

Trusted AP Policies on a Wireless LAN Controller

Document ID: 100368

Introduction

Prerequisites

Requirements

Conventions

Trusted AP Policies

What is a Trusted AP?

How to Configure an AP as a Trusted AP from the WLC GUI?

Understanding Trusted AP Policy Settings

How to Configure Trusted AP Policies on the WLC?

Trusted AP Policy Violation Alert Message

Related Information

Introduction

This document describes the *trusted AP* wireless protection policies on a Wireless LAN Controller (WLC), defines trusted AP policies, and provides a brief description of all trusted AP policies.

Prerequisites

Requirements

Ensure that you have a basic understanding of Wireless LAN security parameters (such as SSID, encryption, authentication, and so on).

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Trusted AP Policies

Trusted AP policies is a security feature in the controller that is designed to be used in scenarios where customers have a parallel autonomous AP network along with the controller. In that scenario, the autonomous AP can be marked as the trusted AP on the controller, and the user can define policies for these trusted APs (which should use only WEP or WPA, our own SSID, short preamble, and so on). If any of these AP fail to meet these policies, the controller raises an alarm to the network management device (Wireless Control System) that states a trusted AP violated a configured policy.

What is a Trusted AP?

Trusted APs are APs that are not part of an organization. However, they do not cause a security threat to the network. These APs are also called friendly APs. Several scenarios exist where you might want to configure an AP as a trusted AP.

For example, you might have different categories of APs in your network such as:

- APs you own that do not run LWAPP (perhaps they run IOS or VxWorks)

- LWAPP APs that employees bring in (with the knowledge of the administrator)
- LWAPP APs used to test the existing network
- LWAPP APs that neighbors own

Normally, trusted APs are APs that fall into **category 1**, which are APs you own that do not run LWAPP. They might be old APs that run VxWorks or IOS. In order to ensure that these APs do not damage the network, certain features can be enforced, such as correct SSIDs and authentication–types. Configure the trusted AP policies on the WLC, and make sure that the trusted APs meet these policies. If not, you can configure the controller to take several actions, such as raise an alarm to the network management device (WCS).

Known APs that belong to the neighbors can be configured as trusted APs.

Normally, MFP (Management Frame Protection) should prevent APs that are not legitimate LWAPP APs from joining the WLC. If NIC cards support MFP, they are not allowed to accept deauthentications from devices other than the real APs. Refer to Infrastructure Management Frame Protection (MFP) with WLC and LAP Configuration Example for more information about MFP.

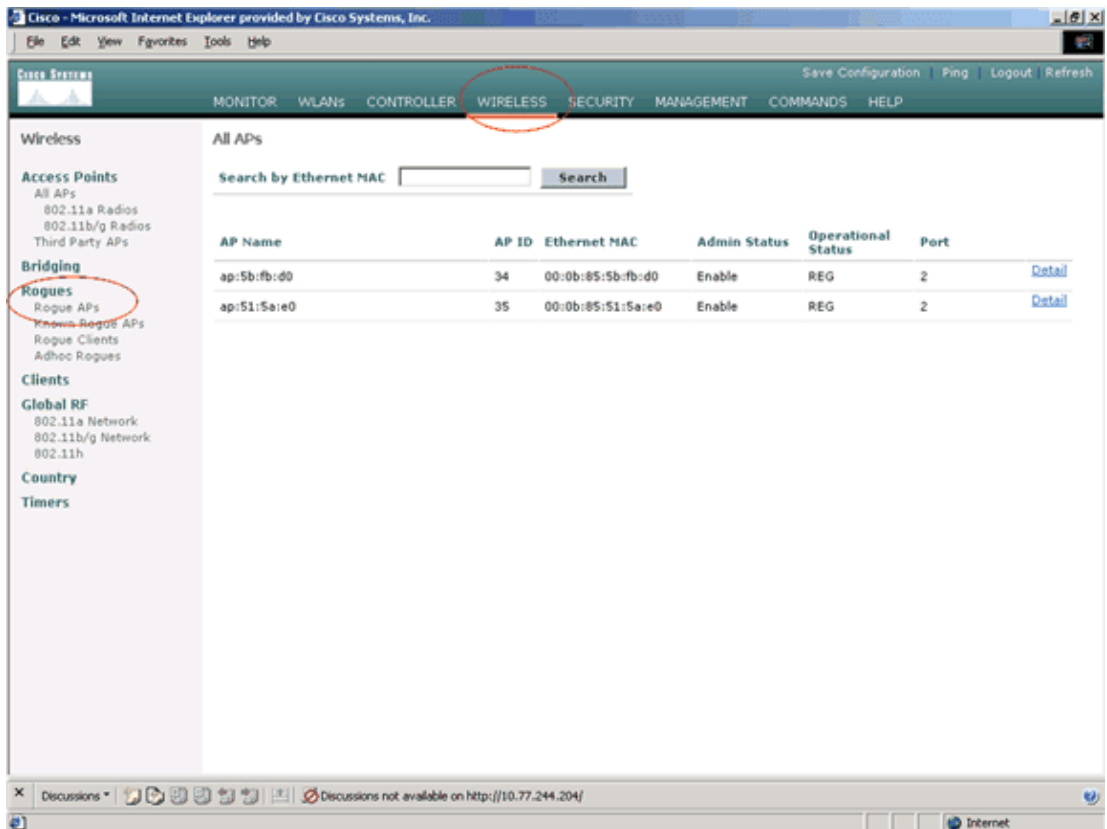
If you have APs that run VxWorks or IOS (as in category 1), they will never join the LWAPP group or do MFP, but you might want to enforce the policies listed on that page. In such cases, trusted AP policies needs to be configured on the controller for the APs of interest.

