Introduction

This document describes the steps required in order to authenticate Cisco Security Manager (CSM) Versions 4.3/4.4 with Access Control Server (ACS) Version 5.x. In this configuration, user authentication is managed by ACS while authorization is managed on CSM with the local Role Based Access Control (RBAC) feature.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic Knowledge of Authentication, Authorization, and Accounting (AAA)
- CSM Server and Device Administration
- Authentication and Authorization Policies Configuration on ACS Version 5.x

Components Used

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

- CSM Version 4.4
- ACS Version 5.4

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.

Background Information

In previous versions of CSM, external authentication and authorization services were possible with
ACS Version 4.x only. The use of ACS Version 5.x was not officially tested or supported. The ACS Version 4.x integration was often difficult to scale because it required manual synchronization of the ACS and CSM network device configurations. In order to overcome this administrative burden, local RBAC capabilities are integrated directly into CSM Version 4.3 and later. In production deployments where both CSM Versions 4.3/4.4 and ACS Version 5.x are deployed, it is now possible to integrate the two in order to service user authentication externally and maintain granular authorization policies locally on CSM.

Configure

Configure ACS Server

Complete these steps in order to configure the ACS server:

1. From the ACS Version 5.x administrative GUI, navigate to Network Resources > Network Devices and AAA Clients > Create, and add the CSM server as a Network Access Device (NAD). Although TACACS+ is more commonly used for network device authentication, both ACS and CSM can be configured in order to use RADIUS if required.

2. Navigate to Users and Identity Stores > Internal Identity Stores > Users, and create a new local user for CSM access. Associate the user account with an Identity Group as required, such as CSM_Admins. Alternatively, an external identity store, such as Active Directory, can be used.
3. Navigate to **Access Policies > Access Services > Default Device Admin > Identity**, and associate the **Identity Source** to be used for user authentication. In this example, the **Internal Users** identity source is chosen because the CSM user accounts are locally defined on ACS. An external identity source can be selected when you integrate it with Active Directory.

4. Navigate to **Access Policies > Access Services > Default Device Admin > Authorization**, and configure an authorization policy that permits access to the user Identity Group defined previously (**CSM_Adms**). This is required for ACS order-of-operations processing even though the actual authorization policy is defined/enforced locally on the CSM server.
Configure CSM CiscoWorks Common Services

Complete these steps in order to configure CSM CiscoWorks Common Services:

1. Double-click the **Cisco Security Manager** icon on the CSM server desktop. Alternatively, navigate to **Tools > Security Manager Administration > Server Security** with the CSM Configuration Manager client in order to cross launch the Server Security Tools within the CSM Common Services backend.

2. Enter the CSM administrative user credentials, and click **Login**. Choose the **Server Administration** option from the Cisco Security Management Suite launch page.

3. Navigate to **Server > Security > AAA Mode Setup**, and choose **Local RBAC** and either **TACACS+** or **RADIUS**. Click **Change** in order to edit the login server settings.
4. Enter the login server IP or Fully Qualified Domain Name (FQDN), ports, and pre-shared key. Under normal operations, do not change the Login fallback options settings in order to allow fallback access to CSM in the event that the ACS server is unreachable. By default, the local CSM administrative user account is defined for fallback access. If change is necessary, care should be taken in order to prevent accidental lockout of the CSM server.

5. Navigate to Server > Single-Server Management > Local User Setup, and click Add in order to create local user accounts that match the internal or external user accounts defined in ACS. The usernames are case-sensitive and should match ACS exactly. These locally-defined accounts are then mapped to the CSM local RBAC authorization roles. Specific roles such as System Administrator can be chosen for Task Authorization separation or the user can be provided either full or restricted access to a subset of devices. Refer to the CiscoWorks Common Services Default Roles section of the CSM 4.4 Installation Guide for more details about Task Authorization and Roles.
Configure Default Authorization Roles for Undefined Users (Optional)

Complete these steps in order to configure default authorization roles for undefined users:

1. In some CSM deployments, it is not convenient to maintain a one-for-one user mapping between CSM and ACS. An alternative approach is to assign a default set of authorization roles in CSM for users not present in the local CSM database.

2. In order to configure the default authorization roles, double-click the Cisco Security Manager icon on the CSM server desktop and select the Server Administration option from the launch page.

3. Navigate to Server > Single-Server Management > Role Management Setup. By default, the Help Desk role is assigned the Default Role designation. In order to change this designation, check one or more roles, and click the Set as default button.

4. In order to enable this feature, navigate to Tools > Security Manager Administration > Server Security with the Configuration Manager client, and check the check box labeled Allow logon for user ids not available in Local User Database. Click Save in order to save the configuration.
Verify

Use this section in order to confirm that your configuration works properly.

- Review the TACACS+ or RADIUS authentication logs on the ACS server in order to identify whether the CSM user is able to authenticate against the configured identity store.

- Verify that the CSM user is able to perform an available task within the Task Authorization role defined. For example, log in as a user with the System Administrator role and try to add a new device to the CSM inventory.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

1. Errors such these indicate that you attempted to perform a task that you are not authorized to perform as per the local RBAC policy.
2. Log in to the CSM Server Administration interface as an administrative user and navigate to **Server > Single-Server Management > Local User Setup.** Edit the user account in question and review the **Task Authorization** policy defined for the user. When you use the CSM-defined roles, ensure that you review the **CiscoWorks Common Services Default Roles** section of the CSM 4.4 Installation Guide in order to better understand the permissions for each role. For example, the **System Administrator** role provides complete access to all CSM client functions while **Super Admin** only provides access to the backend CiscoWorks operations.

3. If desired, new roles can be defined and default roles edited in order to provide more granular authorization policy control. In order to add/edit, log in to the CSM server manager interface and navigate to **Server > Single-Server Management > Role Management Setup.**

![Role Management](image)

**Related Information**

- **CiscoWorks Common Services Default Roles - CSM 4.4 Installation Guide**
- **Technical Support & Documentation - Cisco Systems**