将ISE配置为RADIUS服务器的SWA外部身份验证

| 目录 |
|--------------|
| |
| <u>先决条件</u> |
| |
| <u>使用的组件</u> |
| |
| 网络拓扑 |
| |
| ISE 配置 |
| <u>SWA配置</u> |
| <u>验证</u> |
| 相关信息 |

简介

本文档介绍在Cisco ISE作为RADIUS服务器的安全Web访问(SWA)上配置外部身份验证的步骤。

先决条件

要求

Cisco 建议您了解以下主题:

- 思科安全网络设备的基础知识。
- 了解ISE上的身份验证和授权策略配置。
- RADIUS基础知识。

Cisco建议您还应具备:

- SWA和ISE管理访问权限。
- 兼容的WSA和ISE版本。

使用的组件

本文档中的信息基于以下软件版本:

- SWA 14.0.2-012
- ISE 3.0.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

当您为SWA的管理用户启用外部身份验证时,设备会使用在外部身份验证配置中指定的轻型目录访问协议 (LDAP)或RADIUS服务器验证用户凭证。

网络拓扑



网络拓扑图

管理用户使用其凭证访问端口443上的SWA。SWA使用RADIUS服务器验证凭证。

配置

ISE 配置

步骤1: 添加新的网络设备。导航到管理>网络资源>网络设备> +Add。

| dentity Services Engine | Home | kt Visibility → Op | erations | ✓ Administration | Work Centers |
|------------------------------------|---------------------------------------|--------------------|--------------------|------------------------|------------------------------|
| System Identity Management | Network Resources | Device Portal I | lanagement pxGrid | Services Feed Servic | Threat Centric NAC |
| ▼ Network Devices Network Device G | roups Network De | vice Profiles Exte | nal RADIUS Servers | RADIUS Server Sequence | es NAC Managers External MDM |
| G | | | | | |
| Network Devices | Network Devi | ces | | | |
| Default Device | | | | | |
| Device Security Settings | 🥖 Edit 🛛 🕂 Add | Duplicate 💽 Ir | nport 🚯 Export 🕐 | Generate PAC X Delete | |
| | Name | ▲ IP/Mask | Profile Name | Location | Туре |
| | | | | | No data available |
| | | | | | |

在ISE中添加SWA作为网络设备

第二步: 为网络设备对象分配名称并插入SWA IP地址。

选中RADIUS 复选框并定义共享密钥。



注意:稍后必须在SWA中配置相同的RADIUS服务器密钥。

| - | | | | | | |
|--------------------------|---------------|-----------------------|----------------|-----------------|--------|------|
| Network Devices | Network Devic | ces List > SWA | | | | |
| Default Device | Network D | evices | | | | |
| Device Security Settings | | * Name | SWA | | | |
| , , | | Description | | | | |
| | | | | | | |
| | I | P Address 💌 * | IP: 10.106.38. | 176 | | / 32 |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | * Device Profile | disco Visco V | Ð | | |
| | | Model Name | | * | | |
| | | Software Version | | | | |
| | | | | - | | |
| | | Network Device Grou | p | | | |
| | | | | | | |
| | | Location All Locati | ons 📀 | Set To Default | | |
| | | IPSEC No | 0 | Set To Default | | |
| | D | evice Type All Device | | Set To Default | | |
| | | All Device | e types 🛛 💟 | Set to Deladit | | |
| | _ | | | | | |
| | ✓ | RADIUS Authentication | n Settings | | | |
| | | | | | | |
| | | RADIUS UDP Set | tings | | | |
| | | | | Protocol | RADIUS | |
| | | | | * Shared Secret | ••••• | Show |
| 配置SWA网络设备共享密钥 | | | | | | |