In general, if you know about a rogue AP and identify that it is not a threat to your network, you can identify that AP as a known trusted AP.

How to Configure an AP as a Trusted AP from the WLC GUI?

Complete these steps in order to configure an AP as a trusted AP:

1. Log into the GUI of the WLC through HTTP or https login.
2. From the controller main menu, click **Wireless**.
3. In the menu located on the left side of the Wireless page, click **Rogue APs**.



The Rogue APs page lists all the APs that are detected as rogue APs on the network.

- From this list of rogue APs, locate the AP that you want to configured as trusted AP that falls under category 1 (as explained in the previous section).

You can locate the APs with the MAC addresses listed on Rogue APs page. If the desired AP is not in this page, click **Next** in order to identify the AP from the next page.

- Once the desired AP is located from the Rogue AP list, click the **Edit** button that corresponds to the AP, which takes you to the detail page of the AP.

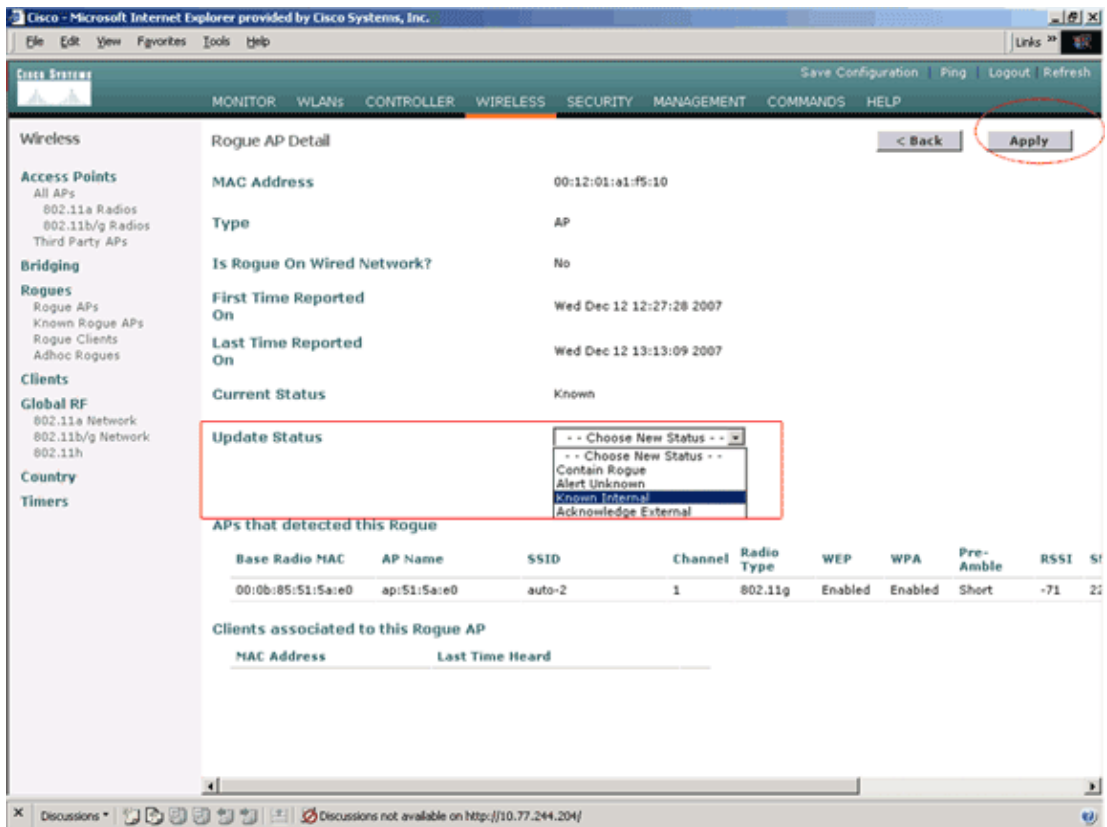
Rogue APs Items 1 to 20 of 26 **Next**

| MAC Address | SSID | # Detecting Radios | Number of Clients | Status | |
|-------------------|---------|--------------------|-------------------|---------------------|----------------------|
| 00:02:8a:0e:33:f5 | Unknown | 1 | 0 | Pending | Edit |
| 00:07:50:d5:cf:b9 | Unknown | 1 | 0 | Pending | Edit |
| 00:0b:85:51:5a:ee | Unknown | 0 | 0 | Containment Pending | Edit |
| 00:0c:85:eb:de:62 | Unknown | 1 | 0 | Alert | Edit |
| 00:0d:ed:be:f6:70 | Unknown | 2 | 0 | Alert | Edit |
| 00:12:01:a1:f5:10 | auto-2 | 1 | 0 | Pending | Edit |

In the Rogue AP details page, you can find detailed information about this AP (such as whether that AP connected to wired network, as well as the current status of the AP and so on).

- In order to configure this AP as a trusted AP, select **Known Internal** from the Update Status drop-down list, and click **Apply**.

