GUI を使用した Aironet アクセス ポイントでの ログイン認証用 TACACS+ の設定例

内容

 概要

 前提条件

 要件

 使用するコンポーネント

 表記法

 設定

 ネットワーク図

 ACS 4.1 を使用したログイン認証用の TACACS+ サーバの設定

 ACS 5.2 を使用したログイン認証用の TACACS+ サーバの設定

 TACACS+ 認証用の Aironet AP の設定

 確認

 ACS 5.2 の検証

 トラブルシュート

 関連情報

<u>概要</u>

このドキュメントでは、TACACS Plus(TACACS+)サーバを使用してログイン認証を実行する ために、Cisco Aironet Access Point(AP; アクセス ポイント)上で TACACS+ サービスを有効に する方法について説明しています。

前提条件

<u>要件</u>

この設定を行う前に、次の要件が満たされていることを確認します。

- Aironet AP での基本的なパラメータの設定方法に関する知識
- Cisco Secure Access Control Server(ACS)のような TACACS+ サーバを設定する方法に関 する知識
- TACACS+の概念に関する知識

TACACS+ の動作の仕組みについては、『<u>RADIUS サーバと TACACS+ サーバの設定』の「</u> <u>TACACS+ について」を参照してください。</u>

<u>使用するコンポーネント</u>

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Aironet 1240/1140 シリーズ アクセス ポイント
- •ソフトウェア バージョン 4.1 が稼働する ACS
- ソフトウェア バージョン 5.2 が稼働する ACS

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

<u>表記法</u>

ドキュメント表記の詳細は、『<u>シスコ テクニカル ティップスの表記法』を参照してください。</u>

設定

このセクションでは、TACACS+ ベースのログイン認証用に Aironet AP および TACACS+ サーバ (ACS)を設定する方法について説明しています。

この設定例では、次のパラメータを使用します。

- ACSのIPアドレス: 172.16.1.1/255.255.0.0
- APのIPアドレス: 172.16.1.30/255.255.0.0
- AP と TACACS+ サーバで使用される共有秘密キー: Example
- この例で ACS に設定するユーザのクレデンシャルは次のとおりです。
 - ユーザ名: User1
 - ・パスワード: Cisco
 - グループ: AdminUsers

Web インターフェイスまたは Command-Line Interface (CLI; コマンドライン インターフェイス)を使用して AP に接続しようとするユーザを検証するように、TACACS+ 機能を設定する必要があります。 この設定を実現するには、次の作業を行う必要があります。

1. <u>ログイン認証用の TACACS+ サーバの設定</u>

2. TACACS+ 認証用の Aironet AP の設定

注: このドキュメントで使用されているコマンドの詳細を調べるには、<u>Command Lookup</u> <u>Tool(登録</u>ユーザ専用)を使用してください。

<u>ネットワーク図</u>

このドキュメントでは、次のネットワーク セットアップを使用します。



<u>ACS 4.1 を使用したログイン認証用の TACACS+ サーバの設定</u>

最初に、AP へのアクセスを試みるユーザを検証するように、TACACS+ デーモンを設定します。 TACACS+ 認証用に ACS を設定し、ユーザ データベースを作成する必要があります。任意の TACACS+ サーバを使用できます。この例では、ACS を TACACS+ サーバとして使用しています 。次のステップを実行します。

 次の手順を実行して、AP を Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウンティング) クライアントとして追加します。ACS の GUI で、Network Configuration タブをクリックします。AAA Clients の下で [Add Entry] をクリックします。 Add AAA Client ウィンドウで、AP ホスト名、AP の IP アドレス、および共有秘密キーを入力します。この共有秘密キーは、AP に設定する共有秘密キーと一致する必要があります。 Authenticate Using ドロップダウン メニューから、TACACS+ (Cisco IOS) を選択します。 設定を保存するには、Submit + Restart をクリックします。以下が一例です。

CISCOSECURE ALS - MICROSO	it Internet Lighteer	
Ele Edt Yew Favorites	Iools Help	Leis » 🏨
Address A http://127.0.0.1:10	65/	🚽 🔁 🐼
Casco Statems Ne	etwork Configuration	×
Liser Setup Erroup Setup SharedProfile Components Network Configeration	Add AAA Client AA Client Hostname AccessPoint AA Client IP Address 172.16.1.30	AAA Client Hestname AAA Client Hestname AAA Client He Address Shated Sector Shate
Suprem Configuration S Configuration R Configuration R Configuration R Configuration R Configuration R Configuration R	hared Secret Example CADIUS Key Wrap Cey Encryption Key Message Authenticator Code	AAA Client Log BADEVS Innerling Packets from this AAA Client Replace RADEVS Port info with Username from this AAA Client Match Framed IP: Address with user IP address for accounting packets from this AAA Stient
Postule Validation	ey Input Format C ASCII @ Hexadecimal	AAA Cliest Hostname
A Reports and	uthenticate Using TACACS+ (Cisco IOS)	name assigned to the AAA client.
Contine Documentation	Log Update/Watchdog Packets from this AAA Client	AAA Client IP Address The AAA Client IP Address is the IP address assigned to the
	Replace RADIUS Port info with Username from this AAA Client Match Framed-IP-Address with user IP address for accounting packets from this AAA Client Submit Submit + Apply Cancel	If you want to designate more than one AAA client with a single AAA client entry in ACS, you can spacify the IP address for each AAA client to be represented by this AAA client entry. To separate each ID address, press fater.

