# Configuration de l'administration WCS et NCS avec ACS 5.x

## Contenu

Introduction Conditions préalables Conditions requises Components Used Conventions Configuration Étape 1. Ajoutez le WCS aux clients ACS AAA. Étape 2. Ajoutez Cisco Secure ACS en tant que serveur TACACS+ dans WCS. Étape 3. Configurez le profil de shell correct sur ACS. Étape 4. Configurez Cisco Secure ACS pour renvoyer les attributs. Vérification Dépannage Informations connexes

## **Introduction**

Ce document décrit comment utiliser Cisco Secure Access Control Server (ACS) 5.x afin de configurer l'administration de Cisco Wireless Control System (WCS) et Cisco Prime Network Control System (NCS).

# **Conditions préalables**

### **Conditions requises**

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Système de contrôle sans fil Cisco
- Système de contrôle réseau Cisco Prime
- Serveur Cisco Secure Access Control

#### **Components Used**

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

• Système de contrôle sans fil Cisco 7.0.172.0

#### Cisco Secure ACS 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**

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco.</u>

## **Configuration**

Cet exemple de configuration décrit comment authentifier un utilisateur avec TACACS+.

**Remarque :** Bien que plusieurs options et possibilités existent lorsque vous authentifiez les utilisateurs WCS/NCS avec Cisco Secure ACS 5.x, toutes les combinaisons ne sont pas décrites dans ce document. Cependant, cet exemple vous fournit les informations nécessaires pour comprendre comment modifier l'exemple en fonction de la configuration précise que vous souhaitez obtenir.

## Étape 1. Ajoutez le WCS aux clients ACS AAA.

1. Sur Cisco Secure ACS, sélectionnez **Ressources réseau > Périphériques réseau et clients** AAA.

<ul> <li>My Workspace</li> </ul>	Network Resources > N	stwork Devices and AAA Clients > Edit "WCS"		
<ul> <li>Metwork Resources</li> </ul>				
<ul> <li>Network Device Groups</li> <li>Location</li> </ul>	o Name: WCS			
Device Type	Network Device G	roups		
Default Network Device	Location	All Locations	Select	
External RADIUS Servers	Device Type	All Device Types	Select	
Solution     Solution	IP Address			Authentication Options
+ 🔂 Access Policies	<ul> <li>Single IP /</li> </ul>	Address () IP Range(s)		+ TACACS+ ☑
Monitoring and Reports	0 IP: 10.48.76.1	18		Shared Secret: cisco
<ul> <li>System Administration</li> </ul>				Single Connect Device  Legacy TACACS+ Single Connect Support  TACACS+ Draft Compliant Single Connect Support
				FADIUS
	6 = Champs obligation	doines		

- 2. Saisissez un nom dans le champ Nom.
- 3. Saisissez l'adresse IP WCS dans le champ IP address.
- 4. Sous la zone Options d'authentification, cochez la case TACACS+ afin d'activer TACACS+, puis entrez un terme à utiliser comme secret partagé. Remarque : cet exemple utilise *cisco* comme secret partagé ; cependant, pour des raisons de sécurité, il faut utiliser un terme moins évident.

#### Étape 2. Ajoutez Cisco Secure ACS en tant que serveur TACACS+ dans WCS.

- 1. Connectez-vous à WCS, puis sélectionnez Administration > AAA.
- 2. Cliquez sur **TACACS+**.

TACACS+ Server De	tail :	10.48.76.48
Administration > AAA > <u>TACAU</u>	<u>5+</u> > 1A	CACS+ Server Detai
TACACS+ Server		
Port	49	
Shared Secret Format	ASCI	I 🗘
Shared Secret		6
Confirm Shared Secret	•••••	
Retransmit Timeout	5	(secs)
Retries	1	
Authentication Type	PAP	\$
Local Interface IP	10.48	3.76.118
	TACACS+ Server Det         Administration > AAA > TACAC         TACACS+ Server         Port         Shared Secret Format         Shared Secret         Confirm Shared Secret         Retransmit Timeout         Retries         Authentication Type         Local Interface IP	TACACS+ Server Detail :         Administration > AAA > TACACS+ > TA         TACACS+ Server         Port       49         Shared Secret Format       ASCI         Shared Secret       ••••••         Confirm Shared Secret       ••••••         Retransmit Timeout       5         Retries       1         Authentication Type       PAP         Local Interface IP       10.48

- 3. Entrez votre terme secret partagé dans les champs Shared Secret et Confirm Shared Secret.
- 4. Sélectionnez l'adresse IP Cisco ACS dans le champ Local Interface IP.
- 5. Dans la zone de navigation de gauche, cliquez sur **Mode AAA**.



6. Cliquez sur la case d'option TACACS+.Remarque : Pour des raisons de sécurité, Cisco vous recommande de choisir en cas de panne d'authentification ou d'absence de réponse du serveur dans la liste déroulante Activer le retour arrière vers le routeur local. Si vous choisissez cette option, vous ne serez pas verrouillé en cas de problème. Vous pouvez modifier l'option une fois que tout fonctionne correctement.