When you update the AP status to *Known Internal*, this AP is configured as the trusted AP of this network.

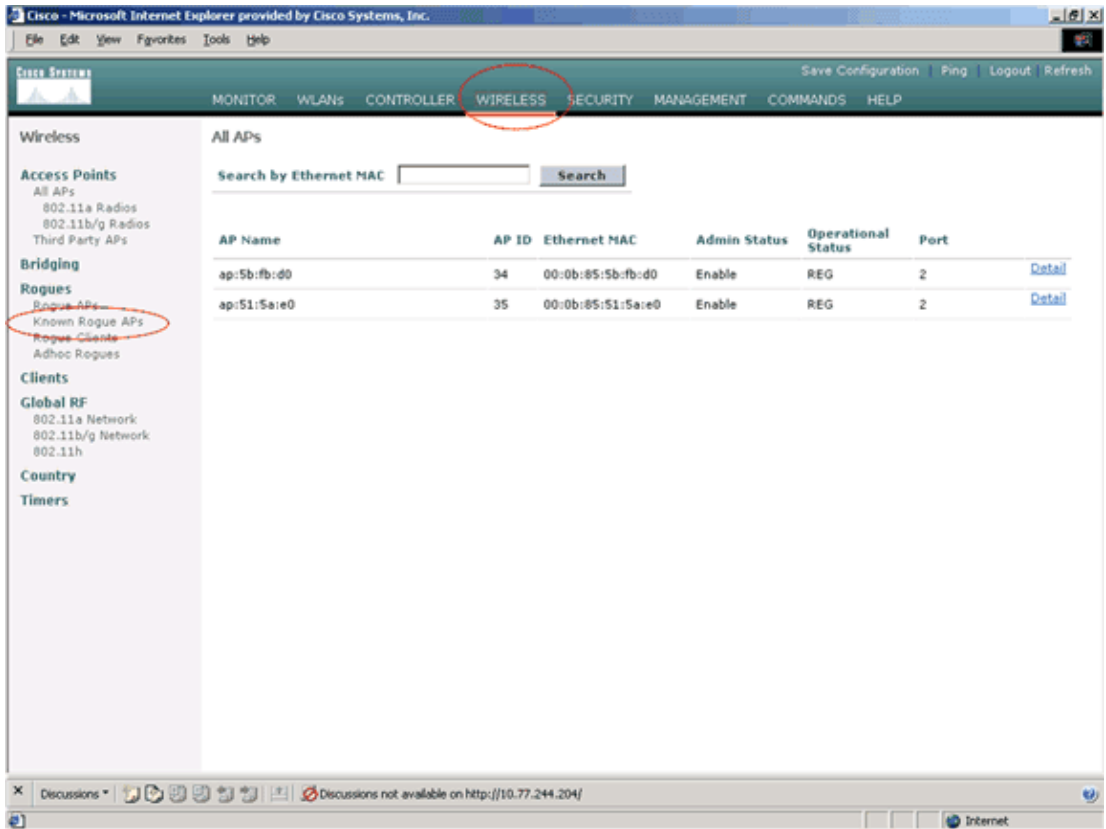


7. Repeat these steps for all APs you want to configure as trusted APs.

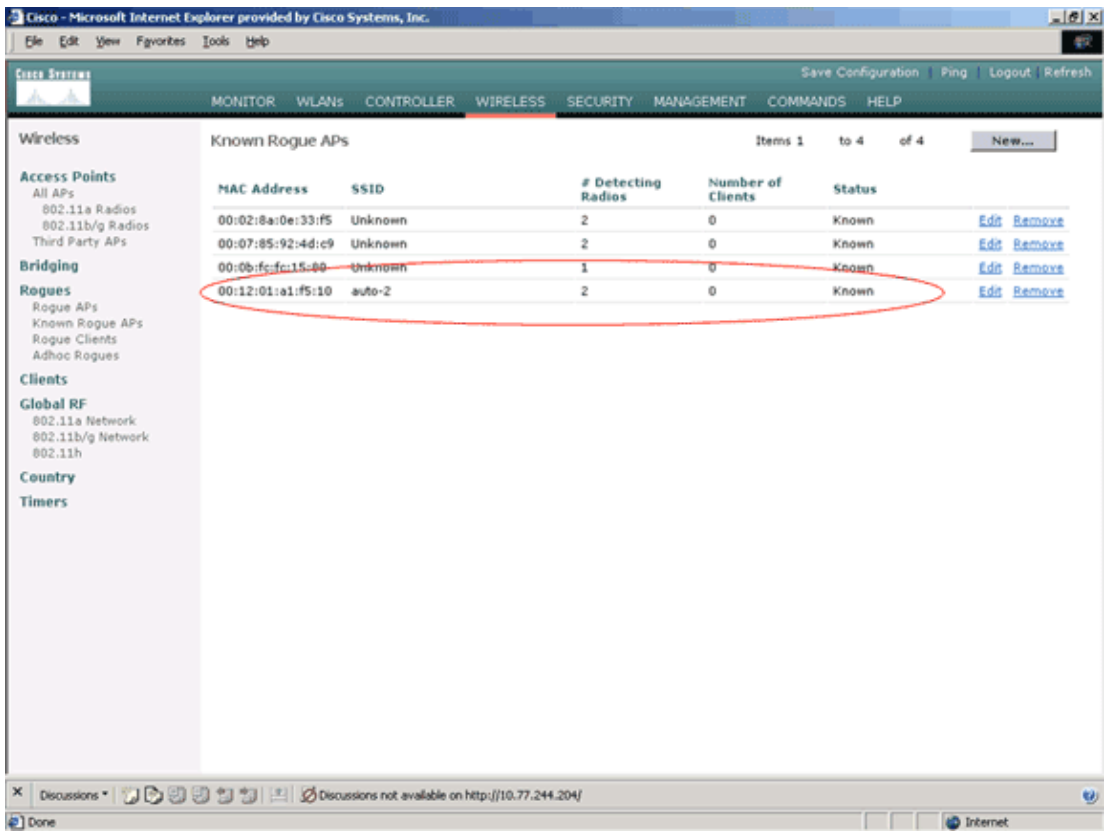
Verify the Trusted AP Configuration

Complete these steps in order to verify that the AP is correctly configured as trusted AP from the controller GUI:

1. Click **Wireless**.
2. In the menu located on the left side of the Wireless page, click **Known Rogue APs**.



The desired AP should appear on the Known Rogue APs page with the status listed as *Known*.



Understanding Trusted AP Policy Settings

The WLC has these trusted AP policies:

- Enforced Encryption Policy
- Enforced Preamble Policy
- Enforced Radio Type Policy
- Validate SSID
- Alert if trusted AP is Missing
- Expiration Timeout for Trusted AP Entries (seconds)

Enforced Encryption Policy

This policy is used to define the encryption type that the trusted AP should use. You can configure any of these encryption types under Enforced encryption policy:

- None
- Open
- WEP
- WPA/802.11i

The WLC verifies whether the encryption type configured on the trusted AP matches the encryption type configured on "**Enforced encryption policy**" setting. If the trusted AP does not use the designated encryption type, the WLC raises an alarm to the management system in order to take appropriate actions.

Enforced Preamble Policy

The radio preamble (sometimes called a header) is a section of data at the head of a packet that contains information that wireless devices need when they send and receive packets. **Short** preambles improve throughput performance, so they are enabled by default. However, some wireless devices, such as SpectraLink NetLink phones, require **long** preambles. You can configure any of these preamble options under Enforced preamble policy:

- None
- Short
- Long

The WLC verifies whether the Preamble type configured on the trusted AP matches the preamble type configured on "**Enforced preamble policy**" setting. If the trusted AP does not use the specified preamble type, the WLC raises an alarm to the management system in order to take appropriate actions.

Enforced Radio Type Policy

This policy is used to define the radio type that the trusted AP should use. You can configure any of these Radio types under Enforced radio type policy:

- None
- 802.11b only
- 802.11a only
- 802.11b/g only

The WLC verifies whether the radio type configured on the trusted AP matches the radio type configured on "**Enforced radio type policy**" setting. If the trusted AP does not use the specified radios, the WLC raises an alarm to the management system in order to take appropriate actions.

Validate SSID

You can configure the controller to validate a trusted APs SSID against the SSIDs configured on the controller. If the trusted APs SSID matches one of the controller SSIDs, the controller raises an alarm.

Alert if Trusted AP is Missing

If this policy is enabled, the WLC alerts the management system if the trusted AP is missing from the known Rogue APs list.

Expiration Timeout for Trusted AP Entries (Seconds)

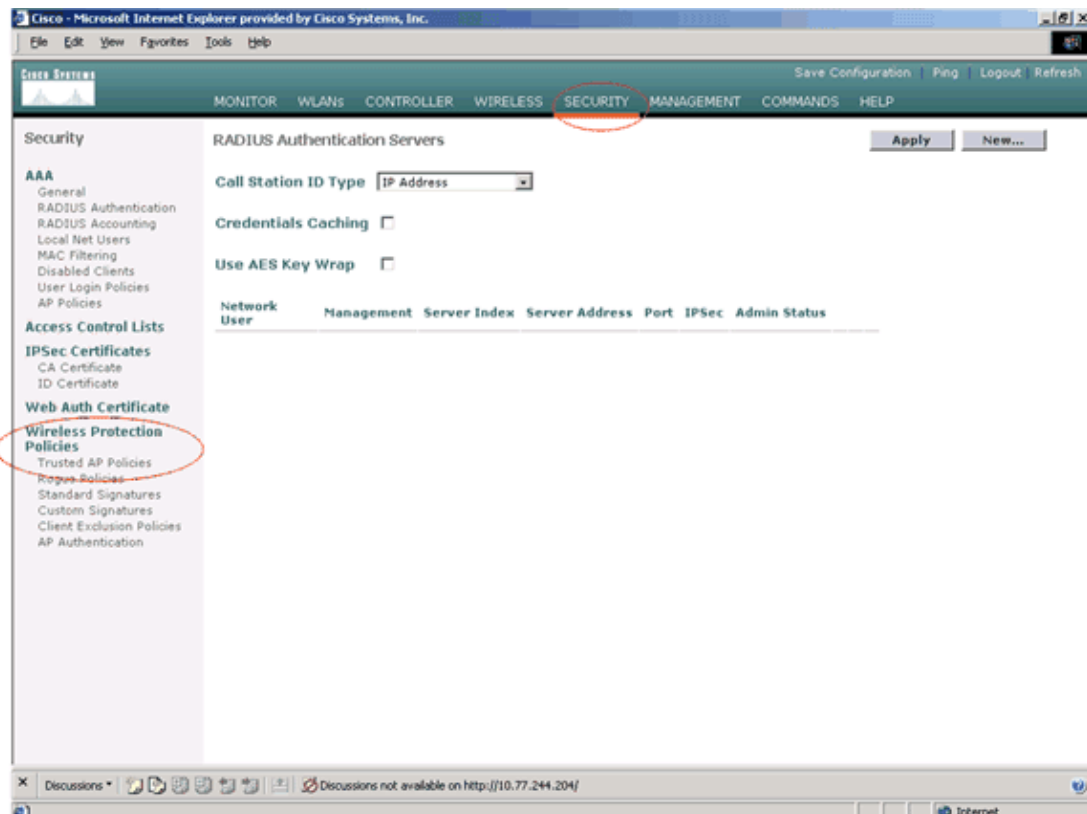
This Expiration Timeout value specifies the number of seconds before the trusted AP is considered expired and flushed from the WLC entry. You can specify this timeout value in seconds (120 – 3600 seconds).

