

Autorisierungsablauf für passive ID-Sitzungen in ISE 3.2 konfigurieren

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfiguration](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Autorisierungsregeln für passive ID-Ereignisse konfiguriert werden, um den Sitzungen SGTs zuzuweisen.

Hintergrundinformationen

Passive Identitätsdienste (passive ID) authentifizieren Benutzer nicht direkt, sondern erfassen Benutzeridentitäten und IP-Adressen von externen Authentifizierungsservern wie Active Directory (AD), auch Anbieter genannt, und geben diese Informationen dann an Teilnehmer weiter.

ISE 3.2 enthält eine neue Funktion, mit der Sie eine Autorisierungsrichtlinie konfigurieren können, um einem Benutzer ein Security Group Tag (SGT) auf Basis der Active Directory-Gruppenmitgliedschaft zuzuweisen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco ISE 3.x
- Passive ID-Integration mit beliebigen Anbietern
- Active Directory (AD)-Verwaltung
- Segmentierung (TrustSec)
- PxGrid (Platform Exchange Grid)

Verwendete Komponenten

- Identity Service Engine (ISE) Softwareversion 3.2
- Microsoft Active Directory

- Syslogs

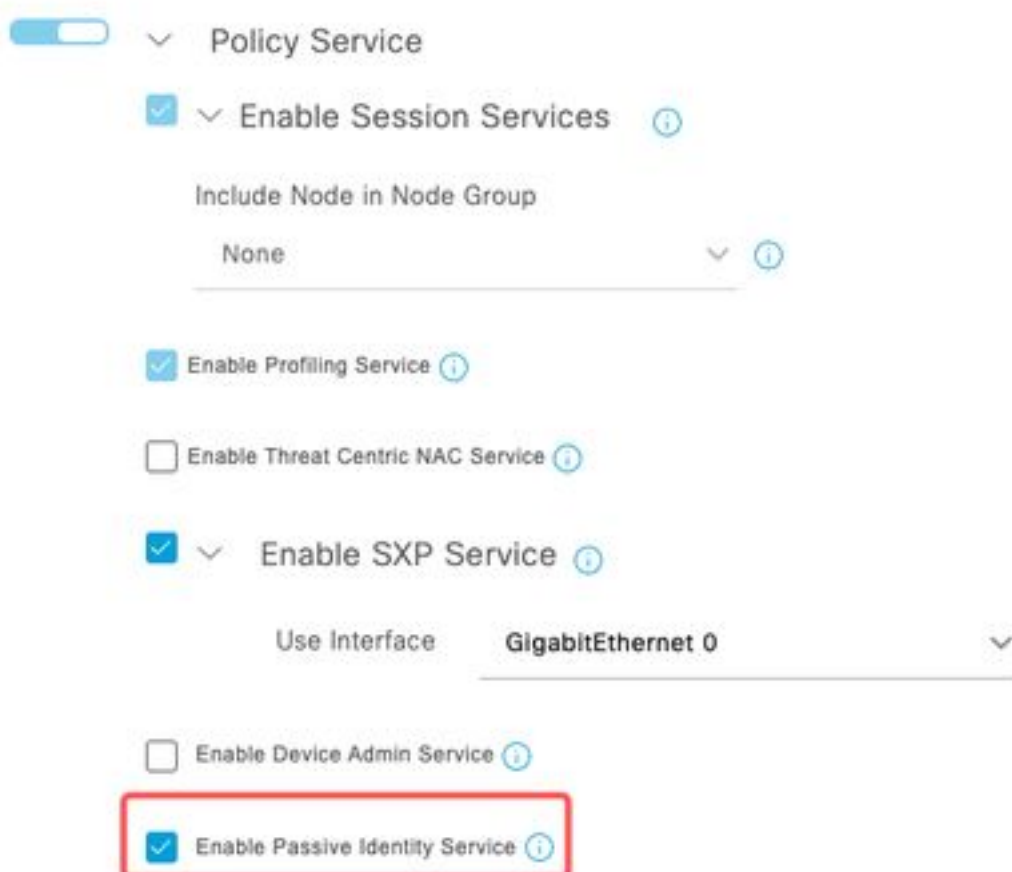
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konfiguration

Schritt 1: Aktivieren Sie die ISE-Services.

1. Navigieren Sie auf der ISE zu Administration > **Deployment**, wählen Sie den ISE-Knoten aus, und klicken Sie auf **Edit**, **Enable Policy Service (Bearbeiten)** und wählen Sie **Enable Passive Identity Service (Passiven Identitätsdienst aktivieren)** aus. Optional können Sie SXP und PxGrid aktivieren, wenn die passiven ID-Sitzungen über jede einzelne Sitzung veröffentlicht werden müssen. Klicken Sie auf **Speichern**.

