

IPS 7.X: User Login Authentication using ACS 5.X as Radius Server Configuration Example

Document ID: 112974

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Configure IPS for Authentication from ACS Server using IME
- Configure ACS as a RADIUS Server

Verify

Troubleshoot

Related Information

Introduction

This document provides information on how to configure the Cisco Intrusion Prevention System (IPS) for user login authentication using a RADIUS server. ACS is used as the RADIUS server.

Prerequisites

Requirements

This document assumes that the Cisco Intrusion Prevention System (IPS) is fully operational and configured to allow the Cisco Intrusion Prevention System Manager Express (IME) or CLI to make configuration changes. In addition to local AAA authentication, you can now configure RADIUS servers to perform sensor user authentication. The ability to configure the IPS to use AAA RADIUS authentication for user accounts, which aids in the operation of large IPS deployments, is available in Cisco Intrusion Prevention System 7.0(4)E4 and later.

Note: There is no option to enable Accounting on the IPS. There is RADIUS authentication support in IPS 7.04, but TACACS or Authorization or Accounting are not supported.

Components Used

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

- Cisco Intrusion Prevention System version 7.0(4)E4 and later
- Intrusion Prevention System Manager Express Version 7.1(1) and later
- Cisco Secure Access Control Server 5.x

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

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

Configure

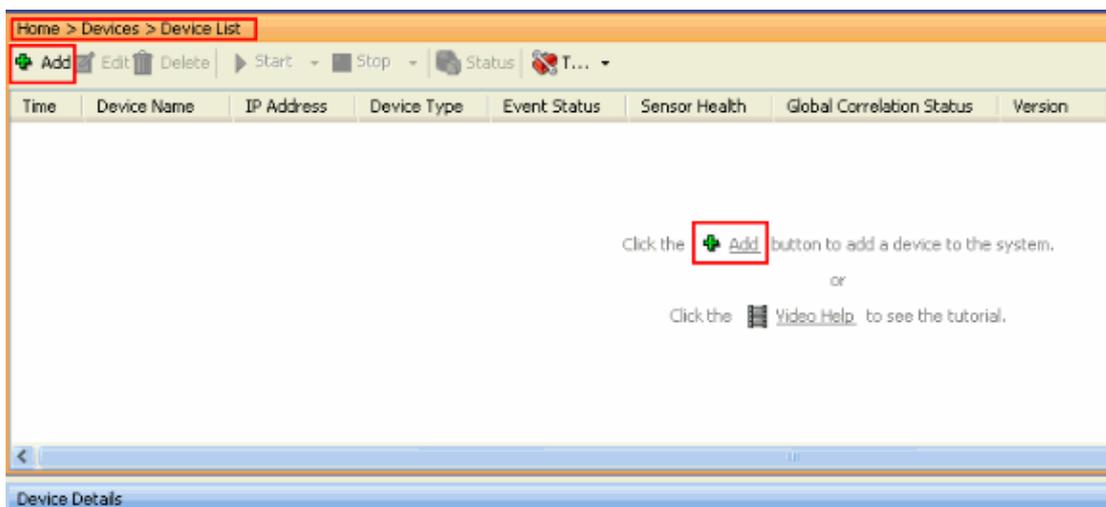
In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Configure IPS for Authentication from ACS Server using IME

Complete these steps in order to add the IPS to IME and then configure the IPS for authentication from the ACS server:

1. Choose **Home > Devices > Device List > Add** in order to add an **IPS** to the **IME**.



2. Complete the fields in the **Add Device** window, as shown here, in order to provide the details about the IPS. The sensor name used here is **IPS**. Click **OK**.

Add Device

Sensor Name:

Sensor IP Address:

Web Server Port:

Communication protocol

Use encrypted connection (https)

Use non-encrypted connection (http)

Authentication

Configuration User Name: ⓘ

Configuration Password:

Use the Same Account for Configuration and Event Subscription (This is not recommended):

Event Subscription User Name: ⓘ

Event Subscription Password:

Event Start Time (UTC)

