# Политики для доверенных точек доступа на контроллере беспроводной сети

## Содержание



## Введение

Этот документ описывает *доверяемую* политику обеспечения защиты радио *AP* по Контроллеру беспроводной локальной сети (WLC), определяет политику AP, которой доверяют и предоставляет краткое описание всей доверяемой политики AP.

## Предварительные условия

### Требования

Гарантируйте, что у вас есть основное понимание параметров Безопасности беспроводной локальной сети (таких как SSID, шифрование, аутентификация, и так далее).

### Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

## Доверяемая политика AP

Доверяемая политика AP является характеристикой безопасности в контроллере, который разработан, чтобы использоваться в сценариях, где у клиентов есть параллельная автономная сеть AP наряду с контроллером. В том сценарии автономный AP может быть отмечен как доверяемый AP на контроллере, и пользователь может определить политику

для этих доверяемых AP (который должен использовать только WEP или WPA, наш собственный SSID, короткую преамбулу, и так далее). Если какой-либо из них сбой AP для совещания этой политики контроллер выдает аварийный сигнал к устройству управления сетью (беспроводная Система управления), который сообщает, что доверяемый AP нарушил настроенную политику.

## Что такое Доверяемый AP?

Доверяемые AP являются AP, которые не являются частью организации. Однако они не вызывают угрозу безопасности к сети. Эти AP также называют дружественными AP. Несколько сценариев существуют, где вы могли бы хотеть настроить AP как доверяемый AP.

Например, у вас могли бы быть другие категории AP в вашей сети, такие как:

- **AP, которыми вы владеете, которые не выполняют LWAPP (возможно, они выполняют IOS или VxWorks),**
- AP LWAPP, которые сотрудники вводят (со знанием администратора)
- AP LWAPP использовали тестировать существующую сеть
- AP LWAPP, который граничит собственный

Обычно, доверяемые AP являются AP, которые попадают **в категорию 1**, которые являются AP, которыми вы владеете, которые не выполняют LWAPP. Они могли бы быть старыми AP, которые выполняют VxWorks или IOS. Чтобы гарантировать, что эти AP не повреждают сеть, определенные функции могут быть принуждены, такие как корректный SSIDs и типы проверки подлинности. Настройте доверяемую политику AP по WLC и удостоверьтесь, что доверяемые AP встречают эту политику. В противном случае можно настроить контроллер для принятия нескольких мер, тех, которые выдают аварийный сигнал к устройству управления сетью (WCS).

Известные AP, которые принадлежат соседним узлам, могут быть настроены как AP, которым доверяют.

Обычно, MFP (Защита Кадра управления) должен предотвратить AP, которые не являются легитимными AP LWAPP от присоединения к WLC. Если платы NIC поддерживают MFP, им не разрешают принять deauthentications от устройств кроме реальных AP. См. защиту кадров управления (MFP) Инфраструктуры с WLC и Примером конфигурации LAP для получения дополнительной информации о MFP.

Если у вас будут AP, которые выполняют VxWorks или IOS (как в категории 1), то они никогда не будут присоединяться к группе LWAPP или делать MFP, но вы могли бы хотеть принудить политику, перечисленную на той странице. В таких случаях политика AP, которой доверяют, должна быть настроена на контроллере для AP интереса.

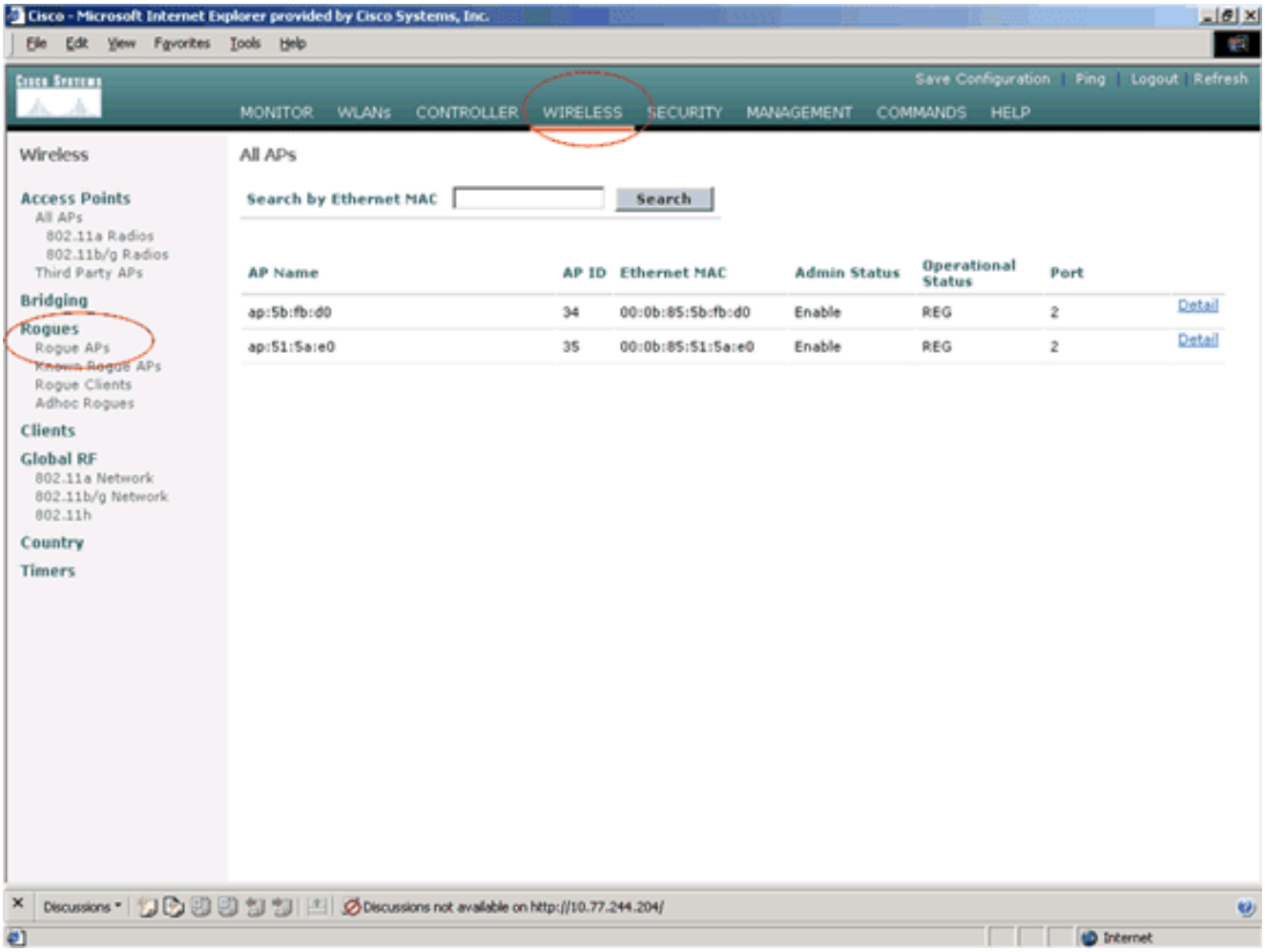
В целом, если вы знаете о постороннем AP и определяете это, это не угроза вашей сети, можно определить тот AP, поскольку известное доверяло AP.

