

# VMS to Authenticate with Cisco Secure ACS Configuration Example

Document ID: 51518

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Conventions

#### Configure

- ACS Configuration
- Enabling SecMon and IDSMC in ACS and Associating the CMF Device
- Common Services Configuration Requirements
- VMS Configuration Requirements

#### Verify

#### Troubleshoot

#### Related Information

## Introduction

This document provides a sample configuration for configuring VPN/Security Management Solution (VMS) to authenticate with Cisco Secure Access Control Server (ACS).

## Prerequisites

## Requirements

Verify that the Cisco Secure ACS server is running version 3.1 or later. CiscoWorks Common Services Software is not compatible with earlier versions of Cisco Secure ACS. If your Cisco Secure ACS server is running a software version earlier than 3.1, upgrade your Cisco Secure ACS server before continuing.

## Components Used

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

- Cisco Secure ACS 3.2
- VMS

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 the Cisco Technical Tips Conventions.

# Configure

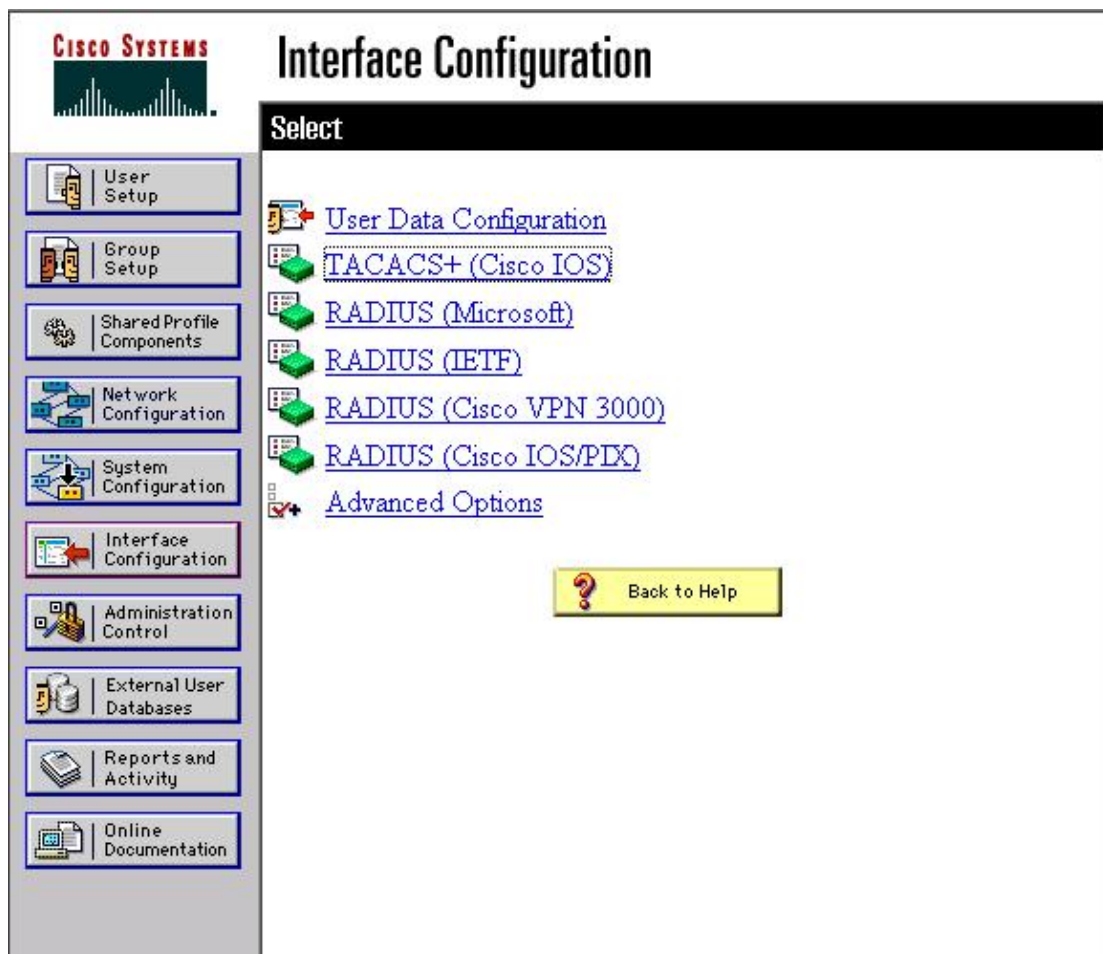
In this section, you are presented with the information to configure the features described in this document.

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

## ACS Configuration

Complete these steps to configure the ACS. Within ACS, add the VMS server as the AAA client.

1. Open a Web browser.
2. Enter `http://ACS-ip-address:2002/` in the address bar to browse to the ACS server.
3. Choose **Interface Configuration > TACACS+ (Cisco IOS)**.