Most Recent Alerts

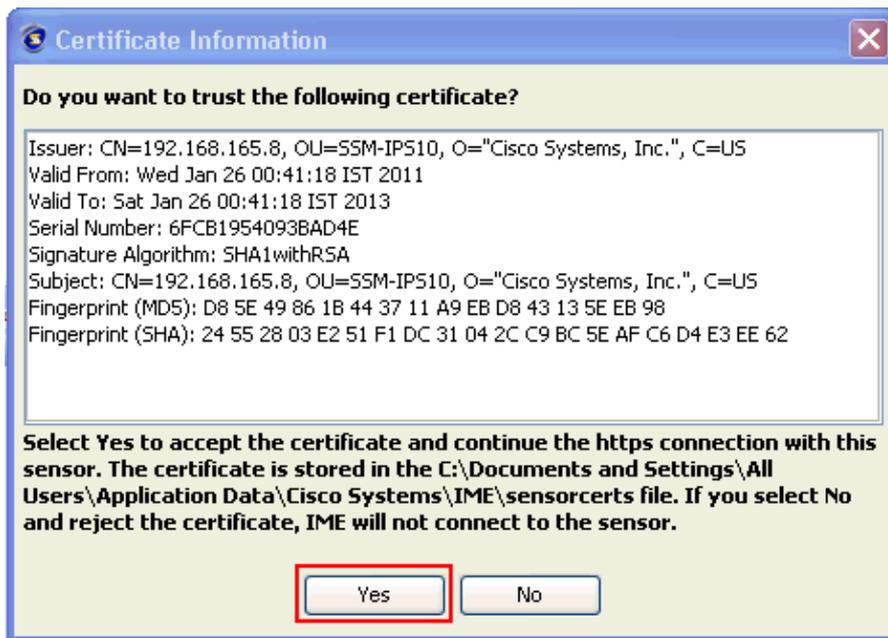
Start Date (YYYY:MM:DD): : :

Start Time (HH:MM:SS): : :

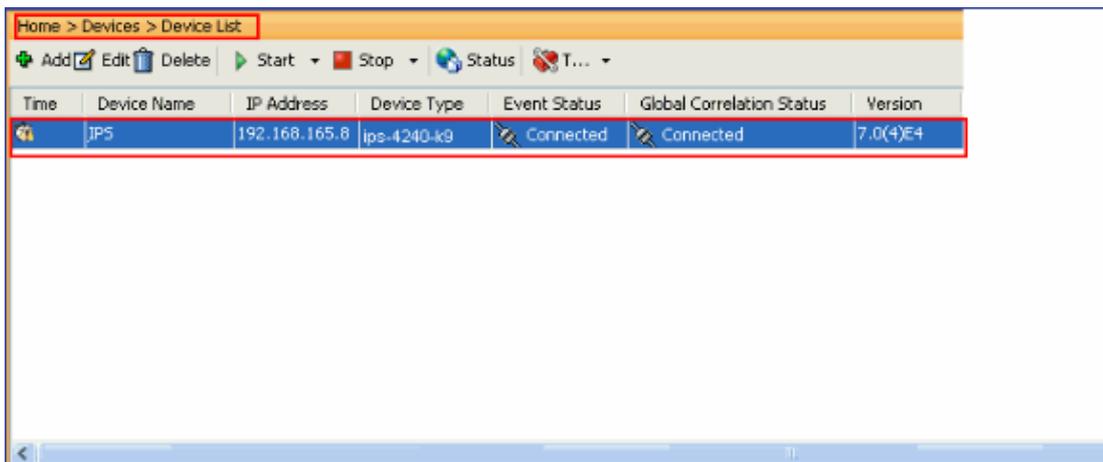
Exclude alerts of the following severity level(s)

Informational Low Medium High

3. Click **Yes** in order to accept the certificate and continue the https connection to the sensor. You must accept the certificate in order to connect to and access the sensor.



The IPS named **IPS** is added to the **Intrusion Prevention System Manager Express (IME)**.



4. Choose **Configuration > IPS > Sensor Setup > Authentication**, and complete these steps:

- Click the **RADIUS Server** radio button in order to select the RADIUS Server as the Authenticating device.
- Provide the **RADIUS Authentication** parameters, as shown.
- Choose **Local and RADIUS** as the Console Authentication, so that local authentication is used when the RADIUS Server is not available.
- Click **Apply**.

Configuration > IPS > Sensor Setup > Authentication

User Authentication: Local Radius Server

Local Authentication

Specify the users that have access to the sensor. The service role is a special role that allows you to bypass the CLI if needed. Only one service account is allowed.