## Как настроить AP как доверяемый AP от GUI WLC?

Выполните эти шаги для настройки AP как доверяемого AP:

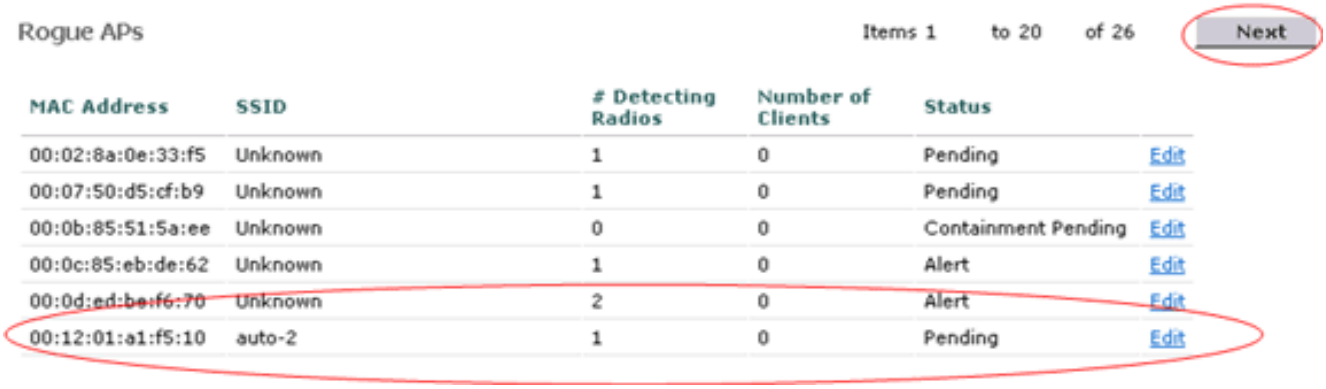
1. Войдите в GUI WLC посредством входа в систему https или HTTP.

2. Из главного меню контроллера нажмите **Wireless**.
3. В меню, расположенном на левой части theWireless страницы, нажмите **Rogue APs**.




Страница Rogue APs перечисляет все AP, которые обнаружены как посторонние AP в сети.

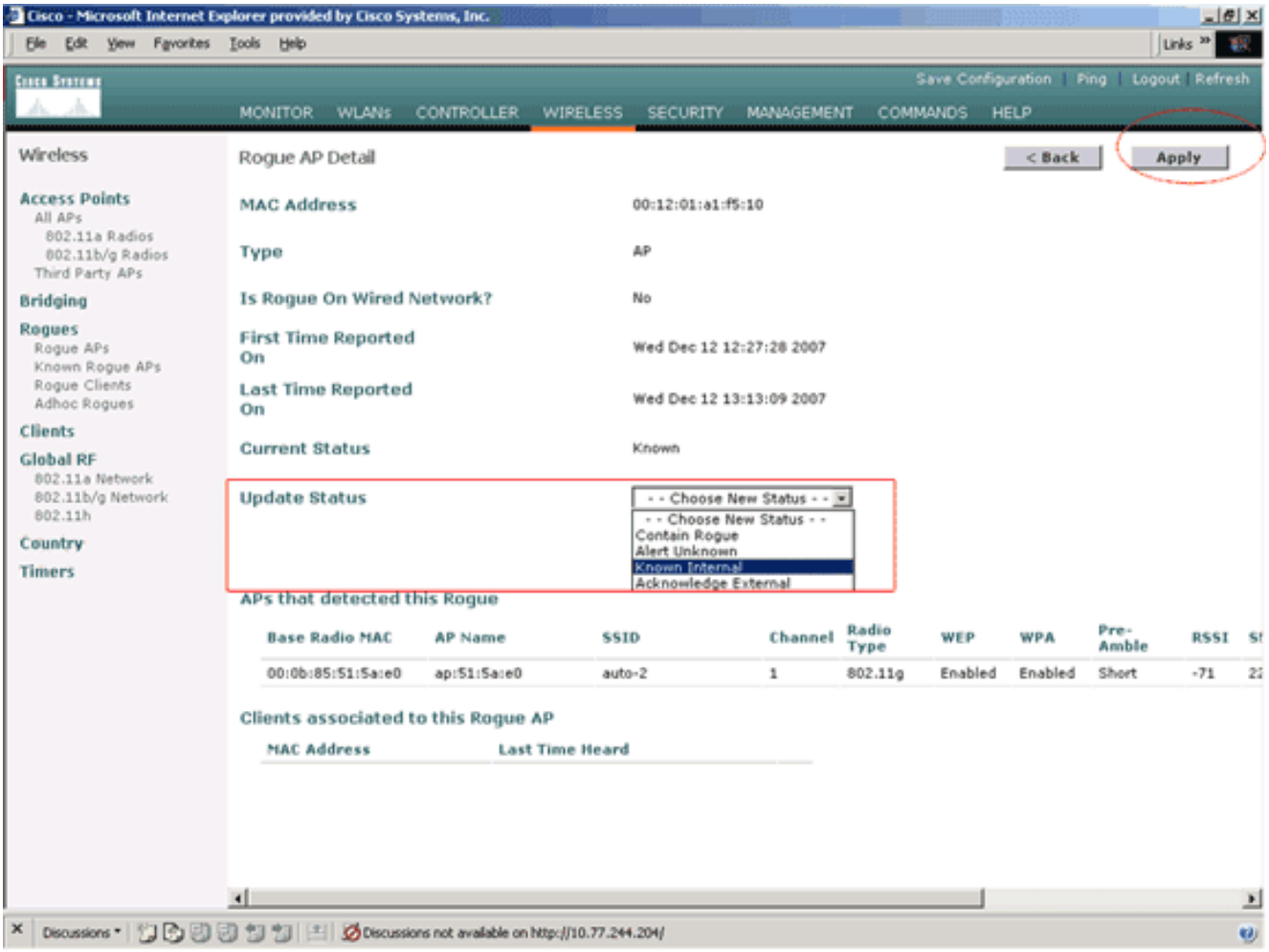
4. Из этого списка посторонних AP найдите AP, который вы хотите к настроенному как AP, которому доверяют, который подпадает под категорию 1 (как объяснено в предыдущем разделе).Можно определить местоположение AP с MAC-адресами, перечисленными на странице Rogue APs. Если желаемый AP не находится на этой странице, нажмите **Next** для определения AP от следующей страницы.
5. Как только желаемый AP расположен из Постороннего списка точек доступа, нажмите **кнопку Edit**, которая соответствует AP, который берет вас к подробной странице AP.




На Посторонней подробной странице AP можно найти подробные сведения об этом AP (такой как, соединился ли тот AP с проводной сетью, а также текущим статусом AP и

так далее).