How to Configure Trusted AP Policies on the WLC?

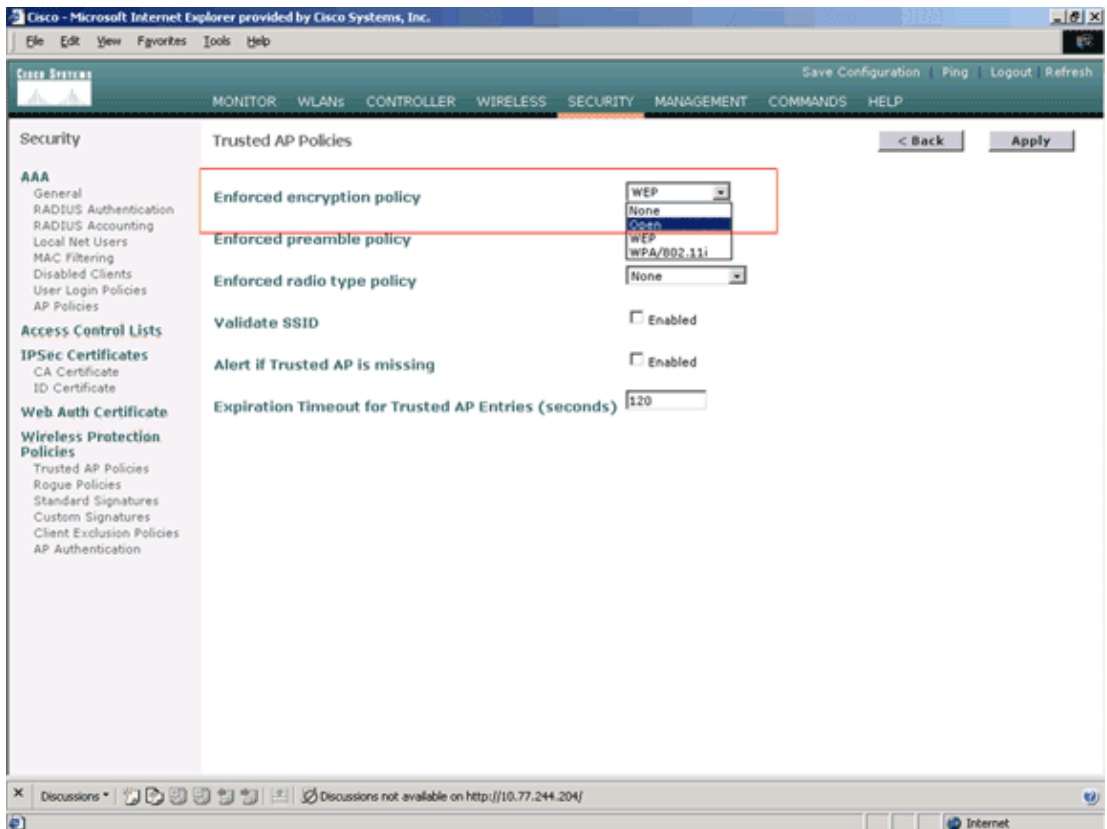
Complete these steps in order to configure trusted AP policies on the WLC through the GUI:

Note: All the trusted AP policies reside on the same WLC page.

