

# Exemplo de configuração da Prime Infrastructure Integration com ACS 4.2 TACACS

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configurações](#)

[Adicionar o ACS como servidor TACACS no PI](#)

[Configurações do modo AAA no PI](#)

[Recuperar atributos da função de usuário do PI](#)

[Configurar o ACS 4.2](#)

[Verificar](#)

[Troubleshoot](#)

## Introduction

Este documento descreve o exemplo de configuração do Terminal Access Controller Access Control System (TACACS+)

autenticação e autorização no aplicativo Cisco Prime Infrastructure (PI).

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Definir PI como um cliente no Access Control Server (ACS)
- Defina o endereço IP e uma chave secreta compartilhada idêntica no ACS e no PI

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ACS versão 4.2
- Prime Infrastructure versão 3.0

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.

# Configurar

## Configurações

### Adicionar o ACS como servidor TACACS no PI

Conclua estes passos para adicionar o ACS como um servidor TACACS:

Etapa 1. Navegar para **Administração > Usuários > Usuários, funções e AAA no PI**

Etapa 2. No menu da barra lateral esquerda, selecione **TACACS+ Servers**, em **Add TACACS+ servers**, clique em **Go** e a página aparecerá como mostrado na imagem:

The screenshot shows the Cisco Prime Infrastructure web interface. The top navigation bar includes the Cisco logo and 'Prime Infrastructure'. Below it, the breadcrumb path is 'Administration / Users / Users, Roles & AAA'. A left sidebar contains a menu with items like 'AAA Mode Settings', 'Active Sessions', 'Change Password', 'Local Password Policy', 'RADIUS Servers', 'SSO Server Settings', 'SSO Servers', 'TACACS+ Servers' (highlighted), 'User Groups', and 'Users'. The main content area is titled 'Add TACACS+ Server' and contains the following fields:

- \* IP Address: [Empty text box]
- \* DNS Name: [Empty text box]
- \* Port: [49]
- Shared Secret Format: [ASCII]
- \* Shared Secret: [Empty text box with help icon]
- \* Confirm Shared Secret: [Empty text box]
- \* Retransmit Timeout: [5] (secs)
- \* Retries: [1]
- Authentication Type: [PAP]
- Local Interface IP: [10.106.68.130]

At the bottom of the form are 'Save' and 'Cancel' buttons.

Etapa 3. Adicione o endereço IP do servidor ACS.

Etapa 4. Insira o segredo compartilhado TACACS+ configurado no servidor ACS.

Etapa 5. Digite novamente o segredo compartilhado na caixa de texto **Confirmar segredo compartilhado**.

Etapa 6. Deixe o restante dos campos em sua configuração padrão.

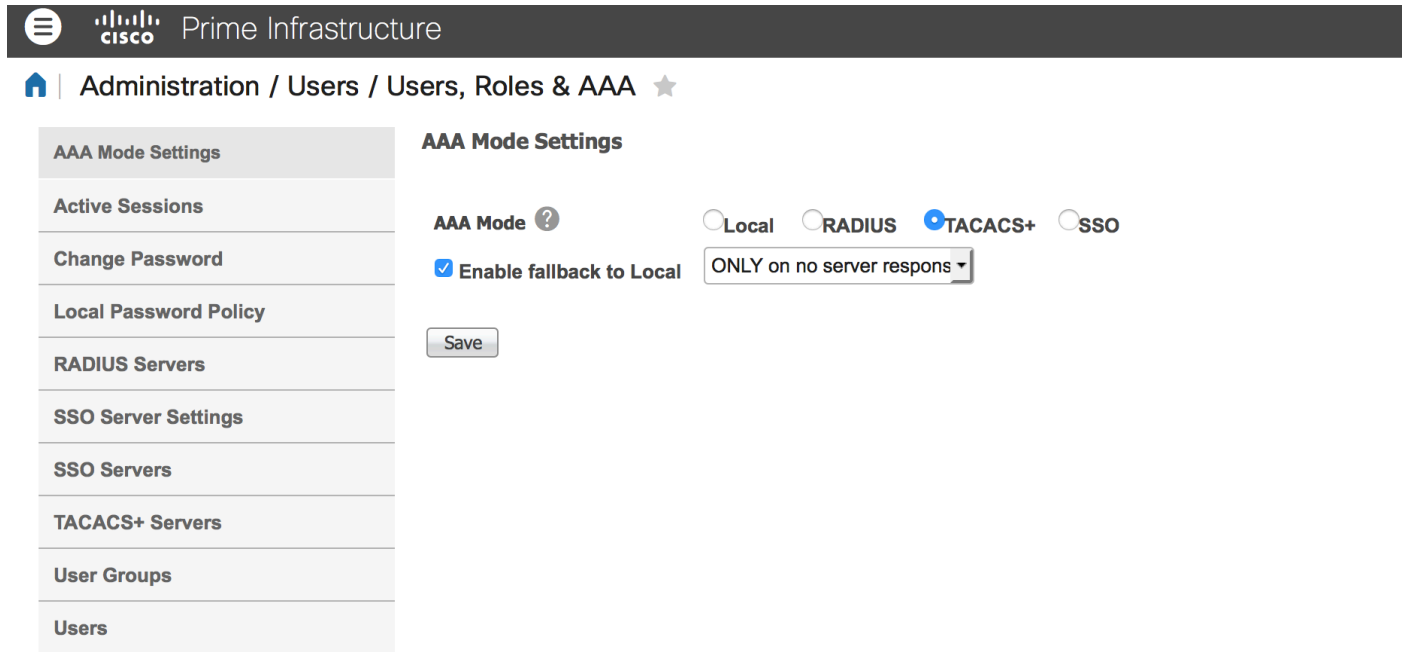
Passo 7. Clique em Submit.

