



Configuring the CiscoWorks Wireless LAN Solution Engine TACACS+/RADIUS Authentication Using Cisco Secure ACS

Revised: December 21, 2005, OL-8740-01

This document describes the procedure to configure the CiscoWorks Wireless LAN Solution Engine (WLSE) using ACS as a TACACS+/RADIUS authentication module.

- [ACS TACACS+ Setup for WLSE](#)
- [ACS RADIUS Setup for WLSE](#)

See also the Managing the WLSE System chapter of the *User Guide for the CiscoWorks Wireless LAN Solution Engine* on [cisco.com](http://www.cisco.com) at

http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_list.html

Prerequisites

- Cisco Secure ACS 3.3.2 or ACS 4.0
- CiscoWorks Wireless LAN Solution Engine 2.13



Note

This document applies to the Cisco Secure ACS versions listed above only. Non-Cisco applications are not supported.

ACS TACACS+ Setup for WLSE

To set up ACS TACACS+ for WLSE, you need to perform the following steps:

1. Add WLSE as a AAA client in ACS.
2. Set up the ACS group for WLSE.
3. Log in to WLSE and select the TACACS+ authentication module.



Corporate Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2005 Cisco Systems, Inc. All rights reserved.

Procedure

-
- Step 1** Log in to ACS with the *admin* user ID.
- Step 2** Click **Network Configuration** on the left panel, then click **Add Entry**.
- Step 3** In the Add AAA Client form, enter the following information:
- AAA Client Hostname
 - AAA Client IP Address (Use your WLSE IP address.)
 - Key (You must either record or remember the key to configure WLSE.)
 - Authenticate Using TACACS+ (Cisco IOS)
- Step 4** Click **Submit**.
- Step 5** Click **Interface Configuration** on the left panel, then click **TACACS+ (Cisco IOS)**.
- Step 6** Under New Services, in the Service field, enter **WLSE** (case sensitive) and enter **IP** in the Protocol field, then click **Submit**.
- You now need to set up the ACS group for WLSE.
- Step 7** Click **Group Setup**. Select the group you will create for the WLSE users. Optional: Select a group ID and rename the group.
- Step 8** Click **Edit Settings**. At the bottom of the TACACS+ Settings section, check the **WLSE IP** and **Custom Attributes** checkboxes. In the Custom Attributes field, enter the following parameters, then click **Submit + Restart**.

```
cmd=groups
cmd-arg="System Admin"
```




- Note** WLSE supports multiple user groups for a given user. In this case, the user will have combined privileges. The format to configure multiple group privileges for a given user is
- ```
cmd-arg="Role1", "Role2", "Role3".
```

In this example, `cmd-arg="System Admin"` gives the users in the ACS group the *System Admin* role.

To create limited access roles for specific users, you must log in to WLSE and create a specific role with the necessary permissions and then enter the role name in TACACS+ using `cmd-arg`. For example, on the WLSE you can create the role called *MyRole*. Then, `cmd-arg="MyRole"` gives the users in that ACS group the role *MyRole*.

- Step 9** Click **User Setup** on the left panel.
- Step 10** Enter a username, for example *user1*, in the User field, then click **Add/Edit** to create a user, or you can edit a user that already exists.
- Step 11** Enter a password and confirm the password. From the pulldown menu **Group to which the user is assigned**, select the group that you just created for WLSE. See [Figure 1](#). (Optional: Add or edit Real Name and Description.)
- Step 12** Click **Submit** to complete the ACS Configuration.

**Figure 1**      **Setting Attributes**

**User Setup** 

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

---

Group to which the user is assigned:

144734

- Step 13** Log in to WLSE as *admin*.
- Step 14** Select **Admin > Appliance > Security > Authentication Modules**, then select TACACS+ as the module. Enter the shared secret key you entered when you defined the AAA client, then enter the ACS server IP address as the primary server. Click **Apply**.
- Step 15** To verify that the setup was successful, log out of WLSE and log back in again as the ACS user you just created or modified.