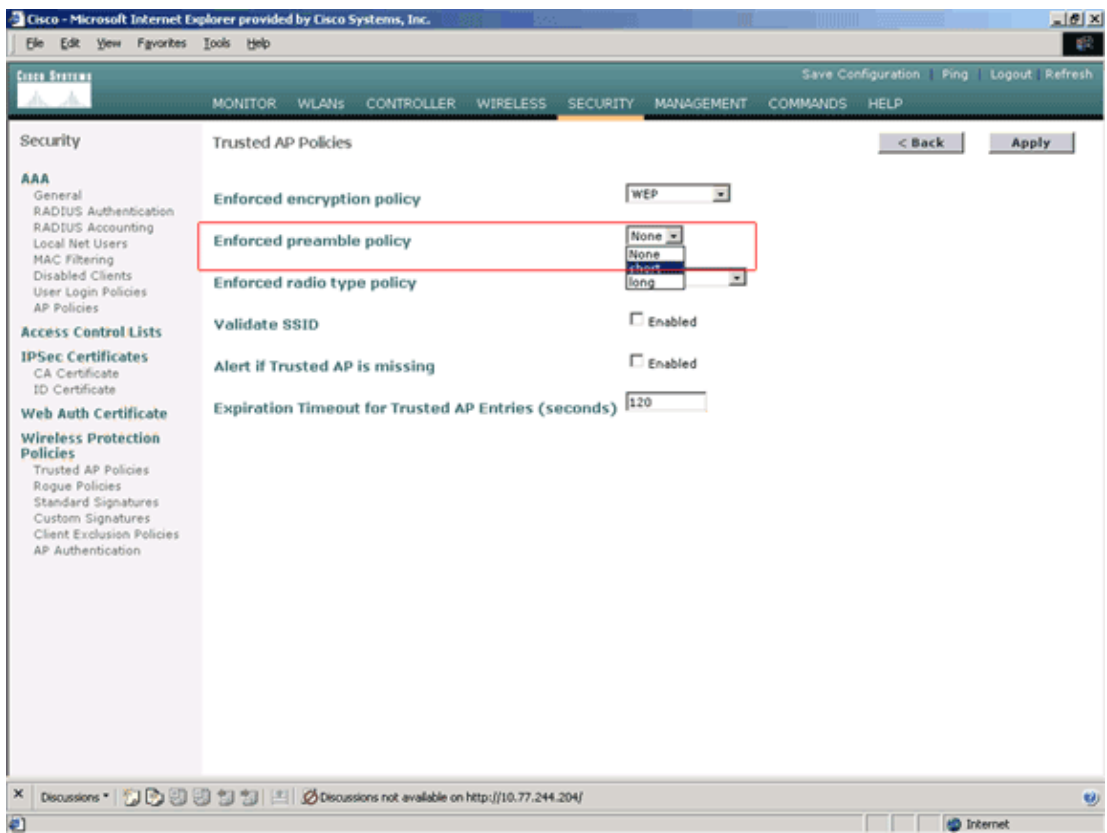
1. From the WLC GUI main menu, click **Security**.
2. From the menu located on the left side of the Security page, click **Trusted AP policies** listed under the Wireless Protection Policies heading.



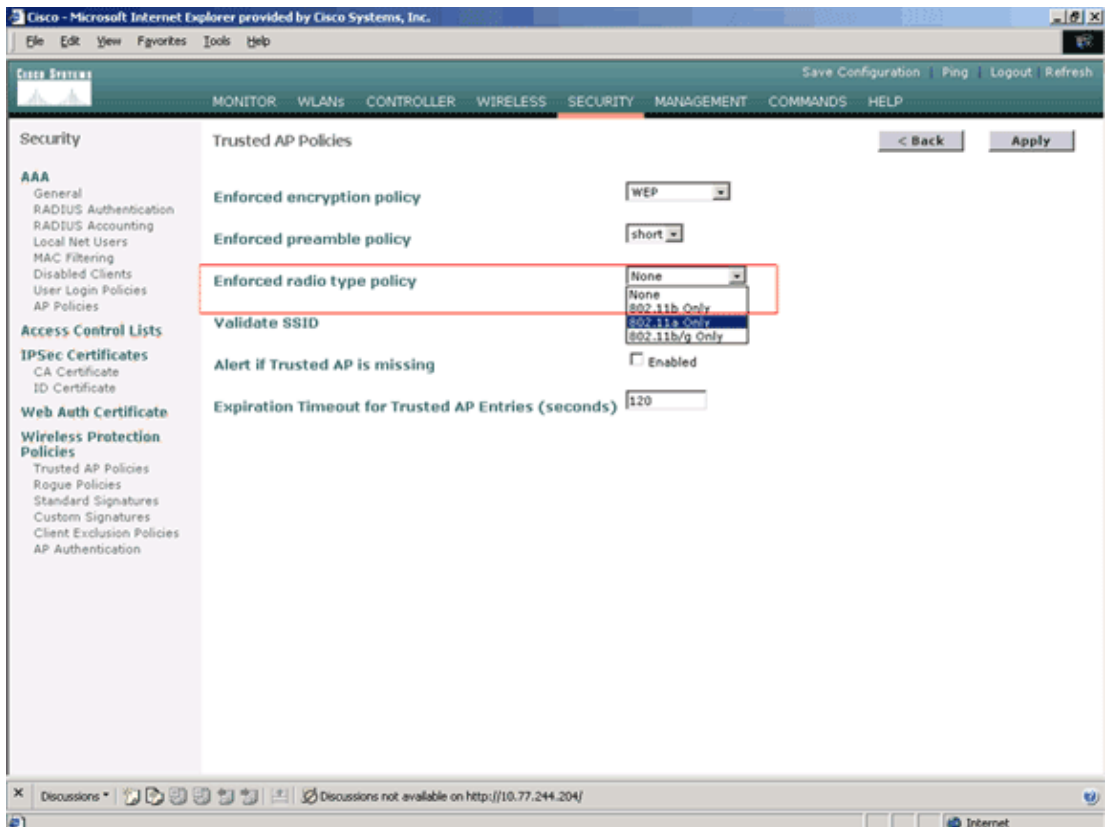
3. On the Trusted AP policies page, select the desired encryption type (None, Open, WEP, WPA/802.11i) from the Enforced encryption policy drop-down list.