步骤 2.1单击"Submit"。

| _ | | |
|--------------|---|------------------|
| \checkmark | RADIUS Authentication Settings | |
| | | |
| | RADIUS UDP Settings | |
| | Protocol RADIUS | |
| | * Shared Secret | Show |
| | Use Second Shared Secret 🗌 🛈 | |
| | | Show |
| | CoA Port 1700 | Set To Default |
| | RADIUS DTLS Settings (i) | |
| | DTLS Required 🗍 🕧 | |
| | Shared Secret radius/dtls | (I) |
| | CoA Port 2083 | Set To Default |
| | Issuer CA of ISE Certificates for CoA Select if rec | uired (potional) |
| | DNS Name | |
| | | |
| | General Settings | |
| | Enable KeyWrap 🗌 🥡 | |
| | * Key Encryption Key | Show |
| | * Message Authenticator Code Key | Show |
| | Key Input Format 💿 ASCII 🔘 | HEXADECIMAL |
| | | |
| | TACACS Authentication Settings | |
| | ► SNMP Settings | |
| | Advanced TrustSec Settings | |
| | | |
| Submit | Cancel | |

提交网络设备配置

第三步: 创建所需的用户身份组。导航到管理>身份管理> Groups >用户身份组> + Add。



注意:您需要配置不同的用户组以匹配不同类型的用户。

| dentity Services Engine Home | Context Visibility Operations Policy | |
|--|--|---|
| System Identity Management Network Re | esources | ervices |
| Identities Groups External Identity Sources | Identity Source Sequences | |
| Identity Groups | User Identity Groups | |
| ↓ | 📝 Edit 🕂 Add 🗙 Delete 👻 💽 Import 😱 F | Export 👻 |
| Endpoint Identity Groups | Name | Description |
| User Identity Groups | ALL_ACCOUNTS (default) | Default ALL_ACCOUNTS (default) User Group |
| | Æ Employee | Default Employee User Group |
| | GROUP_ACCOUNTS (default) | Default GROUP_ACCOUNTS (default) User Group |
| | GuestType_Contractor (default) | Identity group mirroring the guest type |

添加用户身份组

第四步:输入组名称、说明(可选)和提交。对每个组重复这些步骤。在本示例中,您为管理员用 户创建一个组,为只读用户创建另一个组。

| diale Iden | tity Services Engine | Home | ➤ Context Visibility | Operations | ▶ Policy | Administration | |
|---|--------------------------|-------------------|--|--------------------------------|----------------|------------------------------------|---------------------------|
| System | ✓ Identity Management | Network F | Resources | Portal Managemen | t pxGrid S | ervices Feed Se | Prvice Threat Centric NAC |
| Identities | Groups External | Identity Sources | Identity Source Seque | ences I Setting | IS | | |
| | | | | | | | |
| Identity | Groups | | User Identity Grou | ps > New User Id | entity Group | | |
| • | | Q | Identity Group | þ | | | |
| - | | ÷ | * Name | SWA Admin | | | |
| 🕨 🚞 E | ndpoint Identity Groups | | Description | SWA Admin ISE | Local | | |
| ▶ □ □ 添加用户身 | Iser Identity Groups | | Submit Can | cel | | | |
| alulu Identi | ty Services Engine | Home ▶ Conte | ext Visibility • Operations | ; → Policy 🚽 | Administration | Work Centers | |
| In System | + Identity Management | Network Resources | Device Portal Managem | ent pxGrid Service | es 🔸 Feed Se | rvice + Threat Centric | NAC |
| Identities | Groups External Identity | Sources Identity | Source Sequences + Set | tings | | | |
| Identity (- + En + Us # Us # # | Groups | Luse Ide | er Identity Groups > New User entity Group * Name SWA ReadO Description SWA Read C Identi Cancel | r Identity Group |] | | |

