cradlepoint

PCI Compliance

CradlePoint Enablers for PCI Compliant Systems

White Paper

January 8, 2014

Preface

Right of Revision

CradlePoint reserves the right to revise this publication and to make changes in the content thereof without obligation to notify any person or organization of any revisions or changes.

Revision Tracking

Revision	Date	Description	Author
1.0	Sept. 8, 2011	Initial Release	Ken Hosac
2.0	Sept. 13, 2013	Updates for ECM, firmware changes	Alecia Hoobing
3.0	Jan. 8, 2014	Updated per the PCI DSS 3.0 requirements.	Alecia Hoobing

Intellectual Property

Table of Contents

805 West Franklin Street | Boise, Idaho 83702 | **p** 1-208.424.5054 | **f** 1-208.429.6852

1. Overview

Business Driver

Point-of-Sale (POS) businesses are paranoid, with good reason, about protecting sensitive customer and company information. Financial institutions require that any company that stores, processes, or transmits credit card information comply with the PCI DSS (Payment Card Industry Data Security Standards).

Companies that fail to comply are subject to fines, lawsuits, and can even be banned from processing credit cards. Worse, companies that are breached can find themselves in the news headlines, significantly impacting goodwill with customers, partners, and shareholders.

Summary

When properly configured, monitored, and maintained, CradlePoint devices meet the requirements of PCI DSS 3.0. Enabling features include network segmentation (ethernet ports, SSIDs, and VLANs), stateful firewall, MAC/IP/URL filtering, authentication/encryption, event logging, event alerts, time synchronization, and configuration/upgrade management from CradlePoint Enterprise Cloud Manager. Required for PCI compliance, CradlePoint Enterprise Cloud Manager runs in real time.

CradlePoint specializes in network connectivity solutions for the Retail POS market. Our products are deployed broadly in several Retail POS segments that process credit card transactions, including:

- Retail Stores
- Restaurants & Bars
- Convenience Stores
- Coffee Shops
- Kiosks
- ATMs
- Service Locations
- Entertainment & Recreational Venues
- Special Events
- Temporary Vending Locations

Objective of this Document

The objective of this White Paper is to help our customers better understand how to create and maintain a PCI Compliant network using CradlePoint devices for network connectivity.

805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852

2. PCI Security Standards

Overview

The objective of the PCI Security Standards is to protect cardholder data. The standards are developed and published by the PCI Security Standards Council (SSC), which consists of hundreds of industry participants who have a vested interested in reducing vulnerabilities in the card-processing ecosystem.

The PCI SSC was founded by the following five global payment brands:

- American Express
- Discovery Financial Services
- JCB International
- MasterCard Worldwide
- Visa, Inc.

Scope

The PCI SSC publishes the following standards:

PCI Data Security Standards (DSS): Applies to any entity that stores, processes, and/or transmits cardholder data. The standard covers technical and operational components included in or connected to cardholder data. If a business accepts or processes payment cards, it must comply with the PCI DSS.

PIN Transaction Security Requirements (PTS): Applies to manufacturers who develop PIN (personal identification number) entry terminals used for payment card financial transactions.

Payment Application Data Security Standards (PA-DSS): Applies to software developers and integrators of applications that store, process or transmit cardholder data as part of authorization or settlement.

Compliance

Merchants who process credit card transactions are responsible for complying with the PCI DSS. “PCI Compliance” is achieved when merchants successfully demonstrate (via external audits or self-certification) that their entire system and processes comply with the 12 requirements of the PCI DSS.

Requirements

Version 3.0 of the PCI DSS was released in November 2013. The PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. The PCI DSS is organized around the following high-level goals and requirements:

805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852

Goals	Requirements
Build and Maintain a Secure Network and Systems	Requirement 1: Install and maintain a firewall configuration to protect cardholder data. Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	Requirement 3: Protect stored cardholder data. Requirement 4: Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs. Requirement 6: Develop and maintain secure systems and applications
Implement Strong Access Control Measures	Requirement 7: Restrict access to cardholder data by business need to know. Requirement 8: Identify and authenticate access to system components Requirement 9: Restrict physical access to cardholder data
Regularly Monitor and Test Networks	Requirement 10: Track and monitor all access to network resources and cardholder data Requirement 11: Regularly test security systems and processes.
Maintain an Information Security Policy	Requirement 12: Maintain a policy that addresses information security for all personnel.
Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers	Requirement A.1: Shared hosting providers must protect the cardholder data environment

805 West Franklin Street | Boise, Idaho 83702 | **p** 1-208.424.5054 | **f** 1-208.429.6852

What's New in Version 3.0

Version 3.0 of the PCI DSS was released on November 7, 2013 and consists of three major themes. First, the updated specification represents a philosophical shift from "quarterly or annual audit-based compliance" to "business-as-usual processes with 24x7 monitoring". Second, the new requirements added specific testing procedures to clarify what validation is expected for each requirement. There were wide variations in how auditors applied the previous requirements, and the new version seeks to minimize these differences to drive more consistency in the validation process. Third, the new requirements represent an evolution of the process based on experience, with several updates to address specific gaps as well as new and emerging threats.

The core 12 security areas remain the same, but the updates include several new sub-requirements that did not exist previously. The nature of the changes reflects the growing maturity of the payment security industry since the PCI DSS's formation in 2006, and the strength of the PCI Standards as a framework for protecting cardholder data. Cardholder data continues to be a target for criminals.

Lack of education and awareness of payment security and poor implementation and maintenance of the PCI Standards leads to many of the security breaches happening today. The updated requirements address these challenges by building in additional guidance and clarification on the intent of the requirements and ways to meet them. Additionally, the changes in Version 3.0 focus on some of the most frequently seen threats and risks that precipitate incidents of cardholder-data compromise.

Certification

While the standards are driven by the PCI SSC, each payment card financial institution has its own program for compliance. In general, compliance can be certified by the merchant through a Self-Assessment Questionnaire (SAQ) or through a qualified assessor such as a Qualified Security Assessor (QSA) or Approved Scanning Vendor (ASV).

It is the merchants' responsibility to work with their payment card financial institution to determine what form of certification is required.

805 West Franklin Street | Boise, Idaho 83702 | **p** 1-208.424.5054 | **f** 1-208.429.6852

3. CradlePoint Recommendations for PCI Compliance

Overview

The PCI SSC does not publish any certification standards for network equipment other than PIN entry terminals. As a result, there is no such thing as a "PCI Compliant Router.".

To become "PCI Compliant," merchants must verify that their entire system (POS devices, network devices, servers, applications, policies, and procedures) complies with the PCI DSS 3.0. As part of that overall effort, merchants must verify that their network equipment (including CradlePoint devices) is properly configured and managed to ensure overall compliance with the PCI DSS.

CradlePoint cannot control how an end user configures and manages a CradlePoint router. Similarly, CradlePoint does not have any control over the other devices, servers, and applications that compose an end-to-end card payment system. As such, PCI compliance can only be obtained by merchants in the context of their entire system. Merchants are also responsible for obtaining certification of their end-to-end system from a QSA (Qualified Security Assessor) or ASV (Approved Scanning Vendor).

CradlePoint devices are used in several PCI Compliant systems. This section provides a summary of CradlePoint features and capabilities that have been used by other customers to help achieve PCI Compliance for their end-to-end systems.