6. Для настройки этого AP как доверяемого AP выберите **Known Internal** от выпадающего списка Состояния обновления и нажмите **Apply**.При обновлении статуса AP к *Внутреннему Известному* этот AP настроен как доверяемый AP этой сети.

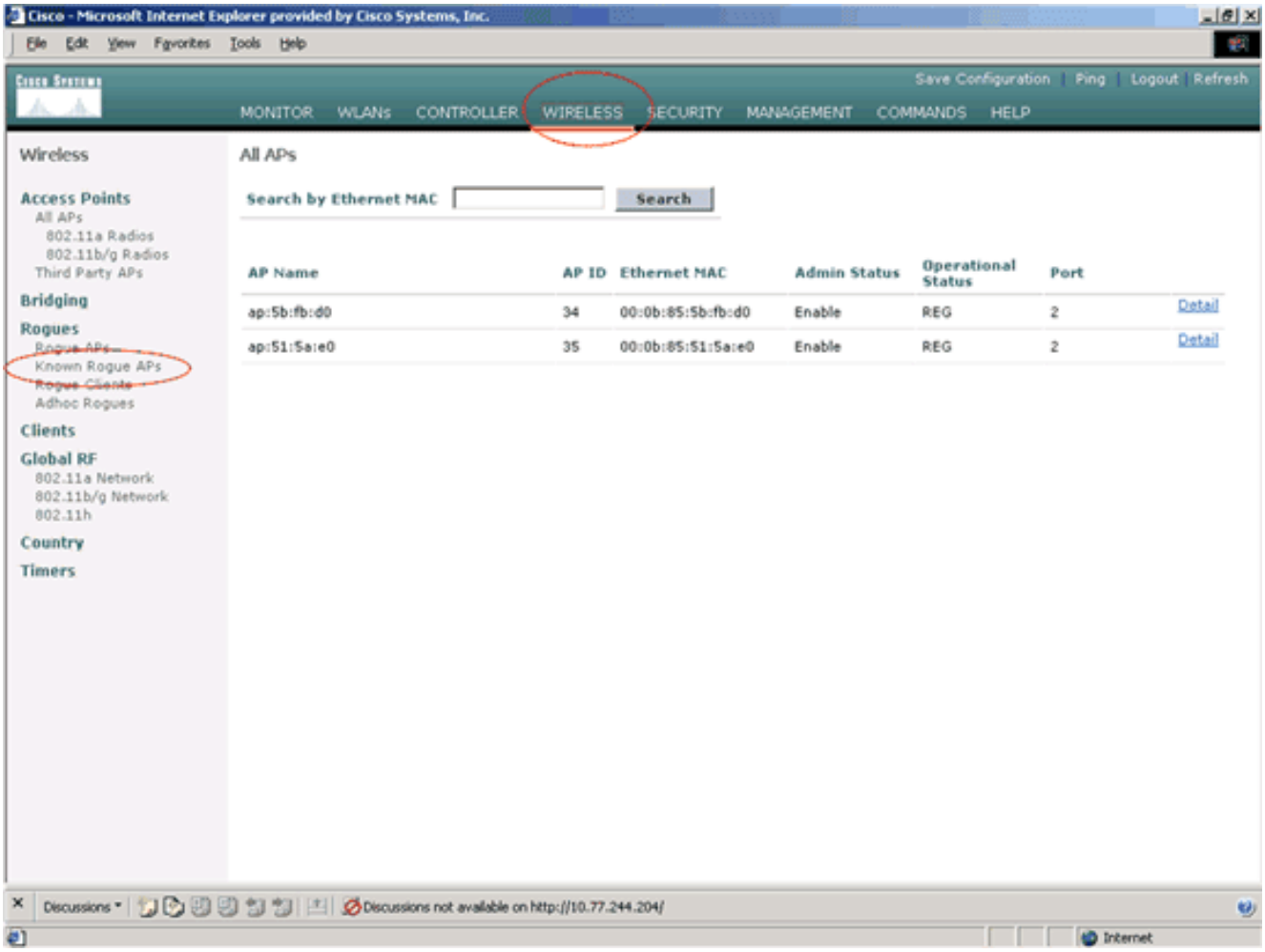



7. Повторите эти шаги для всех AP, которые вы хотите настроить как AP, которым доверяют.

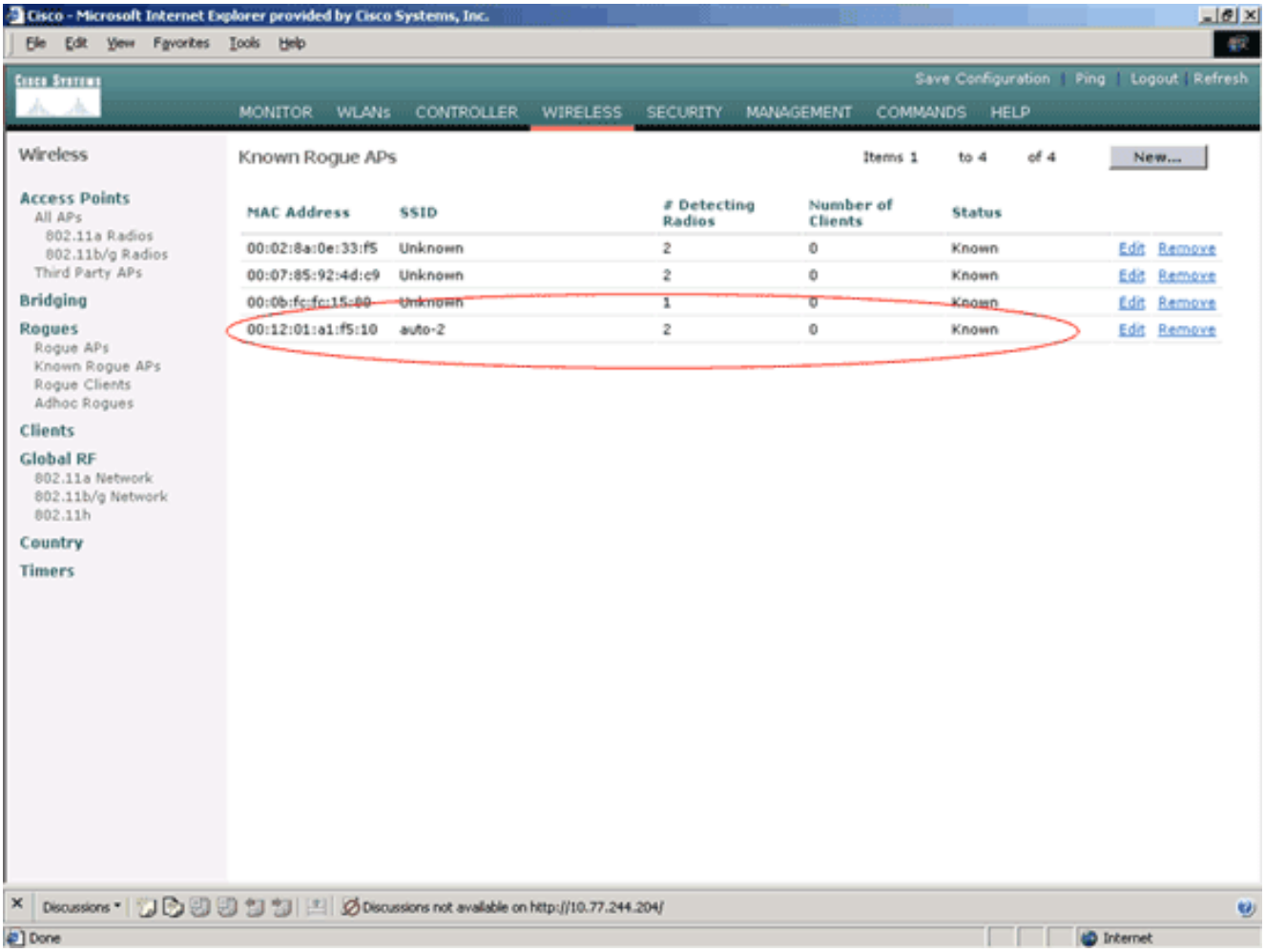
## Проверьте доверяемую конфигурацию точки доступа

