

ISE 2.x に対してプライム記号 3.1 TACACS認証を設定して下さい

目次

[はじめに](#)

[要件](#)

[設定](#)

[設定の発動を促して下さい](#)

[ISE 設定](#)

[トラブルシューティング](#)

概要

この資料に Prime Infrastructure を ISE 2.x の TACACS によって認証するために設定する方法を記述されています。

要件

次の項目に関する基本的な知識があることが推奨されます。

- Identity Services Engine (ISE)
- Prime Infrastructure

設定

Cisco Prime Network Control System 3.1

Cisco 識別 サービス エンジン 2.0 またはそれ以降。

(注 : ISE はバージョン 2.0 から開始する TACACS だけをサポートしますが Radius を使用するためにプライム記号を設定することは可能性のあるです。プライム記号は ISE またはサードパーティ ソリューションのより古いバージョンの TACACS に加えて Radius を使用するために好んだら RADIUS特性のリストが含まれています。)

主な設定

次の画面への Navigate: 次を見られる管理/ユーザ ユーザ、ロール及び AAA。

そこに、TACACS+ サーバ タブを選択したら、そして上部右上隅の追加 TACACS+ サーバオプションを選択し、『Go』を選択して下さい。

Next 画面で TACACSサーバ エントリの設定は利用できます (これは各々の個々の TACACSサーバのためにされなければなりません)

AAA Mode Settings	Add TACACS+ Server
Active Sessions	<input checked="" type="radio"/> IP Address <input type="text"/>
Change Password	<input type="radio"/> DNS Name <input type="text"/>
Local Password Policy	* Port <input type="text" value="49"/>
RADIUS Servers	Shared Secret Format <input type="text" value="ASCII"/>
SSO Server Settings	* Shared Secret <input type="text"/>
SSO Servers	* Confirm Shared Secret <input type="text"/>
TACACS+ Servers	* Retransmit Timeout <input type="text" value="5"/> (secs)
User Groups	* Retries <input type="text" value="1"/>
Users	Authentication Type <input type="text" value="PAP"/>
	Local Interface IP <input type="text" value="192.168.10.154"/>

サーバの IP アドレスか DNS アドレス、また共有秘密キーを入力する必要があります。またこの同じ IP アドレスが ISE で AAA クライアントにあとで使用できるように、使用するために望む以下の事項に注意して下さい:ローカルインターフェイス IP。

プライム記号の設定を完了するため。AAA モード設定タブの下で管理/ユーザ/ユーザ、役割及び AAA の下で TACACS をイネーブルにする必要があります。

(注: 特に設定をテストしている間) 無応答または失敗オプションまたはとサーバレスポンスのだけローカル オプションにイネーブル フォールバックを、チェックすることを推奨します、

AAA Mode Settings	AAA Mode Settings
Active Sessions	AAA Mode <input type="radio"/> Local <input type="radio"/> RADIUS <input checked="" type="radio"/> TACACS+ <input type="radio"/> SSO
Change Password	<input checked="" type="checkbox"/> Enable fallback to Local <input type="text" value="ONLY on no server respon:"/>
Local Password Policy	<input type="button" value="Save"/>
RADIUS Servers	
SSO Server Settings	
SSO Servers	
TACACS+ Servers	
User Groups	
Users	

ISE 設定

プライム記号を ISE の AAA クライアントで作業センター/デバイス 管理/ネットワークリソース /ネットワークデバイスで設定して下さい/追加して下さい

Network Devices	Network Devices												
Default Devices	Selected 0 Total 0												
TACACS External Servers	<input type="button" value="Edit"/> <input checked="" type="button" value="Add"/> <input type="button" value="Duplicate"/> <input type="button" value="Import"/> <input type="button" value="Export"/> <input type="button" value="Generate PAC"/> <input type="button" value="Delete"/>												
TACACS Server Sequence	Show <input type="text" value="All"/>												
	<table border="1"> <thead> <tr> <th>Name</th> <th>IP/Mask</th> <th>Profile Name</th> <th>Location</th> <th>Type</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td colspan="6" style="text-align: center;">No data available</td> </tr> </tbody> </table>	Name	IP/Mask	Profile Name	Location	Type	Description	No data available					
Name	IP/Mask	Profile Name	Location	Type	Description								
No data available													

主なサーバのための情報を入力して下さい。含む必要がある必須属性はネーム、IP アドレスで

、TACACS および共有秘密にオプションを選択します。これがオプションであるどんなに承認規則か他の情報を条件としてあとで使用するためにその上にプライム記号に対するデバイスの種類を、とりわけ、追加したい場合もあります。