Username	Role	Status
disco	Administrator	Active
service	Service	Active

Radius Authentication

Network Access ID: Default User Role:

Allow Local Authentication if all Radius Servers are Unresponsive

Primary Radius Server

Server IP Address:
 Authentication Port:
 Timeout (seconds):
 Shared Secret:

Secondary Radius Server (optional)

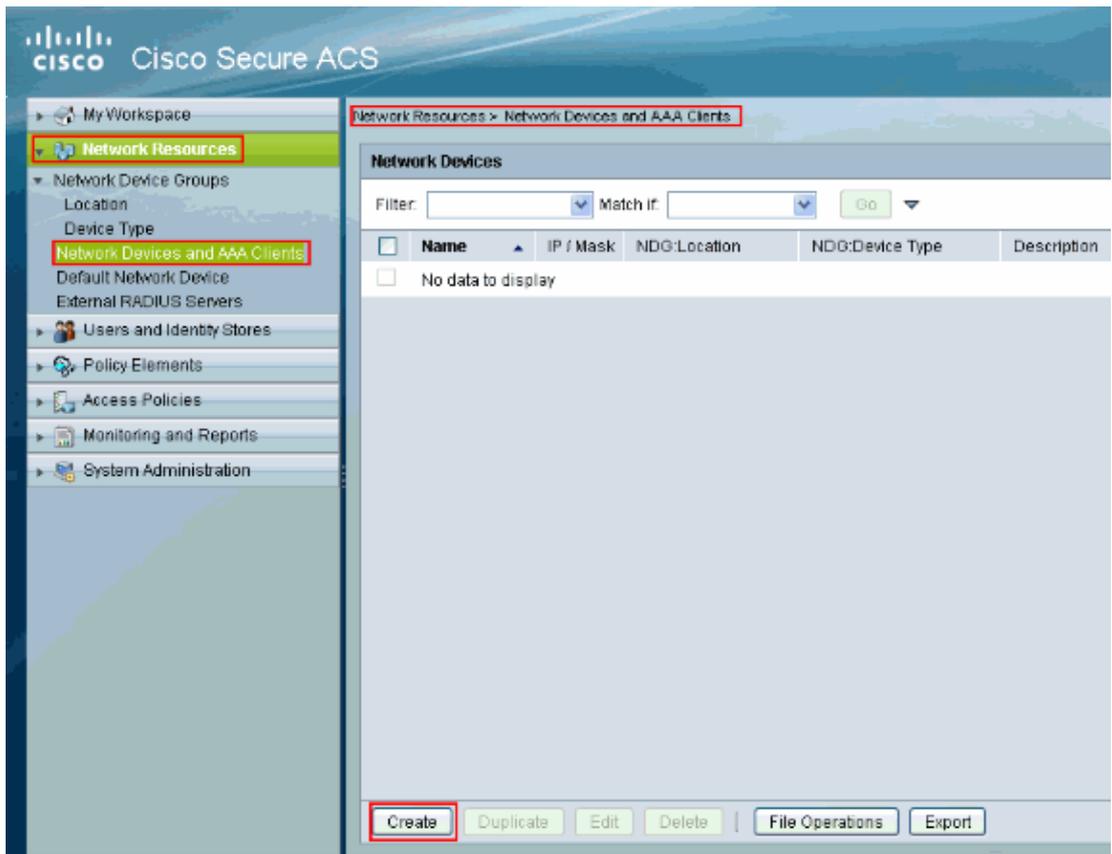
Console Authentication

Console Authentication:

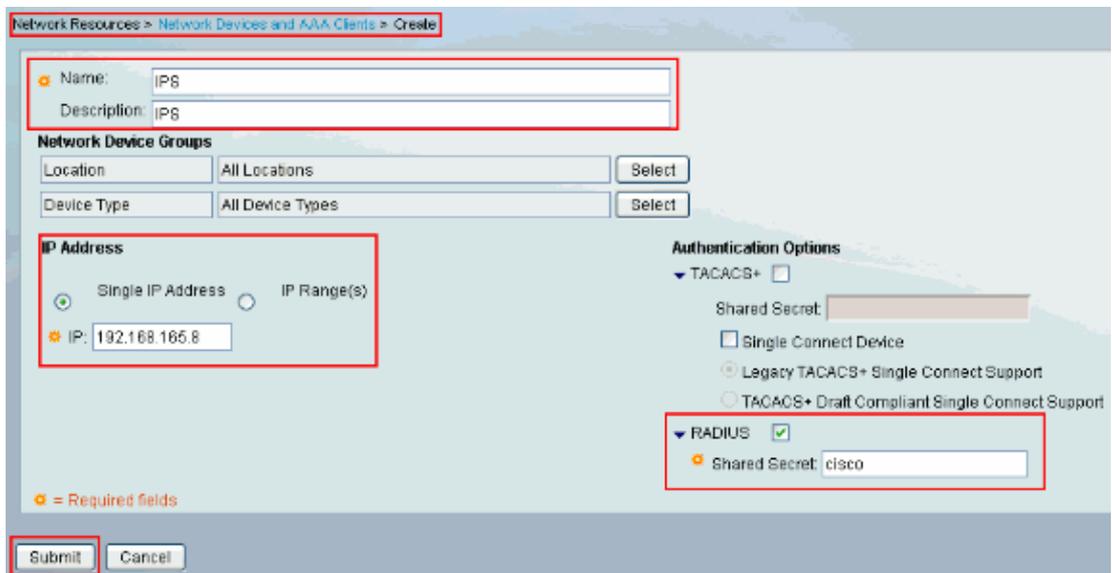
Configure ACS as a RADIUS Server

Complete these steps in order to configure the ACS as a RADIUS server:

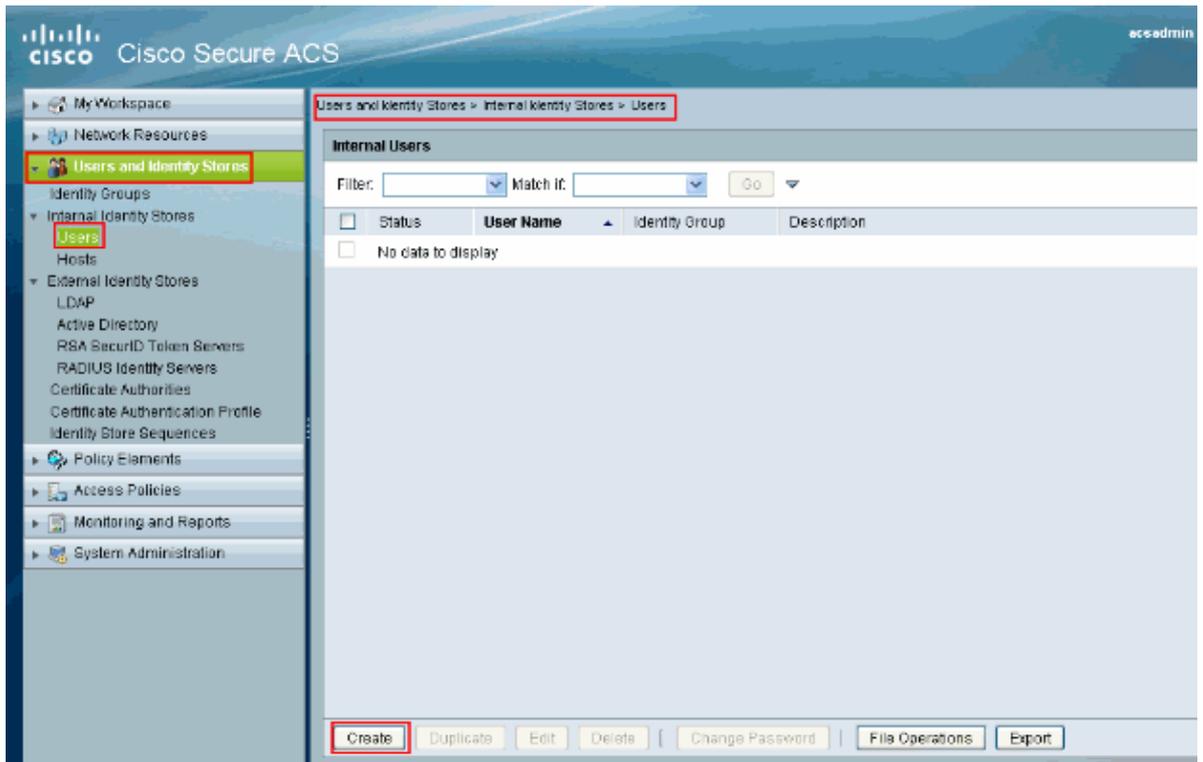
1. Choose **Network Resources > Network Devices and AAA Clients**, and click **Create** in order to add the IPS to the ACS server.