この例では次の設定を使用しています。AAA クライアントのホスト名:AccessPointAAA ク ライアントの IP アドレス:172.16.1.30/16共有秘密キー:Example

2. 次の手順を実行して、すべての管理(admin)ユーザを含むグループを作成します。左側の

メニューで Group Setup をクリックします。新しいウィンドウが表示されます。Group Setup ウィンドウで、設定するグループをドロップダウン メニューから選択して、Rename Group をクリックします。この例では、Group 6 をドロップダウン メニューから選択し、グ ループの名前を AdminUsers に変更します。[Submit] をクリックします。以下が一例です。

CiscoSecure ACS -	Microsoft Internet Explorer	
Ele Edt Yew Fg	workes Iools Help	Leás 🍅 🍂
Address http://127.	0.0.1:1065/	🗾 🛃 🐼
Cinco Statems	Group Setup	×
dis dis		
	Select	Help
Setup	Renaming Group: Group 6	Rename Group
Braup Betus		
an I Sharet Profile		
Components	Group AdminUsers	Raname Group
Network Configuration	Submit Cancel	Type a new group name and click Submit to assign a more descriptive name to the group profile. This is useful if different groups.
20 Suten		as PPP or Telest-only capability.
Listerfus	P Back to Help	Click Cancel to return to the Group Satup window without saving a
Configuration		new group name.
Administration Control		[Back to Tap]
12 External User		
BC I Dutabases		
Validation		
Network Access Profiles		
Reports and		
Activity		
Documentation		
(a)		Dirternet

 次の手順を実行して、TACACS+ データベースにユーザを追加します。User Setup タブをク リックします。新しいユーザを作成するには、User フィールドにユーザ名を入力し、 Add/Edit をクリックします。次に示す例では、User1 を作成しています。



Add/Edit をクリックすると、このユーザに対する Add/Edit ウィンドウが表示されます。

このユーザに固有のクレデンシャルを入力し、Submit をクリックして設定を保存します。
 入力できるクレデンシャルは次のものです。補足ユーザ情報ユーザ設定ユーザが割り当てられているグループ以下が一例です。