Выполните эти шаги, чтобы проверить, что AP правильно настроен как AP, которому доверяют, от графического интерфейса контроллера:

1. **Выберите Wireless (Беспроводные сети).**
2. В меню, расположенном на левой части theWireless страницы, нажмите **Known Rogue APs**.




Желаемый AP должен появиться на странице Known Rogue APs со статусом, перечисленным, как
*Известный*.




## Понимание параметров настройки политики AP, которым доверяют,

WLC имеет эту доверяемую политику AP:

- Вынужденная политика шифрования
- Вынужденная политика преамбулы
- Вынужденная радио-политика типа
- Проверьте SSID
- Предупреждение, если Отсутствует доверяемый AP
- Таймаут истечения для доверяемых записей AP (секунды)

### Вынужденная политика шифрования

Эта политика используется для определения типа шифрования, который должен использовать доверяемый AP. Можно настроить любой из этих типов шифрования под Вынужденной политикой шифрования:

- Нет
- Открытый
- WEP
- WPA/802.11i

WLC проверяет, совпадает ли тип шифрования, настроенный на доверяемом AP, с типом шифрования, настроенным на **"Вынужденной политике шифрования"** установка. Если доверяемый AP не использует определяемый тип шифрования, WLC выдает аварийный

сигнал к системе управления для принятия соответствующих мер.

### Вынужденная политика преамбулы

Радио-преамбула (иногда названный заголовком) является разделом данных во главе пакета, который содержит информацию, в которой нуждаются беспроводные устройства, когда они передают и получают пакеты. **Короткие** преамбулы улучшают производительность пропускной способности, таким образом, им включают по умолчанию. Однако некоторые беспроводные устройства, такие как SpectraLink NetLink звонит, потребуйте **длинных** преамбул. Можно настроить любую из этих опций преамбулы под Вынужденной политикой преамбулы:

- Нет
- Короткое замыкание
- Долгий

WLC проверяет, совпадает ли тип Преамбулы, настроенный на доверяемом AP, с типом преамбулы, настроенным на "**Вынужденной** установке" **политики преамбулы**. Если доверяемый AP не использует указанный тип преамбулы, WLC выдает аварийный сигнал к системе управления для принятия соответствующих мер.

### Вынужденная радио-политика типа

Эта политика используется для определения радио-типа, который должен использовать доверяемый AP. Можно настроить любой из этих Радио-типов под Вынужденной радио-политикой типа:

- Нет
- 802.11b только
- 802.11a только
- 802.11b/g только

WLC проверяет, совпадает ли радио-тип, настроенный на доверяемом AP, с радио-типом, настроенным на "**Вынужденной радио-**установке" **политики типа**. Если доверяемые APdoes не используют указанные радио, WLC выдает аварийный сигнал к системе управления для принятия соответствующих мер.

### Проверьте SSID

Можно настроить контроллер для проверки доверяемого SSID AP против SSIDs, настроенного на контроллере. Если доверяемый SSID AP совпадает с одним из контроллера SSIDs, контроллер выдает аварийный сигнал.

### Предупреждение, если Отсутствует Доверяемый AP

Если эта политика включена, WLC предупреждает систему управления, если доверяемый AP отсутствует в известном Постороннем списке AP.

### Таймаут истечения для доверяемых записей AP (секунды)

Это Значение таймаута Истечения задает кол-во секунд, прежде чем доверяемый AP будут

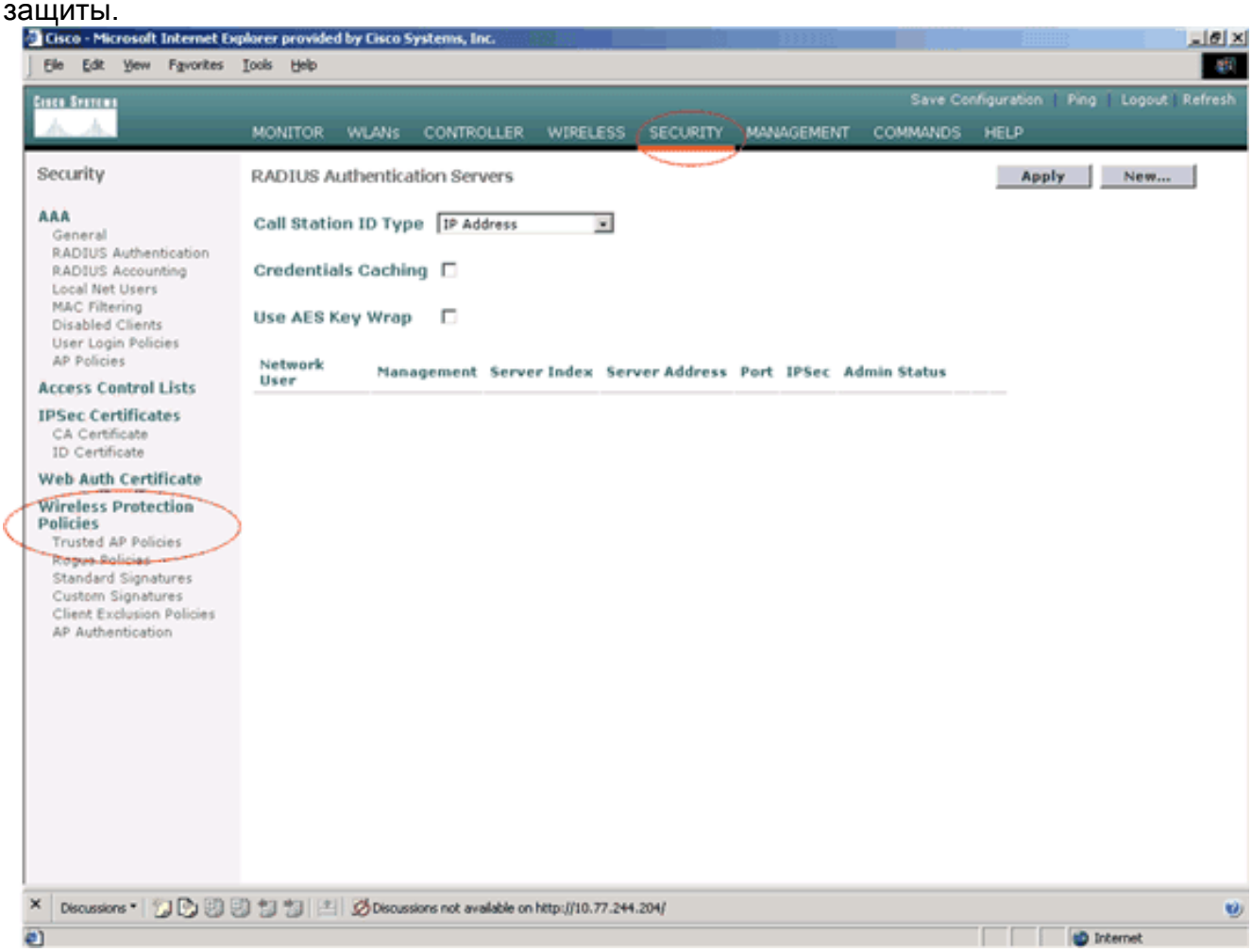
считать с истекшим сроком и вспыхнувшим от записи WLC. Можно задать это значение таймаута в секундах (120 - 3600 секунд).