第五步:您需要创建与SWA中配置的用户名匹配的网络访问用户。

创建网络访问用户并将其添加到其对应组。导航到管理>身份管理>身份> + Add。

| dent | tity Services Engine | Home Conte | ext Visibility → O | perations Policy | - Administration | ► Work Center | ers | |
|--------------|----------------------------|----------------------|--------------------|---------------------------------|-------------------|----------------|------------------|---------------|
| ▶ System | ◄ Identity Management | Network Resource | s | Management pxGrid Se | ervices I Feed Se | rvice Ir Threa | at Centric NAC | |
| ◄ Identities | Groups External Ident | tity Sources Identit | y Source Sequences | Settings | | | | |
| | G | | | | | | | |
| Users | Users Network Access Users | | | | | | | |
| Latest Manua | l Network Scan Results | / Edit 🕂 Add | 🔀 Change Status | 👍 Import 🔹 Export 👻 | 🗙 Delete 🛛 🖓 Du | plicate | | |
| | | Status | Name | Description | Firs | t Name l | Last Name | Email Address |
| | | | | | | | No data availabl | e |

在ISE中添加本地用户

步骤 5.1您需要创建具有管理员权限的网络访问用户。指定名称和密码。

| dent dent | tity Services Engine | Home + Contex | tt Visibility → Operations | Policy - Adm | ninistration 🔹 Wo | ork Centers |
|----------------------------|------------------------|---|--|-----------------|-------------------|--------------------|
| System | + Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | Threat Centric NAC |
| ✓ Identities | Groups External Ide | ntity Sources Identity S | Source Sequences | | | |
| Users Latest Manua | l Network Scan Results | Network Access U Network Access U Network Acc * Name ad Status Email | isers List > New Network Access ccess User dminuser Enabled v | s User | | |
| | | ✓ Passwords Password * Login Pas | Type: Internal Users Password ssword | Re-E | nter Password | Generate P |

添加管理员用户

步骤 5.2在User Groups部分中选择SWA Admin。

| Account Disable Policy | 1 | |
|--|------------------------|--------------|
| Disable account if d | ate exceeds 2024-03-28 | (yyyy-mm-dd) |
| ▼ User Groups | | |
| SWA Admin | o — | |

步骤 5.3您需要创建具有只读权限的用户。指定名称和密码。

| dentity Services Engine | Home Context Visibility Operations Policy Administration Work Centers |
|-------------------------------------|---|
| + System - Identity Management | Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC |
| - Identities Groups External Identi | tity Sources Identity Source Sequences + Settings |
| Users | Network Access Users List > New Network Access User |
| Latest Manual Network Scan Results | * Name rouser |
| | Status ZEnabled 👻 |
| | Email |
| | ▼ Passwords |
| | Password Type: Internal Users - |
| | Password Re-Enter Password |
| | * Login Password Generate Password (|
| | Enable Password Generate Password (|

添加只读用户

步骤 5.4在User Groups部分中选择SWA ReadOnly。

| Account Disable Policy | | |
|--|------------|--------------|
| Disable account if date exceeds | 2024-03-28 | (yyyy-mm-dd) |
| ▼ User Groups | | |
| SWA ReadOnly | | |
| Submit Cancel | | |

将只读用户组分配给只读用户

第六步:为管理员用户创建授权配置文件。

导航到策略>Policy元素>结果>授权>授权配置文件> +Add。

定义授权配置文件的名称,并确保将访问类型设置为ACCESS_ACCEPT。

| dentity Services Engine | Home | Operations | ✓ Policy | Administration | Work Centers |
|---------------------------------|--|--------------------------------|----------|------------------------------------|--------------|
| Policy Sets Profiling Posture C | ient Provisioning Policy Eleme | ents | | | |
| Dictionaries Conditions Result | s | | | | |
| Authentication | Authorization Profiles > New Authorization Profile | uthorization Profile | | | |
| - Authorization | * Name | SWA Admin | | | |
| Authorization Profiles | Description | | | | |
| Downloadable ACLs | * Access Type | ACCESS_ACCEPT | Ţ |] | |
| ▶ Profiling | Network Device Profile | 💼 Cisco 👻 🕀 | | | |
| ▶ Posture | Service Template | | | | |
| Client Provisioning | Track Movement | (i) | | | |
| | Passive Identity Tracking | i | | | |
| | | | | | |
| | | | | | |

