Security Benchmarks™
A DIVISION OF CENTER FOR INTERNET SECURITY

CIS Cisco Wireless LAN Controller 7 Benchmark

v1.0.0

Export Date 10-18-2012

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview

This document, Security Configuration Benchmark for Cisco Wireless LAN Controllers, provides prescriptive guidance for establishing a secure configuration posture for Cisco Wireless LAN Controller firmware version 7.2. This guide was tested against Cisco Wireless LAN Controller firmware v7.2.103.0. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Cisco IOS on a Cisco routing and switching platforms.

Consensus Guidance

This benchmark was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author
Brian Sak

Contributor
Sergey Pavlov
Vikki Taxdal
Don Thomas
Justin Opatrny
Rael Daruszka, *VMC*
Steven Piliero, *Center for Internet Security*

Recommendations

1 Wireless LAN Controller

This section prescribes controls to secure wireless termination points and access controllers in a wireless system.

1.1 Install the Latest Firmware (Not Scored)

Profile Applicability:

- Level 1

Description:

The Wireless LAN Controllers should be upgraded to the latest firmware to resolve any discovered security vulnerabilities.

Rationale:

Wireless LAN Controllers running firmware with documented vulnerabilities could be subject to attacks including ones that may allow for unauthorized configuration changes or denial of service.

Audit:

Validate that the running Product Version is the same as the latest released version.

1. Run the following command to display the running Product Version:

```
(Cisco Controller) >show sysinfo
```

2. Compare the Product Version to the latest version on Cisco's website.

Remediation:

Download the latest firmware from the Cisco Website and apply it to the Wireless LAN Controller.

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp1320208

1.2 Ensure 'Password Strength' is Strong for configured 'User Names' (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines if local administrative passwords meet minimum complexity requirements and are determined as "strong" by the Wireless LAN Controller. To meet the "strong" requirement the selected password must meet the following criteria:

- It is at least eight characters long.
- It contains a combination of upper- and lowercase letters, numbers, and symbols.
- It is not a word in any language.

Rationale:

Password complexity for administrative accounts reduces the risk of an attacker guessing the password. An attacker could gain unauthorized access to the Wireless LAN Controller by guessing a weak password.

Audit:

1. Perform the following to determine if the local management users are configured to use strong passwords.

```
(Cisco Controller) >show mgmtuser
```

2. Verify returned users have **Strong** listed in the Password Strength column.

```
User Name            Permissions      Description     Password Strength
-----------------    -------------    -------------   -----------------
<Username>           read-write                       Strong
```

Note: Cisco bug (CSCuc22601) may cause **show mgmtuser** to show only User Name and Permissions, but not Description and not Password Strength.

Remediation:

Change the management user's password to one that meets the strong password requirements. The Wireless LAN Controller determines a password is strong if it meets the following requirements:

- It is at least eight characters long.
- It contains a combination of upper- and lowercase letters, numbers, and symbols.
- It is not a word in any language.

The new password can be applied using:

```
(Cisco Controller) >config mgmtuser password <username> <password>
```

1.3 Delete the 'User Name' admin (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines if the default system usernames and passwords have been removed. The recommended setting is to delete admin (default account).

Rationale:

Default usernames and passwords are known to attackers and could allow unauthorized administrative access or to change the configuration of Access Points and/or the Wireless LAN Controller. The default is username is admin with a default password of admin.

Audit:

1. Perform the following to determine the local management users configured on the Access Controller.

```
(Cisco Controller) >show mgmtuser
```

2. Verify the return value **does not** include the default User Name **admin**.

```
User Name                 Permissions    Description            Password Strength
-----------------------   ------------   --------------------   -----------------
<User Name>                read-write                             Strong
```

Remediation:

New management users can be configured using the following command.

```
(Cisco Controller) >config mgmtuser add <username> <password> <privilege
level>
```

After the creation of a new administrative username with the appropriate privileges the default one can be removed.

```
(Cisco Controller) >config mgmtuser delete admin
```

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp7649595

1.4 Ensure 'Telnet' is disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines whether the device allows administration via the telnet protocol. The recommended setting is telnet disabled.

Rationale:

Administrative access to the controller should be allowed only using cryptographically secure access methods. Unsecured administrative access methods, such as telnet, do not encrypt traffic between the client and the administrative interface. This could allow for interception or manipulation of the administrative session or capture of administrative credentials.