## Как настроить политику AP, которой доверяют, по WLC?

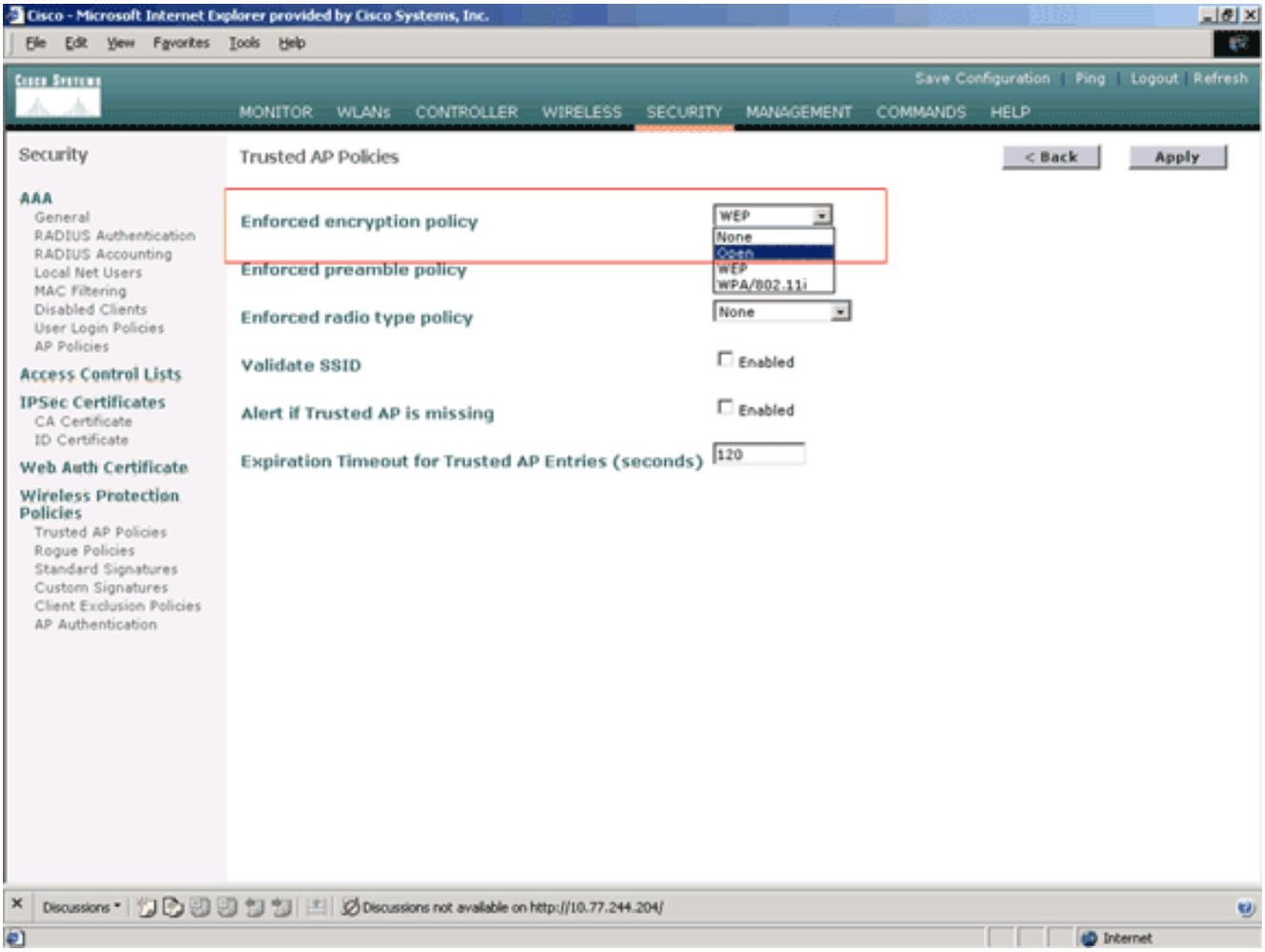
Выполните эти шаги для настройки доверяемой политики AP по WLC через GUI:

**Примечание:** Вся доверяемая политика AP находится на той же странице WLC.

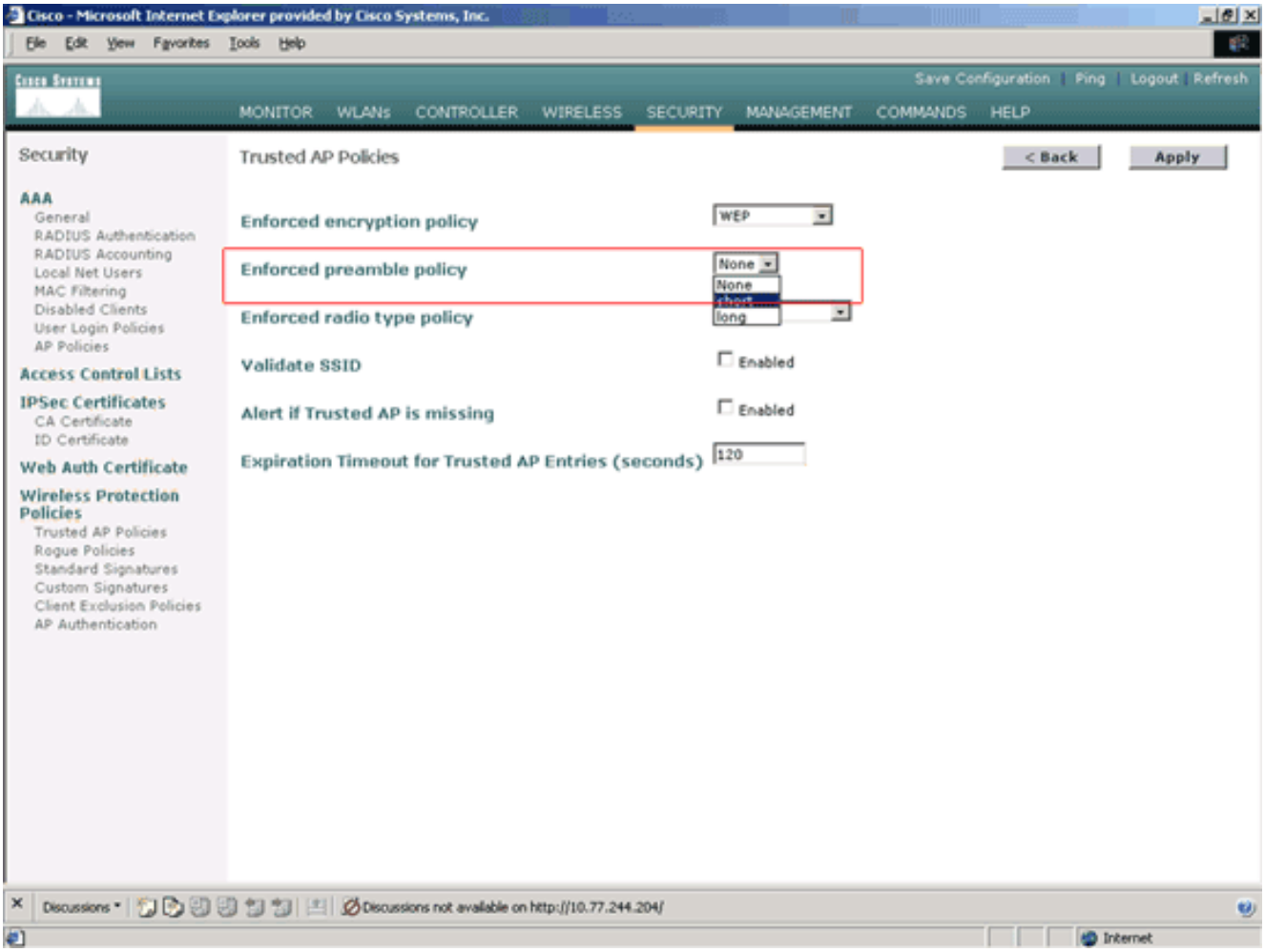
1. Из главного меню GUI WLC нажмите **Security**.
2. Из меню, расположенного на левой части страницы Security, нажмите **политику Trusted AP**, перечисленную под беспроводным заголовком Политики обеспечения защиты.



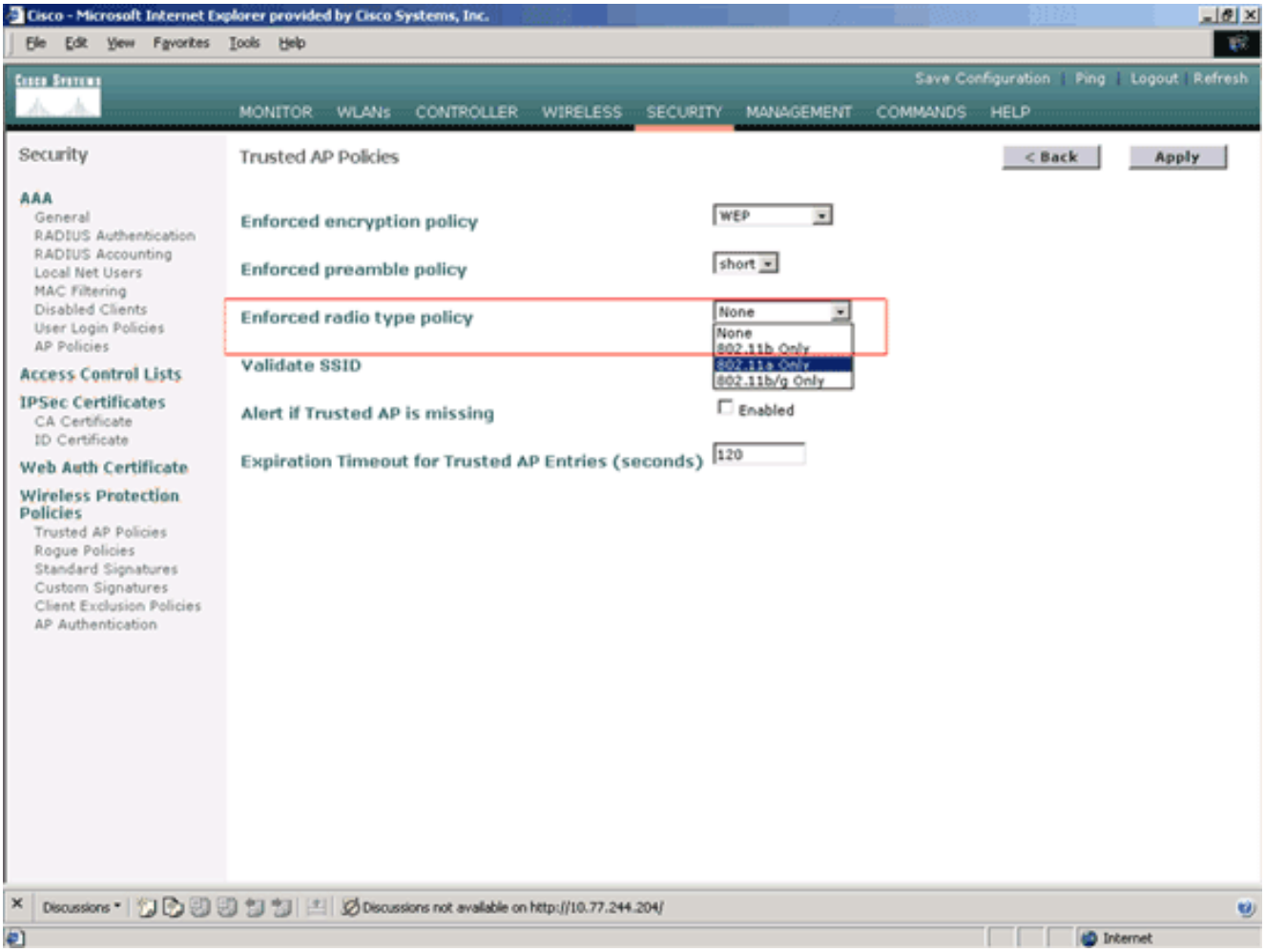

3. На Доверяемой странице политики AP выберите желаемый тип шифрования (Ни один, Открытый, WEP, WPA/802.11i) от Вынужденного выпадающего списка политики шифрования.