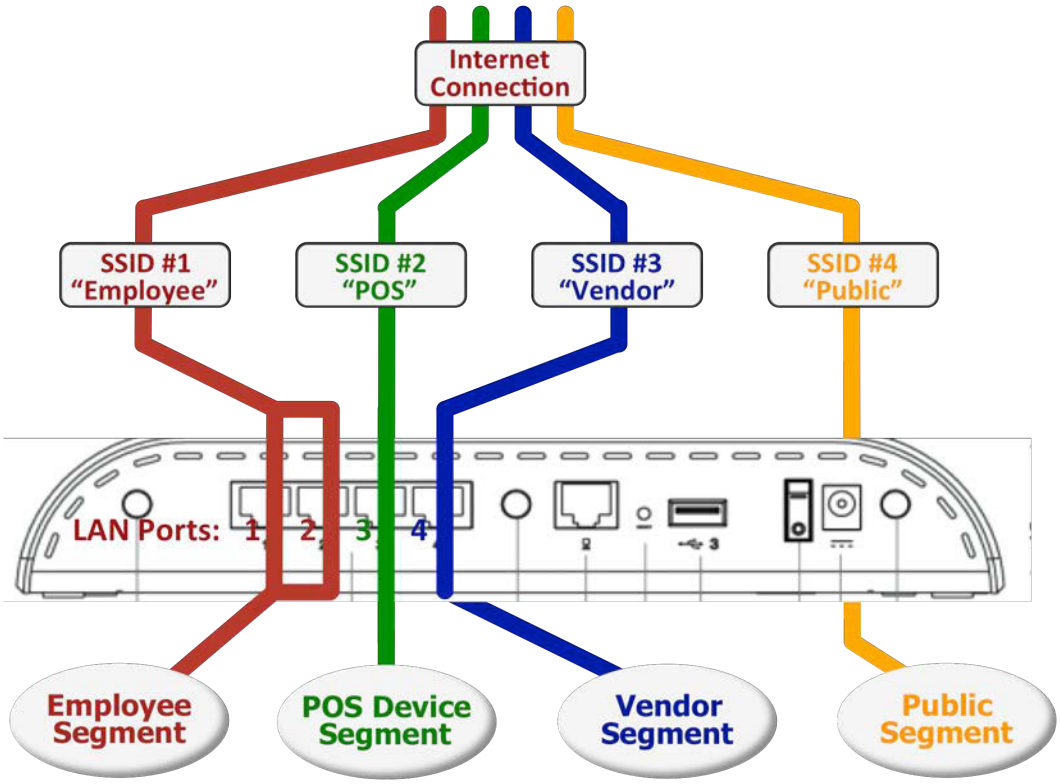
Reference Implementation

The following reference implementation represents a reasonably complex topology that includes:

- Ethernet access for POS devices
- Ethernet and WiFi access for employee computers and printers
- Ethernet and WiFi access for 3rd-party vendor
- WiFi access for customers

We recognize that retail POS enterprises may only implement certain subsets of this topology. However, the more complete topology is shown to highlight the capabilities provided by CradlePoint to address a wide range of target applications while maintaining PCI Compliance.

805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852



Recommendations

Step 1: Upgrade the router with the latest firmware.
Step 2: Change the default passwords.
Step 3: Lock down the router entry points.
Step 4: Configure the firewall.
Step 5: Segment the network into individual "security zones."
Step 6: Create secure WAN connectivity.
Step 7: Configure communication with an external SysLog server.
Step 8: Configure communication with an external Time server.
Step 9: Lock down the configuration with CradlePoint Enterprise Cloud Manager.
Step 10: Monitor device usage with CradlePoint Enterprise Cloud Manager.
Step 11: Keep device firmware updated with CradlePoint Enterprise Cloud Manager.

805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852

Key Features

The following describes several of the CradlePoint features and capabilities that are pertinent to PCI Compliance:

- Network Segmentation (Ethernet, SSID, and VLAN)
- Ethernet ports (4) that can be individually assigned to specific segments
- WiFi SSIDs (4) that can be individually secured and assigned to specific segments
- Virtual LAN support and tagging
- Stateful Packet Inspection (SPI)
- Network Address Translation
- Application Level Gateways (ALG)
- Inbound filtering of IP addresses
- De-Militarized Zone (DMZ)
- Virtual Server
- Ability to disable WAN services (ping, WNMP, web-based mgmt, etc.)
- MAC filtering
- Session filtering (non-UDP/TCP/ICMP)
- Layer 2 Tunneling Protocol (L2TP)
- VPN Client with support for up to 20 tunnels (product-specific)
- IPSec
- GRE
- WiFi security (WPA/WPA2 Personal/Enterprise, AES/TKIP)
- RADIUS user authentication on WiFi
- SysLog support
- Alerting
- CradlePoint Enterprise Cloud Manager managed service – to manage configuration, perform firmware updates, and monitor usage.

Additional Information

For additional information about how CradlePoint can help enable PCI Compliant card payment systems, please contact CradlePoint directly. Our Professional Services organization can provide consulting services and best practices that can help guide you towards PCI Compliance.

805 West Franklin Street | Boise, Idaho 83702 | **p** 1-208.424.5054 | **f** 1-208.429.6852

Step 1 Upgrade the router with the latest firmware.

CradlePoint has an engaged customer base that provides valuable feedback for feature requests and security enhancements, particularly with regard to PCI Compliance. We also have a talented development team that actively translates this feedback into new firmware releases. To get the benefit of these improvements, CradlePoint strongly recommends upgrading the router with the latest firmware.

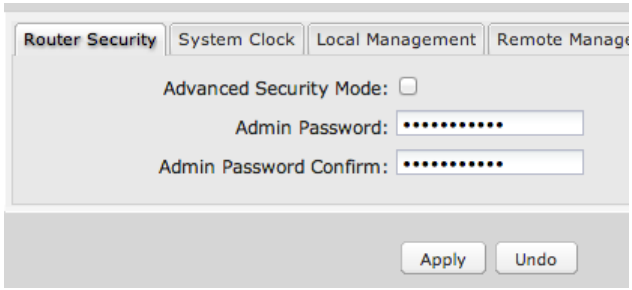
Additionally, the PCI DSS 3.0 recognizes that software and firmware upgrades in general are an important component of securing cardholder data. PCI DSS 3.0 Requirement 6.2 points out that new firmware releases often contain security patches that close potential security vulnerabilities. As a result, the PCI DSS requires merchants to use the latest software and firmware for all of their system components, including network routers. The PCI DSS also requires that critical software patches must be installed within one month of release.

The CradlePoint Enterprise Cloud Manager cloud-based management service plays a key role with many of our customers to ensure that remotely deployed CradlePoint routers are automatically upgraded (per customer-specific admin policies) with the latest firmware.

Step 2 Change the default passwords.

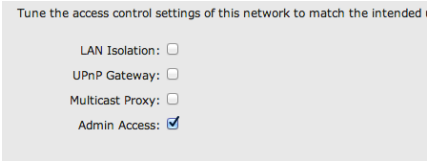
For out-of-box security, CradlePoint products do not ship with a generic default password. Rather, each router has a unique password that uses a portion of the router's MAC address.

PCI DSS Requirement 2.1 requires that the merchant change the default password on the router. Even though the CradlePoint passwords are unique to each individual router, CradlePoint recommends that the customer select a new unique password for each device that is only known to system administrators with a need-to-know.

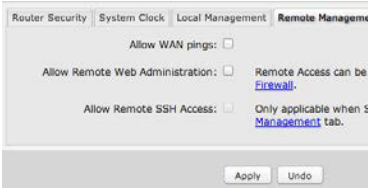


805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852

Step 3 Lock down the router entry points.