#### Étape 3. Configurez le profil de shell correct sur ACS.

Cette étape décrit comment configurer Cisco Secure ACS pour renvoyer les attributs corrects afin de déterminer les privilèges utilisateur sur WCS.

 Dans la zone de navigation de gauche, cliquez sur Groupes. Une liste des types d'utilisateurs s'affiche. Cet exemple authentifie un utilisateur à partir du type d'utilisateur Lobby Ambassador. 2. Cliquez sur le lien Liste des tâches en regard du groupe

Change Password Local Password Policy	Export Task List Administration > AAA > Export Task List @Please cut and paste the appropriate protocol data	below into the custom/vendor-specific attribute field in your AAA server.
AAA Mode	TACACS+ Custom Attributes	RADIUS Custom Attributes
Users	role0=LobbyAmbassador	Wireless-WCS:role0=LobbyAmbassador
Groups	task0=Configure Guest Users task1=Lobby Ambassador User Preferences	Wireless-WCS:task0=Configure Guest Users Wireless-WCS:task1=Lobby Ambassador User Preferences
Active Sessions		
TACACS+		
RADIUS		

**Remarque :** vous devez configurer le rôle d'utilisateur (Lobby Ambassador pour cet exemple) et une liste des tâches qu'ils peuvent effectuer et des éléments de menu auxquels ils peuvent accéder. Si vous utilisez une version récente de WCS, vous devez également configurer le domaine virtuel auquel appartient l'utilisateur.

- 3. Sélectionnez Administration > Domaines virtuels.
- 4. Cliquez sur

#### Exporter. Virtual Domain Custom Attributes

Please cut and paste the appropriate protocol specific data below into the custom/vendor-specific attribute field in access to.

#### TACACS+ Custom Attributes

virtual-domain0=root	
virtual-domain1=w1	

**RADIUS Custom Attributes** 

Wireless-WCS:virtual-domain0=root Wireless-WCS:virtual-domain1=w1

- 5. Choisissez Eléments de stratégie > Autorisation et autorisations > Administration de périphériques > Profils de shell afin de créer un nouveau profil de shell.
- 6. Entrez un nom significatif (tel que WCS), puis cliquez sur l'onglet Attributs personnalisés.
- 7. Configurez les attributs tels qu'ils existent sur
  - WCS.

Manually Entered

Attribute	Requirement	Value	
role0	Mandatory	LobbyAmbassador	
task0	Mandatory	Configure Guest Users	
task1	Mandatory	Lobby Ambassador User Preferences	
virtual-domain0	Mandatory	root	

**Remarque :** dans les versions d'ACS antérieures à la version 5.2 du correctif 7, vous pouvez rencontrer des problèmes lorsque vous entrez une tâche qui contient le mot « alerte ». Ceci est corrigé dans les versions ACS ultérieures. Le même problème existe dans les versions d'ISE (Identity Services Engine) antérieures à la version 1.2.Voici un exemple de saisie manuelle des attributs :

-type "role0" in the "Attribute" field -type "LobbyAmbassador" in the Value field -click the "add" button. Etc... for the other attributes.

**Remarque :** dans ACS 4, il était possible de copier/coller la liste des attributs de l'interface utilisateur graphique WCS vers l'interface utilisateur graphique ACS 4. Dans ACS 5, elles doivent être entrées une par une.Dans NCS et Prime Infrastructure, l'attribut doit être entré

dans un ordre très spécifique. L'ordre est le domaine virtuel, le rôle et la liste des tâches. S'il est entré dans le mauvais ordre, NCS/Prime refuse l'authentification.

NCS:virtual-domain0=ROOT-DOMAIN NCS:role0=Super Users NCS:task0=View Alerts and Events

#### Étape 4. Configurez Cisco Secure ACS pour renvoyer les attributs.

1. Configurez un utilisateur (cet exemple utilise *Lobbyad*) en tant qu'utilisateur sur ACS.



**Remarque :** Pour faciliter la configuration, cet exemple ajoute l'utilisateur Lobbyad au groupe *WCS-users*. (Cette étape est facultative.)

 Dans les stratégies Access, sous Default Device Admin > Authorization, configurez une règle correspondant à l'authentification WCS.

1 Section 2012 11 Section 2012

- 3. Si le nom d'utilisateur appartient au groupe *WCS-users*, renvoyez le profil de l'interpréteur de commandes *wcs* (qui contient les attributs du groupe).
- 4. Si vous souhaitez configurer d'autres types d'utilisateurs (tels que les administrateurs), vous devez configurer un autre profil de shell pour renvoyer différents attributs. À partir de ce moment, vous devez regrouper les administrateurs dans un groupe différent afin de différencier et de savoir quel profil de shell retourner.

# **Vérification**

Aucune procédure de vérification n'est disponible pour cette configuration.

## **Dépannage**

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

## Informations connexes

- Guide de configuration du système de contrôle sans fil Cisco, version 7.0.172.0
- Guide de l'utilisateur de Cisco Secure Access Control System 5.2
- Support et documentation techniques Cisco Systems