CiscoSecure ACS - Mi	rosoft Internet Explorer	2 (B)
Address http://127.0.0	rees Toos Geb	Unis ** 🧃 • 🛐 60
Cisco Systems	User Setup	×
addisaaddisa.	Edit	A Help
User Setup	User: User1 (New User)	Account Disabled District and Disabled
Setup	Account Disabled	Supplementary User Infe Password Authentication
Components	Supplementary User Info 🦻	Grant IP Address Assignment Grant IP Address Assignment
Configuration	Real Name User1	Advanced Settings Network Access Restrictions Max Sections
Configuration	Description	Usage Overlan Account Disable
Administration		Develoadable ALs Advanced IACACS - Settings TACACS - Enable Control
External User	User Setup 🙎	TACACS - Enable Passmeet TACACS - Outbound Passmeet TACACS - Shall command Authorization
Pesture Validation	Password Authentication:	Econsand Antherization Fee Network Device Management Applications Econsand Antherization Fee Network Device Management Applications TACACS - Unknown Services
Network Access Profiles	CiscoSecure PAP (Also used for CHAP/MS-	ELTE BADIUS Attributes BADIUS Yender Specific Attributes
Reports and Activity	CHAP/ARAP, if the Separate held is not checked.)	
Online Documentation	Confirm	Account Disabled Status Select the Account Disabled check box to disable this account clear
	Separate (CHAP/MS-CHAP/ARAP)	the check box to enable the account.
	Password	Deleting a Usersame
	Password	The Delete button appears only when you are editing an existing user
	When a token server is used for authentication,	 account not when you are adding a new user account. To delete the current user account from the database, click Delete. When asked to
[Submit Cancel	contirm your action, click OK.
a)		[Rack to Top]
この例では、	ユーザ User1 をグループ AdminUse	ers に追加しています。
EiscoSecure ACS - Mi	rosoft Internet Explorer	_10 ×
Ele Edt Yew Fgvo	ites Iools Heb	Unks * 🌋
Agaress g http://127.0.0	.1:1065/	· 200
Cisto Statead	User Setup	
anna anna.	licar Satura	- Help
User Setup		Account Disabled
Group	Password Authentication:	Celeting a Username Similar Infe
and the second	CiscoSecure PAP (Also used for CHAP/MS-	Password Authentication
Components	CHAP/ARAP, if the Separate field is not	Group to which the user is assigned Callback
Network Configuration	checked.)	Client IP Address Assignment
Man I compared		Network Access Restrictions
Configuration	Password •••••	
Interface	Password Confirm	Max Sections Unage Ountas
Configuration	Password Confirm Password Separate (CHAP/MS-CHAP/ARAP)	Man Sessions Manage Obstact Account Disable
	Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password	Man Seasing Usage Owntas Accept Disable Operational State Advanced IACACS - Settlings
Administration Control	Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Confirm	Man Seating Water Orestan Water Orestan Account Disable Overmissionable Account Disable Account Office Account Advanced IACACS - Settlings TACACS - Insubic Constant TACACS - Insubic Constant
Administration Centrel	Password Confirm Password CHAP/MS-CHAP/ARAP) Password Confirm Password Confirm Password	Max Seating Wasay Oraclas Account Disable Oremalizadable ACLs Advanced MACACS - Settings TACACS - Enable Control MACACS - Enable Control TACACS - Configured TACACS - Outbound Disarreed
Administration Centrel	Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password When a token server is used for authentication,	Man Section Manage Contex Manage Contex Account Disable Dermisedable ACLs Advanced DACAGS - Settings TACAGS - Easile Parametel TACAGS - Easile Parametel TACAGS - Dathered Parametel TACAGS - Shell Command Autorization
Administration Control Databases Parbase Parbase	Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is	Mass Seatime Mass Seatime Mass Contracts Access Darks Access Darks Dermisodable ACLs Advanced TACACS- Settings TACACS- Louble Contral TACACS- Continent Parametel TACACS- Continent Parametel TACACS- Shell Command Authorization Command Authorization for Network Device Management Applications TACACS- Uninnerm Services
Administration Control Databases Pasture Validation	Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.	Huner Content Huner Content Huner Content Account Datable Derminadable.AELe Advanced IACACS - Settlings IACACS - Inskin Content IACACS - Inskin Content IACACS - Continent Constant IACACS - Continent Constant IACACS - Continent Constant IACACS - Inskin Constant III IIIIIIIIIIIIIIIIIIIIIIIII
Administration Control Databases Pastare Validation Wetwork Access Profiles	Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled. Commente which the user is estimated	Mass Sections Masse Quertes Account Deable Reconst Deable Reconst Deable Decombadable.ALLs Advanced TACACS - Settings TACACS - Deable.Passment TACACS - Deable.Passment TACACS - Deable.Passment TACACS - Settings
Administration Control Deternal User Outabases Validation Weinschacces Profiles Reports and Access	Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled. Group to which the user is assigned:	Max Sessions Maxage Overlas Account Disable Overnisadable ACLs Advanced MACACS - Settings JACACS - Inable Control MACACS - Settings JACACS - Cotherend Passmeed MACACS - Shell Command Authorization Command Authorization Command Authorization MACACS - Shell Command Authorization MACACS - Universe Services ICUP RADUE Attributes RADUE Yunder Specific Attributes
Administration Control Control Deternal User Databases Partne Partne Partne Partne Partne Profiles Reports and Activity	Password Confirm Password Separate (CHAP/M5-CHAP/ARAP) Password Confirm Password Confirm Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled. Group to which the user is assigned: AdminUsers	Max Sessions Manage Overlas Account Disable Derminadable ACLs Advanced UACAGS - Settings TACAGS - Easile Parameted TACAGS - Easile Parameted TACAGS - Setting Parameted TACAGS - Shell Command Antherization Command Antherization for Network Device Management Applications TACAGS - Unknown Services TACAGS - Unknown Services TACAGS - Unknown Services REF RADIUS Attributes Account Disabled States
Administration Control Databases Databases Pastase Validation Wetwork Access Profiles Reports and Activity Daline Documentation	Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled. Group to which the user is assigned: AdminUsers Callback	Human Sensions Human Deable Account Deable Account Deable Advanced INCACS - Settings TACACS - Deable control TACACS - Deable Desensed TACACS - Control Desensed TACACS - Settings T
Control Control Control Control Detabases Parture Validation Perfus Perfus Reports and Cocumentation Documentation	Password Confirm Password Separate (CHAP/M5-CHAP/ARAP) Password Confirm Password Confirm Password Confirm Password Confirm Password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled. Group to which the user is assigned: AdminUsers Caliback Caliback Cuse group setting	Man Section Mana Contax Account Disable TatAASS - Settings TatAASSS - Settings TatAASS - Settings TatAASS -
Administration Control Detabases Detabases Partice Validation Wetwork Access Profiles Reports and Reports and Documentation	Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled. Group to which the user is assigned: AdminUsers Callback Callback C Use group setting C No callback allowed	Huas Services Huase Contex Access Disable Dermisodable.ACLs Advanced Disable.ACLs Advanced Disable.Contex Disable.Context Disable.Con
Administration Control Databases Posture Validation Validation Validation Validation Validation Validation Validation Validation	Password Conferm Password Separate (CHAP/MS-CHAP/ARAP) Password Conferm Password Conferm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled. Group to which the user is assigned: AdminUsers Callback Callback Callback allowed Callback using this number	Human Sections Home Contex Acceant Disable Description of States Acceant Disable States Select the Acceant Disabled check box to disable this accounty clear the check box to enable the account. Deleting a Unername The Deleting a Unername

注:特定のグループを作成しない場合、ユーザはデフォルトグループに割り当てられます。 5. 次の手順を実行して、特権レベルを定義します。Group Setup タブをクリックします。この ユーザに割り当ててあるグループを選択し、Edit Settings をクリックします。この例では、 グループ AdminUsers を使用しています。TACACS+ Settings で、Shell (exec) チェック ボ ックスおよび値を 15 にした Privilege level チェック ボックスにチェックマークを付けます 。[Submit + Restart] をクリックします。