添加管理员用户的授权配置文件

步骤 6.1在"高级属性设置"中,导航到Radius > Class—[25],输入值Administrator,然后点击提交

| Advanced Attributes 8 | Settings | | |
|--|-----------------------------------|-----|--|
| Radius:Class | Administrator | - + | |
| | | | |
| Attributes Details | | | |
| Access Type = ACCESS_ACCE Class = Administrator | ग | | |
| | - /4 | | |

添加管理员用户的授权配置文件

o

步骤 7. 重复第6步为只读用户创建授权配置文件。

| dentity Services Engine | Home | Operations | ▼ Policy | Administration | ▶ Work Centers |
|---------------------------------|--|--------------------------------|----------|----------------|----------------|
| Policy Sets Profiling Posture C | lient Provisioning Policy Eleme | ents | | | |
| Dictionaries Conditions Resul | ts | | | | |
| Authentication | Authorization Profiles > New Au Authorization Profile | thorization Profile | 2 | | |
| - Authorization | * Name | SWA ReadOnly | | | |
| Authorization Profiles | Description | | | | |
| Downloadable ACLs | * Access Type | ACCESS_ACCEPT | | <u>.</u> | |
| ▶ Profiling | Network Device Profile | dete Cisco 👻 🕀 | | | |
| Posture | Service Template | | | | |
| Client Provisioning | Track Movement | i | | | |
| | Passive Identity Tracking | i) | | | |

为只读用户添加授权配置文件

第7.1 步: 使用值ReadUser创建Radius: Class,这次使用Administrator。

| Radius:Class | 📀 = ReadUser | - + |
|---|--------------|------------|
| | 0 | |
| | | |
| | | |
| | | |
| Attributes Details | | |
| | | |
| Access Type = ACCESS_ACCEPT | | |
| Access Type = ACCESS_ACCEPT Class = ReadUser | | |
| Access Type = ACCESS_ACCEPT Class = ReadUser | | |
| Access Type = ACCESS_ACCEPT Class = ReadUser | | |

步骤 8 创建与SWA IP地址匹配的策略集。这是为了防止使用这些用户凭证访问其他设备。

导航到策略>策略集,点击位于左上角的+图标。

| ahaha cisco | Identity | Services | Engine | Home | ▸ Conte | ext Visibility | Operations | ▼Policy | ► Administration | Work Centers |
|----------------|----------|-----------|-----------|----------------|---------|----------------|--------------------------------|---------|------------------|--------------|
| Policy | Sets | Profiling | Posture | Client Provisi | oning | Policy Element | nts | | | |
| | | | | | | | | | | |
| Polic | y Sets | ; | | | | | | | | |
| + | St | atus | Policy So | t Namo | | Description | | Condi | tions | |
| | 3 | latus | Policy Se | IName | | Description | | Condi | lions | |

