

Configurar servidores RADIUS externos no ISE

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar o ISE \(servidor front-end\)](#)

[Configurar o servidor RADIUS externo](#)

[Verificar](#)

[Troubleshooting](#)

[Cenário 1. Evento - 5405 Solicitação RADIUS Descartada](#)

[Cenário 2. Evento - Falha na autenticação 5400](#)

Introdução

Este documento descreve a configuração de um servidor RADIUS no ISE como um servidor proxy e de autorização. Aqui dois servidores ISE são usados e um atua como um servidor externo. Porém, qualquer servidor RADIUS compatível com RFC pode ser utilizado.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do protocolo RADIUS
- Experiência em configuração de políticas do Identity Services Engine (ISE)

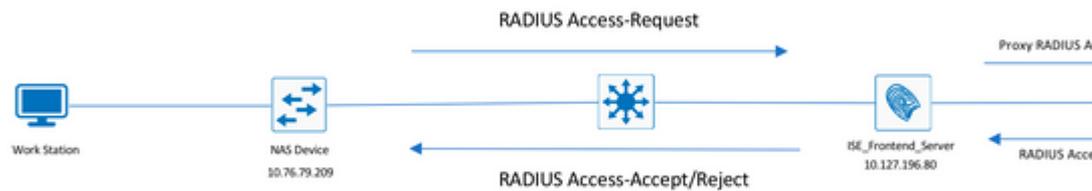
Componentes Utilizados

As informações neste documento são baseadas nas versões 2.2 e 2.4 do Cisco ISE.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

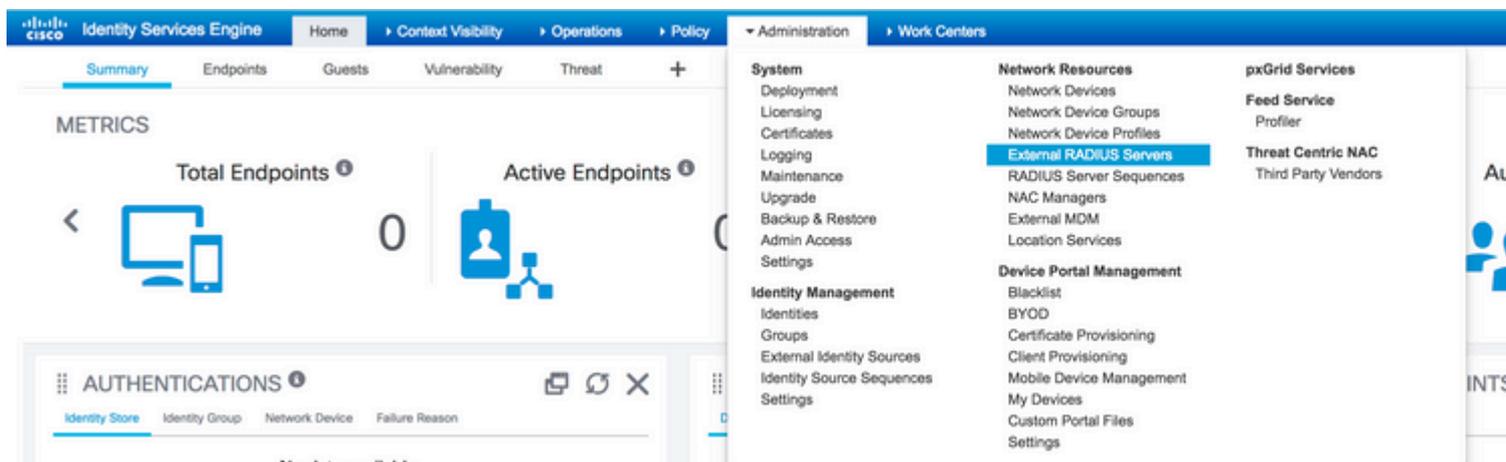
Configurar

Diagrama de Rede



Configurar o ISE (servidor front-end)