Audit:

Perform the following to determine if telnet is enabled.

1. Run the command below:

```
(Cisco Controller) >show network summary
```

2. Ensure telnet is disabled.

```
Telnet..................................... Disable
```

Remediation:

1. Disable command-line administration through telnet.

```
(Cisco Controller) >config network telnet disable
```

2. Enable command-line administration through Secure Shell Version 2 (SSHv2).

```
(Cisco Controller) >config network ssh enable
```

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp1319452

1.5 Ensure 'Webmode' is disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines whether the device allows administration via webmode. The recommended setting is network webmode disabled.

Rationale:

Administrative access to the controller should only be allowed using cryptographically secure access methods. Unsecured administrative access methods, such as Hypertext Transfer Protocol (HTTP), do not encrypt traffic between the client and the administrative interface. This could allow for interception or manipulation of the administrative session or capturing administrative credentials. Enable Secure Shell Version 2 (SSHv2) or Hypertext Transfer Protocol Secure (HTTPS) for administration. The default setting is enabled.

Audit:

Perform the following to determine if telnet is enabled.

1. Run the command below:

```
(Cisco Controller) >show network summary
```

2. Validate that webmode is disabled.

```
Webmode..................................... Disable
```

Remediation:

1. Disable administration through webmode.

```
(Cisco Controller) >config network webmode disable
```

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp1319452

1.6 Disable 'Management via Wireless Interface' (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines whether wireless clients can manage only the Cisco wireless LAN controller associated with the client and the associated Cisco lightweight access point. That is, clients cannot manage another Cisco wireless LAN controller with which they are not associated. The recommended setting is network mgmt-via-wireless disabled.

Rationale:

Administrative access should not be allowed from wireless clients because the wireless client is mobile; it can be stolen, misplaced, or lent to an unauthorized user. Allowing administrative access from the wireless network increases the possibility of an attacker gaining access to the admin interface. The default setting for mgmt-via-wireless is enabled.

Audit:

Perform the following to determine if administrative access is allowed from wireless clients.

1. Run the command below:

```
(Cisco Controller) >show network summary
```

2. Validate that Mgmt Via Wireless Interface is set to disable.

```
Mgmt Via Wireless Interface..................... Disable
```

Remediation:

Disable access to the admin interface from wireless clients using the following command.

```
(Cisco Controller) >config network mgmt-via-wireless disable
```

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp1324232

1.7 Ensure the 'CLI Login Timeout (minutes)' is less than or equal to 5 (Not Scored)

Profile Applicability:

- Level 2

Description:

This control determines how long a command-line session will stay idle before it is logged out. The recommended setting is 5 minutes or less, but not set to zero.

Rationale:

Command-line sessions timeout after a period of inactivity to reduce the risk of an unauthorized individual taking over an unattended, authenticated session. Validate that the inactivity timeout for CLI session's has not been set for more than the default or disabled altogether. The default inactivity timeout is 5 minutes.

Audit:

Validate the currently configured inactivity timeout.

1. Run the following command:

```
(Cisco Controller) >show sessions
```

2. Validate the timeout value is set to 5 minutes or less, but not 0. Zero indicates that timeout is disabled.

```
CLI Login Timeout (minutes)..... 5
```

Remediation:

Reset the default authentication timeout value to 5 minutes.

```
(Cisco Controller) >config sessions timeout 5
```

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp1319842

1.8 Ensure 'SNMP v1 Mode' is disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines whether or not Simple Network Management Protocol Version 1 (SNMP v1) can be used for remote network management. The recommended setting is disabled.

Rationale:

Simple Network Management Protocol Version 1 (SNMPv1) is not encrypted and is authenticated using a shared password. Encryption thwarts eavesdropping and attempts to manipulate network management protocols.

Audit:

Perform the following to determine which versions of Simple Network Management Protocol are enabled on the Wireless LAN Controller.

1. Run the following command:

```
(Cisco Controller) >show snmpversion
```

2. Ensure SNMP v1 Mode is set to **Disable**.

```
SNMP v1 Mode..................................... Disable
```

Remediation:

Disable SNMP version v1

```
(Cisco Controller) >config snmp version v1 disable
```

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp1319918

1.9 Ensure 'SNMP v2c Mode' is disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines whether Simple Network Management Protocol version 2c (SNMP v2) can be used for remote network management. The recommended setting is disabled.

