ENIRA technologies

respond.
command.
control.

Product Overview

ENIRA INSP: Network Configuration Management

ENIRA Quick Facts:

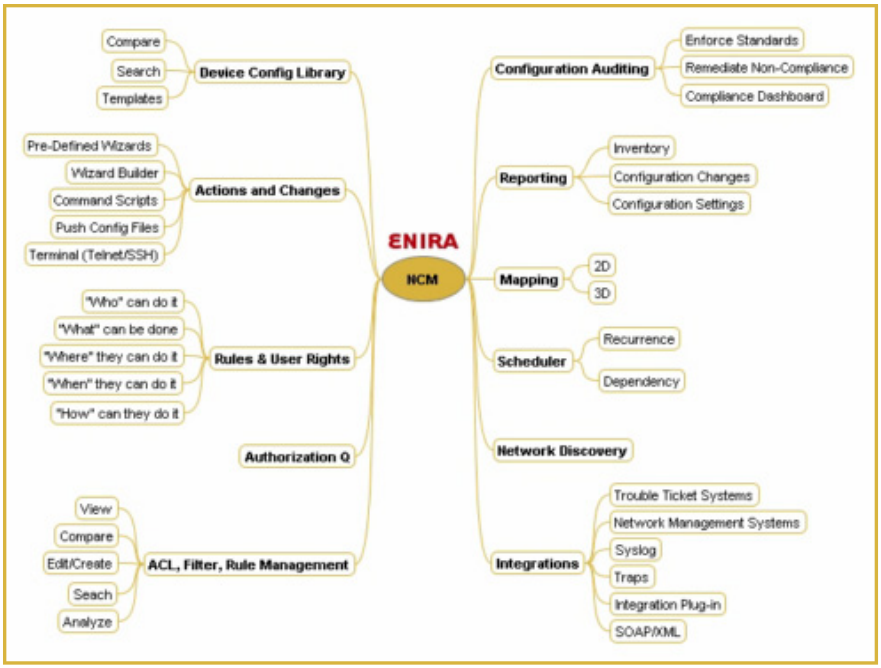
- *Command and Control over your network configuration*
- *Quickly deploy configuration changes*
- *Schedule one-time or reoccurring changes*
- *Multi-vendor support*
- *Workflow process and Access Control for large scale Enterprise and Institutions*
- *Highly Secure*
- *Works in conjunction with Automated Policy Management and Network Response Management*

Enabling network engineers to get back to network engineering through safe, intelligent automation

ENIRA's Network Configuration Management (NCM) module automates network configuration changes, manages and audits the change process, and provides sanitized information to those that need it.

NCM's easy to use wizards, granular user rights, and business rules allow you to better leverage and utilize Tier 1 & 2 helpdesk and support staff. This enables common administration tasks and troubleshooting steps to be offloaded from higher-tier network engineers.

ENIRA NCM interacts with your network devices like a network engineer would, using any combination of telnet, SSH, TACACS/Radius accounts, or local accounts. NCM does not use SNMP. This architecture ensures, that you do not have to make any changes to your infrastructure when deploying ENIRA. ENIRA NCM is a completely self-contained appliance and does not require any additional servers or external databases. It uses an easy to understand web-based user interface and does not use any consoles, applets, or thick clients.



Rules and User Rights

Flexible rules and granular user rights enable easy and powerful control of:

- who can work with devices
- what they can do to those devices
- when they can do it
- how they are able to interact with the devices

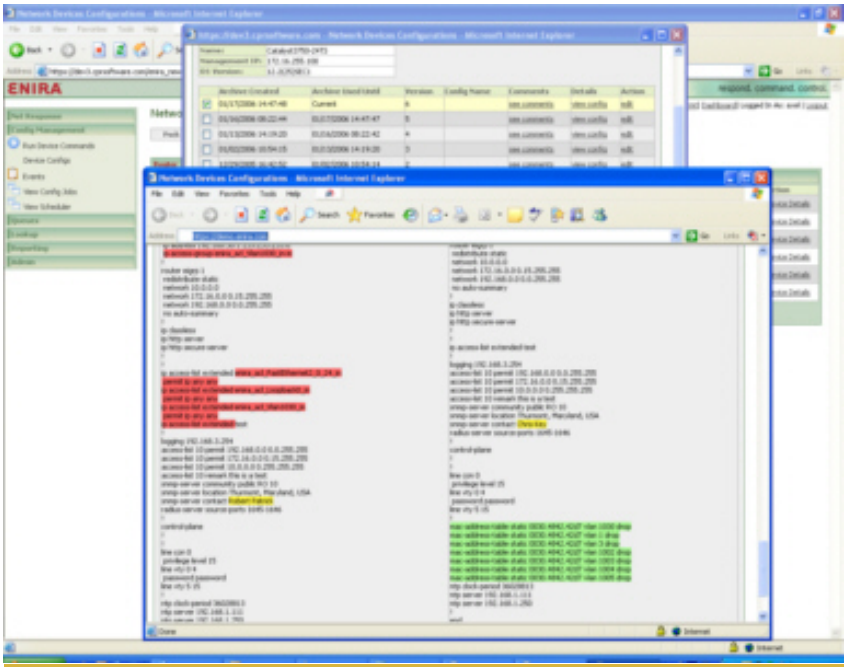
"Require Authorization" and "Deny" rules help to build and enforce an auditable change management process. User rights also control the type of configuration information a user is allowed to see and how they can access it. Filters can be applied to restrict access to sensitive information.