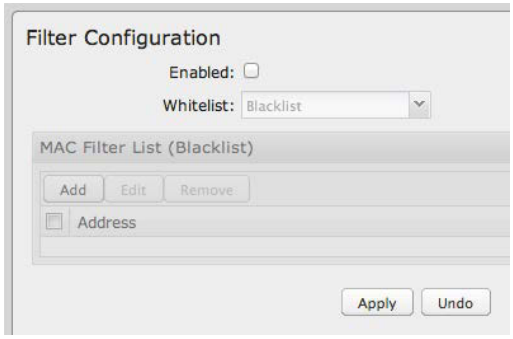


Disable UPnP: UPnP (Universal Plug and Play) is a set of networking protocols standardized by the UPnP Forum that enable clients to determine network configuration and configure the network to allow traffic through the firewall without direct user interaction. UPnP can simplify the use of consumer devices and other applications that require network configuration, but can also allow unprivileged users to manipulate network configuration.



Disable WAN Pings: When disabled, the router does not respond to ping requests from external WAN clients. This is often used by hackers to probe security vulnerabilities.

Disable Remote Administration: This prevents external users from accessing the router administration web UI through the WAN. CradlePoint recommends using CradlePoint Enterprise Cloud Manager to manage the routers, since it uses a secure device-initiated protocol that is less vulnerable to hacking. If you decide that you do want to enable remote admin access, be sure to configure it to require Hypertext Transfer Protocol Secure (HTTPS) on a non-standard port.



Use MAC Filtering: The MAC Filter allows you to create a list of devices that have either exclusive access (white list) or no access (black list) to your wireless LAN.

Use IP Filter Rules: "Incoming" IP filter rules restricts remote access to computers on your local network. "Outgoing" IP filter rules prevent computers on your local network from initiating communication to the address range specified in the rule.

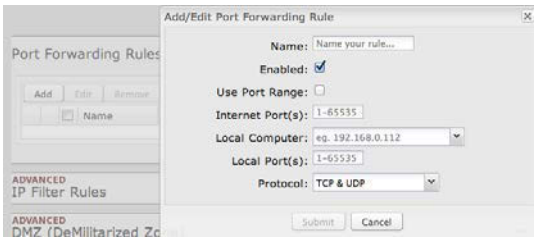
This feature is especially useful when combined with port forwarding and/or DMZ to restrict remote access to a specified host or network range. With an incoming IP filter rule, you can restrict the access to your LAN to only the specific computers or devices authorized to be on the network.

805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852

Step 4 Configure the firewall.

The merchant is responsible for configuring the router in a manner that maintains PCI Compliance. Since each application is different, CradlePoint can't provide a specific configuration that works for every environment. However, the following capabilities are available for the merchant to tailor for their application.

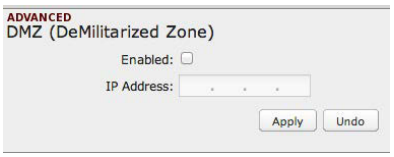
Firewall with Stateful Packet Inspection: The firewall in CradlePoint devices support Stateful Packet Inspection (SPI), which monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests are allowed to pass though the firewall. Unless you configure the router to the contrary, the router does not respond to unsolicited incoming requests on any port, thereby hiding your LAN from unauthorized external attackers.



In addition, the firewall supports the following:

Port Forwarding Rules: Some POS applications cannot run with a tight firewall. A port forwarding rule provides a controlled method of opening the firewall to address the needs of specific types of applications, allowing external traffic to reach a computer or device on the inside of the network.

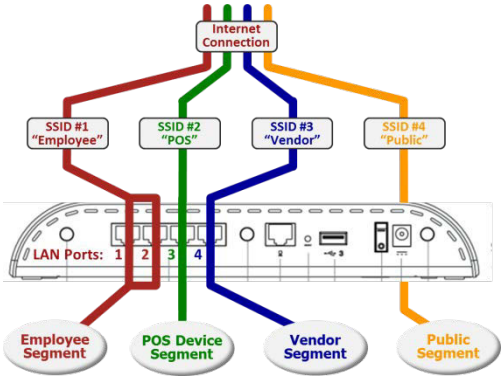
Anti-Spoof: Anti-Spoof dynamically checks packets to help protect against malicious users faking the source address in packets they transmit in order to either hide themselves or to impersonate someone else. Once the user has spoofed the address, they can either launch a network attack without revealing the true source of the attack, or attempt to gain access to network services that are restricted to certain addresses.



DMZ Host: A De-Militarized Zone (DMZ) host is effectively not firewalled in the sense that any computer on the internet may attempt to remotely access network services at the DMZ IP address. Input the IP Address of a single device in your network to create a DMZ for that device. To ensure that the IP address of the selected device remains consistent.

805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852

Step 5 Segment the network into individual "security zones."



Per the Retail POS example at the beginning of this chapter, this network will be configured with the following segments:

Employee Computer Network Segment

- Ethernet Port #1 for Manager's PC
- Ethernet Port #2 for Manager's Printer
- WiFi SSID "Corp Employee" (Hidden SSID, WPA2/Ent, corporate employee RADIUS Server)

POS Device Network Segment

- Ethernet Port #3
- WiFi SSID "POS Devices (CDE)" (Hidden SSID, WPA2/Ent, separate "POS" RADIUS Server)
- VLAN ID#5

Vendor Network Segment

- Ethernet Port #4
- WiFi SSID "Vendor" (Hidden SSID; WPA2/Enterprise, separate "vendor" RADIUS Server)

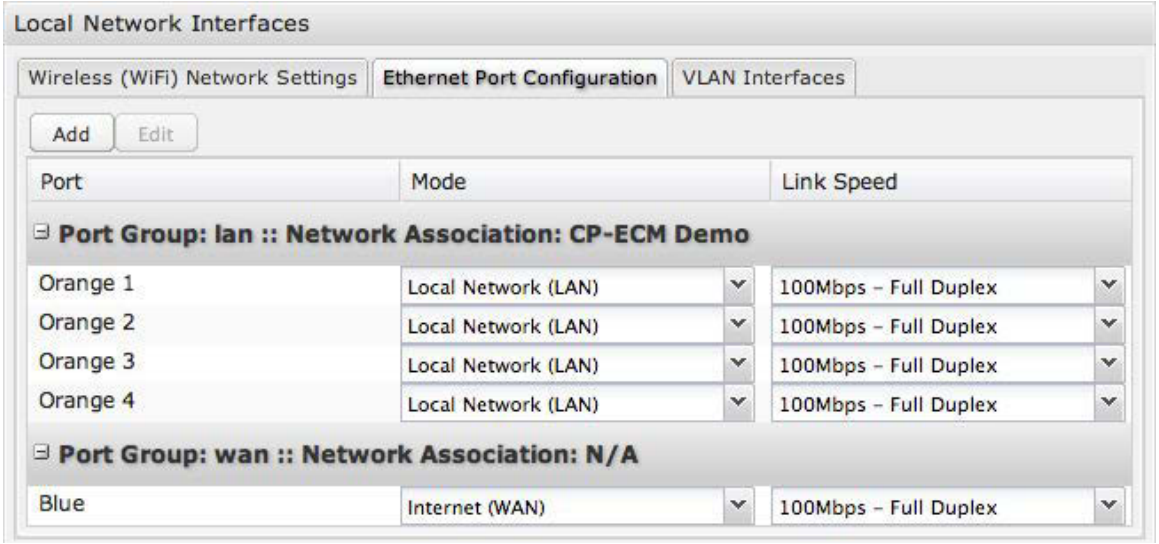
Public Guest Network Segment

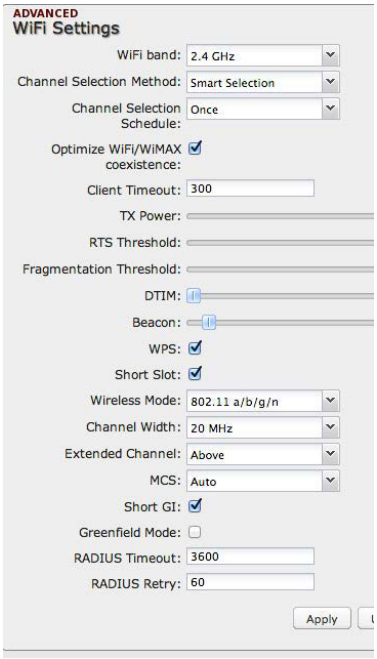
- WiFi SSID "Public Guest" (Open, but channeled into captive portal with branding and Terms-of-Service)

Create the Ethernet Port Groups: A Port Group represents a logical grouping of Ethernet ports. This is sometimes referred to as an Ethernet segment since any computers physically connected to these ports will be allowed to freely communicate with each other (unless "LAN Isolation" is enabled).