Rationale:

Simple Network Management Protocol Version 2c is not encrypted and is authenticated using a shared password. Encryption thwarts eavesdropping and attempts to manipulate network management protocols.

Audit:

Perform the following to determine which versions of SNMP are enabled on the Wireless LAN Controller.

1. Run the following command:

```
(Cisco Controller) >show snmpversion
```

2. Ensure that SNMP v2c Mode is set to **Disable**.

```
SNMP v2c Mode..................................... Disable
```

Remediation:

Disable SNMP version v2c

```
(Cisco Controller) >config snmp version v2c disable
```

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp1319918

1.10 Delete the 'SNMP v3 User Name' default (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines whether the `default` Simple Network Management Protocol Version 3 (SNMPv3) username included in the default configuration has been removed. The recommended setting is to delete the SNMP v3 User Name `default`.

Rationale:

Default username and password combinations are known to attackers and could be used to gain unauthorized access to the Wireless LAN Controller. SNMPv3 is disabled by default, however if enabled could allow unauthorized configuration changes using the default user.

Audit:

Validate that the default Simple Network Management Protocol Version 3 user **does not** exist.

1. Run the following command:

```
(Cisco Controller) >show snmpv3user
```

Ensure `default` is not present for SNMP v3 User Name.

```
SNMP v3 User Name      AccessMode    Authentication   Encryption
---------------------  ----------    --------------   ----------
default                Read/Write    HMAC-SHA         CFB-AES
```

Remediation:

Delete the default Simple Network Management Protocol Version 3 user.

```
(Cisco Controller) >config snmp v3user delete default
```

If Simple Network Management Protocol Version 3 is to be used for network management, create a new Simple Network Management Protocol Version 3 user:

```
(Cisco Controller) >config snmp v3user create <username> <ro/rw> <authentication
type> <encryption type> <authentication key> <encryption key>
```

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp1319901

1.11 Configure 'an authorized IP Address' for 'Logging Syslog Host' (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines if the Wireless LAN Controller is configured to send logging information to a centralized syslog server for processing and alerting. The recommended setting is to configure an authorized IP address for logging syslog.

Rationale:

Logging should be enabled on Wireless Termination Points and Access Controllers to detect access attempts, configuration changes, and system level events. Logs should be centrally collected and reviewed on a regular basis. It is recommended that logging is enabled on all

devices and archived for a minimum of 12 months with 90 days of logs to be immediately available. Logging of wireless activity and administrative access is essential to detect anomalies and attacks on and from the wireless network.

Audit:

Validate that logging is enabled and a syslog host is defined. This can be done using one of two methods.

Method 1

1. Run the command below:

```
(Cisco Controller) >show logging
```

2. Verify that a syslog server is defined under the "Logging to syslog:" section.

```
 Logging to syslog :
- Number of remote syslog hosts..................... 1
  - Host 0..................................... <IP Address>
```

Method 2

1. Show the running configuration to the screen using the following command:

```
 (Cisco Controller) >show run-config commands
```

2. Validate the return pattern matches:

```
 logging syslog host <IP Address>
```

Remediation:

To enable external logging to a syslog server execute the following command:

```
 (Cisco Controller) >config logging syslog host <IP Address>
```

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp5110363

1.12 Configure 'an authorized IP Address' for 'NTP Server' (Not Scored)

Profile Applicability:

- Level 2

Description:

This control determines if Network Time Protocol is configured to synchronize time from an authorized external time source to the Wireless LAN Controller.

Rationale:

Network Time Protocol is configured on the Wireless LAN Controller to synchronize the local time with an external time source. Consistent, accurate time is important for certificate validation, logging, and forensic analysis. Network Time Protocol is not configured by default.

Audit:

1. Perform the following to determine if NTP is enabled.

```
(Cisco Controller) >show time
```

2. Verify an authorized NTP Server address is configured:

```
NTP Polling Interval.........................     86400

     Index     NTP Key Index      NTP Server               NTP Msg Auth Status
    -------  ------------------------------------------------------------------
       1              0          <IP Address>             <Authentication Status>
```

Remediation:

Configure an authorized IP address for time NTP Server.

```
(Cisco Controller) >config time ntp server <index> <IP Address>
```

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp2505839

1.13 Ensure 'Signature Processing' is enabled. (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines whether Intrusion Detection System (IDS) signature processing is enabled for all IDS signatures. The recommended setting is enabled.