步骤 8.1 新行位于策略集的顶部。

为新策略命名并为RADIUS NAS-IP-Address属性添加一个条件以匹配SWA IP地址。

单击Use以保留更改并退出编辑器。

Conditions Studio

ØX

| Search by Name Catalyst_Switch_Local_Web_Authentication Switch_Local_Web_Authentication Switch_Web_Authentication Switch_Web_Authentication Wired_802.1X Wireless_602.1X Wireless_Access Wireless_Access Wireless_Access | Libra | Ŋ | | Editor | | | | | |
|--|----------|--|-------------|--------|-----------------|------------|---------------|-----------|------|
| Image: Catalyst_Switch_Local_Web_Authentication Image: Switch_Local_Web_Authentication Image: Switch_Web_Authentication Image: Wired_802.1X Image: Wireless_Access Image: Wireless_Access <th>Sea</th> <th>rch by Name</th> <th></th> <th></th> <th>Radius·NA</th> <th>S-IP-Addre</th> <th>SS</th> <th></th> <th>8</th> | Sea | rch by Name | | | Radius·NA | S-IP-Addre | SS | | 8 |
| Set to 'Is not' Duplicate Save Set to 'Is not' Set to 'Is not' Duplicate Save Set to 'Is not' Set to 'Is not' <th>Q</th> <th>0 🛎 🗢 🖵 🗣 🕾 🖻 🖪 🕑 上 🔇</th> <th>) ະ</th> <th>•</th> <th>Equals</th> <th>~</th> <th>10.106.38.176</th> <th></th> <th></th> | Q | 0 🛎 🗢 🖵 🗣 🕾 🖻 🖪 🕑 上 🔇 |) ະ | • | Equals | ~ | 10.106.38.176 | | |
| Switch_Local_Web_Authentication Switch_Web_Authentication Wired_802.1X Wired_MAB Wired_MAB Wireless_802.1X Wireless_Access Wireless_Access Wireless_MAB | | Catalyst_Switch_Local_Web_Authentication | | | Set to 'Is not' | | | Duplicate | Save |
| Switch_Web_Authentication Wired_802.1X Wired_MAB Wireless_802.1X Wireless_602.1X Wireless_Access Wireless_Access Wireless_ACCess Wireless_MAB Wireless_MAB | | Switch_Local_Web_Authentication | | | | | | | |
| Wired_802.1X Wired_MAB Wireless_802.1X Wireless_802.1X Wireless_Access Wireless_Access Wireless_ACCess Wireless_MAB | | Switch_Web_Authentication | | | | | + New AND O | R | |
| Wired_MAB Wireless_802.1X Wireless_Access Wireless_Access | | Wired_802.1X | | | | | | | |
| Wireless_802.1X Wireless_Access Wireless_Access | | Wired_MAB | | | | | | | |
| Wireless_Access Wireless_MAB | | Wireless_802.1X | | | | | | | |
| Wireless_MAB () | | Wireless_Access | | | | | | | |
| | | Wireless_MAB | | | | | | | |
| WLC_Web_Authentication () | | WLC_Web_Authentication | <i>(i</i>) | | | | | | |

Close Use

添加策略以映射SWA网络设备

步骤 8.2Click Save.

| Policy | Sets | | | | | | | R | eset Pol | icyset Hitcoun | ts Rese | | Save |
|--------|---------|-----------------|--------------------|-----|--|------|-----------------------|--------|----------|----------------|---------|---|------|
| + | Status | Policy Set Name | Description | Con | fitions | Alle | owed Protocols / Ser | ver Se | quence | Hits | Actions | 1 | View |
| Search | | | | | | | | | | | | | |
| 1 | \odot | SWA Access | | 0 | Radius-NAS-IP-Address EQUALS 10,106.38,176 | D | efault Network Access | , | + | | ٥ | | > |
| | \odot | Default | Default policy set | | | D | efault Network Access | , | + | 0 | ¢ | | > |
| | | | | | | | | | | | Rese | | Save |

策略保存



提示:在本文中,默认网络访问协议列表是允许的。您可以创建新列表并根据需要缩小范 围。

步骤 9要查看新的策略集,请点击查看列中的> 图标。展开Authorization Policy菜单并单击+图标以 添加新规则,从而允许对具有管理员权限的用户进行访问。

设置名称。

步骤 9.1要创建匹配管理员用户组的条件,请点击+图标。

添

| ✓ Author | ✓ Authorization Policy (0) | | | | | | | | | | | |
|----------|----------------------------|-----------|------------|------------|--|--|--|--|--|--|--|--|
| + | Status | Rule Name | Conditions | | | | | | | | | |
| Search | | | | | | | | | | | | |
| 1 | \odot | SWA Admin | | <i>→</i> + | | | | | | | | |
| 加授权策略 | 条件 | | | | | | | | | | | |

步骤 9.2设置条件以匹配Attribute Name Equals User Identity Groups: SWA admin. Select Identity Group as Condition的字典身份组

步骤 9.3向下滚动并选择User Identity Groups: SWA admin.