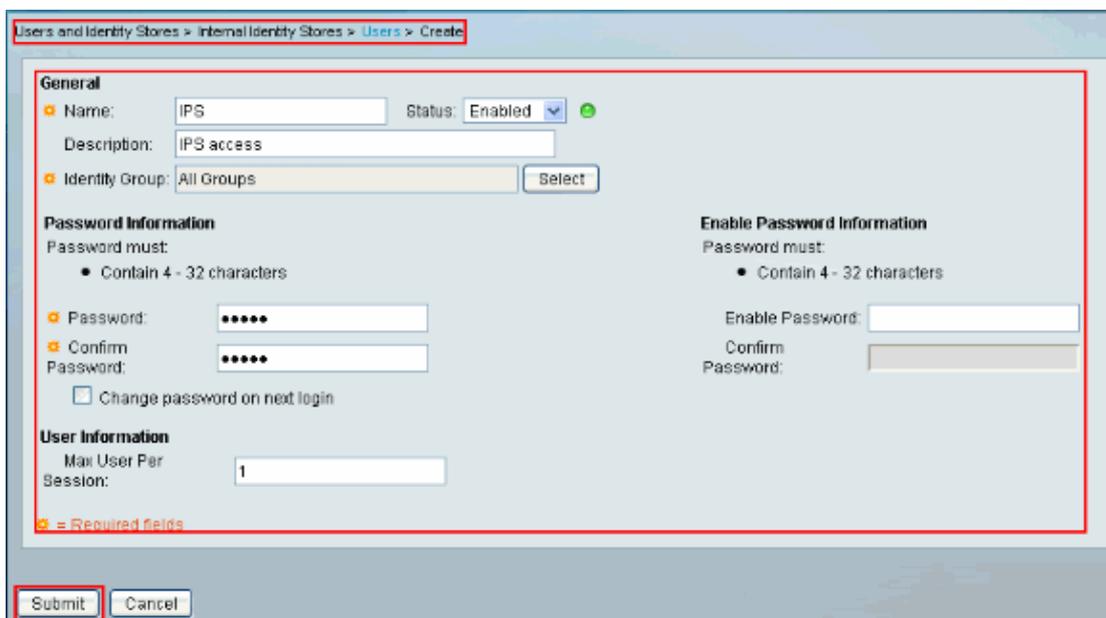
2. Provide the required information about the **client** (IPS is the client here), and click **Submit**. This enables the IPS to get added to the ACS server. The details include the **IP Address** of the IPS and the **RADIUS server** details.



3. Choose **Users and Identity stores > Internal Identity Stores > Users**, and click **Create** in order to create a new user.



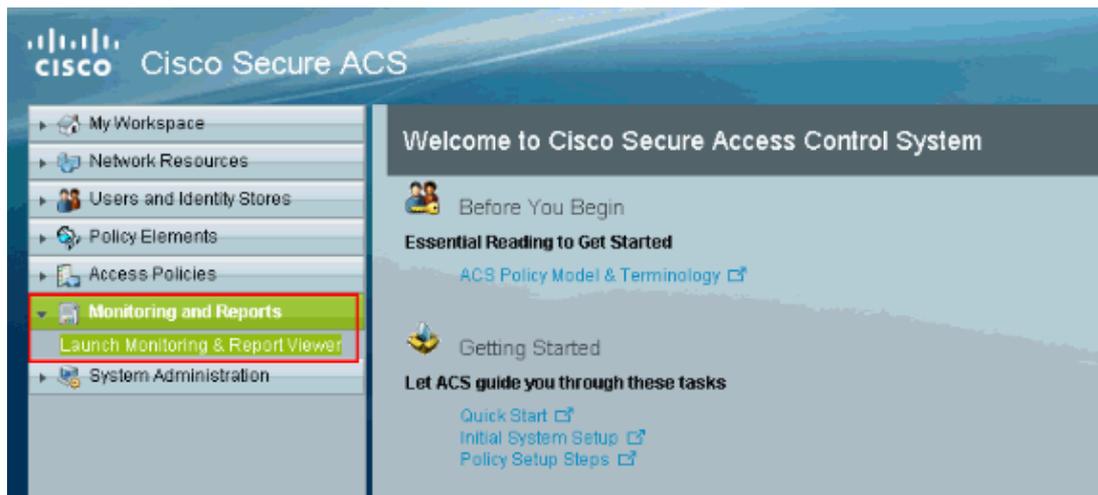
4. Provide the **Name and Password** information. When you finish, click **Submit**.



