WLAN ごとの認証用 ACS バージョン 5.2 および WLC の設定例

内容

| <u>概要</u> |
|------------------------------|
| <u>前提条件</u> |
| <u>要件</u> |
| <u>使用するコンポーネント</u> |
| <u>設定</u> |
| <u>WLC の設定</u> |
| <u> Cisco Secure ACS の設定</u> |
| <u>確認</u> |
| トラブルシュート |

概要

このドキュメントでは、サービス セット識別子(SSID)に基づいてワイヤレス LAN(WLAN)へのユーザ別アクセスを制限するための設定例について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ワイヤレス LAN コントローラ(WLC)と Lightweight アクセス ポイント(LAP)の基本動作のための設定方法
- Cisco Secure Access Control Server(ACS)の設定方法
- Lightweight アクセス ポイント プロトコル(LWAPP)とワイヤレスのセキュリティ方式

使用するコンポーネント

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。

- ・ファームウェアバージョン7.4.110が稼働するCisco 5500シリーズWLC
- Cisco 1142 シリーズ LAP
- Cisco Secure ACSサーババージョン5.2.0.26.11

設定

この設定用にデバイスを設定するには、次の手順を実行します。

1.2 つの WLAN と RADIUS サーバ用の WLC を設定します。

2. Cisco Secure ACS を設定します。

3. ワイヤレスクライアントを設定し、設定を確認します。

WLC の設定

このセットアップのために WLC を設定するには、次の手順を実行します。

 ユーザクレデンシャルを外部RADIUSサーバに転送するようにWLCを設定します。設定する と、外部 RADIUS サーバ(この場合は Cisco Secure ACS)は、ユーザ クレデンシャルを検 証し、ワイヤレス クライアントにアクセス権を付与します。次のステップを実行します。 コントローラのGUIから[Security] > [RADIUS Authentication]の順に選択して、[RADIUS Authentication Servers]ページを表示します。



RADIUS サーバ パラメータを定義するには、[New] をクリックします。 RADIUS サーバ IP アドレス、共有秘密、ポート番号、サーバ ステータスなどのパラメータがあります。 [Network User]チェックボックスと[Management]チェックボックスでは、RADIUSベースの 認証が管理ユーザとネットワークユーザに適用されるかどうかが決まります。この例では、 次のように、Cisco Secure ACS を IP アドレスが 10.104.208.56 である RADIUS サーバと して使用しています。

| ahaha | | | | Sage Configuration Eing Legent Befrech |
|---|----------------------------|--------------------------------------|------------------------------------|--|
| CISCO | MONITOR MUANE CONTROLLS | R AGRELESS <u>SECURITY</u> MENAGEMEN | Т ОДИМАНОВ НЕЦЯ ЕВЕОВАСК | |
| Security | RADIUS Authentication Serv | rrs > New | | < 8 ack Apply |
| * AAA | Server Index (Priority) | 1 . | | 1 |
| * RADIUS | Server 37 Address | 10104.80555 | | |
| Authentication | Shared Secret Format | 45.03 | | |
| Fallback | Shared Secret | | | |
| LDAP | Confirm Shared Secret | ******* | | |
| Local Net Users MRC Effering Disabled Clients | Key Wrap | Cangrantor FRG automations and the | a key arep conclude RADE 6 server) | |
| Hoar Logo Rolisses | Pert Bandier | 1:12 | | |
| Parement Policiae | Server Status | Teachieri e | | |
| E Local EAP | Support for RFC 3576 | paulot in | | |
| Priority Order | Server Trosout | 2 excende | | |
| Eertificate | Notwork User | 2 Charles | | |
| Access Control Lists | Planagement | E Grade | | |
| Wireless Protection Pulicies | IP300 | 📰 incbie | | |
| Web Auth | | | | |
| TrestSec SXP | | | | - |
| Advanced | | | | |

[Apply] をクリックします。

2. SSID **Employee**の従業員に1つのWLANを設定し、SSID Contractorの請負業者用にもう1つ のWLANを設定するには、次の手順を実**行します**。 WLAN を作成するために、コントロー ラの GUI で [WLANs] をクリックします。WLANs ウィンドウが表示されます。このウィン ドウには、コントローラに設定されている WLAN の一覧が表示されます。新しい WLAN を 設定するために [New] をクリックします。この例では、Employeeという名前のWLANを作 成し、WLAN IDを1にします。[**Apply**]をクリック**します**。

| cisco | MONITOR MLANE | CONTROLLER 4 | greless geolikt | T NEVAGENENT | ODAWANCS | HE,S | ESEDBACK | Sage Configuration 2mg Logical Batteric |
|---|------------------------------------|---------------------------------------|-----------------|--------------|----------|------|----------|---|
| WLANs | WLANs > New | | | | _ | | | < Back Apply |
| WLANS WLARS WLAR Manual | Type Profile Name SSID ID | wijati Employee Deployee 1 w | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