| Con | ditions Studio | | | | | 6 |)× |
|----------|--|------------|--------|-----------------|------|--|----|
| Librar | у | | Editor | | | | |
| Sea | rch by Name | | | IdentityGroup | Name | | 8 |
| Q | |) t; 🤶 | 盡 | Equals | ~ | Choose from list or type | |
| | BYOD_is_Registered | | | Set to 'Is not' | | User Identity Groups:GuestType_Contractor (default) User Identity Groups:GuestType_Daily (default) Sav | /e |
| | Catalyst_Switch_Local_Web_Authentication | | | | | User Identity Groups:GuestType_SocialLogin (default) | |
| | Compliance_Unknown_Devices | () | | | | User Identity Groups:GuestType_Weekly (default) User Identity Groups:OWN_ACCOUNTS (default) | |
| | Compliant_Devices | <i>(</i>) | | | | User Identity Groups:SWA Admin | |
| | EAP-MSCHAPv2 | | | | | User Identity Groups:SWA ReadOnly | |
| | EAP-TLS | <i>()</i> | | | | | |
| | Guest_Flow | <i>()</i> | | | | | |
| | MAC_in_SAN | | | | | | |
| | Network_Access_Authentication_Passed | 0 | | | | | |
| | Non_Cisco_Profiled_Phones | <i>()</i> | | | | | |
| | Non_Compliant_Devices | <i>(</i>) | | | | | |
| | Switch_Local_Web_Authentication | () | | | | | |

Scroll Down abd Select Identity Group Name

步骤 9.4单击Use。

Close Use

Conditions Studio

| Libra | У | | Editor | | | | | | |
|------------|--|-------------|----------|-----------------|--------|-------|------------------------------|-------|------|
| Sea | rch by Name | | | IdentityGrou | p∙Name | | | | 0 |
| Q E | | 🕽 ະ 후 | # | Equals | ~ | ×Us | er Identity Groups:SWA Admin | | |
| | BYOD_is_Registered | <i>(i)</i> | | Set to 'Is not' | | You c | an only select 1 item | | Save |
| | Catalyst_Switch_Local_Web_Authentication | n (j) | | | | | | | |
| | Compliance_Unknown_Devices | () | | | | + | New AND OR | | |
| | Compliant_Devices | <i>()</i> | | | | | | | |
| | EAP-MSCHAPv2 | <i>i</i>) | | | | | | | |
| | EAP-TLS | 0 | | | | | | | |
| | Guest_Flow | <i>(i</i>) | | | | | | | |
| | MAC_in_SAN | () | | | | | | | |
| | Network_Access_Authentication_Passed | () | | | | | | | |
| | Non_Cisco_Profiled_Phones | 1 | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | Close | Use |

为SWA管理员用户组选择授权策略

步骤 10 单击+图标可添加第二条规则,用于为具有只读权限的用户提供访问权限。

设置名称。

设置条件以匹配Dictionary Identity Group和Attribute Name Equals User Identity Groups: SWA ReadOnly,然后单击Use。

Conditions Studio

| Librar | Library | | | | | | | | | | | |
|------------|--|-------------|--|--|--|--|--|--|--|--|--|--|
| Sear | rch by Name | | | | | | | | | | | |
| Q 🛱 | | ÷ # | | | | | | | | | | |
| | BYOD_is_Registered | () | | | | | | | | | | |
| | Catalyst_Switch_Local_Web_Authentication | () | | | | | | | | | | |
| | Compliance_Unknown_Devices | () | | | | | | | | | | |
| | Compliant_Devices | () | | | | | | | | | | |
| | EAP-MSCHAPv2 | () | | | | | | | | | | |
| | EAP-TLS | () | | | | | | | | | | |
| | Guest_Flow | () | | | | | | | | | | |
| | MAC_in_SAN | () | | | | | | | | | | |
| | Network_Access_Authentication_Passed | () | | | | | | | | | | |
| | Non_Cisco_Profiled_Phones | <i>(i</i>) | | | | | | | | | | |
| | | | | | | | | | | | | |

| | - internative roup | Tunic | | | | | | | | |
|---|--------------------|-------|-------------------------------------|-----------|------|--|--|--|--|--|
| • | Equals | ~ | × User Identity Groups:SWA ReadOnly | | | | | | | |
| | Set to 'Is not' | | | Duplicate | Save | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | + New AND OR | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