Etapa 1. Vários servidores RADIUS externos podem ser configurados e usados para autenticar usuários no ISE. Para configurar servidores RADIUS externos, navegue até Administration > Network Resources > External RADIUS Servers > Add, conforme mostrado na imagem:



External RADIUS Servers List > ISE_BackEnd_Server

External RADIUS Server

* Name

Description

* Host IP

* Shared Secret

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

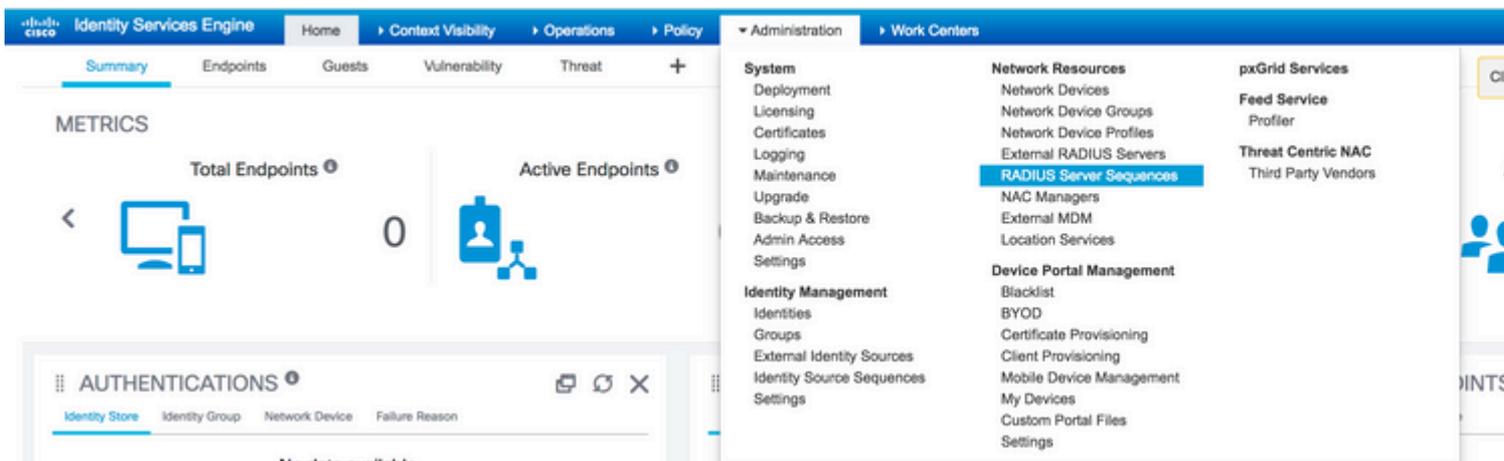
* Authentication Port (Valid Range 1 to 65535)

* Accounting Port (Valid Range 1 to 65535)

* Server Timeout Seconds (Valid Range 1 to 120)

* Connection Attempts (Valid Range 1 to 9)

Etapa 2. Para usar o servidor RADIUS externo configurado, uma sequência de servidor RADIUS deve ser configurada de forma semelhante à sequência de origem da identidade. Para configurar o mesmo, navegue até Administration > Network Resources > RADIUS Server Sequences > Add, conforme mostrado na imagem.





RADIUS Server Sequences List > **New RADIUS Server Sequence**

RADIUS Server Sequence

General

Advanced Attribute Settings

* Name

Description

Sequence in which the external servers should be used.

▼ User Selected Service Type

Select the set of external RADIUS servers to use to process requests. Servers are accessed in sequence until a

Available

* Selected

ISE_BackEnd_Server



Remote accounting

Local accounting

Submit

Cancel

Observação: uma das opções disponíveis durante a criação da sequência de servidores é escolher se a contabilização deve ser feita localmente no ISE ou no servidor RADIUS externo. Com base na opção escolhida aqui, o ISE decide se deseja usar proxy nas solicitações de contabilização ou armazenar esses logs localmente.