[WLAN] > [Edit]ウィンドウを選択し、WLAN固有のパラメータを定義します。 [Layer 2 Security]タブで、[802.1x]を選択します。デフォルトでは、レイヤ 2 セキュリティ オプショ ンは 802.1x です。これにより、WLANの802.1 x/Extensible Authentication Protocol(EAP)認 証が有効になります。

| cisco | ROVITOR WITHNE COVIESDITES AUGERERS RECIEILA NEVERENAL COMMANDE HETE EEEDRACK | age Configuration Drop Legant Befre |
|-------------|---|-------------------------------------|
| WLANs | WLANs > Edit 'Employee' | < Back Apply |
| WLANS MLANS | General Security QaS Advanced | |
| Advanced | Loyer 2 Loyer 3 AAA Servers | |
| | Lagar 2 Security • Yes - er og • RAG Titter og • | i |
| | Paul Transform | |
| | 199 Deschaller | - |
| | WPA IWPA2 Parameters | |
| | WPA I vicy WPA Policy V | |
| | WEAL Distriguish DRAFS E TYP | |
| | Authentic down Key Management | - |
| | CCVP Exchange | |
| | PSK E trabia | |
| | | |
| | Front Notes 2 Web Policy count in and in conduction with Planc 2 Subsciences inval Symptocia is not according with Theory 2019/0777 in manifestion in According Interface (Plan | |

[AAA servers]タブで、[RADIUS Servers]のドロップダウンリストから適切なRADIUSサーバ を選択します。WLAN ネットワークの要件に基づいて、その他のパラメータを変更できます 。[Apply] をクリックします。

| /LANs | WLANs > Edit 'Employee' | | | |
|----------------|---------------------------------|--|--------------------|--------------|
| | | | | < Back Apply |
| WLANS WLANS | General Security QaS | idvanced | | |
| Advanced | Layer 2 Layer 3 AAA Se | TREPS | | |
| | Select AAA servers below to ove | rride use of default servers on this WLAS | | Î. |
| | Radius Servers | | LDBP Servers | |
| | Rent of the other of the second | - Carovec | Server 1 to e | |
| | | Authentisation Servers Assessing Servers | Server 2 Bone | = |
| | | W Taskar V Practed | Survey 9 Rock Inc. | |
| | A cover 1 | 12.0.04210.16,16.0.02 x 3164 x | | |
| | Since 2 | to c | | |
| | Securi 3 | tore a 3ree a | | |
| | 2000 | in the second se | | |
| | Server 5 | tore w 9104 w | | |
| | Server 6 | tore w Teti w | | |
| | Radius Server Accounting | | | |
| | Interim Update 📰 | | | |
| | Local EAP Authentication | | | - |
| | * [| 11 | | |
| | Fost Notes | | | |

同様に、請負業者のWLANを作成するには、手順b ~ dを繰り返します。

Cisco Secure ACS の設定

Cisco Secure ACS サーバで、次の操作を実行します。

- 1. WLC を AAA クライアントとして設定します。
- 2. SSIDベース認証のユーザデータベース(クレデンシャル)を作成します。
- 3. EAP 認証をイネーブルにします。

Cisco Secure ACS で次の手順を実行します。

- 1. コントローラをACSサーバ上のAAAクライアントとして定義するには、ACS GUIから [**Network Resources] > [Network Devices and AAA Clients]**を選択します。[Network Devices and AAA Clients]で[**Create**]を**クリック**し**ま**す。
- 2. [Network Configuration]ページが表示されたら、WLCの名前、IPアドレス、および共有秘密 と認証方式(RADIUS)を定義します。

| X Sheri Browner WebEr • | man / P + O Cettle. 2 d X Circo Secure ACS × | | | | |
|--------------------------|--|---------|--|-------------------------|--------------------|
| cisco Eval(Days left, 5) | CS | | esetnin | aca longibile (Primary) | Log Out About Help |
| | Network Resources > Mathem Dockes and AAA Olemb > Orad Peorgian: Retwork Device Geoges Location All Jocations Device Type All Device Types # Address @ Single IP Address @ Single IP Address @ IP: 10.105.98.4 | Serect. | Adhertication Options • TACACS+ Shared Secret Single Connect Device © Leguxy TACACS+ Single Connect Suppo • RADUS • RADUS • Shared Secret, X0000X CAAppet 1780 C Enable Rey/Wap Nary Encryption Rey. | n. | |
| | Stone Carce | | | | |