dress 🛃 http://127	.0.0.1:1065/	
Cisco Systems	Group Setup	
albadba	Jacobia Access Restrictions	Help
Berry Setup Setup Setup Setup Shared Profile Components Defrom the Configuration System Configuration Interface Configuration Administration	In access control list Out access control list Route Routing Routing Routing Route Shell (exec) Access control list Auto command Callback line	Group Disabled Yeicn-aver-IP (VoIP) Support Default Time-of-Day Access Settings Callback Nativersk Access Restrictions Usage Operan Usage Operan Usage Operan Descriptions Table Options Token Carl Settings Description Advise Raiss ID Assignment Description Active TACACS+ Shell Command Authorization Command Authorization for Network Device Management Applications TACACS+ Unknown Services TACACS+ Construction
Databases Porture Validation Network Access Reports and Activity Online Documentation	□ Callback rotary □ □ Idle time □ □ No callback verify □ Enabled □ No escape □ Enabled □ No hangup □ Enabled □ Privilege level 15 □ Timeout □ Shell Command Authorization Set ○ None ○ Assign a Shell Command Authorization Set for any	 RADIUS Yeader Specific Attributes To enable administrators to tailor what authorizations are displayed for a configuration and to simplify the interface, ACS displays only the information for the current configuration. Specific Group Setup configuration options and security protocol attributes are displayed in Group Setup only in the following circumstances: A AAA dient that uses the specified protocol has been configured the Network Configuration section. For example, RADIUS settings appear only if you have configured a AAA client that uses RADIUS The specific services, protocols, and attributes have been selected for display for the appropriate protocol in the Interface Configurat section. A Token Card Server has been configured in the External User Databases section. Group Setup is used to enable and configure the particular authorizations assigned to an entire group of users. The group a user is assigned to is configured in the User Setup

注:レベル15でアクセスするには、GUIとTelnetに特権レベル15を定義する必要があります 。レベル1としてアクセスできるのは、デフォルトの場合のみです。特権レベルが定義され ていない場合、CLIでイネーブルモードに入ると(Telnetを使用)、

AccessPoint>**enable**

% Error in authentication

TACACS+ データベースにさらにユーザを追加する場合は、この手順のステップ2~4を繰り返します。以上の手順を終了すると、TACACS+ サーバは AP にログインしようとするユーザを検証できる状態になります。次に、TACACS+ 認証用に AP を設定する必要があります。

<u>ACS 5.2 を使用したログイン認証用の TACACS+ サーバの設定</u>

最初のステップは、AP を AAA クライアントとして ACS に追加し、ログイン用の TACACS ポリ シーを作成することです。

 AP を AAA クライアントとして追加するには、次の手順を実行します。ACS GUI で、 [Network Resources] をクリックしてから、[Network Devices and AAA Clients] をクリック します。[Network Devices] で、[Create] をクリックします。[Name] に AP のホスト名を入 力して、AP に関する説明を入力します。これらのカテゴリが定義されている場合は、 [Location] **と [Device Type] を選択します。**1 つの AP しか設定しないため、[Single IP Address] をクリックします。[IP Range(s)] をクリックすることによって、複数の AP の IP アドレスの範囲を追加できます。 次に、AP の IP アドレスを入力します。[Authentication Options] で、[TACACS+] **ボックスをオンにして、[Shared Secret]** を入力します。以下が一例です。

cisco Cisco Secure A	cs			ersetnin experientit Phoney Lig Cd. Abol	
* 😳 My Workspace	Network Resources > Network De	vices and AAA Clents > Create			
Childrenk Processor Network Device Groups Location Device Type Device Type Definic Type Definic Network Device Definic Network Device	Harrie AP1160 Description Autonomou Network Device Groups Location All Device Type All	us AP 1140 at Boor 1 Locations Device Types	_Beloct Select		
Gr Policy Elements Gr Access Policies Gr Access Policies Gr Access Policies Software Administration	Gingle IP Address P 17216130	C IP Fange(s)		TRACE+ @ Shared Secret: Croco Englis Connect Desce Eligiory TRACE+ Single Connect Support TRACE+ Point Compliant Single Connect Support RADUS	
	Bubryz Cancel				

 次のステップは、ログイン ユーザ名とパスワードを作成することです。[Users and Identity Stores] をクリックしてから、[Users] をクリックします。[作成(Create)] をクリックしま す。[Name] にユーザ名を入力して、説明を入力します。もしあれば、[Identity Group] を選 択します。[Password] テキスト ボックスにパスワードを入力して、[Confirm Password] に 再入力します。[Enable Password] にパスワードを入力することによって、有効なパスワー ドを変更できます。再入力して確認します。以下が一例です。

- 🖓 My Workspace Us	ers and identity Stores × Internal identity Stores × User I × Create				
Network Resources Network Resources Internative Annual Stores Internative Annual Stores Internative Annual Stores Internative Annual Stores Love Notis Love Active Directory RAL Security Taken Denvers RADUG Storethy Denvers RADUG Storethy Denvers RADUG Storethy Denvers RADUG Storethy Denvers Conticute ActiveDirectory Reductions Policy Denvers Access Policies Mentioning and Reports Montolong and Reports Sprant. Administration	Conservat Parame Login for Autonomous AP Conservat All Groups Password Information Password Information Password Information Continn Password Informa	e e	Enable Password Info Password must • Contain 4 - 32 Enable Password Continn Password	ernation characters	
Monitoring and Reports Monitoring Administration	• = Required facts				

3. 次の手順を実行して、特権レベルを定義します。[Policy Elements] > **[Authorizations and Permissions] > [Device Administration] > [Shell Profiles]** の順にクリックします。[Permit Access] **チェック ボックスをオンにして、[Duplicate]** をクリックします。