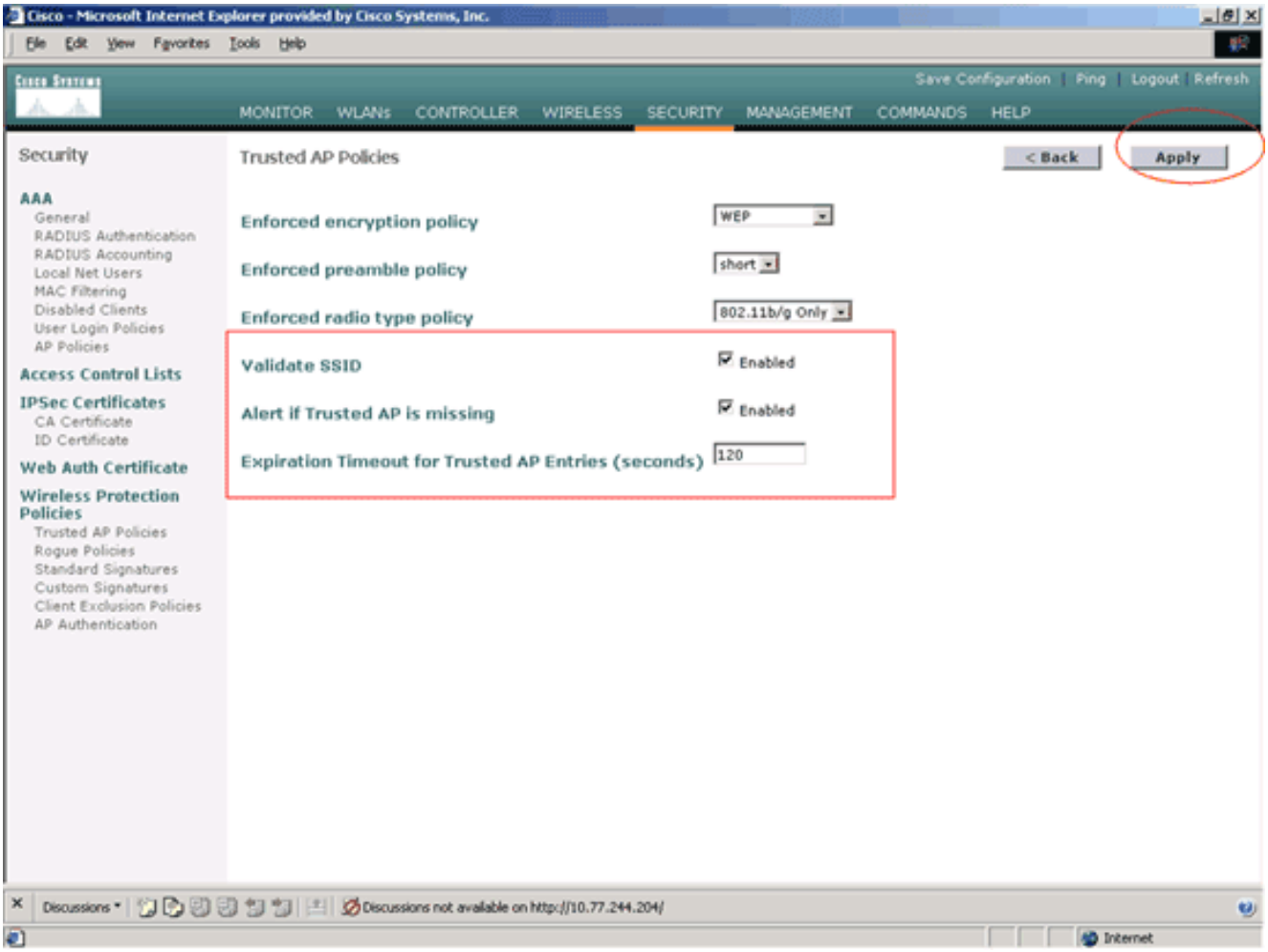

4. Выберите желаемый тип преамбулы (Ни один, короткое замыкание, Долго) из Вынужденной преамбулы вводят выпадающий список политики.




5. Выберите желаемый радио-тип (Ни один, 802.11b только, 802.11a только, 802.11b/g только) от Вынужденного радио-выпадающего списка политики типа.




6. Проверьте или снимите флажок с флажком **Validate SSID Enabled**, чтобы включить или отключить Проверить значение SSID.
7. Проверьте или снимите флажок **с Предупреждением, если доверяемый AP пропускает** флажок **Enabled**, чтобы включить или отключить Предупреждение, если доверяемый AP избегает устанавливать.
8. Введите значение (в секундах) для **Таймаута Истечения для Доверяемой** опции **записей**
**AP**.




9. **Щелкните "Применить".**

**Примечание:** Для настройки этих параметров настройки от CLI WLC можно использовать **команду config wps trusted-ap** с соответствующей опцией policy.

```
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.
```

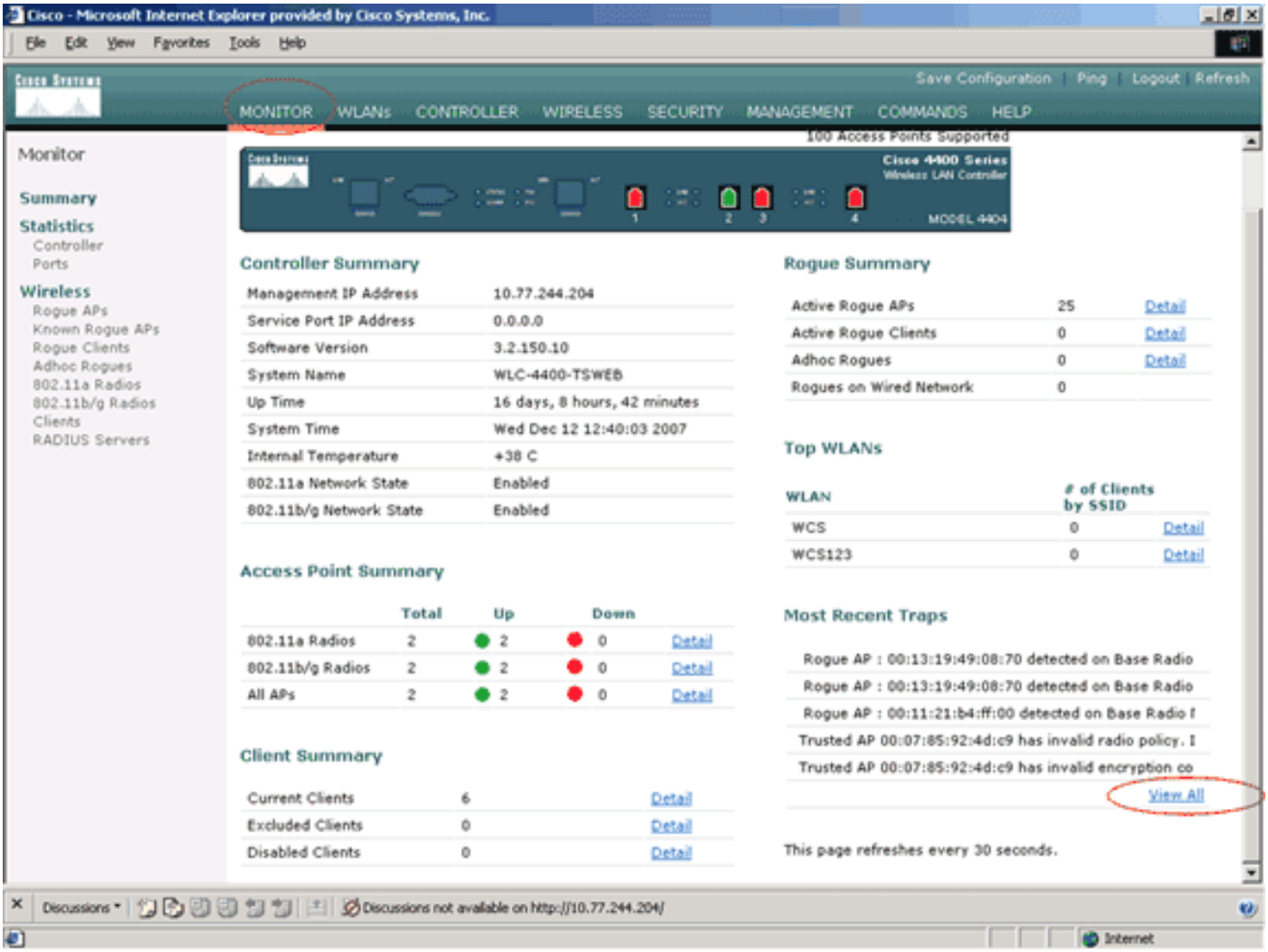
## Доверяемое сигнальное сообщение нарушения политики AP