 ACS GUIから[Users and Identity Stores] > [Identity Groups]を選択します。従業員および請 負業者の各グループを作成し、「作成」をクリックします。この例では、作成したグループ

の名前はEmployeesです。

| 1 4 1 · 8 8 | | Statute Harland Harad Har | | |
|--|--|---------------------------|-----------|--|
| Imper/20.184.208.56/scrade | nn/ D + O Cettro. E d X 🧭 Cisco Secure Al | cs × | | 6.2 |
| X Gara Browner WebEc - | | | | |
| | | | | |
| Infinition Cisco Secure Al | CS | | econtrain | acatiomphate (Primary) Log Out About Hel |
| CISCO EVAL(Days left: 5) | | | | |
| St MyWorkspace | Users and Identity Stone > Kenity Groups > Create | | | |
| > (3) Nelwork Resources | Control | | | |
| - 🗃 Users and identity Stores | Name: Employees | | | |
| Herity Groupe | Description | | | |
| Internal Identity Stores | - Paulation | (data and) | | |
| Hosts | All Groups | Denect | | |
| External Identity Stores | D = Hequired telds | | | |
| LDAP | | | | |
| RSA SecuriD Taken Senera | | | | |
| RADIUS Identity Servers | | | | |
| Conflicate Authorities | | | | |
| Kenth Store Sequences | | | | |
| > Qv PolicyElements | | | | |
| + 🔂 Access Policies | | | | |
| Monitoring and Reports | | | | |
| » 🧏 System Administration | | | | |
| | | | | |
| | | | | |
| | | | | |
| | Butter Carro | | | |
| | and a second sec | | | |

4. 「ユー**ザーとIDストア」>「内部IDストア」を選択します**。[Create]をク**リック**し、ユーザ名 を入力します。これらを正しいグループに配置し、パスワードを定義し、[送信]をクリック します。この例では、グループEmployeeのemployee1という名前のユーザが作成されます 。同様に、contractor1という名前のユーザをグループcontractorsの下に作成します。

| a second s | ALL OF TAXABLE PARTY OF | |
|---|--|----------------|
| C (C) (C) (T) (C) (C) (C) (C) (C) (C) (C) (C) (C) (C | sriu/ D + Q Cetter B C X Circo Securi ACS × | 6 17 6 |
| 🗶 🥌 Shara Browner - WebEc 💌 | | |
| Cisco Secure Al Cisco Eval(Days left b) | ACS examine examine (Primary) Log | Out About Help |
| MyWorkspace | Usara and kierdity Storea > Hierral Kentity Storea > Usera > Oreale | |
| Polevork Resources Polevork Resources Hennik Users Hennik Users Deer Hennik Users() Stores LOVP Active Directory REASecurit Taken Senses RADUS Mently Senses Active Directory Active Directory REASecurit Taken Senses RADUS Mently Senses RADUS Mently Senses Active Directory Active Directory REASecurit Taken Senses RADUS Mently Senses RADUS Mently Senses Active Directory Active Directory Active Directory Monitoring and Reports Monitoring and Reports | General • Name: employee1 Description: • Identity Group: Al Groups Employee • Identity Group: Al Groups Employee • Contain 4 - 32 characters | |
| | s j " Buonit Carce | |
| | | |

5. [**Policy Elements] > [Network Conditions] > [End Station Filters]を選択します**。[作成 (Create)]をクリックします。



意味のある名前を入力し、[**IP address**]タブでWLCのIPアドレスを入力します。この例では、名前はEmployeeとContractorです。



[CLI/DNIS]タブで、[CLI]を – ANY – のままにし、「DNIS」を*<SSID>として入力します。 この例では、DNISフィールドに「*Employee」と入力します。このエンドステーションフィ ルタは、従業員WLANへのアクセスのみを制限するために使用されます。DNIS 属性は、ユ ーザがアクセスを許可される SSID を定義します。WLC は SSID を DNIS 属性で RADIUS サーバに送信します。Contractorエンドステーションフィルタについても同じ手順を繰り返 します。