Based on the above requirements, create the groups of ethernet ports to use for the four network segments.

805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852





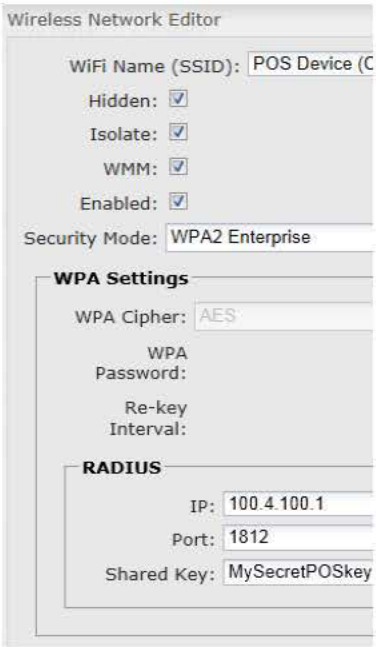
Create and Configure the WiFi SSIDs: CradlePoint routers can broadcast as many as four SSIDs (service set identifiers — the names for WiFi networks). One primary WiFi network is enabled by default, while you may have enabled a second guest network when using the First Time Setup Wizard. You have the ability to change the settings for either of these networks and/or enable two additional networks.

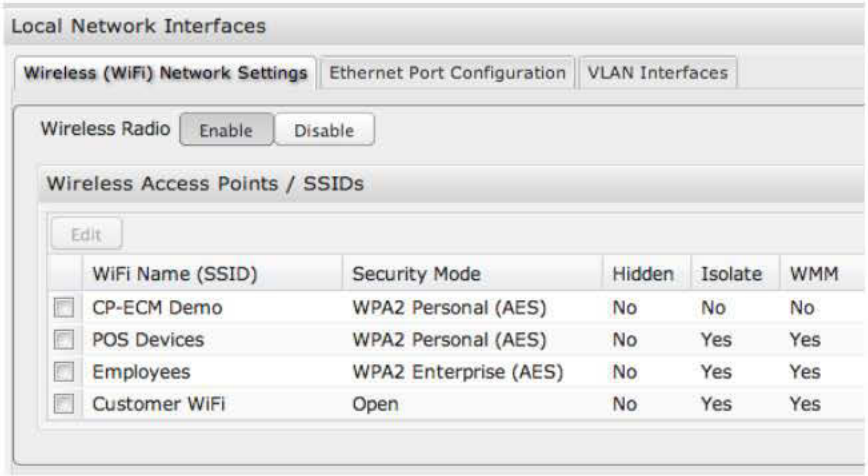
Note that you can disable the WiFi radio if desired. This configuration be locked down by CradlePoint Enterprise Cloud Manager to prevent the WiFi radio from being purposely or accidentally enabled. Additionally, any or all of the individual WiFi SSIDs can also be disabled.

To configure WiFi access per the example in this section, create the individual SSIDs that will be used in the network segments, and configure the appropriate security mode. For each individual SSID, select which ones you want to hide, and whether or not you want to isolate the other devices on the SSID from each other.

Use WPA2/Enterprise: CradlePoint strongly recommends using WPA2/Enterprise in conjunction with a RADIUS server. This provides a central repository for users or devices that are allowed to access the network, and allows for the use of Certificates to authenticate both the server and device. Each SSID can use a different RADIUS server, providing separate authentication sources for each group (i.e., employees, POS devices, vendors).

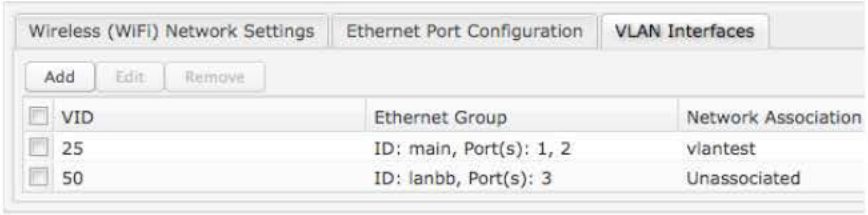
805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852

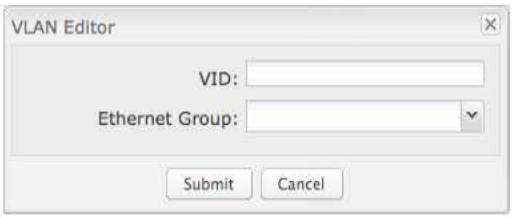




Create and Configure VLAN Segments: A virtual local area network, or VLAN, functions as any other physical LAN, but it enables computers and other devices to be grouped together even if they are not physically attached to the same network switch.

To enable a VLAN, select a VID (virtual LAN ID) and a group of Ethernet ports through which users can access the VLAN. Then go back up to the Local Network Editor to attach your new VLAN to a network. To use a VLAN, the VID must be shared with another router or similar device so that multiple physical networks have access to the one virtual network. Once the VLAN(s) is created, select the LAN port(s) or ethernet groups that you want to associate to the VLAN ID.



