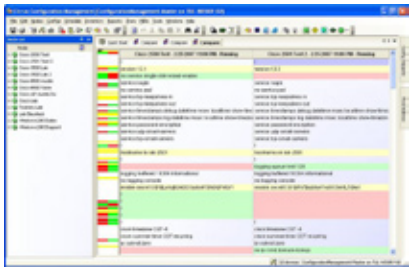
SOLARWINDS

Cirrus Configuration Manager

Affordable, easy-to-use network configuration and change management for multi-vendor network infrastructures



Unless your remote is broken, we're guessing you don't leave the couch to change the channels on your television. So, why would you Telnet into each and every network device to make network configuration changes if you can do it automatically from a central location? Meet Cirrus.

Cirrus is an affordable, easy-to-use network configuration and change management solution that automates device configuration management across multi-vendor network infrastructures. Cirrus delivers a unique combination of scalability and robust functionality, such as:

- Automating network configuration changes – a process that our customers report is 10 to 50 times faster than manually updating devices
- Managing and controlling device configurations from a central console
- Detecting and alerting on network configuration problems in real time
- Rolling back configuration changes on demand
- Supporting 25 or 25,000 devices in a multi-vendor network environment

Cirrus Features

Scheduled Configuration Backups

One of the most popular features in Cirrus is the ability to automatically backup network device configurations. Configuration backups can be scheduled to run whenever you would like them to – whether that's everyday, every other Monday, or every two hours.

In fact, Cirrus includes a default configuration backup job that can be run out-of-the-box. With just a few mouse clicks, you can easily modify the job to customize it for your particular backup needs. Cirrus also makes it easy to create your own job from scratch. Each job performs backups of network device configurations based on naming convention, machine type or other custom groups.

"We are extremely pleased with Cirrus' ability to backup our 100-plus Cisco devices, which include a wide variety of PIX firewalls, switches and routers in just 60 seconds!"

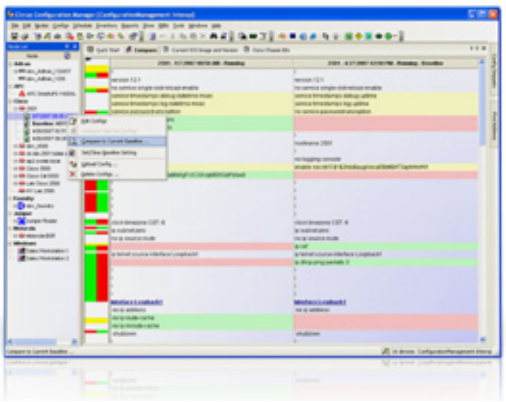
- Gary Hills, Senior Network Engineer, Belzberg Technologies, Inc.

Configuration Change History

Cirrus detects changes that occur to the configurations of monitored devices in real time and notifies you instantly of these changes – giving you more control, instant visibility, and improved security in your network environment. Additionally, this feature enables you to quickly isolate and eliminate a configuration change as the cause of a network problem.

Side-by-Side Configuration Change Comparisons

Cirrus enables you to quickly and easily compare network configuration files between two routers or switches or to compare the running configuration file to the startup configuration file on a single device. Cirrus makes it simple to baseline network configurations and to compare newer versions to the baseline as they are distributed.



Transfer IOS Images

Cirrus enables IOS/firmware updates to be performed in real-time or to be scheduled to run during a future time frame. With the enhanced grouping capability of Cirrus, images can be uploaded to devices based on a specific grouping or combination of grouping properties, allowing you to easily manage each type of network device separately.

Configuration Rollback

Cirrus includes roll-back functionality, enabling you to immediately "rollback" to a previous "known good" device configuration. This enables you to quickly repair unauthorized network configuration changes or recover devices from failed configuration changes, eliminating unnecessary downtime and security risks.

Multi-vendor Device Support

Cirrus provides built-in configuration management support for network devices from more than 16 different hardware vendors, including Cisco Systems, Nortel Networks, Motorola, Extreme Networks, Dell, HP, Adtran, Aruba Networks, ARRIS, Marconi, Foundry Networks, Fortinet, Enterasys Cabletron, Citrix Systems, Radware, and Juniper Networks. Additionally, users can easily modify or build device templates, enabling Cirrus to scale to highly heterogeneous environments.