6. [Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profiles]を選択します。[Permit Access]にはデフォルトプロファイルが必要です。

| X Shere Browner WebEr • | n/ D + Q Centricu ≅ C X Science Secure AC5 × | | | - □ - × A ☆ 6 |
|--|--|----------|------------------------|--------------------------------|
| CISCO CISCO Secure Al CISCO EVAL(Days left, 5) | | scaatnin | acationybile (Primary) | Log Cul About 1940 |
| » ∯ MyWorkspace | Policy Bernets > Authorization and Permissions > Network Access > Authorization Profiles | | | |
| > 53 Network Resources | Authorization Profiles | | Stowing 1-1 of 1 | 0 • perpage 00 |
| B Users and Identity Stores | Filer. • Mech # 00 • | | | |
| - Or Policy Elements | Name • Description | | | |
| Date and Time | Permit Access | | | |
| Custom * NationS Canditiane End Statum Pitans Device Pitans * Authorization and Permissions * NationAccess Status Device Patrimisstation * Named Permission Objects * Cost Policies * Cost Pol | | | | |
| | Create Duplicate Edit Delate | | H 4 Page | 1 of 1 1 11 |
| | | | | |

7. [Access Policies] > [Access Services] > [Service Selection Rules]を選択します。[Customize] をクリックします。 適切な条件を追加します。この例では、照合条件としてProtocol as Radiusを使用しています。[作成(Create)]をクリックします。ルールに名前を付けます。 「プロトコル」を選択し、「Radius」を選択します。[Results] で、適切なアクセスサービ スを選択します。この例では、[Default Network Access]のままにしておきます。

| I Webpage Dialog | | x |
|--|-------------------------|---------------------|
| 😂 https://10.104.208.56/acsadm | in/PolicyInputAction.do | 😮 Certificate error |
| Customize Conditions Available: ACS Host Name Compound Condition Device Filter Device IP Address Device Port Filter End Station Filter NDG:Device Type NDG:Location Time And Date UseCase | Selected: Protocol N | |
| OK Cancel | | |

| Cisco Secure ACS Webpage Dial | log | X |
|---|--|--|
| https://10.104.208.56/acsadmin/P- | olicyInputAction.do | 😮 Certificate error |
| General | | |
| Name: Rule-4 | Status: Enabled 🔻 \Theta | |
| The Customize butto conditions and resul | on in the lower right area of the po Its are available here for use in po | plicy rules screen controls which policy plicy rules. |
| Conditions | | |
| Protocol: match | Radius | Select |
| Results | | |
| Service: Default Network Access | s * | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| OK Cancel | | Help |

8. [Access Policies] > [Access Services] > [Default Network Access] > [Identity]を選択します。 [Single Result Selection]と[Identity Source]を[Internal users]に選択します。

| Concernance Concernan | | | and the second second second | | | |
|---|--|--|------------------------------|-----------|-----------------------|--------------------|
| X ² Hey Howner White • 11.11. Cisco Secure ACS Cisco Evaluations ² Hey Montragete - Q Havanin Resources ² Single result selection - Q Havanin Resources ² Advanced Optore - Multicing and Repote ² Advanced Optore - Q Havanin Resources ² Bound Repote - Q Havanin Resources ² Bound Repote - Q Havanin Resources ² Advanced Optore - Q Havanin Resources ² Bounin Resources | 🗲 🛞 🍊 https://10.184.208.56/scrade | nin/ D + O Cattle., E d X 6 Cisco Secure Ad | cs × | | | 6 🔶 🖯 |
| Intellit: Clsco Secure ACS Reader Water Reader Read | 🗶 🍘 Shara Browner WebEc 🔹 | | | | | |
| Image: Strate | cisco Secure Al | CS | | acasteria | acatemplate (Primery) | Log Out About Help |
| | CISCO EVAL(Daps with 5) Solution Solution | Access Robers - Access Service - Default live of Acce Single result selection Rule based result se Identity Boune Internal Users Advanced Options Seve Changes Depart Changes | etection Servet. | | | |
| | | | | | | |

[Access Policies] > [**Access Services] > [Default Network Access] > [Authorization]を選択し ます。[Customize]をクリック**し、[Customized]**条件**を追加します。この例では、[Identity Group]、[NDG:Device Type]、および[End Station Filter]の順に使用しています。