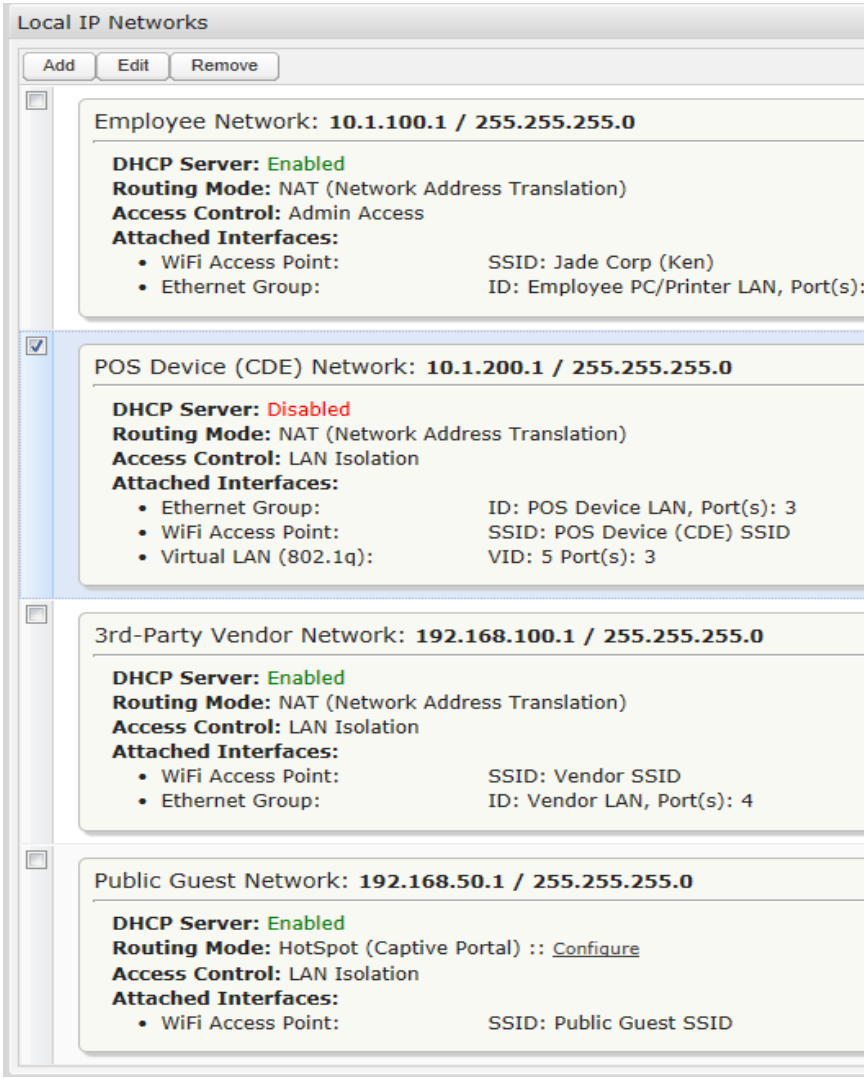


805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852

Once the individual Ethernet ports/groups, WiFi SSIDs and VLANs have been created, create and configure each of the individual network segments that you intend to deploy.

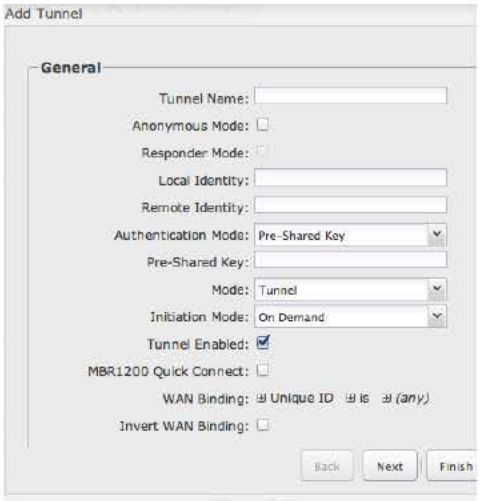
Each network segment can have its own:

- IP Address configuration (static, dynamic, range)
- Routing Mode (NAT, non-NAT, Public Hotspot/Captive Portal)
- Access Control (Admin Access, LAN Isolation, etc.)
- Interfaces (choose from WiFi SSIDs, Ethernet Groups and VLANs)

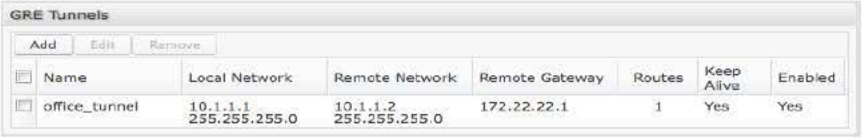


805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852

Step 6 Create secure WAN connectivity.



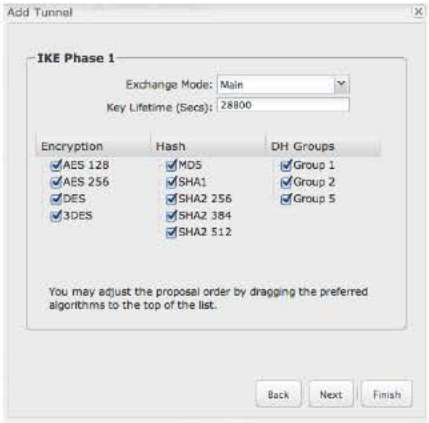
GRE: GRE tunnels can be used to create a connection between two private networks. CradlePoint routers support both GRE and VPN tunnels. GRE tunnels are simpler to configure and more flexible for different kinds of packet exchanges, but VPN tunnels are much more secure.

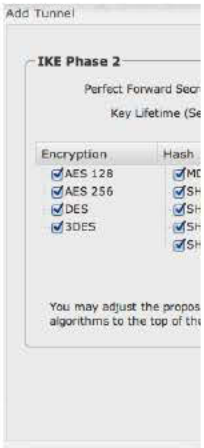


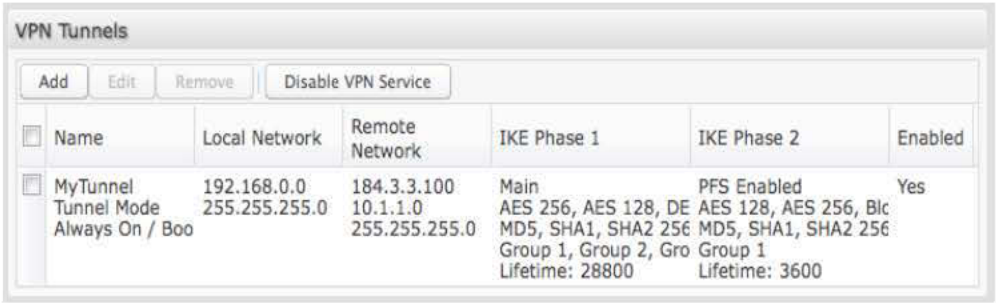
VPN: VPN tunnels are used to establish a secure connection to a remote network over a public network. For example, VPN tunnels can be used across the internet by an individual store location to connect to the corporate data center or by two individual store locations to function as if connected with one network. The two networks set up a secure connection across the (normally) unsecure Internet by assigning VPN encryption protocols.

IPsec: CradlePoint routers use IPsec to authenticate and encrypt packets exchanged across the tunnel. To set up a VPN tunnel with a CradlePoint router on one end, there must be another device (usually a router) that also supports IPsec on the other end.

Internet Key Exchange (IKE): IKE is the security protocol in IPsec. IKE has two phases, Phase 1 and Phase 2. CradlePoint routers have several different security protocol options for each phase, but the default selections will be sufficient for most users.





