

# Настройте Внешнюю веб-аутентификацию с Установившимся Доступом (5760/3650/3850)

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Настройка](#)

[Схема сети](#)

[Конфигурация интерфейса командой строки CLI](#)

[Конфигурация графического интерфейса пользователя \(GUI \)](#)

[Проверка](#)

## Введение

Этот документ определяет, как настроить аутентификацию внешней web - страницы с Установившимися Контроллерами доступа. Гостевая страница портала и учетная аутентификация находятся оба на платформе Identity Services Engine (ISE) в данном примере.

## Предварительные условия

### Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

1. Cisco сходилась контроллеры доступа.
2. Web-аутентификация
3. Cisco ISE

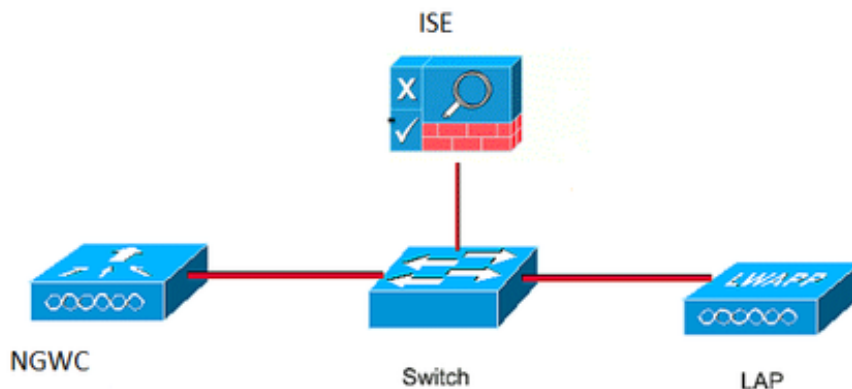
### Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

1. Контроллер Cisco 5760 (NGWC на ниже схемы), 03.06.05E
2. ISE 2.2

## Настройка

## Схема сети



## Конфигурация интерфейса командой строки CLI

Конфигурация RADIUS на контроллере

шаг 1: Определите внешний сервер RADIUS

```
radius server ISE.161
address ipv4 10.48.39.161 auth-port 1812 acct-port 1813
timeout 10
retransmit 5
key Cisco123
```

шаг 2: Определите группу AAA Radius и задайте сервер RADIUS, который будет использоваться

```
aaa group server radius ISE-Group
server name ISE.161
deadtime 10
```

шаг 3. Определите список методов, указывающий на группу радиуса, и сопоставьте его под WLAN.

```
aaa authentication login webauth group ISE-Group
```

Конфигурация карты параметра

шаг 4. . Настройте карту глобального параметра с виртуальным IP - адресом, который требуется для внешнего и внутреннего webauth. Виртуальное IP использование кнопки выхода из системы. Всегда полезный прием для настройки немаршрутизуемого виртуального IP.

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 1.1.1.1
```

**шаг 5. : Настройте именованную карту параметра. Это будет действовать как тип webauth метода. Это вызовет под config WLAN.**

```
parameter-map type webauth web
type webauth
redirect for-login https://10.48.39.161:8443/portal/PortalSetup.action?portal=0c712cd0-6d90-
11e5-978e-005056bf2f0a
redirect portal ipv4 10.48.39.161
```

**Пред опознавательный ACL. Это также вызовет под WLAN.**

**шаг 6: Настройте Preauth\_ACL, который предоставляет доступ к ISE, DHCP и DNS, прежде чем аутентификация будет закончена**

```
ip access-list extended Preauth_ACL
permit ip any host 10.48.39.161
permit ip host 10.48.39.161 any
permit udp any eq bootps any
permit udp any any eq bootpc
permit udp any eq bootpc any
permit udp any eq domain any
permit udp any any eq domain
```

## Config WLAN

**шаг 7: настройте WLAN**

```
wlan ext-webauth 7 ext-webauth
client vlan vlan232
ip access-group web Preauth_ACL
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list webauth
security web-auth parameter-map web
session-timeout 1800
no shutdown
```

**шаг 8: Включите http server.**