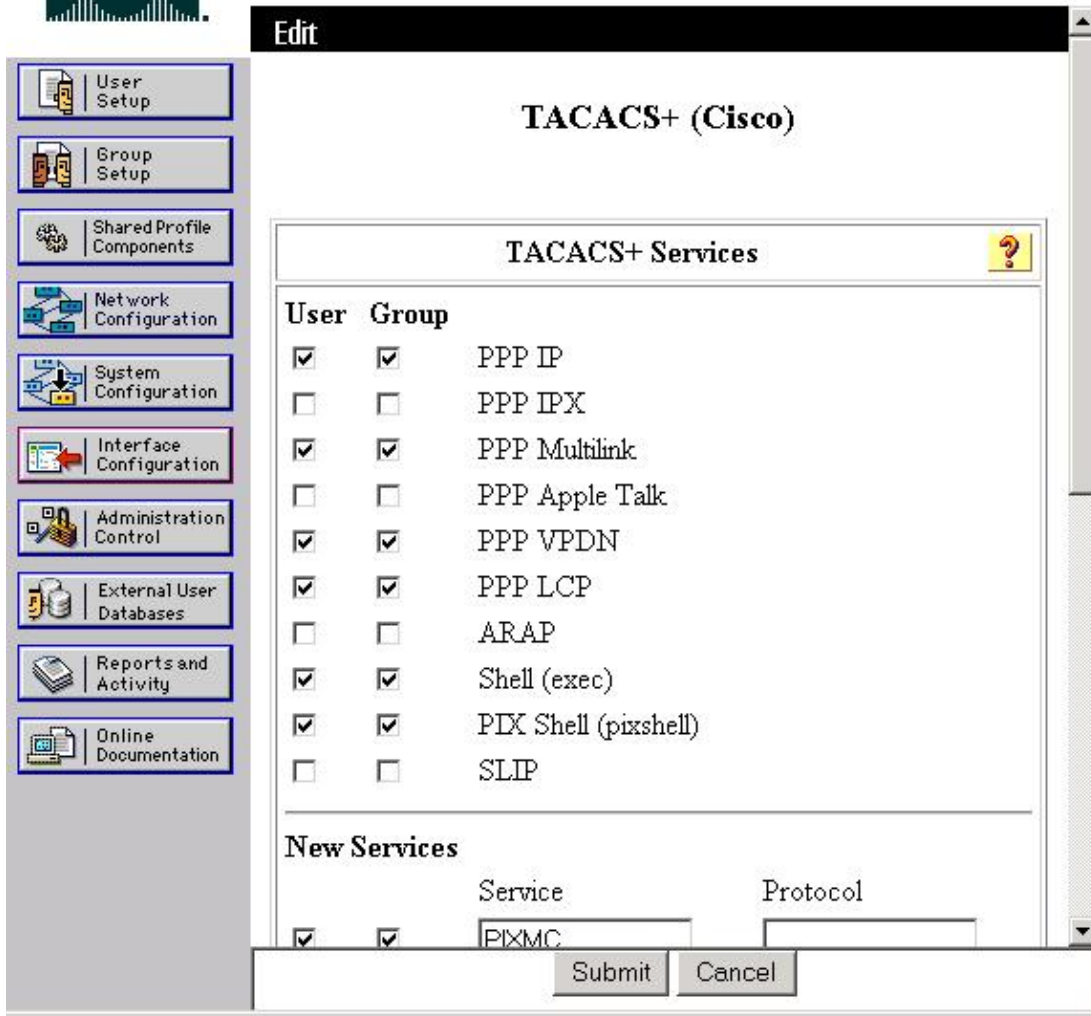


4. Choose these TACACS+ Services options:

```
PPP/IP          user [x]      group [x]
Shell (exec)   user [x]      group [x]
```



# Interface Configuration



5. Add the New Services (the new services are displayed; to set user privilege levels, choose **user**) and Advanced Configuration Options. Click **Submit** after each choice.

```
PIXMC          user [x]      group [x]
Idscfg         user [x]      group [x]
Iosmdc         user [x]      group [x]
Idsmon         user [x]      group [x]
[x]           Advanced TACACS+ Features
[x]           Display a window for each service selected in which you can
enter customized TACACS+ attributes
```



# Interface Configuration

User Setup	
Group Setup	
Shared Profile Components	
Network Configuration	
System Configuration	
Interface Configuration	
Administration Control	
External User Databases	
Reports and Activity	
Online Documentation	

New Services		Service	Protocol
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	PIXMC	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Idscfg	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	losmdc	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Idsmom	
<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>		

Advanced Configuration Options	
<input checked="" type="checkbox"/>	Advanced TACACS+ Features
<input type="checkbox"/>	Display a Time-of-Day access grid for every TACACS+ service where you can override the default Time-of-Day settings
<input checked="" type="checkbox"/>	Display a window for each service selected in which you can enter customized TACACS+ attributes
<input type="checkbox"/>	Display enable default (Undefined) service configuration

Back to Help


6. Choose **Network Configuration > Network Device Groups (Add Entry) > AAA Server IP address**. Enter your IP address.




# Network Configuration

Select

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration**
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation


Network Device Groups 			
Network Device Group	AAA Clients	AAA Servers	Remote Agents
<a href="#">test</a>	0	0	0
<a href="#">groupa</a>	0	0	0
<a href="#">ASDF</a>	0	0	0
<a href="#">AAA Server IP address</a>	0	0	0
<a href="#">(Not Assigned)</a>	6	2	0

Add Entry Search

Proxy Distribution Table 			
Character String	AAA Servers	Strip	Account
<a href="#">(Default)</a>	rtp_acs_appl2	No	Local

Add Entry Sort Entries

7. Choose **Network Configuration > Network Device Groups (Add Entry) > Shared key**. Enter your shared key.
8. Choose **Network Configuration > Network Device Groups (Add Entry) > Network Device Group**. Enter any group or not assigned.
9. Choose **Network Configuration > Network Device Groups (Add Entry) > Server Type**. Enter Cisco Secure ACS.