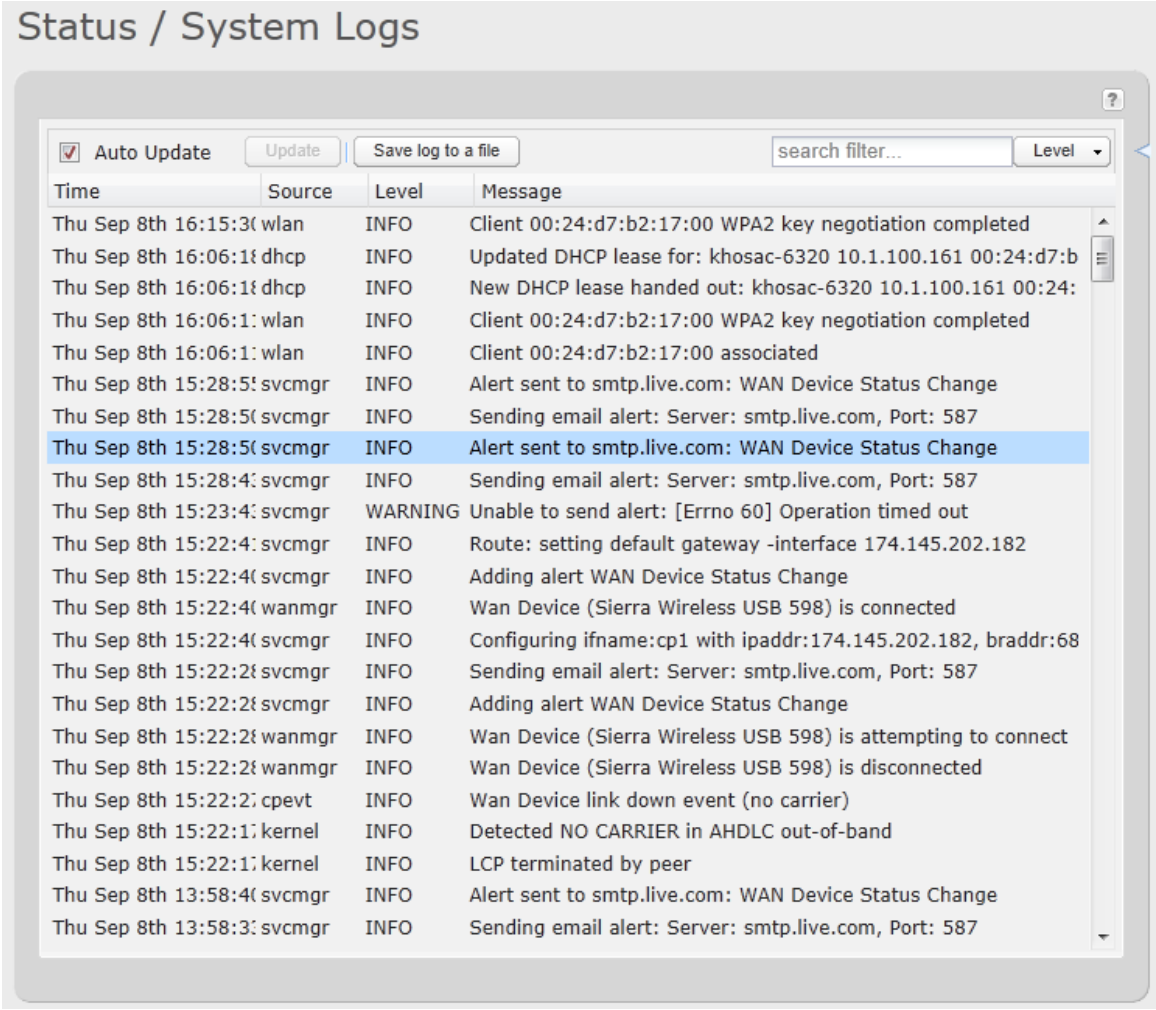


805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852

Step 7 Configure communication with an external SysLog server.

The router automatically logs (records) events of possible interest in its internal memory. The log options allow you to filter the router logs based on categories, allowing customization of the types and level of events to record and the level of events to view.

To persist the system logs, use the CradlePoint Enterprise Cloud Manager management service to synchronize and store the system logs. Alternatively, the router can be configured to communicate with an external Syslog Server.

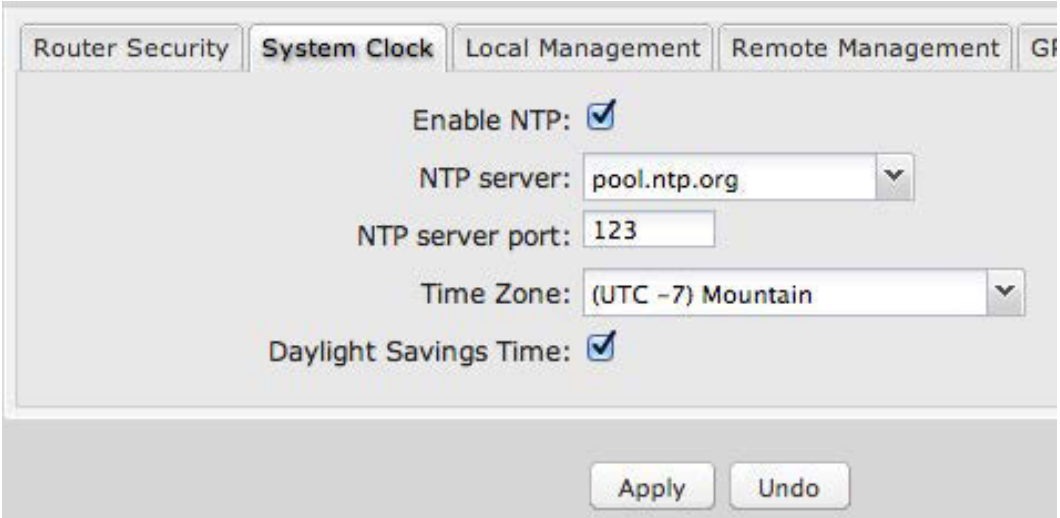


Step 8 Configure communication with an external Time server.

Network Time Protocol (NTP) enables the router to synchronize its system time with a remote server on the internet. NTP is an important part of using System Logs to accurately monitor PCI Compliance.

Options for NTP servers include:

805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852



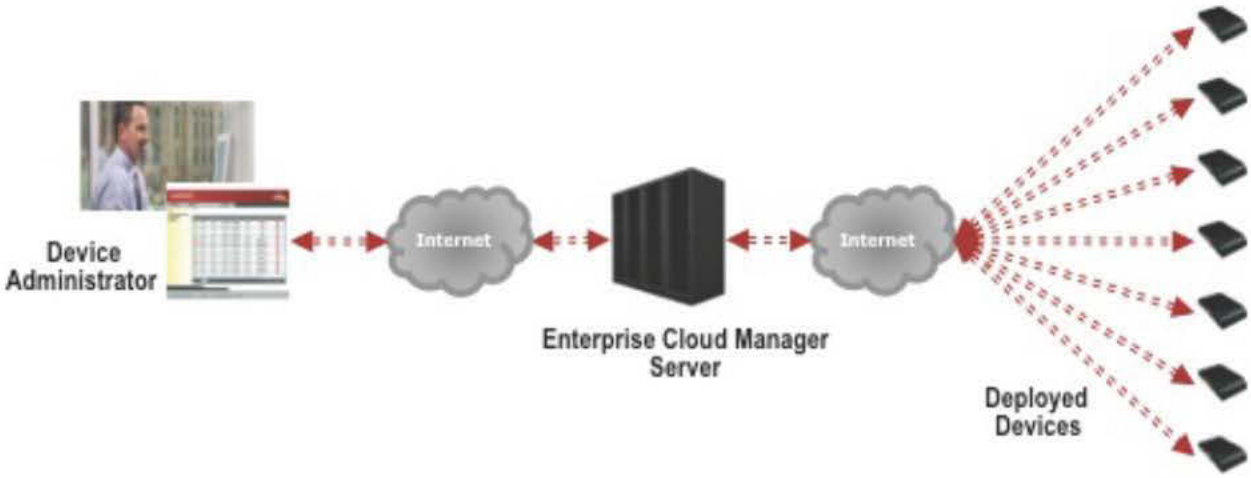
Step 9 Lock down the configuration with CradlePoint Enterprise Cloud Manager.

CradlePoint Enterprise Cloud Manager was developed to monitor and manage large numbers of remotely deployed devices using a secure cloud-based management service. CradlePoint Enterprise Cloud Manager is hosted at a world-class, third-party storage facility. CradlePoint Enterprise Cloud Manager servers are located within a physically secured area at a Tier IV datacenter that is SAS70 (SSAE Type II) certified. Only datacenter-authorized personnel have access to the secured area.

CradlePoint devices include an embedded CradlePoint Enterprise Cloud Manager agent that uses a device-initiated, encrypted protocol to establish communication with the CradlePoint Enterprise Cloud Manager server. Because the protocol is device-initiated, CradlePoint Enterprise Cloud Manager can operate behind firewalls that NAT the router IP address and does not require static IP addresses. The protocol is designed to minimize overhead and bandwidth, important elements in a mobile broadband environment.