[作成(Create)] をクリックします。ルールに名前を付け、[All Groups]で適切なIDグループ を選択します。この例では、Employeeです。

| Cisco Secure ACS Webpage Dialog | Cisco Secure ACS Webpage Dialog |
|---|--|
| 🖉 het pos/128.214.200.16/no outroin: Policyle postation du 💿 Carificate arm | 🍘 https://10/104200. 🖬 has a dwirs. Plataeck 🛛 wise Groups Flegut Action de Promite Data, estarra Filters Educity Groups Standy Fleg |
| General Name: Rule 2 Datus: Enabled • • • Image: Rule 2 Datus: Enabled • • • • • • Image: Rule 2 Datus: Enabled • • • • Image: Rule 2 Datus: Enabled • • • • Image: Rule 2 Datus: Enabled • • • • Image: Rule 2 Datus: Enabled • • • • Image: Rule 2 Datus: Enabled • • • • Image: Rule 2 Datus: Enabled • • • • Image: Rule 2 Datus: Enabled • • • • Image: Rule 2 Datus: Enabled • • • Image: Rule 2 Datus: Enabled • • • Image: Rule 2 Datus: Enable 2 • • Image: Rule 2 Datus: Enable 2 • • • Image: Rule 2 Datus: Enable 2 • • • Image: Rule 2 Datus: Enable 2 • • • | Network Device Groups Pite: • Match it • 💿 🐨 Name • Description • • All Docat Here Root Contractor |
| Conditions | • Instance |
| 2 Idently Droup: In | MLC 2.M |
| R NDO.Devke Type: In | |
| 2 End Station Filter: math • Select | al Clara Server d.C. Metapoge Claring |
| fenuts | 😸 terped/10. 10.201. We wai mich faharen bruh einen Herpatiz-ten dele esteration untersale terafische Type all mich Type 😦 Territorie en Namen en eine einen |
| You may select multiple subortation profiles. Attitudes defined in multiple profiles will use the value from the first profile defined. | |

[Employee End Stn Filter]**オプションボタンをクリ**ックするか、[Configure the WLC]セクシ ョンのステップ1bで入力した名前を入力します。

| ē | Cisco | Secure ACS Webpa | ge Dia | log | | |
|---|---------|------------------------|---------|--|---------------------|---------------------|
| 8 | 🗿 https | ://10.104.208.56/acsad | min/N | IARsLPInputAction.do?listType=EndStation | | 😵 Certificate error |
| | End St | tation Filters | | | Showing 1-2 of 2 50 | ▼ per page Go |
| | Filter: | - Ma | tch if: | - Go - | | |
| | | Name | | Description | | |
| | ۲ | Contractor End Stn F | ilter | | | |
| | ۲ | Employee End Stn F | ilter | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | Crea | ite Duplicate | Edit | Delete | 💽 🖣 Page | 1 of 1 🕨 🕅 |
| | OK C | Cancel | | | | Help |
| | | | | | | |

[Permit Access]チェックボックスをオンにします。

| Cisco Secure ACS Webpage Dialog | | × |
|--|---------------------|---------------------|
| G https://10.104.208.56/acsadmin/NetworkAccessLPEnputAction.do | | 😵 Certificate error |
| Authorization Profiles | Showing 1-2 of 2 50 | ▼ per page Go |
| Filter: 🔹 Match if: 🔹 Go 👻 | | |
| Name Description | | |
| DehyAccess | | |
| Permit Access | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| Create Duplicate Edit Delete | I Page | 1 of 1 🕨 📕 |
| OK Cancel | | Help |
| | | |
| | | |

契約作業員ルールについても、上記と同じ手順を繰り返します。[Default Action]が[**Deny**

Access]になっていることを確認します。 手順eを完了すると、ルールは次の例のようになります。

| ISCO EVAL(Days left-5) | ACS | | | | | | | | activation pro- | ana (i tag ta sata |
|---|-----|--|--------|------------------------|--|--|--|-----------------------------------|-----------------|----------------------|
| MyWorkspace Network Resources Users and Identity Stores | A: | Access Policies > Access Services > Default Hele of Access > Authorization Standard Policy Encoded in Policy | | | | | | | | |
| Qv PolicyElements | | Filter | Status | - | Match if Figure + | • Clear F | ter De v | | | |
| Access Policies Access Services | 1 | l | Sta | lus Name | Identity Group | Conditions NDG.Device Type | End Station Filter | Results Authorization Profiles | HECOV E | |
| O Default/Device Admin Identity Authorization O Default/Network Access | | 1 2 | | Contractor Employee | in Al Groups:Contractor in Al Groups:Employee | in Al Device Types://LC in Al Device Types://LC | match Contractor End Str Filter match Employee End Str Filter | Permit Access Permit Access | 7 5 | |
| Monitoria and Records | | | | | | | | | | |
| System Administration | | | | | | | | | | |
| | Ŀ | Г | Def | ault | Frio tales defined at no e | enabled rule matches. | | DetyAccess | _ | |
| | | _ | | | Intelligence III & La | the liter | | | _ | Contractor II united |

これで設定は終了です。このセクションの後、接続するには、SSIDとセキュリティパラメータに 従ってクライアントを設定する必要があります。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。