

4. Right-click a node or group of nodes, and then click **Execute Command Script**.

5. Type the following command script:

```
config t
no snmp-server community public RO
snmp-server community 123@dm1n RO
exit
wr mem
```

Where *123@dm1n* is the new community string.

6. Click **Execute Command Script**.

7. To verify that the script executed successfully,

   a. Click the node or group of nodes you updated, and then click **Nodes > Download Configs**.

   b. Check **Compare to last Config Downloaded**.

   c. Click **Download**. When the download completes, a comparison window opens. Changes to the community string are highlighted in red and green.

Changing Wireless Settings on All Access Points

The following procedure changes the interface for a wireless access point, and then pushes that same change to additional access points by uploading only the lines in the configuration file that have changed. The procedure references other sections of the guide:

- "Downloading Configuration Files" on page 23
- "Comparing Configurations" on page 24
- "Uploading Selected Lines" on page 29
- "Executing Command Scripts" on page 39

To change wireless settings on all access points:

1. Back up the running configuration prior to making any changes.

2. Click the group of nodes you want to update, and then click **Nodes > Download Configs**.

3. Click **Download**.

4. Click an access point in the node tree, and then click **Nodes > Browse Node**.

5. Use the web user interface of the access point to make changes, and then close the browser tab.

6. Click the access point in the node tree, and then click **Nodes > Download Configs**.

7. Check **Compare to last Config Downloaded**.

8. Click **Download**. When the download completes, a comparison window opens. Changes to the wireless settings are highlighted in yellow if the settings are different from previous. If the settings were not previously specified, changes are highlighted in red and green.

9. Select the lines that changed, and then click **Actions > Upload Selected Lines**.

10. Click **Add Devices**.

11. Select all the access points you want to update, and then click **OK**.

12. Click **Create Upload Script**.

13. Click **Execute Command Script**.

14. *If you want to verify the script executed successfully,* complete the following procedure:

    a. Right-click the node or group of nodes, and then click **Download Configs**.

    b. Check **Compare to last Config Downloaded**.

    c. Click **Download**.

    d. Review the comparison window. Changes to the community string are highlighted in red and green.

Changing an Interface Description

Updating interface descriptions with Cirrus Configuration Manager saves time because you do not have to remember IP addresses or login credentials for the device you are updating. Complete the following procedure to modify an interface description. The procedure references other sections of the guide:

- "" on page 15

- "Downloading Configuration Files" on page 23

- "Comparing Configurations" on page 24

- "Executing Command Scripts" on page 39

To update an interface description on a node:

1. Back up the running configuration prior to making any changes.

2. Click the node that is to be updated, and then click **Nodes > Download Configs**.

3. Click **Download**.

4. Click the node that you want to update, and then click **Nodes > Execute Command Script**.

5. Type the following command script:

```
config t
interface Ethernet0
no description
description Link to Upstairs Lab
exit
exit
wr mem
```

Where *Link to Upstairs Lab* is the new description.

6. Click **Execute Command Script**.

7. Verify the script was executed successfully by complete the following procedure:

  a. Click the node that was updated, and then click **Nodes > Edit Selected Nodes**.

  b. Click the Interfaces tab.

  c. Select **Interface / Port Configuration** in the **Interface Details** list.

  d. Click **Refresh**.

  e. Verify that the new description has been applied to the interface you modified.

Upgrading IOS and Firmware

IOS images can be uploaded using the Cirrus Configuration Manager internal scripting engine. You can transfer these image files using TFTP, FTP, HTTP, or any other transfer protocol.

The following example takes advantage of the SolarWinds TFTP Server, included with Cirrus Configuration Manager, to transfer an IOS image to the router. The TFTP Server must be running and configured to send and receive files. Also, the IOS image file must reside in the TFTP Root Directory.

IOS image management can be very complex. SolarWinds recommends you follow the upgrade guidelines outlined by your hardware manufacturer.