Rationale:

Wireless Protection Policies are a basic set of signatures that can detect attacks on the wireless network or clients. The Wireless LAN Controller can monitor the RF spectrum and detect attackers attempting to compromise or manipulate wireless networks. The Wireless LAN Controller should be configured to detect rogue Access Points or attacks on the wireless infrastructure or wireless clients. By default Protection Policies are not enabled.

Audit:

To validate that Wireless Protection Signature Policy Processing is enabled,

1. Run the following command:

```
(Cisco Controller) >show wps summary
```

2. Check output to ensure that Signature Processing is enabled.

```
Signature Policy
 Signature Processing..................... Enabled
```

Remediation:

Enable all Wireless Protection Policies.

```
(Cisco Controller) > config wps signature enable
```

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp6871472

1.14 Enable 'all' Policies for 'wps client-exclusion' (Not Scored)

Profile Applicability:

- Level 2

Description:

This control determines the client exclusion policies that are enforced when clients attempt to associate with the device:

- `802.11-assoc` excludes clients on the sixth 802.11 association attempt, after five consecutive failures,
- `802.11-auth` excludes clients on the sixth 802.11 authentication attempt, after five consecutive failures,
- `802.1x-auth` excludes clients on the sixth 802.11X authentication attempt, after five consecutive failures,
- `ip-theft` excludes clients if the IP address is already assigned to another device,
- `web-auth` excludes clients on the fourth web authentication attempt, after three consecutive failures,
- **all** excludes clients for all of the above reasons.

The recommended setting is all.

Rationale:

Client Exclusion Policies are a group of settings that can automatically restrict client access if the Wireless LAN Controller detects excessive authentication failures or the theft or reuse of IP addressing. Excessive authentication attempts could be an indication that a client is attempting to brute force entry onto the wireless network or executing a denial-of-service attack. The default setting is enabled.

Audit:

Validate the Client Exclusion Policies are enabled.

1. Execute the following command:

```
(Cisco Controller) >show wps summary
```

2. Validate the the output shows that all of the Client Exclusion Policies are set to **Enabled.**

```
Client Exclusion Policy
 Excessive 802.11-association failures..... Enabled
 Excessive 802.11-authentication failures..... Enabled
 Excessive 802.1x-authentication..... Enabled
 IP-theft..... Enabled
 Excessive Web authentication failure..... Enabled
```

Remediation:

Enable the Client Exclusion Policies:

```
(Cisco Controller) >config wps client-exclusion all
```

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp9541897

1.15 Ensure 'Rogue Location Discovery Protocol' is enabled (Not Scored)

Profile Applicability:

- Level 2

Description:

This control determines whether the device will generate an alarm only, or automatically contain a rogue access point that is advertising your network's service set identifier (SSID).

Rationale:

Rogue Access Points that do not require authentication or encryption could allow unauthorized or malicious users to connect to the network. Rogue Location Discovery Protocol can actively seek out these Rogue Access Points and alert administrators to their existence after validating that they are connected to the network. By default RLDP is not enabled.

Audit:

Validate that Rogue Location Discovery Protocol is enabled.

1. Execute the following command:

```
(Cisco Controller) >show rogue ap rldp summary
```

2. Validate the output shows that Rogue Location Discovery Protocol is set to **Enabled.**

```
Rogue Location Discovery Protocol.............. Enabled
```

Remediation:

Enable the Rogue Location Discovery Protocol:

```
(Cisco Controller) >config rogue ap rldp enable {alarm-only | auto-contain}
```

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp4999879

1.16 Ensure 'Control Path Rate Limiting' is enabled (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines whether the switch control path rate limiting feature is enabled. The recommended setting is enabled.

Rationale:

If the Wireless LAN Controller is not able to keep up with the volume of management traffic it is receiving, a denial-of-service condition could occur. When control plane policing is enabled this ensures that the CPU is not overwhelmed by management traffic. The default state is enabled.