## ACS RADIUS Setup for WLSE

To set up ACS RADIUS for WLSE, you need to perform the following steps:

1. Add WLSE as a AAA client in ACS.
2. Set up the ACS group for WLSE.
3. Log in to WLSE and select the RADIUS authentication module.

## Prerequisites

Before you can set up ACS RADIUS for WLSE, you need to make sure

- RADIUS (Cisco/Aironet) appears in the list when you click Interface Configuration.
- After you configure the network client as shown in the steps below, the cisco-av-pair must be enabled when you click Interface Configuration and then click the link for RADIUS (Cisco IOS/Pix 6.x).

Consult the CiscoSecure ACS documentation for steps on how to configure these settings if they are not already configured.

### Procedure

- 
- Step 1** Log in to ACS with the *admin* user ID.
- Step 2** Click **Interface Configuration** on the left panel. If **RADIUS (Cisco IOS/PIX)** appears in the list, click on it and go to step 7. If **RADIUS (Cisco IOS/PIX)** does not appear in the list, continue with step 3.
- Step 3** Click **Network Configuration** on the left panel, then click **Add Entry**.
- Step 4** In the Add AAA Client form, enter the following information to create the RADIUS (Cisco IOS/PIX) module:
- AAA Client Hostname (for example, *Radius Placeholder*)
  - AAA Client IP Address (for example, *1.1.1.1*)
  - Key (for example, *placeholder.*)
  - Authenticate Using RADIUS (Cisco Aironet)
- Step 5** Click **Submit**.
- Step 6** Click **Interface Configuration** on the left panel, then click **RADIUS (Cisco IOS/PIX)**. The Interface Configuration window appears.
- Step 7** Make sure the cisco-av-pair checkbox is checked, then click **Submit**.
- Step 8** Click **Network Configuration** on the left panel, then click **Add Entry**.
- Step 9** In the Add AAA Client form, enter the following information:
- AAA Client Hostname
  - AAA Client IP Address (Use your WLSE IP address.)
  - Key (You must either record or remember the key to configure WLSE.)
  - Authenticate Using RADIUS (Cisco Aironet)
- Step 10** Click **Submit**.
- Step 11** Click **Group Setup**. Select any group. Optional: Select a group ID and rename the group.
- Step 12** Click **Edit Settings**. Under the Cisco IOS/Pix 6.x RADIUS Attributes section, enter the following parameters for the cisco-av-pair
- ```
WLSE:groups="System Admin" (case sensitive)
```
- Step 13** Click **Submit+Restart**.



Note WLSE supports multiple user groups for a given user. In this case, the user will have combined privileges. The format to configure multiple group privileges for a given user is
`WLSE:groups="Role1", "Role2", "Role3".`

The command `WLSE:groups="System Admin"` gives the users in the ACS group the *System Admin* role. To create limited access roles for specific users, you must log in to WLSE and create a specific role with the necessary permissions and then enter the role name in RADIUS using `WLSE:groups`. For example, on the WLSE you can create the role called *MyRole*. Then, `WLSE:groups="MyRole"` gives the users in that ACS group the role *MyRole*.

- Step 14** Click **User Setup** on the left panel.
- Step 15** Enter a username, for example *user1*, in the User field, then click **Add/Edit** to create a user, or you can edit a user that already exists.
- Step 16** Enter a password and confirm the password. From the pulldown menu **Group to which the user is assigned**, select the group that you just created for WLSE. See [Figure 1](#). (Optional: Add or edit Real Name and Description.) Click **Submit** to complete the ACS Configuration.
- Step 17** Log in to WLSE as *admin*.
- Step 18** Select **Admin > Appliance > Security > Authentication Modules**, then select RADIUS as the module. Enter the shared secret key you entered when you defined the AAA client, then enter the ACS server IP address as the primary server. Click **Apply**.
- Step 19** To verify that the setup was successful, log out of WLSE and log back in again as the ACS user you just created or modified.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

© 2005 Cisco Systems, Inc. All rights reserved.