[Name] と [Description] を入力します。



[Common Tasks] タブを選択して、[Maximum Privilege] で [15] を選択します。

My Workspiece	Policy Denents > Authorizati	on and Permissione	- Device Administ
t Network Resources	Il transference and the		
Users and identity Stores	General Common	Tasks Custor	n Atributes
· Q. Policy Demonts	Privilege Level		
Bession Conditions	Default Privilege	Not in Uper +	
Date and Time	Maximum Privilege:	Static -	Value 15 -
Custom	Shell Attributes		
Network Conditions Authorization and Permissions	Access Control List	Notin Use +	2
+ Network Access	Auto Command:	Notin Use +	1
+ Device Administration	No Caliback Verify	Notin Use +	
Command Bats	No Escape	Notin Use +	1
 Named Permission Objects 	No Hans Litr	Notin Use +	
* 🕞 Access Policies		Real in Line	10
Monitoring and Reports	Laneous.	Per monte +	12
* 💐 Gystern Administration	Idle Time	Notin Use -	13
	Calback Line:	Notin Use +	15
	Caliback Rotary	Notin Use +	
COURSE IN A COURSE OF COURSE OF COURSE	O a Required fields		

[Submit] をクリックします。

4. 次の手順を実行して、認可ポリシーを作成します。[Access Policies] > **[Access Services]** > **[Default Device Admin] > [Authorization]** の順にクリックします。[Create] をクリックして、

新しい認可ポリシーを作成します。認可ポリシーのルールを作成するための新しいポップア ップが表示されます。もしあれば、特定のユーザ名と AAA クライアント(AP)の [Identity Group] や [Location] **などを選択します。**[Shell Profile] に対して [Select] をクリックして、 プロファイルにより作成された [Autonomous AP] を選択します。



これが終わったら、[Save Changes] をクリックします。[Default Device Admin] をクリック してから、[Allowed Protocols] をクリックします。[Allow PAP/ASCII] をオンにしてから、 [Submit] をクリックします。[Service Selection Rules] **をクリックして、TACACS を照合し 、Default Device Admin を指しているルールが存在することを確認します。**





<u>TACACS+認証用の Aironet AP の設定</u>

Aironet AP で TACACS+ の機能を有効にするには、CLI または GUI が使用できます。このセクションでは、GUI を使用して TACACS+ ログイン認証用に AP を設定する方法について説明しています。

GUIを使用して AP に TACACS+を設定するには、次の手順を実行します。

 次の手順を実行して、TACACS+ サーバのパラメータを定義します。AP の GUI で、 Security > Server Manager の順に選択します。[Security:Server Manager] ウィンドウが表示 されます。Corporate Servers 領域で、Current Server List ドロップダウン メニューから TACACS+を選択します。同じ領域で、TACACS+ サーバの IP アドレス、共有秘密、およ び認証ポート番号を入力します。[Apply] をクリックします。以下が一例です。

Cisco 105 Series AP - Security	- Server Manager - Microsoft	Internet Exp	lorer provided by Cisco Sys	stems, Inc.	L D L D L D L D L D L D L D L D L D L D
Bie Edit Vew Pavorites	Iools Help				100 E
4+8ack • → • 🕥 🕃 🖉	Search 📄 Favorites 👘	teda 🎯 🗌	👌 🥔 🖾 🕑 🤪 📖 .		
Address () http://10.77.244.194/	ap_sec_network-security_a.shtml#	CorpServers			■ ⁽²⁾ Go Units ¹⁰
to a transm					
LINCO STRIEMO	ALC: NO.				
ي مطالع مطالعة	Cisco	Airon	et 1240AG Seri	es Access Point	65
HOME	SERVER MANAGER	1	OLOBAL PROPERTIES		
EXPRESS SET-UP	Hostname ap				ap uptime is 2 hours, 53 minutes
EXPRESS SECURITY					
ASSOCIATION +	Security: Server Manage				
NETWORK +	Backup DADIIIS Segur				
INTERFACES SECURITY	Dackup roubios Server				
Admin Access	Backup RADIUS Server:			(Hostname or IP Address)	
Encryption Manager	Shared Secret				
SSID Manager	unarea occieti	-			and second second
AP Authantication					Apply Delete Cancel
Intrusion Detection	Corporate Servers				
Local RADIUS Server	Constitution				
Advanced Security	Current Server List				
SERVICES +	TACACS.				
SYSTEM SOFTWARE +	<new></new>	Server:		172.16.1.1	(Hostname or IP Address)
EVENTLOG +	172.16.1.1	Shared	Secret:	*****	
	Delete	Authent	ication Port (optional):	49 (0-65536)	
		Account	ting Port (optional):	DISABLED (0-65536)	
					Apply Cancel
					Pappy Control *
B					😰 Internet

注:デフォルトでは、TACACS+はTCPポート49を使用します。**注**:ACSとAPで設定する共 有秘密キーは一致している必要があります。

2. Default Server Priorities > Admin Authentication (TACACS+) の順に選択し、Priority 1 ドロッ プダウン メニューから先に設定した TACACS+ サーバの IP アドレスを選択して、Apply を クリックします。以下が一例です。