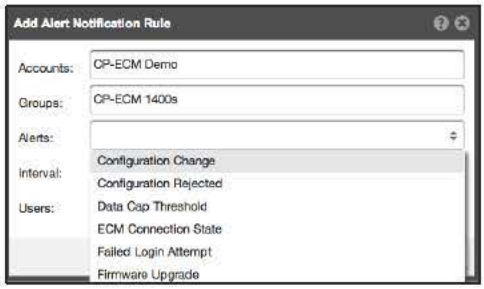
CradlePoint Enterprise Cloud Manager is hosted on a secure, enterprise-class server at an Internet service provider data center, providing equipment redundancy, always-on power, multiple internet channels, and backup/restoration service.

805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852



Important Note: CradlePoint devices do not store any of the data that flows through the device. As a result, CradlePoint Enterprise Cloud Manager has no access whatsoever to any cardholder data.

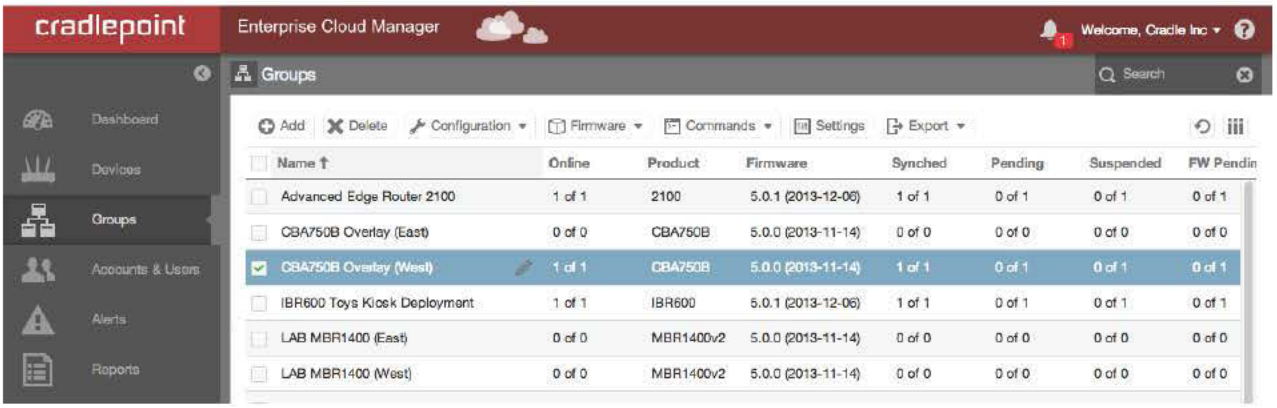
Account Security: Each account requires a secure user name and password. The server uses MD5-encrypted login credentials and HTTP/SSL for data encryption, server authentication and message integrity. CradlePoint Enterprise Cloud Manager provides multi-layered SQL injection protection to defend against automated breach attempts, and uses two layers of network firewall. Web-based users are automatically assigned restricted privileges that prohibit them from code execution. CradlePoint Enterprise Cloud Manager uses separate, firewalled databases for user login and device information.



Configuration Control: CradlePoint Enterprise Cloud Manager enables Retail POS network administrators to audit compliance of devices with the carefully-designed configuration originally required to obtain PCI compliance of their end-to-end system. If any unauthorized or accidental configuration changes are made, CradlePoint Enterprise Cloud Manager will automatically reverse the change.

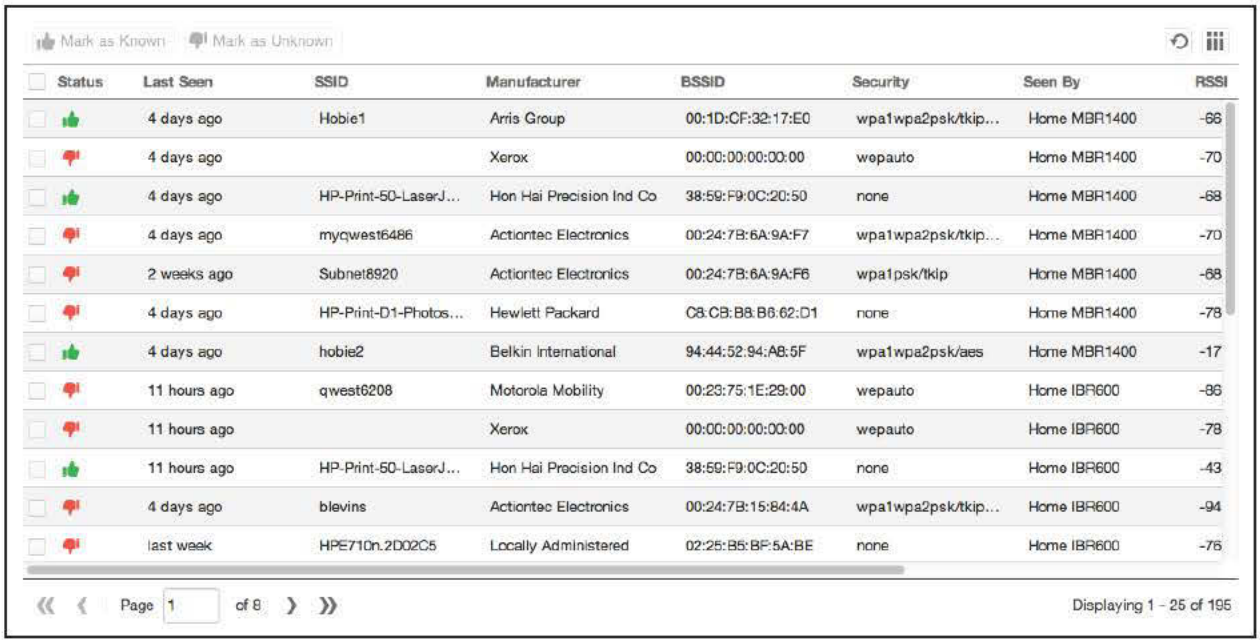
Group-Level Configuration: CradlePoint Enterprise Cloud Manager provides group-level configurations to facilitate management of large number of devices.

805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852



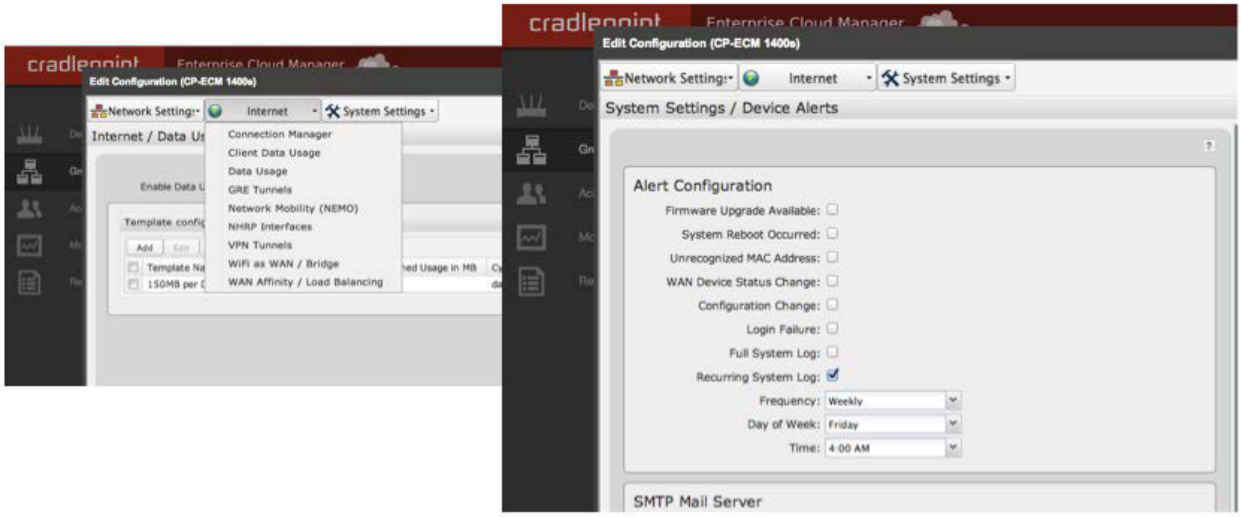
Step 10 Monitor device usage with CradlePoint Enterprise Cloud Manager.