### Configurações do modo AAA no PI

Para escolher um modo de Autenticação, Autorização e Auditoria (AAA), faça o seguinte:

Etapa 1. Navegue até **Administration > AAA**.

Etapa 2. Escolha **AAA Mode** no menu da barra lateral esquerda, você pode ver a página como mostrado na imagem:

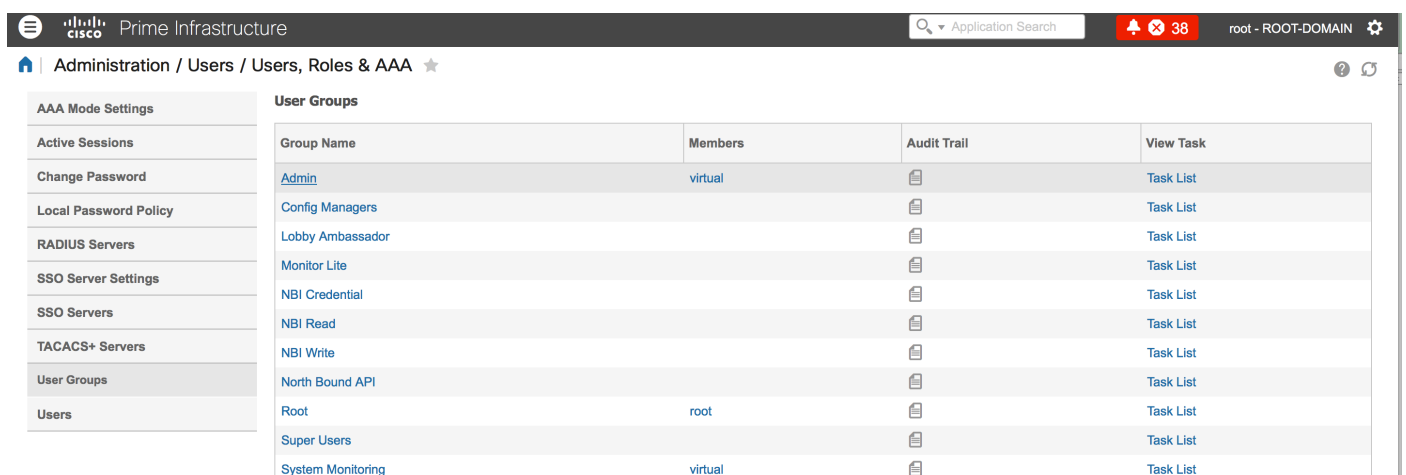


Etapa 3. Selecione **TACACS+**.

Etapa 4. Marque a caixa **Enable Fallback to Local**, se desejar que o administrador use o banco de dados local quando o servidor ACS não estiver acessível. Essa é uma configuração recomendada.

## Recuperar atributos da função de usuário do PI

Etapa 1. Navegue até **Administration > AAA > User Groups**. Este exemplo mostra a autenticação do administrador. Procure o **nome do grupo administrativo** na lista e clique na opção **Lista de tarefas** à direita, como mostrado na imagem:



Quando você clica na opção **Lista de tarefas**, a janela é exibida, como mostrado na imagem:

## Task List

Please copy and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server.