The following procedure references other sections of the guide:

- "Downloading Configuration Files" on page 23
- "Executing Command Scripts" on page 39

To push an IOS image to a network device:

1. Back up the running configuration prior to making any changes.
2. Click the node that is to be updated, and then click **Nodes > Download Configs**.
3. Click **Download**.
4. Click the node that is to be updated, and then click **Nodes > Execute Command Script**.
5. Type the following command script:

    ```
    copy tftp flash

    10.10.2.17

    c2500-i-l.123-9a.bin

    Y
    ```

    Where *10.10.2.17* is the location of the IOS image to copy using TFTP.

6. Click **Execute Command Script**.

Note: This script can be scheduled. For more information, see "Scheduling Jobs" on page 63.

Blocking All Private Addresses with an Access List

Routers connected the Internet are normally configured to discard any traffic using private IP addresses. This isolation gives your private network a basic form of security as it is not usually possible for the outside world to establish a connection directly one of your network devices using these addresses. The following procedure updates the access control list (ACL) to block all private IP addresses on several devices at the same time. The procedure references other sections of the guide:

- "Downloading Configuration Files" on page 23

- "Comparing Configurations" on page 24

- "Executing Command Scripts" on page 39

To update the ACL for a group of nodes:

1. Back up the running configuration prior to making any changes.

2. Click the group of routers that are to be updated, and then click **Nodes > Download Configs**.

3. Click **Download**.

4. Click the group of routers that you want to update, and then click **Nodes > Execute Command Script**.

5. Type the following command script:

    ```
    ${EnterConfigMode}

    access-list 102 deny ip 10.0.0.0 0.255.255.255 any log

    access-list 102 deny ip 172.16.0.0 0.15.255.255 any log

    access-list 102 deny ip 192.168.0.0 0.0.255.255 any log

    exit

    write memory
    ```

    Where *102* is the name of the ACL. *${EnterConfigMode}* is a variable that is equivalent to Config Terminal on Cisco devices.

6. Verify the script executed successfully by completing the following procedure:

    a. Click the router or group of routers you updated, and then click **Nodes > Download Configs**.

    b. Check **Compare to last Config Downloaded**.

    c. Click **Download**. When the download completes, a comparison window opens. Changes are highlighted in red and green.

Blocking a MAC Address on a Wireless Access Point

If you discover a device utilizing unauthorized access through your wireless network, you can block the MAC address to prevent future access. The following procedure uses an access control list (ACL) on a wireless access point to block a specific MAC address. The procedure references other sections of the guide:

- "Downloading Configuration Files" on page 23

- "Comparing Configurations" on page 24

- "Executing Command Scripts" on page 39

To update the ACL for a node:

1. Back up the running configuration prior to making any changes.

2. Click the group of routers that are to be updated, and then click **Nodes > Download Configs**.

3. Click **Download**.

4. Click the group of routers that you want to update, and then click **Nodes > Execute Command Script**.

5. Type the following command script:

    ```
    ${EnterConfigMode}

    access-list 724 deny 000e.0ca1.a2b4 0000.0000.0000

    exit

    wr mem
    ```

    Where *724* is the ACL you are modifying, and where *000E.0CA1.A2B4* is the MAC address to block. `${EnterConfigMode}` is a variable that is equivalent to `Config Terminal` on Cisco devices.

6. Verify the script executed successfully by complete the following procedure:

    a. Click the node or group of nodes, and then click **Download Configs**.

    b. Check **Compare to last Config Downloaded**.

    c. Click **Download**.

    d. When the download completes, a comparison window opens automatically. Changes to the access list are highlighted in red and green.

Appendix A

Variables

Cirrus Configuration Manager uses a variable system that is similar to the one used in Orion Network Performance Monitor. Variables always begin with a dollar sign and a curly brace (`${`), and always end with a curly brace (`}`).

Variables may be used within almost any custom property. They may also be used in any of the user editable system properties.

