SolarWinds Cirrus Configuration Manager

QuickStart Guide

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SolarWinds Cirrus Configuration Manager 12.04.2007 version 4.0

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.

Contents

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

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.

Benefits of Cirrus Configuration Manager

Consider some of the following benefits of Cirrus Configuration Manager.

Out-of-the-box productivity

Within minutes of installing Cirrus you will be able to backup your device configurations and collect detailed inventories. Cirrus includes several wizards, such as setting up a new database or scheduling a job (to get you started right away).

Easy to understand and use

Cirrus Configuration Manager Configuration Manager is the most intuitive configuration management product available. Cirrus Configuration Manager is designed for daily use by staff with other responsibilities. The Cirrus Configuration Manager interface provides what you need where you expect to find it and offers advanced capabilities with minimal configuration overhead.

Affordable value

While Cirrus Configuration Manager provides comparable functionality, cost and maintenance of your Cirrus Configuration Manager installation is less than the initial cost of most other solutions.

Scalable

Cirrus Configuration Manager is friendly enough for even the smallest networks but powerful enough to manage the largest, most complex multi-vendor networks.

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

   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 7.

Software License Key

If you are prompted for your name, e-mail 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 `Instance\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 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 9.

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 11.

Configuring User Access Control

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**.

Configuring Event Logging

Logging events associated with a specific function of Cirrus Configuration Manager enables you to keep a detailed record of events and enables you to troubleshoot any anomalies that 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**.

Chapter 3

Getting Started

A significant amount of time spent managing your network devices can be cut using Cirrus Configuration Manager. The following section steps you through four common use cases. By stepping through this quick introduction, you learn how to add network devices, how to configure nightly backups, how to block private addresses on several devices, and how to update devices with a new community string.

1. Adding network devices
2. Configuring automated nightly backups
3. Changing the community strings on multiple nodes
4. Blocking a MAC address on a wireless access point

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 level 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. ***If you want to confirm the community string is valid,*** 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. Type the user name and password used to access the node, and then 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 the values just as they would be typed when manually logging into the device. For example, if 15 represents enable level 15, then simply type `15` for the value.

9. 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, Cirrus will first attempt to negotiate an SSH2 connection, if SSH2 is not supported, it will then default to SSH1.

10. 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, it will then default to SSH1. SNMP is only supported on Cisco devices.

11. 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, it will then default to SSH1.

12. ***If you want to verify that the login information is accurate,*** click **Verify Login Information**.

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

14. ***If the device uses an intermediary device such as TACACS or Radius,*** select `Yes` in the **Allow** field under the Intermediary Device Support category.

15. 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**.

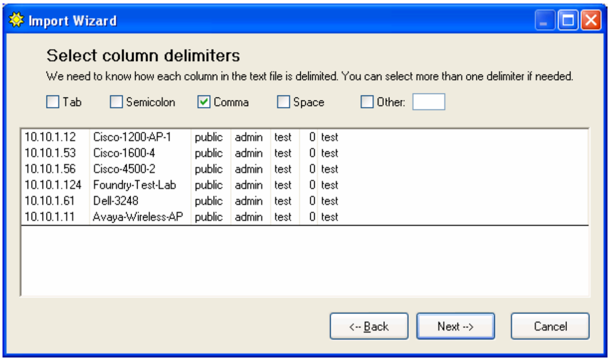
Importing Nodes

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.



Select column delimiters

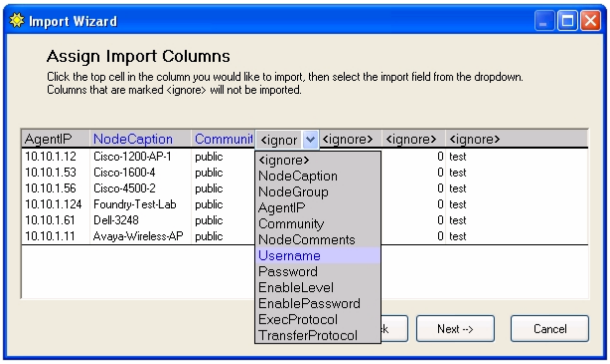
We need to know how each column in the text file is delimited. You can select more than one delimiter if needed.

□ Tab □ Semicolon ☑ Comma □ Space □ Other:

10.10.1.12	Cisco-1200-AP-1	public	admin	test	0	test
10.10.1.53	Cisco-1600-4	public	admin	test	0	test
10.10.1.56	Cisco-4500-2	public	admin	test	0	test
10.10.1.124	Foundry-Test-Lab	public	admin	test	0	test
10.10.1.61	Dell-3248	public	admin	test	0	test
10.10.1.11	Avaya-Wireless-AP	public	admin	test	0	test

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.



Assign Import Columns

Click the top cell in the column you would like to import, then select the import field from the dropdown.
Columns that are marked <ignore> will not be imported.

AgentIP	NodeCaption	Communit	<ignor	<ignore>	<ignore>	<ignore>
10.10.1.12	Cisco-1200-AP-1	public			0	test
10.10.1.53	Cisco-1600-4	public			0	test
10.10.1.56	Cisco-4500-2	public			0	test
10.10.1.124	Foundry-Test-Lab	public			0	test
10.10.1.61	Dell-3248	public			0	test
10.10.1.11	Avaya-Wireless-AP	public			0	test

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.

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.

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 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. 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.

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.

Blocking a MAC Address on a Wireless Access Point

If you discover a device utilizing unauthorized access to 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.

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.