```
ip http server
```

```
ip http secure-server (for secure web-auth, use 'no' to disable secure web)
```

## Конфигурация графического интерфейса пользователя (GUI )

Мы выполняем здесь те же действия как выше. Снимки экрана просто предоставлены для перекрестной ссылки.

**шаг 1: Определите внешний сервер RADIUS**

CISCO Wireless Controller

Home Monitor Configuration Administration

Security

- AAA
  - Method Lists
  - Server Groups
  - RADIUS**
    - Servers

**Radius Servers**

New Remove

	Server Name	Address	Auth Port	Acct Port
<input type="radio"/>	ISE.161	10.48.39.161	1812	1813

шаг 2.: Определите группу AAA Radius и задайте сервер RADIUS, который будет использоваться

Security

- AAA
  - Method Lists
  - Server Groups
  - Radius**

**Radius Server Groups**

New Remove

	Name	Server1
<input type="radio"/>	ISE-Group	ISE.161

шаг 3. Определите список методов, указывающий на группу радиуса, и сопоставьте его под WLAN.

Security

- AAA
  - Method Lists
    - General
    - Authentication**
    - Accounting
    - Authorization

**Authentication**

New Remove

	Name	Type	Group Type	Group1
<input type="radio"/>	default	login	local	N/A
<input type="radio"/>	webauth	login	group	ISE-Group

Конфигурация карты параметра

шаг 4. . Настройте карту глобального параметра с виртуальным IP - адресом, который требуется для внешнего и внутреннего webauth. Виртуальное IP использование кнопки выхода из системы. Всегда полезный прием для настройки немаршрутизуемого виртуального IP.

шаг 5. : Настройте именованную карту параметра. Это будет действовать как тип webauth метода. Это вызовут под config WLAN.

The screenshot shows the Cisco Wireless Controller interface. The top navigation bar includes 'Home', 'Monitor', 'Configuration', and 'Administration'. The left sidebar shows the 'Security' menu with 'Method Lists' expanded to 'General', 'Authentication', 'Accounting', and 'Authorization'. The main content area is titled 'Webauth Parameter Map' and contains a table with two entries:

Parameter-map name	Parameter-map type
global	Global
web	Named

Пред опознавательный ACL. Это также вызовут под WLAN.

шаг 6: Настройте Preauth\_ACL, который предоставляет доступ к ISE, DHCP и DNS, прежде чем аутентификация будет закончена

The screenshot shows the Cisco Wireless Controller interface for 'Access Control Lists'. The left sidebar shows the 'Security' menu with 'ACL' expanded to 'Access Control Lists'. The main content area is titled 'Access Control Lists' and shows details for 'Preauth\_ACL' (Type: IPv4 Extended). Below the details is a table with 7 sequences:

Seq	Action	Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port	DSCP
10	permit	ip	any	10.48.39.161	-	-	-
20	permit	ip	10.48.39.161	any	-	-	-
30	permit	udp	any	any	eq 67	-	-
40	permit	udp	any	any	-	eq 68	-
50	permit	udp	any	any	eq 68	-	-
60	permit	udp	any	any	eq 53	-	-
70	permit	udp	any	any	-	eq 53	-

At the bottom of the page, there is a summary row for 'ext-webauth':

ext-webauth	7	ext-webauth	232	Enabled	Web-Auth
-------------	---	-------------	-----	---------	----------

Config WLAN

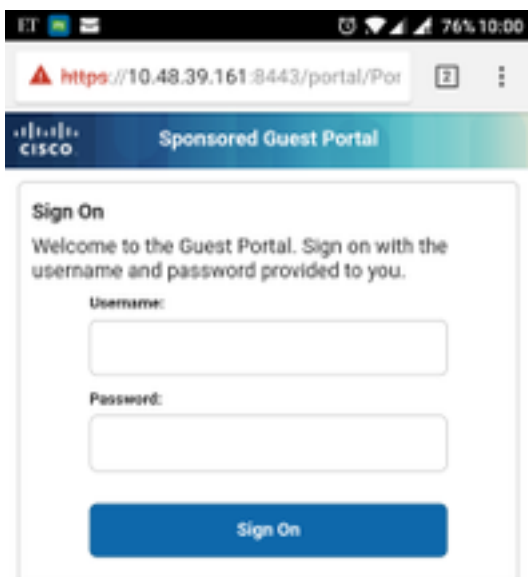
шаг 7: настройте WLAN

The screenshot shows the Cisco Wireless Controller configuration interface. The top navigation bar includes 'Home', 'Monitor', 'Configuration', and 'Administration'. The left sidebar shows a tree view under 'Wireless' with folders for 'WLAN', 'Advanced', 'Access Points', '802.11a/n/ac', '802.11b/g/n', 'Media Stream', and 'QOS'. The main content area is titled 'WLAN > Edit' and has tabs for 'General', 'Security', 'QOS', 'AVC', 'Policy Mapping', and 'Advanced'. The 'Security' tab is active, and the 'Layer3' sub-tab is selected. The configuration table below is as follows:

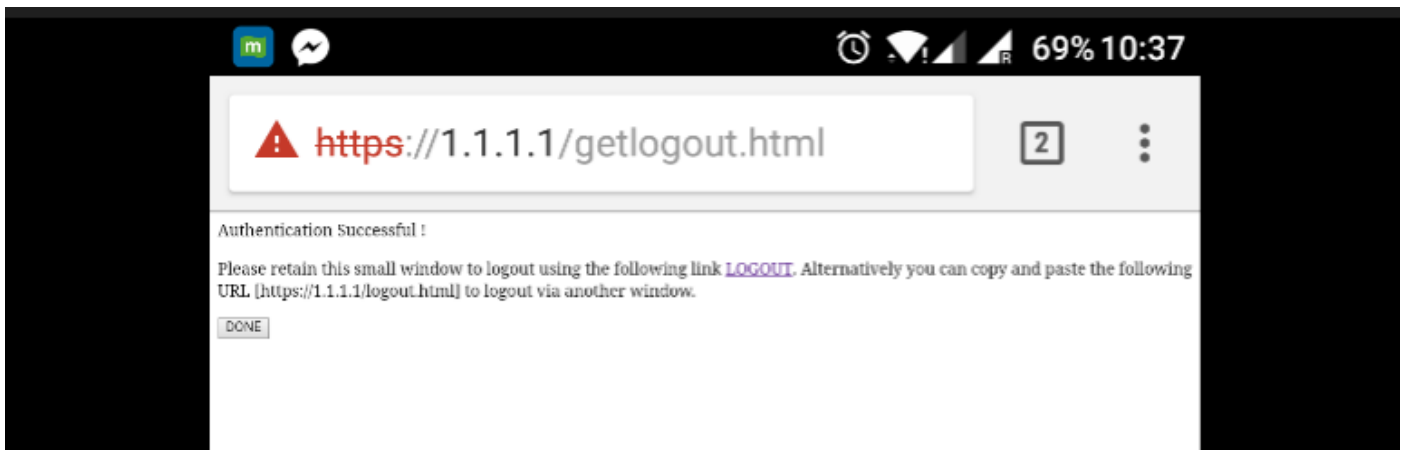
Layer2	Layer3	AAA Server
	<input checked="" type="checkbox"/>	
Web Policy	<input type="checkbox"/>	
Conditional Web Redirect	<input type="checkbox"/>	
Webauth Authentication List	<input type="text" value="webauth"/>	
Webauth Parameter Map	<input type="text" value="web"/>	
Webauth On-mac-filter Failure	<input type="checkbox"/>	
Preauthentication IPv4 ACL	<input type="text" value="Preauth_ACL"/>	
Preauthentication IPv6 ACL	<input type="text" value="none"/>	

## Проверка

Подключите клиента и удостоверьтесь, что, если вы открываете браузер, клиент будет перенаправлен к вашей странице портала входа в систему. Ниже снимка экрана иллюстрирует гостевую страницу портала ISE.



Как только надлежащие учетные данные отправлены, страницу успеха покажут:



Сервер ISE сообщит о двух аутентификациях: один на самой гостевой странице (практический результат с только именем пользователя) и вторая аутентификация, как только WLC предоставляет то же имя пользователя / пароль посредством проверки подлинности RADIUS (только эта аутентификация сделает клиентское перемещение к фазе успеха). Если проверка подлинности RADIUS (с мак адресом и подробными данными WLC как NAS) не происходит, конфигурация RADIUS должна быть проверена.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...
Sep 10, 2017 08:37:37.891 AM	✓			ritmahaj	C0:EE:FB:D7:88:24	Unknown	Default >> D...	Default >> B...	PermitAccess
Sep 10, 2017 08:37:34.506 AM	✓			ritmahaj					