Network Devices List > New Network Device

Network Devices

Name

Description

* IP Address: / 32

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

Location

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

それから ISE からの必須 属性を発動を促すために送信 するように TACACS プロファイルの結果をアクセスの正しいレベルを提供するために作成して下さい。作業センター/ポリシーへのナビゲートは/Tacacs プロファイル生じ、追加オプションを選択します。

Identity Services Engine

Home > Operations > Policy > Guest Access > Administration > Work Centers

TrustSec > Device Administration

Overview > Identities > User Identity Groups > Network Resources > Network Device Groups > Policy Conditions > Policy Results

TACACS Command Sets

TACACS Profiles

Rows/Page 6 << 1 / 1 >> Go 6 Total Rows

Refresh Duplicate Trash Edit Filter

Name	Description
------	-------------

名前を設定し、プロフィール属性ボックスの下で属性を入力するために未加工ビューのオプションを使用して下さい。属性は概要サーバ自体から来ます。

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers License Warning

TrustSec Device Administration Overview Identities User Identity Groups Network Resources Network Device Groups Policy Conditions Policy Results Device Admin Policy Sets Reports Settings

TACACS Profiles > New

TACACS Profile

Name *

Description

Task Attribute View Raw View

Profile Attributes

属性を管理/ユーザ ユーザ、役割及び AAA 画面の下で得、ユーザグループ タブを選択して下さい。提供したいアクセスのグループレベルを選択します。この Admin 例で提供されます左側で適切な課業 表の選択によってアクセスして下さい。

Administration / Users / Users, Roles & AAA

AAA Mode Settings	User Groups			
Active Sessions	Group Name	Members	Audit Trail	View Task
Change Password	Admin	JP		Task List
Local Password Policy	Config Managers			Task List
RADIUS Servers	Lobby Ambassador	User1 , CostaRica , Yfta		Task List
SSO Server Settings	Monitor Lite			Task List
SSO Servers	NBI Credential			Task List
TACACS+ Servers	NBI Read			Task List
User Groups	NBI Write			Task List
Users	North Bound API			Task List
	Root	root		Task List
	Super Users			Task List
	System Monitoring			Task List
	User Assistant			Task List
	User Defined 1			Task List
	User Defined 2			Task List
	User Defined 3			Task List
	User Defined 4			Task List
	mDNS Policy Admin			Task List

TACACS カスタム属性すべてをコピーして下さい。

AAA Mode Settings

Active Sessions

Change Password

Local Password Policy

RADIUS Servers

SSO Server Settings

SSO Servers

TACACS+ Servers

User Groups

Users

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=Discovery Schedule Privilege
task1=Mesh Reports
task2=Saved Reports List
task3=Monitor Menu Access
task4=Device WorkCenter
task5=Inventory Menu Access
task6=Add Device Access
task7=Config Audit Dashboard
task8=Custom NetFlow Reports
task9=Apic Controller Read Access
task10=Configuration Templates Read Access
task11=Alarm Policies Edit Access
task12=High Availability Configuration
task13=View Job
task14=Incidents Alarms Events Access
task15=TAC Case Management Tool
task16=Configure Autonomous Access Point Templates
task17=Import Policy Update
task18=PnP Profile Read-Write Access
task19=SSO Server AAA Mode
task20=Alarm Resource Access
```

RADIUS Custom Attributes

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

```
NCS:role0=Admin
NCS:task0=Discovery Schedule Privilege
NCS:task1=Mesh Reports
NCS:task2=Saved Reports List
NCS:task3=Monitor Menu Access
NCS:task4=Device WorkCenter
NCS:task5=Inventory Menu Access
NCS:task6=Add Device Access
NCS:task7=Config Audit Dashboard
NCS:task8=Custom NetFlow Reports
NCS:task9=Apic Controller Read Access
NCS:task10=Configuration Templates Read Access
NCS:task11=Alarm Policies Edit Access
NCS:task12=High Availability Configuration
NCS:task13=View Job
NCS:task14=Incidents Alarms Events Access
NCS:task15=TAC Case Management Tool
NCS:task16=Configure Autonomous Access Point Templates
NCS:task17=Import Policy Update
NCS:task18=PnP Profile Read-Write Access
NCS:task19=SSO Server AAA Mode
NCS:task20=Alarm Resource Access
```

Virtual Domain custom attributes are mandatory. To add custom attributes related to Virtual Domains, please click here.

それから ISE のプロファイルの未加工ビュー セクションにそれらを貼り付けて下さい。

Identity Services Engine

Home Operations Policy Guest Access Administration Work Centers

TrustSec Device Administration

Overview Identities User Identity Groups Network Resources Network Device Groups Policy Conditions Policy Results Device Admin Policy Sets Reports Settings

TACACS Command Sets

TACACS Profiles

TACACS Profiles > New

TACACS Profile

Name * Prime

Description

Task Attribute View Raw View

Profile Attributes