Etapa 3. Há uma seção adicional que oferece mais flexibilidade sobre como o ISE deve se comportar quando faz o proxy de solicitações para servidores RADIUS externos. Ele pode ser encontrado em *Advance Attribute Settings*, conforme mostrado na imagem.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed S > Network Devices > Network Device Groups > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequ. The main heading is 'RADIUS Server Sequence' with sub-headings 'General' and 'Advanced Attribute Settings'. Under 'Advanced Settings', there are two checkboxes: 'Strip start of subject name up to the first occurrence of the separator' with a text box containing '\', and 'Strip end of subject name from the last occurrence of the separator' with a text box containing '@'. Below this is the 'Modify Attribute in the request' section with a checkbox 'Modify attributes in the request to the External RADIUS Server' and a list builder with 'Add', 'Select an item', '=', and '+'. The 'Continue to Authorization Policy' section has a checked checkbox 'On Access-Accept, continue to Authorization Policy'. The 'Modify Attribute before access accept' section has a checkbox 'Modify attributes before send an Access-Accept' and another list builder. At the bottom are 'Save' and 'Reset' buttons.

- Configurações avançadas: fornece opções para remover o início ou o fim do nome de usuário em solicitações RADIUS com um delimitador.

- **Modificar Atributo na solicitação:** Fornece a opção de modificar qualquer atributo RADIUS nas solicitações RADIUS. A lista aqui mostra os atributos que podem ser adicionados/removidos/atualizados:

User-Name-- [1]
 NAS-IP-Address-- [4]
 NAS-Port-- [5]
 Service-Type-- [6]
 Framed-Protocol-- [7]
 Framed-IP-Address-- [8]
 Framed-IP-Netmask-- [9]
 Filter-ID-- [11]
 Framed-Compression-- [13]
 Login-IP-Host-- [14]
 Callback-Number-- [19]
 State-- [24]
 VendorSpecific-- [26]
 Called-Station-ID-- [30]
 Calling-Station-ID-- [31]
 NAS-Identifier-- [32]
 Login-LAT-Service-- [34]
 Login-LAT-Node-- [35]
 Login-LAT-Group-- [36]
 Event-Timestamp-- [55]
 Egress-VLANID-- [56]
 Ingress-Filters-- [57]
 Egress-VLAN-Name-- [58]
 User-Priority-Table-- [59]
 NAS-Port-Type-- [61]
 Port-Limit-- [62]
 Login-LAT-Port-- [63]
 Password-Retry-- [75]
 Connect-Info-- [77]
 NAS-Port-Id-- [87]
 Framed-Pool-- [88]
 NAS-Filter-Rule-- [92]
 NAS-IPv6-Address-- [95]
 Framed-Interface-Id-- [96]
 Framed-IPv6-Prefix-- [97]
 Login-IPv6-Host-- [98]
 Error-Cause-- [101]
 Delegated-IPv6-Prefix-- [123]
 Framed-IPv6-Address-- [168]
 DNS-Server-IPv6-Address-- [169]
 Route-IPv6-Information-- [170]
 Delegated-IPv6-Prefix-Pool-- [171]
 Stateful-IPv6-Address-Pool-- [172]

- **Continuar com a política de autorização no acesso aceito:** fornece uma opção para escolher se o ISE deve apenas enviar o acesso aceito como está ou continuar a fornecer acesso com base nas políticas de autorização configuradas no ISE, em vez da autorização fornecida pelo servidor RADIUS externo. Se essa opção for selecionada, a autorização fornecida pelo servidor RADIUS externo será substituída pela autorização fornecida pelo ISE.

Observação: esta opção funciona somente se o servidor RADIUS externo enviar

um Access-Accept em resposta à solicitação de acesso RADIUS com proxy.

- Modificar atributo antes de aceitar acesso: semelhante ao Modify Attribute in the request, os atributos mencionados anteriormente podem ser adicionados/removidos/atualizados presentes no Access-Accept enviado pelo servidor RADIUS externo antes de ser enviado ao dispositivo de rede.