Cisco 105 Series AP - Securit	y - Server Manager - Microsoft	Internet Explorer provided by Cisco Sy	stems, Inc.		2 ×
Ele Edit Yew Pavorites	Toola Rep				
4+8ack + → - 🥥 😰 🖾	Search @Favorites 🖓	teda 🎯 🗳 - 🚙 📼 🛥 🎱 📖			
Address () http://10.77.244.194	i[ap_sec_network-security_a.shtml#	CorpServers		💌 🖗 😡	nis »
	Delete	Authentication Port (optional):	49 (0-65536)		
		Accounting Port (optional):	DISABLED (0-65536)		
				Apply Cancel	
	Default Server Priorities				
	EAP Authentication	MAC Authentic	ation	Accounting	
	Priority 1: (NONE)	Priority 1: < NC	DNE > •	Priority 1: < NONE > •	
	Priority 2: (NONE)	Priority 2: KN	ONE > 💌	Priority 2: (NONE > .	
	Priority 3: <none> .</none>	Priority 3: KNC	ONE > •	Priority 3: KNONE > *	
	Admin Authentication (R	ADIUS) Admin Authent	ication (TACACS+)		
	Priority 1: (NONE)	Priority 1: 172	16.1.1		
	Priority 2: NONE > .	Priority 2: < NC	DNE >		
	Priority 3: NONE > .	Priority 3: KNC	ONE > 💌		
				Apply Cancel	
					I
Close W	indow			Copyright (c) 1992-2006 by Cisco Systems, Inc	÷ _
8)				Difernet	

3. Security > Admin Access の順に選択し、Administrator Authenticated by: で Authentication Server Only を選択して、Apply をクリックします。この選択により、AP にログインしよう とするユーザは、認証サーバで認証されるようになります。以下が一例です。



CLI による設定の例を次に示します。

AccessPoint
AccessPoint# show running-config
Current configuration : 2535 bytes
: version 12 3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname AccessPoint
!
•
aaa new-model
<pre>! Enable AAA. ! ! aaa group server radius rad_eap !</pre>
aaa group server radius rad_mac ! aaa group server
radius rad_acct ! aaa group server radius rad_admin
cache expiry 1 cache authorization profile admin_cache
cache authentication profile admin_cache ! aaa group
server tacacs+ tac_admin
172 16 1 1
Add the TACACS+ server 172.16.1.1 to the server
group. cache expiry 1

```
Set the expiration time for the local cache as 24
hours. cache authorization profile admin_cache
cache authentication profile admin_cache
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default group tac_admin
!--- Define the AAA login authentication method list to
use the TACACS+ server. aaa authentication login
eap_methods group rad_eap aaa authentication login
mac_methods local aaa authorization exec default group
tac admin
!--- Use TACACS+ for privileged EXEC access
authorization !--- if authentication was performed with
use of TACACS+. aaa accounting network acct_methods
start-stop group rad_acct aaa cache profile admin_cache
all ! aaa session-id common ! ! username Cisco password
7 00271A150754 ! bridge irb ! ! interface Dot11Radio0 no
ip address no ip route-cache shutdown speed basic-1.0
basic-2.0 basic-5.5 basic-11.0 station-role root bridge-
group 1 bridge-group 1 subscriber-loop-control bridge-
group 1 block-unknown-source no bridge-group 1 source-
learning no bridge-group 1 unicast-flooding bridge-group
1 spanning-disabled ! interface Dot11Radio1 no ip
address no ip route-cache shutdown speed station-role
root bridge-group 1 bridge-group 1 subscriber-loop-
control bridge-group 1 block-unknown-source no bridge-
group 1 source-learning no bridge-group 1 unicast-
flooding bridge-group 1 spanning-disabled ! interface
FastEthernet0 no ip address no ip route-cache duplex
auto speed auto bridge-group 1 no bridge-group 1 source-
learning bridge-group 1 spanning-disabled ! interface
BVI1 ip address 172.16.1.30 255.255.0.0 no ip route-
cache ! ip http server ip http authentication aaa
!--- Specify the authentication method of HTTP users as
AAA. no ip http secure-server ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/ea ip radius source-interface BVI1 ! tacacs-server
host 172.16.1.1 port 49 key 7 13200F13061C082F tacacs-
server directed-request radius-server attribute 32
include-in-access-req format %h radius-server vsa send
accounting ! control-plane ! bridge 1 route ip ! ! !
line con 0 transport preferred all transport output all
line vty 0 4 transport preferred all transport input all
transport output all line vty 5 15 transport preferred
all transport input all transport output all ! end
```

注:この設定のすべてのコマンドが正しく動作するには、Cisco IOSソフトウェアリリース 12.3(7)JA以降が必要です。古い Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用 できない場合があります。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

<u>アウトプット インタープリタ ツール(登録ユーザ専用)(OIT)は、特定の show コマンドをサ</u> <u>ポートします。</u>OIT を使用して、show コマンドの出力の分析を表示します。 設定を確認するには、GUI または CLI を使用して AP にログインしてみます。AP にアクセスを 試みると、ユーザ名とパスワードの入力を求められます。

<mark>Ente</mark> r Netv	vork Passwor	d ? >	4
? >	Please type yo	our user name and password.	
S)	Site:	172.16.1.30	
	Realm	level_1_access	
	User Name	User1	
	Password	****	
	🔲 Save this p	password in your password list	
		OK Cancel	