```
role0=Admin
task0=Discovery Schedule Privilege
task1=Mesh Reports
task2=Saved Reports List
task3=Monitor Menu Access
task4=Device WorkCenter
task5=Inventory Menu Access
task6=Add Device Access
task7=Config Audit Dashboard
task8=Custom NetFlow Reports
task9=Apic Controller Read Access
task10=Configuration Templates Read Access
task11=Alarm Policies Edit Access
task12=High Availability Configuration
task13=View Job
```

Cancel Submit

バーチャルドメイン カスタム属性は必須です。ルートドメイン情報は主な管理の下で -> バーチャルドメインを見つけることができます。

Cisco Prime Infrastructure

Virtual Domain ROOT-DOMAIN | root

Monitor Configuration Inventory Maps Services Reports Administration

Administration > Virtual Domains

Virtual Domains

Virtual Domains

ROOT-DOMAIN

Virtual Domains > ROOT-DOMAIN

ROOT-DOMAIN

Virtual domains are logical groupings of devices and are used to control who can administer a group. After you add devices to Prime Infrastructure, you can configure virtual domains. Virtual domain filters allow users to configure devices, view alarms, and generate reports their assigned part of the network only.

* Name ROOT-DOMAIN

Time Zone -- Select Time Zone --

Email Address

Description ROOT-DOMAIN

Submit Cancel

主なバーチャルドメインの名前は属性 `virtual-domain0="virtual` ドメイン名として」追加されなければなりません

TACACS Profiles > Prime Access

TACACS Profile

Name: Prime Access

Description:

Task Attribute View | Raw View

Profile Attributes

```
task162=Monitor Mobility Devices
task163=Context Aware Reports
task164=Voice Diagnostics
task165=Configure Choke Points
task166=RPM Dashboard
task167=Swim Delete
task168=Theme Changer Access
task169=Import Policy Update
task170=Design Endpoint Site Association Access
task171=Planning Mode
task172=Pick and Unpick Alerts
task173=Configure Menu Access
task174=Ack and Unack Security Index Issues
task175=Ack and Unack Alerts
task176=Auto Provisioning
virtual-domain0=ROOT-DOMAIN
```

Cancel Save

それがすべてできれば作業センター/デバイス管理/デバイス Admin ポリシー セットの下で前の手順で、作成されるシェルプロファイルを割り当てるルールを作成する必要があります

(注: 「きちんとこのルール Filters 要求のようにプライム記号の IP アドレスのようなフィルタのプライム記号が別のタイプのために「デバイスの種類」を特に使用することができるどんなに条件」は配置によっての 1 として「調節します」変わります)

Policy Sets

Search policy names & descriptions.

Summary of Policies

Global Exceptions

Default

Tacacs_Default

Save Order Reset Order

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
<input checked="" type="checkbox"/>	Default	Tacacs_Default

Regular Proxy Sequence

Authentication Policy

Default Rule (if no match) : Allow Protocols : Default Device Admin and use : Internal Users

Authorization Policy

Exceptions (0)

Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	Prime Rule	if DEVICE Device Type EQUALS All Device Types#Prime	then PermitAll AND	Prime
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then	Select Profile(s) Deny All Shell Profile	

この時点で設定は完了したはずですが。

トラブルシューティング

この設定が不成功なら、そしてローカル フォール バック オプションがプライム記号のイネーブル、ISE からプライム記号の IP アドレスの削除によって失敗を、強制できます。これにより ISE は応答し、ローカル信任状の使用を強制します。ローカル フォールバックがリジェクトで実行されたために設定される場合ローカルアカウントはまだ顧客へのアクセスをはたらかせ、提供しません。

ISE が認証の成功を示し、しかし正しいルールを一致すればプライム記号はまだプロファイルで正しく設定される属性を慎重に検査したい場合もある追加属性は送信 されて いません要求を拒否して。