### TACACS+ Custom Attributes

```
role0=Admin
task0=View Alerts and Events
task1=Run Job
task2=Device Reports
task3=Alarm Stat Panel Access
task4=RADIUS Servers
task5=Raw NetFlow Reports
task6=Credential Profile Delete Access
task7=Compliance Audit Fix Access
task8=Network Summary Reports
task9=Discovery View Privilege
task10=Configure ACS View Servers
task11=Run Reports List
task12=View CAS Notifications Only
task13=Administration Menu Access
task14=Monitor Clients
task15=Configure Guest Users
task16=Monitor Media Streams
task17=Configure Lightweight Access Point
Templates
task18=Monitor Chokepoints
task19=Maps Read Write
task20=Administrative privileges under Manage and
```

### RADIUS Custom Attributes

If the size of the RADIUS attributes on your AAA server is more than 4096 bytes, Please copy ONLY role retrieve the associated TASKS

```
NCS:role0=Admin
NCS:task0=View Alerts and Events
NCS:task1=Run Job
NCS:task2=Device Reports
NCS:task3=Alarm Stat Panel Access
NCS:task4=RADIUS Servers
NCS:task5=Raw NetFlow Reports
NCS:task6=Credential Profile Delete Access
NCS:task7=Compliance Audit Fix Access
NCS:task8=Network Summary Reports
NCS:task9=Discovery View Privilege
NCS:task10=Configure ACS View Servers
NCS:task11=Run Reports List
NCS:task12=View CAS Notifications Only
NCS:task13=Administration Menu Access
NCS:task14=Monitor Clients
NCS:task15=Configure Guest Users
NCS:task16=Monitor Media Streams
NCS:task17=Configure Lightweight Access Point
Templates
NCS:task18=Monitor Chokepoints
NCS:task19=Maps Read Write
NCS:task20=Administrative privileges under Manage
```

Etapa 2. Copie esses atributos e salve-os em um arquivo do bloco de notas.

Etapa 3. Talvez seja necessário adicionar atributos de domínio virtual personalizados no servidor ACS. Os atributos de domínio virtual personalizados estão disponíveis na parte inferior da mesma página da lista de tarefas.

Virtual Domain custom attributes are mandatory. To add custom attributes related to Virtual Domains, please click [here](#).

Etapa 4. Clique na opção **clique aqui** para obter a página de atributos do domínio virtual e você pode ver a página, como mostrado na imagem:

### TACACS+ Custom Attributes

```
virtual-domain0=ROOT-DOMAIN
virtual-domain1=test1
```

### RADIUS Custom Attributes

```
NCS:virtual-domain0=ROOT-DOMAIN
NCS:virtual-domain1=test1
```

## Configurar o ACS 4.2

Etapa 1. Faça login na GUI do administrador do ACS e navegue para a página Interface Configuration > TACACS+.

Etapa 2. Crie um novo serviço para prime. Este exemplo mostra um nome de serviço configurado com o nome NCS, como mostrado na imagem:

## New Services

		Service	Protocol
<input checked="" type="checkbox"/>	<input type="checkbox"/>	ciscowlc	common
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Wireless-WCS	HTTP
<input checked="" type="checkbox"/>	<input type="checkbox"/>	NCS	HTTP
<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>		

Etapa 3. Adicione todos os atributos do bloco de notas criado na Etapa 2 à configuração de usuário ou grupo. Certifique-se de adicionar atributos de domínio virtual.

**NCS HTTP**

**Custom attributes**

```
virtual-domain0=ROOT-DOMAIN
role0=Admin
task0=View Alerts and Events
task1=Device Reports
task2=RADIUS Servers
task3=Alarm Stat Panel Access
```

Etapa 4. Click OK.

## Verificar

Faça login no prime com o novo nome de usuário criado e confirme se você tem a função **Admin**.

## Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Analise o arquivo usermgmt.log da CLI raiz primária disponível no diretório `/opt/CSColumos/logs`. Verifique se há mensagens de erro.

```
user entered username: 138527]
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - [          [TacacsLoginModule]
Primary server=172.18.70.243:49]
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - Thread Id : [835], Entering
Method : [login], Class : [com.cisco.xmp.jaas.tacacs.TacacsLoginClient].
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - Thread Id : [835], Entering
Method : [login], Class : [com.cisco.xmp.jaas.tacacs.SecondaryTacacsLoginClient].
2016-05-12 15:24:18,518 [http-bio-443-exec-10] INFO usermgmt - [Tacacs:connectTacacs()] :
[prepare to ping TACACS+ server (> 0):/172.18.70.243 (-1)].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] INFO usermgmt - [Tacacs:connectTacacs()] :
[Tacacs: Num of ACS is 3].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] INFO usermgmt - [Tacacs:connectTacacs()] :
[Tacacs:activeACSIndex is 0].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] INFO usermgmt - [Tacacs:connectTacacs()] :
[Tacacs: Unable to connect to Server 2: /172.18.70.243 Reason: Connection refused].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] DEBUG usermgmt - [          [Thu May 12 15:24:18
EST 2016] [TacacsLoginModule] exception in client.login( primaryServer, primaryPort,seconda...
com.cisco.xmp.jaas.XmpAuthenticationServerException: Server Not Reachable: Connection refused]
```

**Este exemplo mostra um exemplo de mensagem de erro, que pode ser devido a vários motivos como conexão recusada por um firewall, qualquer dispositivo intermediário etc.**