# Network Configuration

Edit

## Add AAA Server

AAA Server Name	<input style="width: 90%;" type="text"/>
AAA Server IP Address	<input style="width: 90%;" type="text"/>
Key	<input style="width: 90%;" type="text"/>
Network Device Group	<input style="width: 90%;" type="text" value="AAA Server IP address"/>
<input type="checkbox"/> Log Update/Watchdog Packets from this remote AAA Server	
AAA Server Type	<input style="width: 90%;" type="text" value="CiscoSecure ACS"/>
Traffic Type	<input style="width: 90%;" type="text" value="inbound/outbound"/>

10. Choose **Network Configuration > Network Device Groups (Add Entry) > Traffic Type**. Enter inbound or outbound.
11. Click **Submit + Restart**.
12. Choose **User Setup > Add/Edit User**. Enter this information:
  - ◆ User Setup: Password Authentication: Cisco Secure database
  - ◆ Password: cisco (whatever is used to log in to ACS)
  - ◆ IDScfg [x]
  - ◆ (\*) Assign a Management Center for IDS Sensors for network device
  - ◆ [Network Operator] – or select privilege level for user

Click **Submit** after each field.

**Note:** When creating new users, choose the user setup for Security Monitor and IDSMC. Under Security Monitor, choose Assign a Security Monitor for any network device, and choose System administrator. For IDSMC, check the checkbox to enable this action. Assign the user a Management Center for the IDS Sensors for any network device.



# User Setup

## Select

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation

User:

Find

Add/Edit

List users beginning with letter/number:

A B C D E F G H I J K L M  
N O P Q R S T U V W X Y Z  
0 1 2 3 4 5 6 7 8 9



List All Users



Back to Help



# User Setup

Edit

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation

## User: chachacherry (New User)

Account Disabled

### Supplementary User Info

Real Name

Description

### User Setup

Password Authentication:

CiscoSecure Database 

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

Password

Confirm

Password

Submit

Cancel

## Enabling SecMon and IDSMC in ACS and Associating the CMF Device

You are now able to launch SecMon and IDS MC. If you are unable to launch SecMon and IDS MC, these applications were not enabled in ACS, and the CMF device is not associated with appropriate roles. Additional steps need to be performed in ACS to enable SecMon and IDS MC in ACS, and associate the CMF device with the appropriate roles are. Complete these steps:

1. Choose group setup.
2. Click **edit setting** for the group to which your user belongs.
3. Scroll to the idsmon and idscfg section.
4. Choose the idsmon and idscfg toggle.
5. Choose Assign a security Monitor on a per Network Device Group Basis and add associates for the device group containing the CMF workstation with roles in the drop-down list (the second option, Assign a Security Monitor for any network device, works also). This should be done for both the Security Monitor and IDS Sensor.
6. Click **Submit + Restart**.
7. Log in to the CMF desktop. You are now able to launch both applications.

## Common Services Configuration Requirements

Within Common Services, you need to choose **Server Configuration > Setup > Security > Select Login**

**Module.** Choose TACACS+, and specify the AAA server configuration. Under Login Fallback options, choose Allow all Ciscoworks local users to fallback to the CiscoWorks Local login.

## VMS Configuration Requirements

Complete these steps:

1. Within CiscoWorks, choose **VPN/Security Management Solution > Administration > Configuration > AAA Server**.
2. Click **Synchronize**. The radio button at the top changes to "ACS." You are now able to enter the login credentials for the AAA server.
3. Complete the ACS login information.
4. Click **register**.

A pop-up box appears asking which Management Centers and Security Monitors you wish to use AAA authentication for. Choose idscfg and idsmon.

5. Add idscfg and idsmon to the **Selected Applications** box.
6. Click **OK**. A window stating that the registration completed successfully displays.
7. Click **Finish** to complete the VMS server configuration.

## Verify

You can view the privileges from ACS or Common Services:

- On Cisco Secure ACS, choose **Shared Profile Components | Network Operator** (see permissions).
- On Common Services, choose **Server Configuration > Setup > Security > Permissions Report** .

## Troubleshoot

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

## Related Information

- **Configuring CiscoWorks Common Services to use Local Authentication and Authorization**
- **Cisco Secure Access Control Server for Windows – White Papers**
- **Cisco Secure Software Download**
- **VPN/Security Management Solutions(VMS) Software Download**
- **Technical Support – Cisco Systems**

---

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

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Feb 02, 2006

Document ID: 51518

---