Etapa 4. A próxima parte é configurar os conjuntos de políticas para usar a sequência de servidor RADIUS em vez dos protocolos permitidos, de modo que as solicitações sejam enviadas ao servidor RADIUS externo. Ele pode ser configurado em Policy > Policy Sets. As políticas de autorização podem ser configuradas no Policy Set mas só entram em vigor se a Continue to Authorization Policy on Access-Accept opção é escolhida. Caso contrário, o ISE simplesmente atua como um proxy para as solicitações RADIUS para atender às condições configuradas para esse conjunto de políticas.

Status	Policy Set Name	Description	Conditions
On	External_Auth_Policy_Set		DEVICE:Device Type EQUALS All Device Types
On	Default	Default policy set	

Status	Policy Set Name	Description	Conditions
On	External_Auth_Policy_Set		DEVICE:Device Type EQUALS All Device Types

Authentication Policy (1)

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (1)

Status	Rule Name	Conditions	Results
On	Default	PermitAccess	

Configurar o servidor RADIUS externo

Etapa 1. Neste exemplo, outro servidor ISE (versão 2.2) é usado como um servidor RADIUS externo chamado ISE_Backend_Server. O ISE (ISE_Frontend_Server) deve ser configurado como um dispositivo de rede ou tradicionalmente chamado NAS no servidor RADIUS externo (ISE_Backend_Server neste exemplo), já que o NAS-IP-Address na solicitação de acesso que é encaminhada ao servidor RADIUS externo é substituído pelo endereço IP do ISE_Frontend_Server. O segredo compartilhado a ser configurado é o mesmo que o configurado para o servidor RADIUS externo no ISE_Frontend_Server.

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for a Network Device. The breadcrumb navigation shows: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC > Network Devices. The left sidebar contains 'Network devices', 'Default Device', and 'Device Security Settings'. The main content area is titled 'Network Devices List > ISE_Frontend_Server' and 'Network Devices'. The configuration fields are as follows:

- Name: ISE_Frontend_Server
- Description: This will be used as an
- IP Address: 10.127.196.80 / 32
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: (empty)
- Device Type: All Device Types (Set To Default)
- IPSEC: No (Set To Default)
- Location: All Locations (Set To Default)
- Trustsec: SGA (Set To Default)
- Authentication Settings: RADIUS Authentication Settings, TACACS Authentication Settings, SNMP Settings, Advanced TrustSec Settings

Buttons for 'Save' and 'Reset' are located at the bottom left of the configuration area.

Etapa 2. O servidor RADIUS externo pode ser configurado com suas próprias políticas de autenticação e autorização para atender às solicitações intermediadas pelo ISE. Neste exemplo, uma política simples é configurada para verificar o usuário nos usuários internos e depois permitir o acesso se autenticado.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets

Search policy names & descriptions.

Summary of Policies
A list of all your policies

Global Exceptions
Rules across entire deployment

Default
Default Policy Set

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	Default Policy Set

Authentication Policy

Status	Name	Conditions (Identity groups and other conditions)	Allow Protocols	and use
<input checked="" type="checkbox"/>	MAB	if Wired_MAB OR Wireless_MAB	Default Network Access	
<input checked="" type="checkbox"/>	Dot1X	if Wired_802.1X OR Wireless_802.1X	Default Network Access	
<input checked="" type="checkbox"/>	Default Rule (If no match)	Allow Protocols : Default Network Access		and use : Internal Users

Authorization Policy

Exceptions (0)

Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
<input checked="" type="checkbox"/>	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess
<input checked="" type="checkbox"/>	Employee_EAP-TLS	if (Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then PermitAccess AND BYOD
<input checked="" type="checkbox"/>	Employee_Onboarding	if (Wireless_802.1X AND EAP-MSCHAPV2)	then NSP_Onboard AND BYOD
<input checked="" type="checkbox"/>	Wi-Fi_Guest_Access	if (Guest_Flow AND Wireless_MAB)	then PermitAccess AND Guests
<input checked="" type="checkbox"/>	Wi-Fi_Redirect_to_Guest_Login	if Wireless_MAB	then Cisco_WebAuth
<input checked="" type="checkbox"/>	Basic_Authenticated_Access	if Network_Access_Authentication_Passed	then PermitAccess
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess

Save Reset

Verificar

Etapa 1. Verifique os logs ao vivo do ISE se a solicitação for recebida, como mostrado na imagem.

