Authentication for HTTP Admin on AP Version 1.01

Document ID: 64061

Introduction

This document provides a sample configuration for authentication for HTTP admin on Access Point (AP) version 1.01.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Access Control Server (ACS) version 2.6.4 and above

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Background Information

There is no option to configure TACACS+ or RADIUS accounting or command authorization for EXEC sessions in the GUI. These options can be configured in the CLI, but are *not* recommended. If you configure these options, they can severely bog down the AP and ACS with accounting or authorization requests (each element of each page must be accounted or authorized for).

ACS Configuration

Interface Configuration

Complete these steps to configure the interface:

1. In TACACS+ (Cisco IOS), select the group box for the first undefined new service field.
2. In the Service field, enter Aironet.
3. In the Protocol field, enter Shell.
4. In Advanced Configuration Options, choose **Advanced TACACS+ Features > Display a window for each service selected**.
5. Click **Submit**.

User Configuration

Complete these steps to configure the user:

1. In Advanced TACACS+ Settings, select Shell (exec).
2. Select Privilege level.
3. In the field, enter 15.
4. Click **Submit**.

Group Configuration

Complete these steps to configure the group:

1. Choose TACACS+.
2. Choose **Aironet Shell > Custom attributes**.
3. In the Custom Attributes field, enter aironet:admin−capability=write+ident+firmware+admin+snmp.
4. Click **Submit**.
5. Restart.

Network Configuration

Complete these steps to configure the network:

1. Create NAS for the AP using TACACS+ as the protocol.
2. The key is the shared secret from the AP.
3. Click **Submit**.
4. Restart.

Note: If you are using a token server with a one time password, you need to configure token caching in order to avoid being continually prompted for level 1 and level 15 passwords. Complete these steps to configure token caching:

1. Enter group configuration for the group to which your admin users belong.
2. Choose **Token Card Settings**.
3. Select Duration.
4. Choose a duration that balances your needs for security and convenience.

If your typical admin session lasts five minutes or less, then a duration value of five minutes is best. If your session runs longer than five minutes, you are prompted again for your password at five minute intervals. Note that the Session option does not work without accounting enabled. Also, note that token caching is in effect for *all* users in the group, and for *all* of the group's sessions with all devices (not just EXEC sessions to the AP).

AP Configuration for VxWorks

User Configuration

Complete these steps:

1. Choose **Setup > Security > User Information > Add New User**.
2. Add a new user with full administrative capabilities (all capability settings checked).
3. Click **Back**. You are returned to the Security Setup page.
4. Click **User Manager**. The User Manager Setup page appears.
5. Enable User Manager.
6. Click **OK**.

Server Configuration

Complete these steps:

1. Choose **Setup > Security > Authentication Server**.
2. Enter the TACACS+ server IP address.
3. Select the TACACS server type.
4. In the field, enter port 49.
5. In the field, enter shared secret.
6. Choose the User Authentication box.

AP Configuration for IOS

Complete these steps to configure the AP for IOS:

1. Choose **Security > Server Manager**.
2. Choose a configured TACACS+ Server, or configure a new one.
3. Click **Apply**.
4. Choose the TACACS+ server's IP in the Admin Authentication (TACACS+) drop−down.
5. Click **Apply**.
6. Choose **Security > Admin Access**.
7. Create a local user with read−write access (if you have not done so already).
8. Click **Apply**.
9. Choose Authentication Server Only or Authentication Server (if not found in Local List).
10. Click **Apply**.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Terminal Access Controller Access Control System (TACACS+) Technology Support**
- **Cisco Secure Access Control Server for Unix Product Support**
- **Cisco Secure Access Control Server for Windows Product Support**
- **Aironet 1200 Series Product Support**
- **Technical Support − Cisco Systems**

Updated: Nov 16, 2005 Document ID: 64061