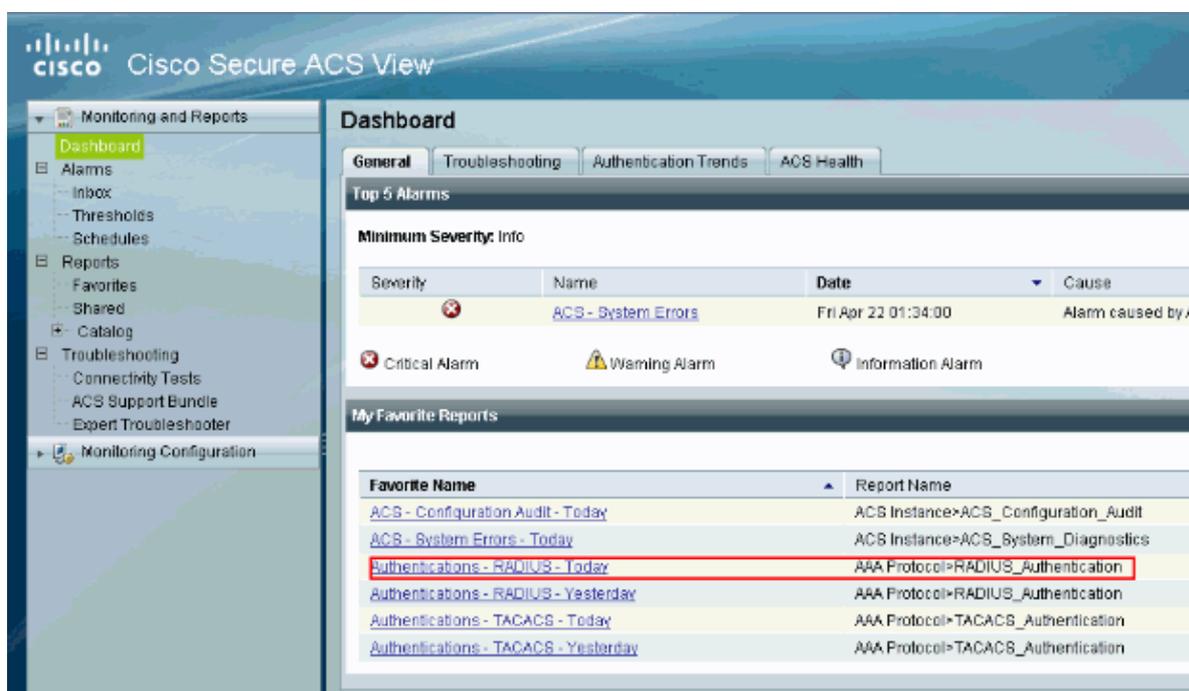
Verify

Use this section to confirm that your configuration works properly.

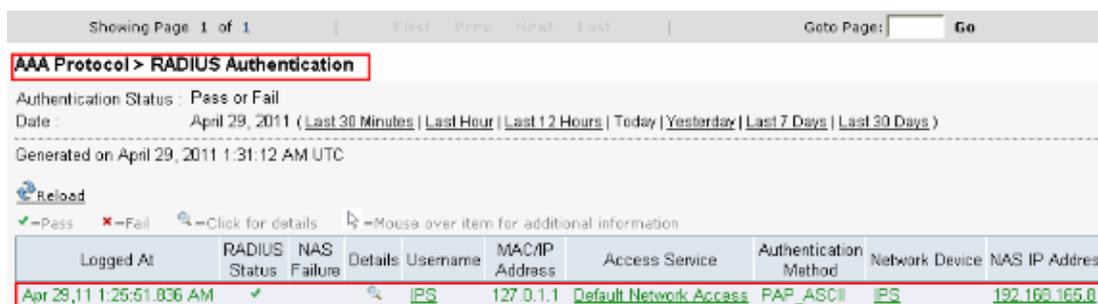
Try to log into the IPS with the newly created user. Once the user is authenticated, check the report on ACS.



Click the **Authentications–RADIUS–Today** in order to view the current report.



This image shows that the user connecting to the IPS is authenticated by the ACS server.



The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Troubleshoot

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

Related Information

- [Cisco IPS 4200 Series Sensors Support Page](#)
 - [Cisco IPS 4200 Series Sensors Command References](#)
 - [Cisco IPS Manager Express](#)
 - [IPsec Negotiation/IKE Protocols Support Page](#)
 - [Cisco Secure Access Control Server for Windows](#)
 - [Requests for Comments \(RFCs\)](#) 
 - [Technical Support & Documentation – Cisco Systems](#)
-

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

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 12, 2011

Document ID: 112974