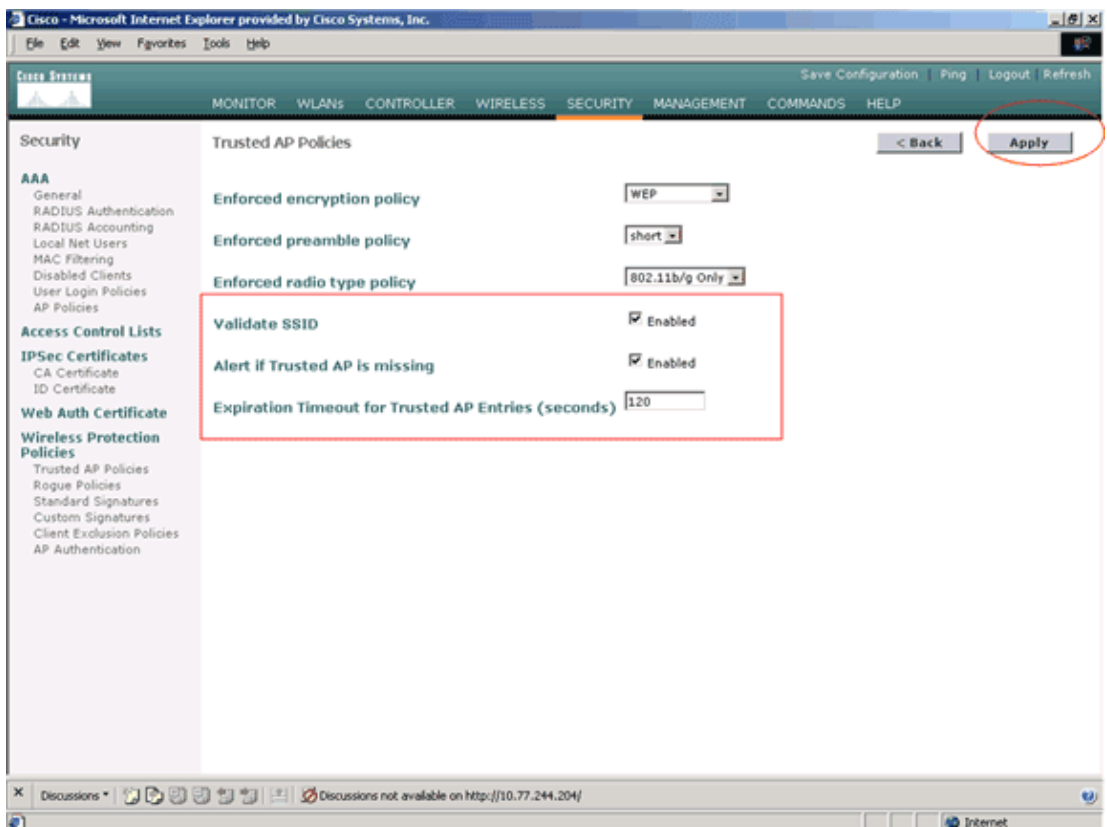
4. Select the desired preamble type (None, Short, Long) from the Enforced preamble type policy drop-down list.



5. Select the desired radio type (None, 802.11b only, 802.11a only, 802.11b/g only) from the Enforced radio type policy drop-down list.



6. Check or uncheck the **Validate SSID Enabled** check box in order to enable or disable the Validate SSID setting.
7. Check or uncheck the **Alert if trusted AP is missing Enabled** check box in order to enable or disable the Alert if trusted AP is missing setting.
8. Enter a value (in seconds) for the **Expiration Timeout for Trusted AP entries** option.



9. Click **Apply**.

Note: In order to configure these settings from the WLC CLI, you can use the **config wps trusted-ap** command with the appropriate policy option.

```
Cisco Controller) >config wps trusted-ap ?
```

```
encryption    Configures the trusted AP encryption policy to be enforced.
missing-ap    Configures alert of missing trusted AP.
preamble      Configures the trusted AP preamble policy to be enforced.
radio         Configures the trusted AP radio policy to be enforced.
timeout       Configures the expiration time for trusted APs, in seconds.
```

Trusted AP Policy Violation Alert Message

Here is an example of trusted AP policy violation alert message shown by the controller.

```
Thu Nov 16 12:39:12 2006 [WARNING] apf_rogue.c 1905: Possible AP
impersonation of xx:xx:xx:xx:xx:xx, using source address of
00:16:35:9e:6f:3a, detected by 00:17:df:7d:e1:70 on slot 0
Thu Nov 16 12:39:12 2006 [SECURITY] apf_rogue.c 1490: Trusted AP Policy
failed for AP xx:xx:xx:xx:xx:xx - invalid SSID 'SSID1'
Thu Nov 16 12:39:12 2006 [SECURITY] apf_rogue.c 1457: Trusted AP Policy
failed for AP xx:xx:xx:xx:xx:xx - invalid encryption type
Thu Nov 16 12:39:12 2006 Previous message occurred 6 times
```

Notice the highlighted error messages here. These error messages indicate that the SSID and the encryption type configured on the trusted AP do not match the Trusted AP policy setting.