ユーザ クレデンシャルを入力すると、AP はクレデンシャルを TACACS+ サーバに転送します。 TACACS+ サーバは、データベースの情報を基にしてクレデンシャルを検証し、認証が成功する と AP へのアクセスを許可します。このユーザの認証が成功したことを確認するには、ACS で **Reports and Activity > Passed Authentication** の順に選択し、Passed Authentication レポートを使 用します。以下が一例です。

Select								
🖹 <u>Refresh</u>	Down	load						
Passed Authentications active.csv								
Date 🕈	<u>Time</u>	Message- <u>Type</u>	<u>User-</u> Name	Group- Name	Caller-ID	$\frac{\underline{NAS}}{\underline{Port}}$	<u>NAS-IP-</u> <u>Address</u>	
05/10/2006	14:57:01	Authen OK	User1	AdminUsers	172.16.1.1	tty1	172.16.1.30	

show tacacs コマンドを使用して、TACACS+ サーバの設定が正しいことを確認することもできます。以下が一例です。

AccessPoint#**show tacacs**

Tacacs+	Server	:	172.16.1.1/49
	Socket opens	:	348
	Socket closes	:	348
	Socket aborts	:	0
	Socket errors	:	0
	Socket Timeouts	:	0
Faile	ed Connect Attempts	:	0
	Total Packets Sent	:	525
	Total Packets Recv	:	525

<u>ACS 5.2 の検証</u>

ACS 5.2 から、ログイン クレデンシャルの試みが失敗したか成功したかを確認できます。

- 1. [Monitoring Reports] > [Launch Monitoring and Report Viewer] の順にクリックします。ダッ シュボード付きの新しいポップアップが表示されます。
- 2. [Authentications-TACACS-Today] をクリックします。これにより、失敗/成功した試みの詳 細が表示されます。

<u>トラブルシュート</u>

設定のトラブルシューティングを行うには、AP で次の debug コマンドが使用できます。

注:debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

```
• debug tacacs events: このコマンドは、TACACS 認証の間に発生したイベントのシーケンス
 を表示します。このコマンドの出力例を次に示します。
 *Mar 1 00:51:21.113: TPLUS: Queuing AAA Authentication request 0 for
 processing
 *Mar 1 00:51:21.113: TPLUS: processing authentication start request id 0
 *Mar 1 00:51:21.113: TPLUS: Authentication start packet created for 0(User1)
 *Mar 1 00:51:21.114: TPLUS: Using server 172.16.1.1
 *Mar 1 00:51:21.115: TPLUS(0000000)/0/NB_WAIT/C6DC40: Started 5 sec timeout
 *Mar 1 00:51:21.116: TPLUS(0000000)/0/NB_WAIT: socket event 2
 *Mar
      1 00:51:21.116: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request
      1 00:51:21.116: TPLUS(0000000)/0/READ: socket event 1
 *Mar
 *Mar 1 00:51:21.117: TPLUS(00000000)/0/READ: Would block while reading
 *Mar 1 00:51:21.120: TPLUS(0000000)/0/READ: socket event 1
 *Mar 1 00:51:21.120: TPLUS(0000000)/0/READ: read entire 12 header bytes (expect
 16 bytes data)
 *Mar 1 00:51:21.120: TPLUS(0000000)/0/READ: socket event 1
 *Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 28 bytes response
      1 00:51:21.121: TPLUS(0000000)/0/C6DC40: Processing the reply packet
 *Mar
 *Mar 1 00:51:21.121: TPLUS: Received authen response status GET_PASSWORD (8)
 *Mar 1 00:51:21.121: TPLUS: Queuing AAA Authentication request 0 for processing
 *Mar 1 00:51:21.121: TPLUS: processing authentication continue request id 0
 *Mar 1 00:51:21.122: TPLUS: Authentication continue packet generated for 0
 *Mar 1 00:51:21.122: TPLUS(0000000)/0/WRITE/C6DC40: Started 5 sec timeout
 *Mar
      1 00:51:21.122: TPLUS(0000000)/0/WRITE: wrote entire 22 bytes request
      1 00:51:21.178: TPLUS(0000000)/0/READ: socket event 1
 *Mar
 *Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect
 6 bytes data)
 *Mar 1 00:51:21.178: TPLUS(0000000)/0/READ: socket event 1
 *Mar 1 00:51:21.178: TPLUS(0000000)/0/READ: read entire 18 bytes response
 *Mar 1 00:51:21.179: TPLUS(0000000)/0/C6DC40: Processing the reply packet
 *Mar 1 00:51:21.179: TPLUS: Received authen response status PASS (2)
```

debug ip http authentication: HTTP 認証の問題をトラブルシューティングするためのコマンドです。
 ドです。
 ルータが使用した認証方式と認証特有の状況メッセージを表示します。
 debug aaa authentication: AAA TACACS+認証に関する情報を表示します。

TACACS+ サーバに存在しないユーザ名をユーザが入力すると、認証は失敗します。失敗した認 証に対する debug tacacs authentication コマンドの出力を次に示します。