For optimum monitoring, CradlePoint offers its new **Rogue Access Point** management in CradlePoint Enterprise Cloud Manager. The Rogue AP solution augments the CradlePoint Enterprise Cloud Manager security offering by providing a solution to monitor the radio spectrum for the presence of unauthorized access points. CradlePoint Enterprise Cloud Manager periodically scans the network and stores information from the scans. Each access point detected can be designated as Known or Unknown. Good network security practices and PCI compliance requirements both require visibility to a list of rogue access points to protect against attacks from malicious access points on your network.



Event Alerting: CradlePoint Enterprise Cloud Manager provides alerting that can be useful in maintaining PCI Compliance. Alerts for specific router events include unauthorized login attempts, WAN connection changes, data usage thresholds, or modem removal.

805 West Franklin Street | Boise, Idaho 83702 | **p** 1-208.424.5054 | **f** 1-208.429.6852



Statistics and Logging Records: CradlePoint Enterprise Cloud Manager additionally provides statistics and logging records that can be used to monitor remotely deployed devices. The network administrator can control the parameters that define how often the routers in the group talk to the server. The types of communication include:

Synchronizing. Routers send a synchronization request on user-determined interval of schedule to determine if there are any pending commands, firmware upgrades or configuration changes.

Heartbeat. Routers send heartbeat messages to inform the server that they are online on a user-defined interval.

Status Reporting. Routers can send detailed reports on modems, Wi-Fi clients, memory usage, etc.

Log Reporting. In addition to synchronizing the logs with CradlePoint Enterprise Cloud Manager or a SysLog server, routers can send their logs on a regular, configurable basis via email directly to the network administrator.

805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852

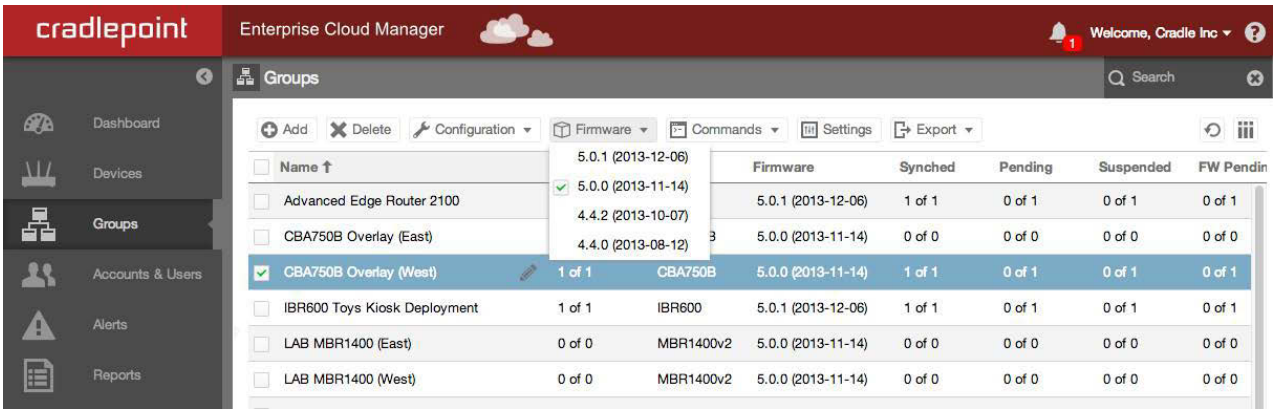
Step 11 Keep device firmware updated with CradlePoint Enterprise Cloud Manager.

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems.

The PCI DSS 3.0 document recognizes that providers of system component (including servers, network devices, applications) regularly test for new vulnerabilities. As issues are discovered, the provider issues software upgrades to address these issues.

PCI DSS Requirement 6.2 mandates that all critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software. The PCI DSS also requires that critical software patches must be installed within one month of release.

Firmware Management: CradlePoint Enterprise Cloud Manager enables each device group to have a selected firmware version used on all devices in the group. Network administrators can choose the firmware version for a given group to use by selecting it from the list. The facility allows the firmware version to be downgraded as well as upgraded. If any devices are upgraded, either accidentally or without authorization, CradlePoint Enterprise Cloud Manager will automatically reverse the upgrade.



805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852

Appendix A: Acronym List

Term	Definition
AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard (WiFi security)
ALG	Application Level Gateway
AP	Access Point
ARC	CradlePoint Router Family Name
ASV	Approved Scanning Vendor (PCI compliance term)
ATM	Automated Teller Machine
AV	Anti-Virus
CDE	Cardholder Data Environment (PCI compliance term)
CDR	Call Detail Records
CM	Configuration Management
CP	CradlePoint?
CSO	Chief Security Officer
DMZ	De-Militarized Zone
DSS	Data Security Standard (PCI compliance term)
ECM	CradlePoint Enterprise Cloud Manager
GRE	Generic Router/ing Encapsulation
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
IT	Information Technology
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LTE	4G wireless network: Long-Term Evolution
M2M	Machine to Machine
MAC	Media Access Control
MD5	Message-Digest (algorithm) 5
NAT	Network Address Translation
NTP	Network Time Protocol
OS or O/S	Operating System
PA	Payment Application (PCI compliance term)
PAN	Personal Account Number (PCI compliance term)
PCI	Payment Card Industry (PCI compliance term)
PIN	Personal Identification Number
POS	Point of Sale
PTS	PIN Transaction Security (PCI compliance term)
QSA	Qualified Security Assessor (PCI compliance term)
RADIUS	Remote Authentication Dial In User Service
SAQ	Self-Assessment Questionnaire (PCI compliance term)
SNMP	Simple Network Management Protocol

805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852

Term	Definition
SPI	Stateful Packet Inspection
SQL	Structured Query Language
SSC	Security Standards Council (PCI compliance term)
SSH	Secure Shell (Cryptology)
SSID	Service Set Identifier
SSL	Secure Sockets Layer
STUN(T)	Session Traversal Utilities for NAT (A NAT traversal protocol)
TCP	Transport Control Protocol (packets)
TKIP	Temporal Key Integrity Protocol (formerly WEP2) (WiFi security)
TLS	Transport Layer Security (Cryptology)
UDP	User Datagram Protocol (packets)
UI	User Interface
UPnP/UPP	Universal Plug and Play
UTM	Unified Threat Management
VLAN	Virtual Local-Area Network
VPN	Virtual Private Network
WEP	Wireless Encryption Protocol (WiFi security control prohibited as of June 30, 2010
WNMP	Wireless Network Management Protocol
WPA	Wireless Protected Access (WiFi security)
WPA2	Wi-Fi Protected Access 2 (Wi-Fi Alliance) (WiFi security)

805 West Franklin Street | Boise, Idaho 83702 | p 1-208.424.5054 | f 1-208.429.6852