Audit:

Perform the following to determine if control plane policing is enabled or disabled.

1. Run the following command:

```
(Cisco Controller) >show advanced rate
```

2. Verify the following output:

```
Control Path Rate Limiting.....................  Enabled
```

Remediation:

Enable control plane policing on the controller.

```
(Cisco Controller) >config advanced rate enable
```

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp7209817

2 Wireless Local Area Network (LAN) Configurations

This section prescribes controls to secure Wireless Local Area Networks (LAN).

2.1 Ensure 'Broadcast SSID' is disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines if the Wireless Local Area Networks (WLANs) Service Set Identifier (SSID) is broadcast. The recommended setting is disabled.

Rationale:

Though it doesn't prevent an attacker from detecting the network, disabling broadcast Service Set Identifiers (SSIDs) will prevent casual users from seeing it on client side network lists. Disabling broadcast SSID will also make the identification of wireless networks more difficult.

Audit:

To validate that broadcast SSIDs are disabled,

1. Run the following command;

```
(Cisco Controller) >show wlan <WLAN ID>
```

2. Check the output for the status of Broadcast SSID for each WLAN. This should be set to Disabled.

```
Broadcast SSID.................................. Disabled
```

Remediation:

1. Determine the WLANs to which the change will be made:

```
(Cisco Controller) >show wlan summary
```

2. Disable broadcast SSID on all WLANs using:

```
(Cisco Controller) >config wlan broadcast-ssid disable <WLAN ID>
```

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp8366770

2.2 Ensure 'WPA2-Enterprise' is Enabled for configured 'Wireless LAN identifiers' (Not Scored)

Profile Applicability:

- Level 1

Description:

This control determines if configured Wireless Local Area Networks (WLANs) are configured to use Wi-Fi Protected Access 2 (WPA2) security protocol. The recommended setting is to enable WPA2 and 802.1x for configured Wireless LAN identifiers (WLAN IDs).

Rationale:

Alternative encryption and authentication methods for connecting wireless clients to the wireless network have drawbacks. WEP has been proven ineffective and methods using pre-shared keys could be defeated by rainbow tables. 802.11i provides authenticated access using 802.1x and EAPoL and encryption using AES-based encryption.

Audit:

1. Run the following command to display a list of WLAN IDs managed by the device:

```
(Cisco Controller) >show wlan summary
```

2. Run the following command for each WLAN ID:

```
(Cisco Controller) >show wlan <WLAN ID>
```

3. Ensure WPA2 is enabled.

```
     WPA2 (RSN IE)............................. Enabled
        AES Cipher............................. Enabled
        802.1x................................. Enabled
```

Remediation:

Run the following command for each WLAN ID when WPA2 is not enabled.

```
(Cisco Controller) >config wlan security wpa2 enable <WLAN ID>
```

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp4891599

2.3 Ensure 'Peer-to-Peer Blocking Action' is set to 'Drop' for All 'Wireless LAN Identifiers' (Scored)

Profile Applicability:

- Level 1

Description:

This control determines whether the Wireless LAN Controller is configured to prevent clients connected to the same Wireless Local Area Controller from communicating with each other.

Rationale:

Wireless Client Isolation prevents wireless clients from communicating with each other over the RF. Packets that arrive on the wireless interface are forwarded only out the wired interface of an Access Point. One wireless client could potentially compromise another client sharing the same wireless network.

Audit:

1. Determine which WLANs will be audited:

```
(Cisco Controller) >show wlan summary
```

2. To validate if peer-to-peer blocking is enabled on a WLAN, run the following command:

```
(Cisco Controller) >show wlan <WLAN ID>
```

3. Validate that the Peer-to-Peer Blocking Action is set to either **Drop** or **Forward-Upstream**.

```
Peer-to-Peer Blocking Action..................... Drop
```

Remediation:

1. Determine which WLANs will be changed:

```
(Cisco Controller) >show wlan summary
```

2. Enable client isolation or Publicly Secure Packet Forwarding on WLANs:

```
(Cisco Controller) >config wlan peer-blocking drop <WLAN ID>
```

References:

1. http://www.cisco.com/en/US/docs/wireless/controller/7.0/command/reference/cli70commands.html#wp10562677

Appendix: Change History

Date	Version	Changes for this version
10-16-2012	1.0.0	Initial release.