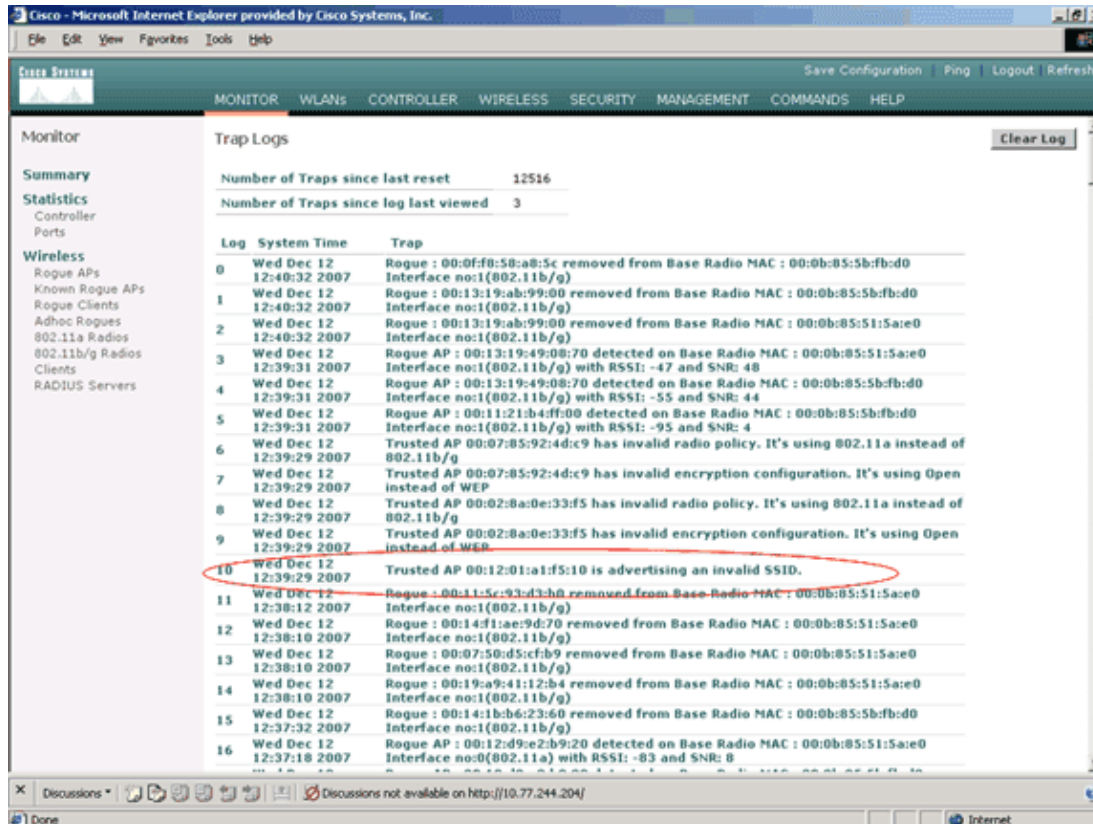
The same alert message can be seen from the WLC GUI. In order to view this message, go to the WLC GUI main menu, and click **Monitor**. In the Most Recent Traps section of the Monitor page, click **View All** in order to view all recent alerts on the WLC.

The screenshot shows the Cisco WLC GUI Monitor page. The 'Monitor' tab is selected. The page displays several summary sections:

- Controller Summary:** Management IP Address: 10.77.244.204, Service Port IP Address: 0.0.0.0, Software Version: 3.2.150.10, System Name: WLC-4400-TSWEB, Up Time: 16 days, 8 hours, 42 minutes, System Time: Wed Dec 12 12:40:03 2007, Internal Temperature: +38 C, 802.11a Network State: Enabled, 802.11b/g Network State: Enabled.
- Access Point Summary:** Table with columns: Total, Up, Down. Rows: 802.11a Radios (2 Up, 0 Down), 802.11b/g Radios (2 Up, 0 Down), All APs (2 Up, 0 Down).
- Client Summary:** Current Clients: 6, Excluded Clients: 0, Disabled Clients: 0.
- Rogue Summary:** Active Rogue APs: 25, Active Rogue Clients: 0, Adhoc Rogues: 0, Rogues on Wired Network: 0.
- Top WLANs:** Table with columns: WLAN, # of Clients by SSID. Rows: WCS (0), WCS123 (0).
- Most Recent Traps:** List of traps including: Rogue AP : 00:13:19:49:08:70 detected on Base Radio, Rogue AP : 00:13:19:49:08:70 detected on Base Radio I, Rogue AP : 00:11:21:b4:ff:00 detected on Base Radio I, **Trusted AP 00:07:85:92:4d:c9 has invalid radio policy. I**, **Trusted AP 00:07:85:92:4d:c9 has invalid encryption co**.

The 'View All' link in the 'Most Recent Traps' section is circled in red. The status bar at the bottom indicates 'Discussions not available on http://10.77.244.204/'.

On the Most Recent Traps page, you can identify the controller that generates the trusted AP policy violation alert message as shown in this image:



Related Information

- [Cisco Wireless LAN Controller Configuration Guide, Release 5.2 – Enabling Rogue Access Point Detection in RF Groups](#)
- [Cisco Wireless LAN Controller Configuration Guide, Release 4.0 – Configuring Security Solutions](#)
- [Rogue Detection under Unified Wireless Networks](#)
- [SpectraLink Phone Design and Deployment Guide](#)
- [Basic Wireless LAN Connection Configuration Example](#)
- [Troubleshooting Connectivity in a Wireless LAN Network](#)
- [Authentication on Wireless LAN Controllers Configuration Examples](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 07, 2009

Document ID: 100368