Variables can also be nested and recursive. That is, a single variable can refer to a Node property that contains more variables that then contain even more variables. The following example demonstrates nested variables.

Node Property	Value of Property
Location	Rack ${Rack} on ${Floor} floor of ${Building} - ${SysLocation}
Building	Building C
SysLocation	Data Center A
Rack	15
Floor	Second

The database value of *Location* is `Rack ${Rack} on ${Floor} floor of ${Building} - ${SysLocation}`. The displayed value of *Location* is `Rack 15 on Second floor of Building C – Data Center A.`

Node Variables

All fields in the nodes table may be used as variables, including any custom properties added to your nodes.

Nodes Table Field	Description
NodeID	Unique ID assigned to each Network Node
NodeCaption	Displayed name for the node. The default for NodeCaption is a variable. ${SysName}
NodeGroup	Group to which this node belongs. Some group examples include Routers, Accounting, or simply ${Building}. The last example refers to a custom property named Building.
AgentIP	The IP address used when communicating with the node. A router or server may have many IP addresses. This IP address is the one used when Cirrus Configuration Manager makes SNMP requests or transfers configuration files.
AgentIPSort	Numeric equivalent of the AgentIP. Used for sorting by IP address in reports.
ReverseDNS	Reverse lookup of the AgentIP
ResponseTime	Current response time of the node in milliseconds
ResponseError	OK if the node is responding. Returns an error message if the node is not responding.
Status	Numeric status of the node. 1 = Up 2 = Down
Community	SNMP community string
SNMPLevel	The version of SNMP supported by the Node. 0 = SNMP not supported 1 = SNMP V1 2 = SNMP V2 3 = SNMP V3
SysName	System name of the node.
SysDescr	System description of the node.
SysContact	System contact information collected from the node.
SysLocation	System location information collected from the node.
SystemOID	System OID discovered from the node.
Vendor	Hardware vendor of this network node.
VendorIcon	Name of the vendor icon used.
MachineType	Type of hardware. This information is discovered by SolarWinds Discovery Engine.
LastBoot	Last time the node rebooted.
OSImage	Operating system running on the node
OSVersion	Version of the operating system running on the node
ConfigTypes	Types of configuration files supported by this node
NodeComments	Any comments about this node entered by the user.

Nodes Table Field	Description
NextDiscovery	Time for next complete discovery of this node
NextPoll	Time for next poll (up/down and response time)
Username	Login username
Password	Login password
EnableLevel	Enable level used when transferring configs or running scripts
EnablePassword	Enable level password
ExecProtocol	The protocol used when executing scripts. This is set to `${GlobalExecProtocol}` by default.
TransferProtocol	The protocol used when downloading configs. This is set to `${GlobalTransferProtocol}` by default.

Configuration Archive Variables

Cirrus Configuration Manager stores all downloaded configurations in a database. It can also store a copy of them in the configuration archive directory. The directory structure can be specified using any of the previous variables.

Additional variables may also be used when specifying the configuration archive directory. Many of these variables use the localization settings for the current language and region.

Property	Description
DateTime	Local date and time in short date and local time format
Date	Date in short date format
LongDate	Date in long date format
MediumDate	Date in medium date format
Time	Time in short time format
LongTime	Time in long time format
MediumTime	Time in "medium time" format
ShortTime	Time in "short time" format
DOW	Day of the week (spelled out)
D	Day of the month
DD	Day of the month (with leading zero, if needed)
ABREVIATEDDOW	Day of the week in abbreviated format
LocalDow	Day of the week in the local language
Month	Number of the current month

Property	Description
M	Number of the current month
MM	Number of the current month (with leading zeros, if needed)
MMM	Abbreviated name of the month
MMMM	Name of the month
LocalMonthName	Name of the month in the local language
DAYOFYEAR	Day number of the year
YYYY	4 digit year
YY	2 digit year
YEAR2	2 digit year
YEAR4	4 digit year
H	Hour
HH	2 digit hour (with leading zero, if needed)
N	Minute
NN	2 digit minute (with leading zero, if needed)
S	Seconds
SS	2 digit seconds (with leading zero, if needed)
AMPM	AM or PM
CRLF	Carriage return - linefeed combination
ConfigType	Type of configuration (running, startup, etc)
Caption	Caption of the node (NodeCaption)

Command Script Variables

Command script variables are used within command scripts, as well as within device command templates. For more information on creating command scripts, see "Working with Command Scripts" on page 39.