*Mar 1 00:07:26.624: TPLUS: processing authentication start request id 0 *Mar 1 00:07:26.624: TPLUS: Authentication start packet created for 0(User3) *Mar 1 00:07:26.624: TPLUS: Using server 172.16.1.1 *Mar 1 00:07:26.625: TPLUS(00000000)/0/NB_WAIT/A88784: Started 5 sec timeout *Mar 1 00:07:26.626: TPLUS(0000000)/0/NB_WAIT: socket event 2 *Mar 1 00:07:26.626: TPLUS(0000000)/0/NB_WAIT: wrote entire 25 bytes request 1 00:07:26.627: TPLUS(0000000)/0/READ: socket event 1 *Mar 1 00:07:26.627: TPLUS(0000000)/0/READ: Would block while reading *Mar *Mar 1 00:07:26.631: TPLUS(0000000)/0/READ: socket event 1 *Mar 1 00:07:26.632: TPLUS(0000000)/0/READ: read entire 12 header bytes (expect 16 bytes data) *Mar 1 00:07:26.632: TPLUS(0000000)/0/READ: socket event 1 *Mar 1 00:07:26.632: TPLUS(0000000)/0/READ: read entire 28 bytes response 1 00:07:26.632: TPLUS(0000000)/0/A88784: Processing the reply packet *Mar *Mar 1 00:07:26.632: TPLUS: Received authen response status GET_PASSWORD (8) *Mar 1 00:07:26.632: TPLUS: Queuing AAA Authentication request 0 for processing *Mar 1 00:07:26.633: TPLUS: processing authentication continue request id 0 *Mar 1 00:07:26.633: TPLUS: Authentication continue packet generated for 0 *Mar 1 00:07:26.634: TPLUS(0000000)/0/WRITE/A88784: Started 5 sec timeout *Mar 1 00:07:26.634: TPLUS(0000000)/0/WRITE: wrote entire 22 bytes request *Mar 1 00:07:26.688: TPLUS(0000000)/0/READ: socket event 1 1 00:07:26.688: TPLUS(0000000)/0/READ: read entire 12 header bytes (expect 6 *Mar bytes data) *Mar 1 00:07:26.689: TPLUS(0000000)/0/READ: socket event 1 *Mar 1 00:07:26.689: TPLUS(0000000)/0/READ: read entire 18 bytes response *Mar 1 00:07:26.689: TPLUS(00000000)/0/A88784: Processing the reply packet *Mar 1 00:07:26.689: TPLUS: Received authen response status FAIL (3)

Reports and Activity > Failed Authentication の順に選択すると、ACS で失敗した認証の試行を確認できます。以下が一例です。

Date 🖊	<u>Time</u>	<u>Message-</u> <u>Type</u>	<u>User-</u> Name	<u>Group-</u> <u>Name</u>	Caller- ID	<u>Authen-</u> Failure-Code	Author- Failure- Code	Author- Data	NAS- Port
05/17/2006	19:40:14	Authen failed	User3			CS user unknown			

Cisco IOS ソフトウェア リリース 12.3(7)JA より前のリリースを AP で使用している場合は、 HTTP を使用して AP へのログインを試みるたびに不具合に遭遇する可能性があります。Cisco Bug ID <u>は、</u>CSCeb52431(<u>登録ユーザ専用)です。</u>

Cisco IOS ソフトウェアの HTTP/AAA の実装では、異なる HTTP 接続ごとに独立した認証が必要 です。ワイヤレス Cisco IOS ソフトウェア GUI には、単一の Web ページ内に多数の異なるファ イル(Javascript や GIF など)の参照が含まれます。 そのため、ワイヤレス Cisco IOS ソフトウ ェア GUI で単一のページをロードする場合、個別の認証/認可要求が大量に AAA サーバに送られ る可能性があります。

HTTP 認証の場合は、RADIUS またはローカル認証を使用してください。RADIUS サーバでも、 やはり複数の認証要求を受け取ります。ただし、RADIUS は TACACS+ よりスケーラビリティが 優れているので、パフォーマンスの低下は小さくて済みます。

TACACS+ を使用する必要があり、Cisco ACS がある場合は、single-connection キーワードを tacacs-server コマンドとともに使用します。コマンドでこのキーワードを使用すると、ACS で の TCP 接続のセットアップ/ティアダウンのオーバーヘッドの大部分がなくなり、サーバの負荷 がある程度まで軽減される可能性があります。

Cisco IOS ソフトウェア リリース 12.3(7) JA 以降を AP で使用している場合は、ソフトウェアに

修正が含まれています。次にこの修正について説明します。

TACACS+ サーバが返す情報をキャッシュするには、AAA の認証キャッシュ機能を使用します。 認証キャッシュおよびプロファイル機能を使用すると、AP は、ユーザに対する認証/認可応答を キャッシュでき、以降の認証/認可要求を AAA サーバに送信する必要がなくなります。CLI でこ の機能を有効にするには、次のコマンドを使用します。

cache expiry cache authorization profile cache authentication profile aaa cache profile

この機能とコマンドについての詳細は、『<u>アクセス ポイントの管理』の「認証キャッシュおよび</u> <u>プロファイルの設定」セクションを参照してください。</u>

この機能を GUI で有効にするには、Security > Admin Access の順に選択し、Enable Authentication Server Caching チェック ボックスにチェックマークを付けます。このドキュメン トでは Cisco IOS ソフトウェア リリース 12.3(7)JA を使用しているので、この修正を「<u>設定</u>」で 示されているように使用しています。

関連情報

- <u>RADIUS サーバと TACACS+ サーバの設定</u>
- <u>重要なお知らせ: IOS アクセス ポイントから TACACS+ サーバに要求が殺到する</u>
- <u>RADIUS サーバとの EAP 認証</u>
- ワイヤレス製品に関するサポート
- <u>テクニカル サポートとドキュメント Cisco Systems</u>