Apr 19, 2018 07:01:54.570 PM testaccount External_Auth_Policy_Set External_Auth_Policy_Set

Etapa 2. Verifique se o conjunto de políticas correto está selecionado, como mostrado na imagem.

Overview

Event 5200 Authentication succeeded

Username testaccount

Endpoint Id

Endpoint Profile

Authentication Policy External_Auth_Policy_Set

Authorization Policy External_Auth_Policy_Set

Authorization Result

Etapa 3. Verifique se a solicitação é encaminhada ao servidor RADIUS externo.

Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 11049 Settings of RADIUS default network device will be used
- 11117 Generated a new session ID
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - DEVICE.Device Type
- 11358 Received request for RADIUS server sequence.
- 11361 Valid incoming authentication request
- 11355 Start forwarding request to remote RADIUS server
- 11365 Modify attributes before sending request to external radius server
- 11100 RADIUS-Client about to send request - (port = 1812)
- 11101 RADIUS-Client received response
- 11357 Successfully forwarded request to current remote RADIUS server
- 11002 Returned RADIUS Access-Accept

4. Se a Continue to Authorization Policy on Access-Accept for selecionada, verifique se a política de autorização foi avaliada.



Overview

Event	5200 Authentication succeeded
Username	testaccount
Endpoint Id	
Endpoint Profile	
Authentication Policy	External_Auth_Policy_Set
Authorization Policy	External_Auth_Policy_Set >> Default
Authorization Result	PermitAccess

Steps

11001 Received RADIUS Access-Request
11017 RADIUS created a new session
11049 Settings of RADIUS default network device will be used
11117 Generated a new session ID
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - DEVICE.Device Type
11358 Received request for RADIUS server sequence.
11361 Valid incoming authentication request
11355 Start forwarding request to remote RADIUS server
11365 Modify attributes before sending request to external radius server
11100 RADIUS-Client about to send request - (port = 1812)
11101 RADIUS-Client received response
11357 Successfully forwarded request to current remote RADIUS server
15036 Evaluating Authorization Policy
15016 Selected Authorization Profile - PermitAccess
22081 Max sessions policy passed
22080 New accounting session created in Session cache
11002 Returned RADIUS Access-Accept

Troubleshooting

Cenário 1. Evento - 5405 Solicitação RADIUS Descartada

- O mais importante a ser verificado são as etapas do relatório detalhado de autenticação. Se as etapas disserem que o RADIUS-Client request timeout expired, significa que o ISE não recebeu nenhuma resposta do servidor RADIUS externo configurado. Isso pode acontecer quando:
 1. Há um problema de conectividade com o servidor RADIUS externo. O ISE não consegue acessar o servidor RADIUS externo nas portas configuradas para ele.
 2. O ISE não está configurado como um dispositivo de rede ou NAS no servidor RADIUS externo.
 3. Os pacotes são descartados pelo servidor RADIUS externo por configuração ou devido a algum problema no servidor RADIUS externo.

Steps

11001 Received RADIUS Access-Request
11017 RADIUS created a new session
11049 Settings of RADIUS default network device will be used
11117 Generated a new session ID
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - DEVICE.Device Type
11358 Received request for RADIUS server sequence.
11361 Valid incoming authentication request
11355 Start forwarding request to remote RADIUS server
11365 Modify attributes before sending request to external radius server
11100 RADIUS-Client about to send request - (port = 1812)
11104 RADIUS-Client request timeout expired (🕒 Step latency=15011 ms)
11356 Failed to forward request to current remote RADIUS server
11353 No more external RADIUS servers; can't perform failover

Verifique também as capturas de pacote para ver se não é uma mensagem falsa, ou seja, o ISE recebe o pacote de volta do servidor, mas ainda relata que a solicitação atingiu o tempo limite.