Property	Description
ConfigType	Value used to specify the type of configuration
CR	Carriage return
CRLF	Carriage return - linefeed combination
DownloadConfig	Series of commands used to download a configuration from a device
EnableIdentifier	Only used when a device does not return the "#" symbol at the end of a prompt to indicate enable mode. Value that is displayed while in enable mode for a device.
EnterConfigMode	Series of commands used to enter the configuration mode of a device
ExitConfigMode	Series of commands used to exit the configuration mode of a device
IPAddress	The IP address of the server where Cirrus Configuration Manager is installed

Property	Description
Precommand	Specifies the device requires a pre-command. For more information and valid pre-command variables, see "Pre-Command Variables" on page 89.
Reboot	Series of commands used to reboot the device
RebootAt	Series of commands used to reboot a device at a specified time. Use the variables listed in the "Configuration Archive Variables" section of this section to assign the date and time.
RESET	Series of commands used to set the length and pagination of the session
Running	Value used to specify a running configuration type
SaveConfig	Series of commands used to write the configuration to the devices memory
Startup	Value used to specify a startup configuration type
Version	Series of commands used to display the software version of the device

Pre-Command Variables

Pre-Command variables are used within command scripts as well as within device command templates. The Pre-Command variables mimic keyboard strokes that are normally entered in the command interface. For more information on creating command scripts, see "Working with Command Scripts" on page 39.

Property	Description
${CTRL+@}	CTRL + @
${CTRL+A}	CTRL + A
${CTRL+B}	CTRL + B
${CTRL+C}	CTRL + C
${CTRL+D}	CTRL + D
${CTRL+E}	CTRL + E
${CTRL+F}	CTRL + F
${CTRL+G}	CTRL + G
${CTRL+H}	CTRL + H
${CTRL+I}	CTRL + I
${CTRL+J}	CTRL + J
${CTRL+K}	CTRL + K
${CTRL+L}	CTRL + L
${CTRL+M}	CTRL + M
${CTRL+N}	CTRL + N

Property	Description
${CTRL+O}	CTRL + O
${CTRL+P}	CTRL + P
${CTRL+Q}	CTRL + Q
${CTRL+R}	CTRL + R
${CTRL+S}	CTRL + S
${CTRL+T}	CTRL + T
${CTRL+U}	CTRL + U
${CTRL+V}	CTRL + V
${CTRL+W}	CTRL + W
${CTRL+X}	CTRL + X
${CTRL+Y}	CTRL + Y
${CTRL+Z}	CTRL + Z
${CTRL+[}	CTRL + [
${CTRL+\}	CTRL + \
${CTRL+]}	CTRL +]
${CTRL+CTRL}	CTRL + CTRL
${CTRL+_}	CTRL + _
${UPARROW}	Up Arrow
${DOWNARROW}	Down Arrow
${RIGHTARROW}	Right Arrow
${LEFTARROW}	Left Arrow
${StorageFilename}	Unique name of configuration file (generated by Cirrus)
${StorageAddress}	TFTP server IP address

Example Pre-Command Device Template Entry

The following line from a device command template specifies the pre-command, the delay, and the text that triggers the pre-command. Delay and trigger text (RegEx) are optional variables.

```
<Command Name="Precommand" Value="${CTRL+Y}" Delay="3"
RegEx="password:"/>
```

Note: Device command templates are located in the DeviceTypes folder of your installation folder. By default, you can find this folder in the following location:
\Program Files\SolarWinds\Configuration Management\DeviceTypes\.