Actions and Changes

NCM provides several different ways of interacting with network devices to collect information or make changes. Pre-defined wizards provide a normalized process of changing standard settings including:

- switch port speed/duplex
- SNMP settings
- local user passwords
- DNS
- SysLog settings

A Wizard Builder allows you to quickly define simple forms. This enables your lower level support staff to implement changes or run commands without needing direct access to network devices or knowledge of command syntax. Command scripts and configuration file templates can also be used to automate changes across multiple devices at once. For engineers that want to work directly with the network device's CLI, there is a web-based Telnet or SSH feature that will automatically capture the user's session for auditing and reporting without requiring the engineer to take additional steps to document the actions taken.



View Configuration Changes

Device Configuration Library

NCM automatically builds and maintains a library of configurations for each device, creating new configuration records as it detects changes to network devices. NCM can display any previously running device configuration and provides easy "rollback" capabilities. Configurations can be compared to visualize changes in different revisions or across devices, using colors to highlight lines that have been **added**, **removed**, or **modified**. Searches can be performed to identify configurations that do or do not contain certain statements or groups of statements. Templates, skeleton configurations, and definitions containing configuration standards can be created, stored, administered, and distributed.

Authorization Queue

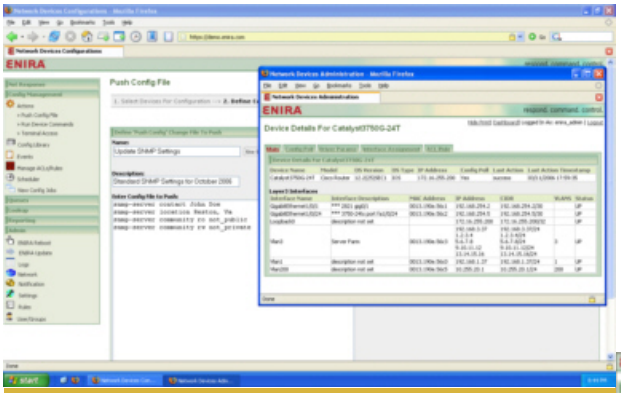
Changes and user actions might require approval by Authorization Groups before being implemented. ENIRA users with Authorization rights are able to approve or deny actions after review. This result automatically becomes part of the audit trail. The Authorization Queue ties into Rules and User Rights enabling lower level technical support staff to be productive within their action rights. They might be enabled to perform changes and device interaction with required approval, which can be based on the impacted devices or the type of change to be performed

ACL, Filer, Rule Management

NCM enables you to centrally view, compare, and search access-control lists, filters, and firewall rules, as well as, review changes before implementing them. Predefined processes implement changes safely and consistently - without fear of locking yourself out of the device or accidentally taking down part of the network.

Configuration Auditing

ENIRA enforces configuration standards, pushes correct configurations in response to audit failures, and regularly reports the status of scheduled configuration audits. A compliance dashboard provides a quick status of how the current network device configurations comply with your organization's standards. Many best practice audits are pre-defined and available by default.



Configuration Details

Reporting

ENIRA NCM provides quick and easy web-based reports for network device inventory information and configuration settings. Audit and Change reports summarize network configuration changes by device, device groups, user, or user groups.

Scheduler

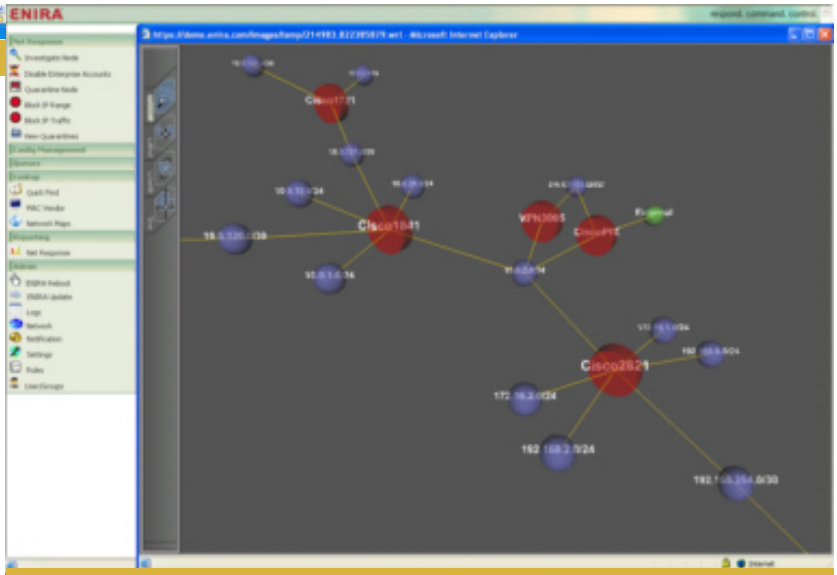
Configuration Changes can be scheduled to occur during maintenance hours. Recurring changes like changing SNMP community strings and local user passwords can be scheduled ahead of time to occur when desired. Bigger projects can be scheduled as combination of multiple actions that depend on each other.