Close Use

Reset Save

选择只读用户组的授权策略

步骤 11 分别为每个规则设置Authorization Profile,然后单击Save。

| Policy | Sets → SV | VA Access | | | | | Reset Policyset Hitcount | s Rese | t Save |
|--------|----------------|--------------------------|--------------------|--|------------------|--------------------|---------------------------|------------|---------|
| | Status | Policy Set Name | Description | Conditions | | | Allowed Protocols / Serve | r Sequence | Hits |
| Search | | | | | | | | | |
| | 0 | SWA Access | | Radius-NAS-IP-Address EQUAL | \$ 10.106.38.176 | | Default Network Access | × * + | 0 |
| > Auti | nentication P | olicy (1) | | | | | | | |
| > Auti | norization Pol | licy - Local Exceptions | | | | | | | |
| > Auti | norization Po | licy - Global Exceptions | | | | | | | |
| ❤ Auti | norization Po | licy (1) | | | | | | | |
| | | | | | Results | | | | |
| • | Status | Rule Name | Conditions | | Profiles | Security Grou | ps | Hits | Actions |
| Searc | h | | | | | | | | |
| 1 | \odot | SWA Read Only | A IdentityGroup-N | ame EQUALS User Identity Groups:SWA ReadOnly | × SWA ReadOnly | + Select from list | * + | | ٥ |
| 1 | Ø | SWA Admin | 識. IdentityGroup-N | ame EQUALS User Identity Groups:SWA Admin | × SWA Admin | + Select from list | * + | | ٥ |
| | ø | Default | | | × DenyAccess | + Select from list | * + | 0 | ٥ |
| | | | | | | | | | |

选择授权配置文件

SWA配置

步骤1:从SWA GUI导航至系统管理,然后点击用户。

第二步:在External Authentication中单击Enable。

| | Cisco See | cure Web Appliance | | | | Secure We |
|---|-----------|----------------------|-------------------|---------|-----------------------|-----------|
| • | Reporting | Web Security Manager | Security Services | Network | System Administration | |
| | | | | | | |

Users

| Users | | | | | | |
|-----------------|------------------|---------------|---------------|----------------|--------------------|--------|
| Add User | | | | | | |
| All Accounts | User Name | Full Name | User Type | Account Status | Passphrase Expires | Delete |
| | admin | Administrator | Administrator | Active | n/a | |
| Enforce Pa | ssphrase Changes | | | | | |

| Local User Account & Passphrase Settings | |
|--|---|
| Account Lock: | Not configured. |
| Passphrase Reset: | Not configured. |
| Passphrase Rules: | Require at least 8 characters. Additional rules configured |
| | Edit Settings |
| | |
| External Authentication | |
| External Authentication is disabled. | |
| | Enable |
| Second Factor Authentication Settings | |
| Two Factor Authentication is disabled. | |
| | Enable |