Regular Expression Pattern Matching

When editing comparison criteria, the following regular expressions can be used for pattern matching. Examples are provided at the end of this section.

Characters

Character	Description	Example
Any character except [,\,^,$,.,|,?,*,+,(,),	All characters except the listed special characters match a single instance of themselves.	a matches a
\ (backslash) followed by any of [,\,^,$,.,|,?,*,+,(,),	A backslash escapes special characters to suppress their special meaning.	\+ matches +
\xFF where FF are 2 hexadecimal digits	Matches the character with the specified ASCII/ANSI value, which depends on the code page used. Can be used in character classes.	\xA9 matches © when using the Latin-1 code page.
\n, \r and \t	Match an LF character, CR character and a tab character respectively. Can be used in character classes.	\r\n matches a DOS/Windows CRLF line break.

Character Classes or Character Sets [abc]

Character	Description	Example
[(opening square bracket)	Starts a character class. A character class matches a single character out of all of the possibilities offered by the character class. Inside a character class, different rules apply. The rules in this section are only valid inside character classes. The rules outside this section are not valid in character classes, except \n, \r, \t and \xFF	
Any character except ^,-,],\ add that character to the possible matches for the character class.	All characters except the listed special characters.	[abc] matches a, b or c
\ (backslash) followed by any of ^,-,],\	A backslash escapes special characters to suppress their special meaning.	[\^\]] matches ^ or]
- (hyphen) except immediately after the opening [	Specifies a range of characters. (Specifies a hyphen if placed immediately after the opening [)	[a-zA-Z0-9] matches any letter or digit

Character	Description	Example
^ (caret) immediately after the opening [	Negates the character class, causing it to match a single character not listed in the character class. (Specifies a caret if placed anywhere except after the opening [)	[^a-d] matches x (any character except a, b, c or d)
\d, \w and \s	Shorthand character classes matching digits 0-9, word characters (letters and digits) and whitespace respectively. Can be used inside and outside character classes	[\d\s] matches a character that is a digit or whitespace

Dot

Character	Description	Example
. (dot)	Matches any single character except line break characters \r and \n.	. matches x or most any other character

Anchors

Character	Description	Example
^ (caret)	Matches at the start of the string to which the regular expression pattern is applied. Matches a position rather than a character. Most regular expression flavors have an option to make the caret match after line breaks (i.e. at the start of a line in a file) as well.	^. matches a in abc\ndef. Also matches d in "multi-line" mode.
$ (dollar)	Matches at the end of the string to which the regular expression pattern is applied. Matches a position rather than a character. Most regular expression flavors have an option to make the dollar match before line breaks (i.e. at the end of a line in a file) as well. Also matches before the very last line break if the string ends with a line break.	.$ matches f in abc\ndef. Also matches c in "multi-line" mode.
\A	Matches at the start of the string to which the regular expression pattern is applied to. Matches a position rather than a character. Never matches after line breaks.	\A. matches a in abc
\Z	Matches at the end of the string to which the regular expression pattern is applied. Matches a position rather than a character. Never matches before line breaks, except for the very last line break if the string ends with a line break.	.\Z matches f in abc\ndef
\z	Matches at the end of the string to which the regular expression pattern is applied. Matches a position rather than a character. Never matches before line breaks.	.\z matches f in abc\ndef

Word Boundaries

Character	Description	Example
\b	Matches at the position between a word character (anything matched by \w) and a non-word character (anything matched by [^\w] or \W) as well as at the start and/or end of the string if the first and/or last characters in the string are word characters.	.\b matches c in abc
\B	Matches at the position between two word characters (i.e the position between \w\w) as well as at the position between two non-word characters (i.e. \W\W).	\B.\B matches b in abc