1041	6.537919	10.127.196.80	10.127.196.82	207	RADIUS	Acc
1718	11.542634	10.127.196.80	10.127.196.82	207	RADIUS	Acc
2430	16.547029	10.127.196.80	10.127.196.82	207	RADIUS	Acc

- Se as etapas disserem Start forwarding request to remote RADIUS server e a etapa imediata é No more external RADIUS servers; can't perform failover, significa que todos os servidores RADIUS externos configurados estão marcados como **inativos** e que as solicitações são atendidas somente após a expiração do temporizador inativo.

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11049	Settings of RADIUS default network device will be used
11117	Generated a new session ID
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - DEVICE.Device Type
11358	Received request for RADIUS server sequence.
11361	Valid incoming authentication request
11355	Start forwarding request to remote RADIUS server
11353	No more external RADIUS servers; can't perform failover

Observação: o **tempo inativo** padrão **para servidores RADIUS externos no ISE é de 5 minutos**. Este valor está codificado e não pode ser modificado a partir desta versão.

- Se as etapas disserem RADIUS-Client encountered error during processing flow e são seguidos por Failed to forward request to current remote RADIUS server; an invalid response was received, isso significa que o ISE encontrou um problema enquanto a solicitação ao servidor RADIUS externo era encaminhada. Isso geralmente é visto quando a solicitação RADIUS enviada do dispositivo de rede/NAS para o ISE não tem o NAS-IP-Address como um dos atributos. Se não houver NAS-IP-Address e se os servidores RADIUS externos não estiverem em uso, o ISE preencherá o NAS-IP-Address com o IP de origem do pacote. No entanto, isso não se aplica quando um servidor RADIUS externo está em uso.

Cenário 2. Evento - Falha na autenticação 5400

- Nesse caso, se as etapas disserem 11368 Please review logs on the External RADIUS Server to determine the precise failure reason, significa que a autenticação falhou no próprio servidor RADIUS externo e enviou um Access-Reject.

Steps

11001 Received RADIUS Access-Request
11017 RADIUS created a new session
11049 Settings of RADIUS default network device will be used
11117 Generated a new session ID
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - DEVICE.Device Type
11358 Received request for RADIUS server sequence.
11361 Valid incoming authentication request
11355 Start forwarding request to remote RADIUS server
11365 Modify attributes before sending request to external radius server
11100 RADIUS-Client about to send request - (port = 1812)
11101 RADIUS-Client received response
11368 Please review logs on the External RADIUS Server to determine the precise failure reason.
11357 Successfully forwarded request to current remote RADIUS server
11003 Returned RADIUS Access-Reject

- Se as etapas disserem 15039 Rejected per authorization profile, isso significa que o ISE recebeu um Access-Accept do servidor RADIUS externo, mas o ISE rejeita a autorização com base nas políticas de autorização configuradas.

Steps

11001 Received RADIUS Access-Request
11017 RADIUS created a new session
11049 Settings of RADIUS default network device will be used
11117 Generated a new session ID
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - DEVICE.Device Type
11358 Received request for RADIUS server sequence.
11361 Valid incoming authentication request
11355 Start forwarding request to remote RADIUS server
11365 Modify attributes before sending request to external radius server
11100 RADIUS-Client about to send request - (port = 1812)
11101 RADIUS-Client received response
11357 Successfully forwarded request to current remote RADIUS server
15036 Evaluating Authorization Policy
15016 Selected Authorization Profile - DenyAccess
15039 Rejected per authorization profile
11003 Returned RADIUS Access-Reject

- Se a Failure Reason no ISE é qualquer outra coisa além daquelas mencionadas aqui no caso de uma falha de autenticação, então pode significar um problema potencial com a configuração ou com o próprio ISE. Recomenda-se abrir um caso de TAC neste ponto.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.