Вот пример доверяемого сигнального сообщения нарушения политики AP, показанного контроллером.

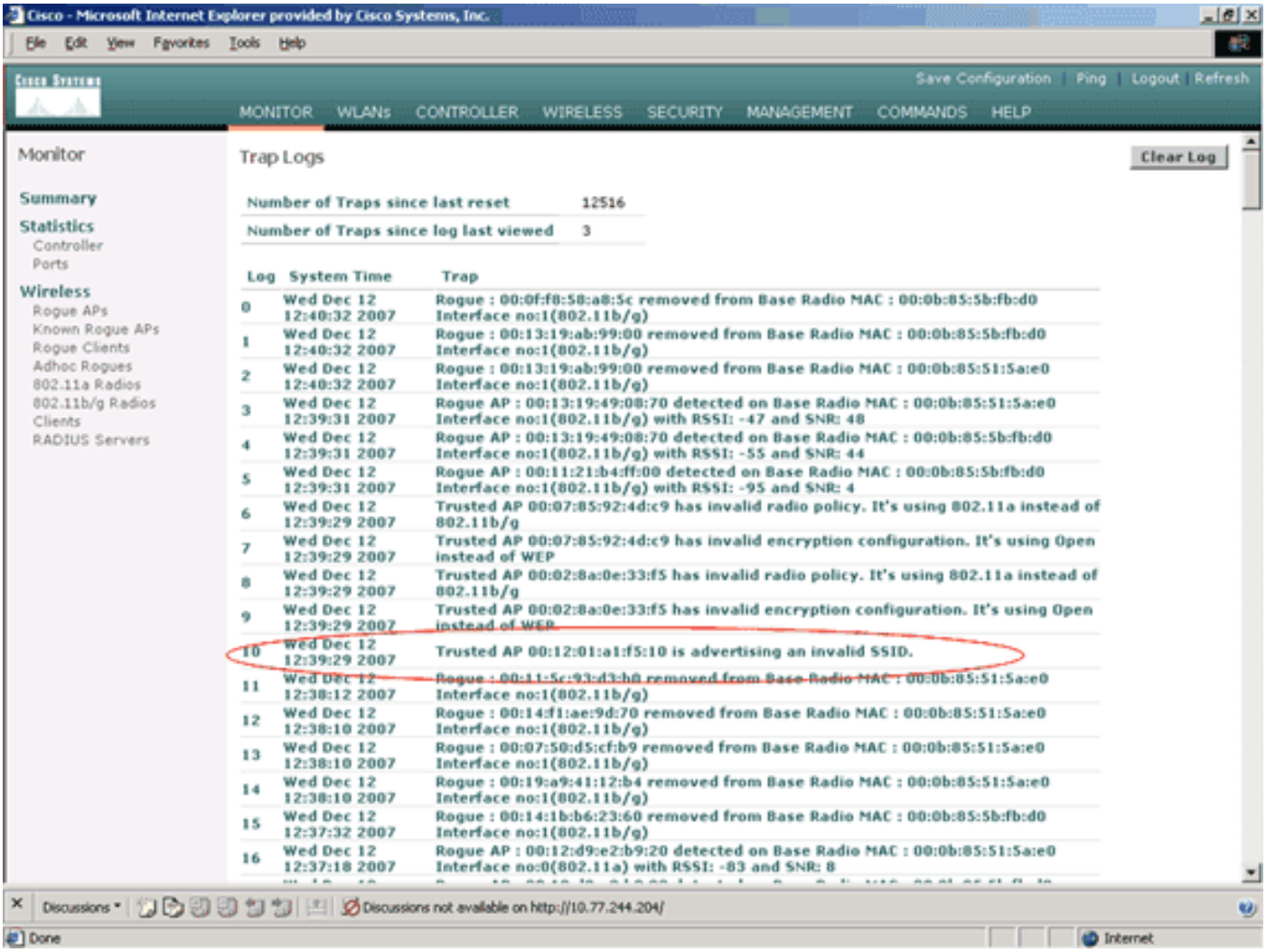
```
Thu Nov 16 12:39:12 2006  [WARNING] apf_rogue.c 1905: Possible AP
impersonation of xx:xx:xx:xx:xx:xx, using source address of
00:16:35:9e:6f:3a, detected by 00:17:df:7d:e1:70 on slot 0
 Thu Nov 16 12:39:12 2006  [SECURITY] apf_rogue.c 1490: Trusted AP Policy failed for AP
xx:xx:xx:xx:xx:xx - invalid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

Заметьте выделенные сообщения об ошибках здесь. Эти сообщения об ошибках указывают, что SSID и тип шифрования, настроенный на доверяемом AP, не совпадают с Доверяемым значением политики AP.

То же сигнальное сообщение может быть замечено по GUI WLC. Для просмотра этого сообщения войдите в главное меню GUI WLC и нажмите **Monitor**. В Новом разделе Trap-сообщений страницы Monitor нажмите **View All** для просмотра всех недавних предупреждений на WLC.




На странице Most Recent Traps можно определить контроллер, который генерирует доверяемое сигнальное сообщение нарушения политики AP как показано в этом образе:




## Дополнительные сведения

- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 5.2 - включение обнаружения точки доступа помады в RF Groups
- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 4.0 - решения по обеспечению безопасности Настройки
- Обнаружение несанкционированных точек доступа в Unified Wireless Networks
- Руководство по разработке и развертыванию SpectraLink Phone
- Пример конфигурации базового беспроводного подключения LAN
- Устранение неисправностей связи в беспроводных сетях LAN
- Примеры настройки проверки подлинности на контроллерах беспроводной сети
- Cisco Systems – техническая поддержка и документация