Alternation

Character	Description	Example
| (vertical bar or "pipe")	Causes the regular expression engine to match either the part on the left side or the part on the right side. Can be strung together into a series of options.	abc|def|xyz matches abc, def or xyz
| (vertical bar or "pipe")	The vertical bar has the lowest precedence of all operators. Use grouping to alternate only part of the regular expression.	abc(def|xyz) matches abcdef or abcxyz

Quantifiers

Character	Description	Example
? (question mark)	Makes the preceding item optional. The optional item is included in the match, if possible.	abc? matches ab or abc
??	Makes the preceding item optional. The optional item is excluded in the match, if possible. This construct is often excluded from documentation because of its limited use.	abc?? matches ab or abc
* (star)	Repeats the previous item zero or more times. As many items as possible will be matched before trying permutations with fewer matches of the preceding item, up to the point where the preceding item is not matched at all.	.* matches "def" "ghi" in abc "def" "ghi" jkl

Character	Description	Example
*? (lazy star)	Repeats the previous item zero or more times. The engine first attempts to skip the previous item before trying permutations with ever increasing matches of the preceding item.	.*? matches "def" in abc "def" "ghi" jkl
#NAME?	Repeats the previous item once or more. As many items as possible will be matched before trying permutations with fewer matches of the preceding item, up to the point where the preceding item is matched only once.	.+ matches "def" "ghi" in abc "def" "ghi" jkl
+? (lazy plus)	Repeats the previous item once or more. The engine first matches the previous item only once, before trying permutations with ever increasing matches of the preceding item.	.+? matches "def" in abc "def" "ghi" jkl
{*n*} where *n* is an integer >= 1	Repeats the previous item exactly *n* times.	a{3} matches aaa
{*n,m*} where *n* >= 1 and *m* >= *n*	Repeats the previous item between *n* and *m* times. Will try to repeat *m* times before reducing the repetition to *n* times.	a{2,4} matches aa, aaa or aaaa
{*n,m*}? where *n* >= 1 and *m* >= *n*	Repeats the previous item between *n* and *m* times. Will try to repeat *n* times before increasing the repetition to *m* times.	a{2,4}? matches aaaa, aaa or aa
{*n,*} where *n* >= 1	Repeats the previous item at least *n* times. Will try to match as many items as possible before trying permutations with fewer matches of the preceding item, up to the point where the preceding item is matched only *m* times.	a{2,} matches aaaaa in aaaaa
{*n,*}? where *n* >= 1	Repeats the previous item between *n* and *m* times. The engine first matches the previous item *n* times before trying permutations with ever increasing matches of the preceding item.	a{2,}? matches aa in aaaaa

Regular Expression Pattern Matching Examples

The following examples illustrate some of the uses of Regular Expression pattern matching.

```
snmp-server community public
```

> Finds any line that includes the text `snmp-server community public`. There can be text before and/or after the string on the same line.

```
service tcp-keepalives-in.*\n(.*\n)*.*service tcp-keepalives-out
```

> Finds the first line `service tcp-keepalives-in` and then looks for `service tcp-keepalives-out` on any line after that. The regular expression string `.*\n(.*\n)*.*` is used to search any number of lines between strings.

```
access-list 105 deny.*tcp any any eq 139 log
```

> Finds the line with `access-list 105 deny`, followed by any number of characters of any type, followed by `tcp any any eq 139 log` on the same line. The regular expression string `.*` finds any character, and any number of characters on the same line. So, this could be used to find spaces, tabs, numbers, letters, or special characters.

```
ntp clock-period \d*
```

> Finds any line that includes `ntp clock-period` followed by any number. The regular expression string `\d*` will find any number at any length, such as `3`, `48`, or `2394887`.

```
user \x2a
```

> Finds any line that includes `user *`. The regular expression string `\x` followed by a hexadecimal value specifies an individual character. In this example, `\x2a` represents the asterisk character, which has a hexadecimal value of `2a`.

Index

Index