Configuration Policy Management

Cirrus' network configuration policy management feature enables you to ensure that device configurations comply with federal regulations, as well as your organization's internal standards. The Cirrus Policy Reporting Manager helps organizations automate the policy compliance process with scheduled reports that identify devices that have configuration violations, that could be accessed by unauthorized users, and that pose a security risk. Several out-of-the-box policy reports were designed specifically for the standards and regulations set forth in HIPAA, SOX, CISP, and Cisco® Security Audit.

With Cirrus' streamlined device remediation feature, you can even automatically remediate any policy violations right from your reports. By simply right-clicking on a policy violation within the report interface, it's easy to immediately apply a remediation script to repair any devices that were found to be in violation with policies. In doing so, Cirrus streamlines the configuration policy verification and remediation process for HIPAA, PCI, and other regulations.

Model	Manages up to:
DL50	50 nodes
DL100	100 nodes
DL250	250 nodes
DL500	500 nodes
DL1000	1000 nodes
DL3000	3000 nodes
DLX	unlimited nodes

Device Inventory

Cirrus is not only a comprehensive configuration management solution, but is also a device management solution. Cirrus creates a detailed network inventory of all managed devices. Serial numbers, interface and port details, IP addresses, ARP tables, installed Windows software and many other details are included in Cirrus's configuration management database.

Configuration Reporting

Cirrus delivers easy-to-read reports on all network configuration data, which can be run in real time or on an automated basis – a key feature in any effective network configuration management solution. Cirrus ships with pre-defined reports for change management, inventory, and policy management. These reports enable you to accomplish a variety of tasks from quickly viewing all configuration changes across your network over the last 30 days to providing the COO with proof that network device configurations are compliant with federal regulations.

User Roles & Permissions – New in v4!

Cirrus enables multiple user accounts to be created with different privileges. This ability offers an additional layer of security by ensuring that particular activities are performed only by the individuals who have appropriate permissions. Additionally, Cirrus can now leverage your existing Active Directory® infrastructure for user account authentication and password management.

Cirrus also enables you to assign device login credentials to users – a feature that is normally reserved for those expensive NCCM solutions that will add at least one extra zero to your bill. This feature allows you to better track who made configuration changes to ensure policy adherence and to aid in troubleshooting network issues.

User Activity Tracking – New in v4!

With Cirrus, you can view who made configuration changes, who backed up configurations, and when users logged in and out of Cirrus. This user activity tracking ability ensures compliance with federal regulations, such as HIPAA and PCI, while also enabling you to provide necessary documentation for external and internal audits. Additionally, activity tracking makes it quick and easy to determine who made what changes when diagnosing a network problem.

Support for SNMP v3 – New in v4!

Cirrus fully supports SNMP v3, enabling you to collect node and inventory information using this secure communications protocol. You can also upload and download configurations from Cisco® devices using SNMP v3. While SNMP v3 support is typically reserved for high-end NCCM solutions, Cirrus brings this important security feature to the mid-market.

System Requirements

Pentium III - 800 MHz, 256 MB RAM, 1 GB Hard Drive Space Available, Windows XP Professional, 2000/2003 Server. Database Support – Microsoft SQL Server 2000, 2005 and 2005 Express. Included with Cirrus – Microsoft SQL Server 2005 Express

Integration with Other SolarWinds Products & Resources

Cirrus offers tight integration with Orion, Engineer's Toolset, and Thwack. Network devices discovered within the Orion Network Discovery Tool can be imported into the Cirrus database, while Cirrus configurations and reports are viewable within the Orion web console. Toolset applications can be directly accessed from Cirrus and now, with version 4.0, users can also access the Thwack community from the Cirrus interface.

SOLARWINDS

For additional information, please contact SolarWinds at 866.530.8100 or e-mail sales@solarwinds.com. To locate an international reseller near you, visit www.solarwinds.com/distributor/locator.html