在SWA中启用外部身份验证

第三步:在RADIUS Server Hostname字段中输入ISE的IP地址或FQDN,并输入在步骤2 ISE配置 中配置的相同共享密钥。

第四步:在Group Mapping中选择Map external authenticated users to multiple local roles。

步骤 4.1在RADIUS CLASS Attribute字段中输入Administrator并选择Role Administrator。

步骤 4.2在RADIUS CLASS Attribute字段中输入ReadUser并选择角色Read-Only Operator。

| Reporting | Web Security Manager | Security Services | Ne | twork | System Adm | ninistration | 1 | | | |
|----------------------------|----------------------------|---|------------|-------------------|----------------|--------------|----------------------------|--------------|----------|--|
| | ,, | | | | | | · | | | |
| it Externa | I Authentication | | | | | | | | | |
| ternal Authenti | cation Settings | | | | | | | | | |
| 🗹 Enable Exter | nal Authentication | | | | | | | | | |
| | Authentication Mode: | Password based Authentica | tion | ~ | | | | | | |
| | Authentication Type: | RADIUS V | | | | | | | | |
| | Protocol | UDP V | | | | | | | | |
| RADIUS Server Information: | | RADIUS Server Hostname | Port | Shared Secret | d Secret | | Authentication protocol | Certificate | Add Row | |
| | | 10.106.38.150 | 1812 | •••• | | 5 | PAP v | Select any v | Ê | |
| External Authe | ntication Cache Timeout: ? | 0 seconds | | | | | | | | |
| | Group Mapping: | Map externally authenticated users to multiple local roles. (recommended) | | | | | | | | |
| | | RADIUS CLASS Attribute | | | Role ? | | | Add Row | | |
| | | administrator | | | Administr | ator | ~ | | <u> </u> | |
| | | ReadUser | | Read-Only | y Operato | r • | ŵ | | | |
| | | RADIUS CLASS attribut | es are cas | se-sensitive. | | | | | | |
| | | O Map all externally authen | ticated us | ers to the Admini | istrator role. | | | | | |

RADIUS服务器的外部身份验证配置

第5步:要在SWA中配置用户,请点击添加用户。输入User Name并选择所需角色所需的User Type。输入Passphrase和Retype Passphrase,如果设备无法连接到任何外部RADIUS服务器,则 需要此口令才能进行GUI访问。



注意:如果设备无法连接到任何外部服务器,它会尝试将用户验证为安全Web设备上定义 的本地用户。

Users

| Users | | | | | | |
|-------------|------------------------|-------------------------------|---|--------------------------------|--|-----------------|
| Add User | | | | | | |
| * When RADI | US external authentica | tion is enabled, all local us | er accounts except "admin" are disabled | . If all RADIUS services fail, | local user accounts will be used for a | authentication. |
| All | | | | | | |
| Accounts | User Name | Full Name | User Type* | Account Status | Passphrase Expires | Delete |
| | adminuser | Admin User | Administrator | Active | n/a | ŵ |
| | rouser | RO User | Read-Only Operator | Active | n/a | ŵ |

SWA中的用户配置

第6步:点击提交并提交更改。

验证

使用配置的用户凭证访问SWA GUI,并检查ISE中的实时日志。要检查ISE中的实时日志,请导航到

操作>实时日志:

dentity Services Engine

| Event | 5200 Authentication succeeded | |
|-----------------------|-------------------------------|--|
| Username | adminuser | |
| Endpoint Id | | |
| Endpoint Profile | | |
| Authentication Policy | SWA Access >> Default | |
| Authorization Policy | SWA Access >> SWA Admin | |
| Authorization Result | SWA Admin | |
| ithentication Details | | |
| Source Timestamp | 2024-01-28 17:28:31.573 | |
| | | |

验证用户登录ISE

相关信息

- <u>思科安全Web设备AsyncOS 14.0用户指南</u>
- <u>ISE 3.0管理员指南</u>
- 安全Web设备的ISE兼容性列表
- 思科技术支持和下载

Steps 11001 Received RADIUS Access-Request 11017 RADIUS created a new session 11117 Generated a new session ID 15049 Evaluating Policy Group 15008 Evaluating Service Selection Policy 15048 Queried PIP - Radius.NAS-IP-Address 15041 Evaluating Identity Policy 22072 Selected identity source sequence - All_User_ID_Stores 15013 Selected Identity Source - Internal Users 24210 Looking up User in Internal Users IDStore - adminuser 24212 Found User in Internal Users IDStore 22037 Authentication Passed 15036 Evaluating Authorization Policy 15016 Selected Authorization Profile - SWA Admin 22081 Max sessions policy passed 22080 New accounting session created in Session cache 11002 Returned RADIUS Access-Accept

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。