Network Discovery

ENIRA NCM supports automatic network device discovery or can leverage data from your existing network management applications already performing device discovery. NCM is designed to fit into your existing management architecture and leverage components you have already deployed, rather than requiring to perform each function itself.

Topology Maps Built from the Device Configurations

ENIRA's comprehensive 2D & 3D network topology map accurately shows you the topology of your network. These maps are automatically updated as NCM detects changes to your network configuration.



3D Topology Map

Integrations

ENIRA provides customizable notification messages that can be sent as emails, SysLog messages to other applications, or generate trouble tickets.

For quick and easy integrations with any type of security or network management system ENIRA provides the Integration Plug-in. This easy to use command line executable is parameter driven for a high degree of flexibility. In addition ENIRA provides a SOAP/XML interface that can be used for tight integration with your own developed applications.

Centrally monitor and control your network configuration across a large and multi-vendor network with the intelligence of ENIRA.

About ENIRA Technologies:

Founded in 2002, **ENIRA Technologies**' mission is to eliminate the challenges that many Network Organizations face, from managing day-to- day operations to reacting to mission critical events in your network.

ENIRA Technologies was founded by network engineers who were driven to break through the barriers of lengthy manual and error prone processes. They invented and implemented "Expert Technology" to fully automate these processes and interactions within the network.

ENIRA has eliminated the manual and frustrating process that customers had to accept in the past. ENIRA's multi-vendor, multi-technology foundation focuses on improving the effectiveness and efficiency of enterprise network security and operations, giving its customers confidence in their ability to respond and stay in command and control.

Available ENIRA Literature:

- ENIRA Intelligent Network Services Platform Overview
- ENIRA NRM - Datasheet
- ENIRA NCM - Datasheet
- ENIRA NPM - Datasheet
- ENIRA Distributed - Datasheet
- White Paper
- FAQ
- Customer Case Studies

ENIRA: Technical Specifications

Change Management

- Automatically track and record configuration changes
- View configuration changes
  - Contextual display
  - Show only changes
  - Diff view –highlighting lines with changes (Deletion, Addition, Modification)
  - Compare configurations side-by-side
- Version Control System for Configuration Library
  - Delivers check in/out capabilities and the ability to generate templates
  - Configuration recovery, rollback
- Configuration Search
- Configuration Audit
- Automatic Notification and Reports sent on configuration changes
- Synchronize device configurations
- Auto-sync option (after approved changes)

Configuration Execution

- Wizards
  - Local user/password
  - Syslog configurations
  - SNMP options
  - Tacacs/Radius/etc
  - Telnet/SSH
  - Management ACLs
- Run Command Change
- Push Configuration File Change
  - Immediate
  - Scheduled (time-of day)
  - Recurring
- Port On/Off, speed and duplex
  - Color coded switch representation (red=off, green=highest speed/full duplex, yellow=half duplex)
  - Find ports
  - Flag configuration exceptions
  - Lock down ports, and prevent them from being changed
- View counters
- Write scripts and execute
- Record scripts
- Automated syntax test and verification
- Hardware & Software Inventory
  - detailed information at the line-card, port and interface level
  - report on OS release info (full, maintenance, special designations)
- File system support
  - checking space
  - pushing to
  - syncing
  - deleting from

Server, storage features

- Syslog server
- Tftp server
- SSH server
- Real-time change detection via traps and "proxy" interface
- Proxy interface for Telnet and SSH access
- Odbc/jdbc and xml file connectivity
- Software image library
- Scalability and data redundancy; easy to use backup and restore

Other features

- Control and push OS updates
- Device auto-discovery
- Search, audit, and report on tasks, sessions, events
- Create, manage equipment groups
- Reporting best practice/compliance
- User credential management (groups)
- Ability to integration network config information stored with external systems
- Configure maintenance windows (exclude device polling during certain times of day)
- Report output - html, pdf, text, csv, xml
- Predefined and custom report template
- Job control authentication queue, scheduling, delete jobs through GUI

ENIRA Technologies, 11921 Freedom Drive, Two Fountain Square, Suite 550, Reston, VA 20190
www.enira.com (888) 277-7638 sales@enira.com