Warnung: SGT-Details der PassiveID-Anmeldebenutzer, die vom API-Anbieter authentifiziert wurden, können nicht in SXP veröffentlicht werden. Die SGT-Details dieser Benutzer können jedoch über pxGrid und pxGrid Cloud veröffentlicht werden.



Dienste aktiviert



Schritt 2: Konfigurieren Sie Active Directory.

1. Navigieren Sie zu Administration > **Identity Management** > **External Identity Sources**, und wählen Sie **Active Directory** aus, und klicken Sie dann auf die Schaltfläche **Add** (Hinzufügen).
2. Geben Sie den **Namen des Verbindungspunkts** und die **Active Directory-Domäne** ein. Klicken

Sie auf **Senden**.

Identities Groups **External Identity Sources** Identity Source Sequences

External Identity Sources

<  

>  Certificate Authentication F

 Active Directory

Connection

* Join Point Name

* Active Directory Domain

Active Directory hinzufügen

3. Ein Popup-Fenster wird angezeigt, um der ISE beim AD beizutreten. Klicken Sie auf **Ja**. Geben Sie den **Benutzernamen** und das **Kennwort ein**. Klicken Sie auf OK.



Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

No

Weiter zur

Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name 

* Password

Specify Organizational Unit 

Store Credentials 

Cancel

ISE *Active Directory beitreten*

4. AD-Gruppen abrufen. Navigieren Sie zu **Gruppen**, klicken Sie auf **Hinzufügen**, dann auf **Gruppen abrufen**, wählen Sie alle interessierten Gruppen aus, und klicken Sie auf **OK**.

Select Directory Groups

This dialog is used to select groups from the Directory.

Domain: aaamexrub.com

Name Filter: _____ SID Filter: _____ Type Filter: All

[Retrieve Groups...](#) 53 Groups Retrieved.

<input type="checkbox"/>	aaamexrub.com/Users/Cloneable Domain Contro...	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Denied RODC Password ...	S-1-5-21-144182218-1144227253-205214604...	DOMAIN LOCAL
<input type="checkbox"/>	aaamexrub.com/Users/DnsAdmins	S-1-5-21-144182218-1144227253-205214604...	DOMAIN LOCAL
<input type="checkbox"/>	aaamexrub.com/Users/DnsUpdateProxy	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input checked="" type="checkbox"/>	aaamexrub.com/Users/Domain Admins	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Domain Computers	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Domain Controllers	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Domain Guests	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input checked="" type="checkbox"/>	aaamexrub.com/Users/Domain Users	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Enterprise Admins	S-1-5-21-144182218-1144227253-205214604...	UNIVERSAL
<input type="checkbox"/>	aaamexrub.com/Users/Enterprise Read-only De...	S-1-5-21-144182218-1144227253-205214604...	UNIVERSAL
<input type="checkbox"/>	aaamexrub.com/Users/Group Policy Creator Ow...	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Protected Users	S-1-5-21-144182218-1144227253-205214604...	GLOBAL

[Cancel](#) [OK](#)

AD-Gruppen abrufen

Connection Allowed Domains PassiveID **Groups**

[Edit](#) [+ Add](#) [Delete Group](#) [Update SID Values](#)

<input type="checkbox"/>	Name	S
<input type="checkbox"/>	aaamexrub.com/Users/Domain Admins	S
<input type="checkbox"/>	aaamexrub.com/Users/Domain Users	S
<input type="checkbox"/>	aaamexrub.com/Users/sponsors	S

Abgerufene Gruppen

5. Autorisierungsablauf aktivieren. Navigieren Sie zu **Erweiterte Einstellungen**, und aktivieren Sie im Abschnitt **PassiveID-Einstellungen** das Kontrollkästchen **Autorisierungsablauf**. Klicken Sie auf **Speichern**.

PassiveID Settings

The PassiveID settings that are configured in this section are applied to all the join points in Cisco ISE.

History interval*	10
Domain Controller event inactivity time* (monitored by Agent)	0
Latency interval of events from agent*	0
User session aging time*	24

Authorization Flow ⓘ

Autorisierungsablauf

aktivieren

Schritt 3: Konfigurieren Sie den Syslog-Anbieter.

1. Navigieren Sie zu Work Centers > **PassiveID** > **Providers**, wählen Sie **Syslog Providers** aus, klicken Sie auf **Add (Hinzufügen)**, und geben Sie die Informationen an. Klicken Sie auf **Speichern**

Achtung: In diesem Fall empfängt die ISE die Syslog-Meldung einer erfolgreichen VPN-Verbindung in einer ASA, diese Konfiguration wird in diesem Dokument jedoch nicht beschrieben.

Syslog Providers

Name*
ASA

Description


Status*
Enabled

Host FQDN*
asa-rudelave.aaamexrub.com

Connection Type*
UDP - Port 40514

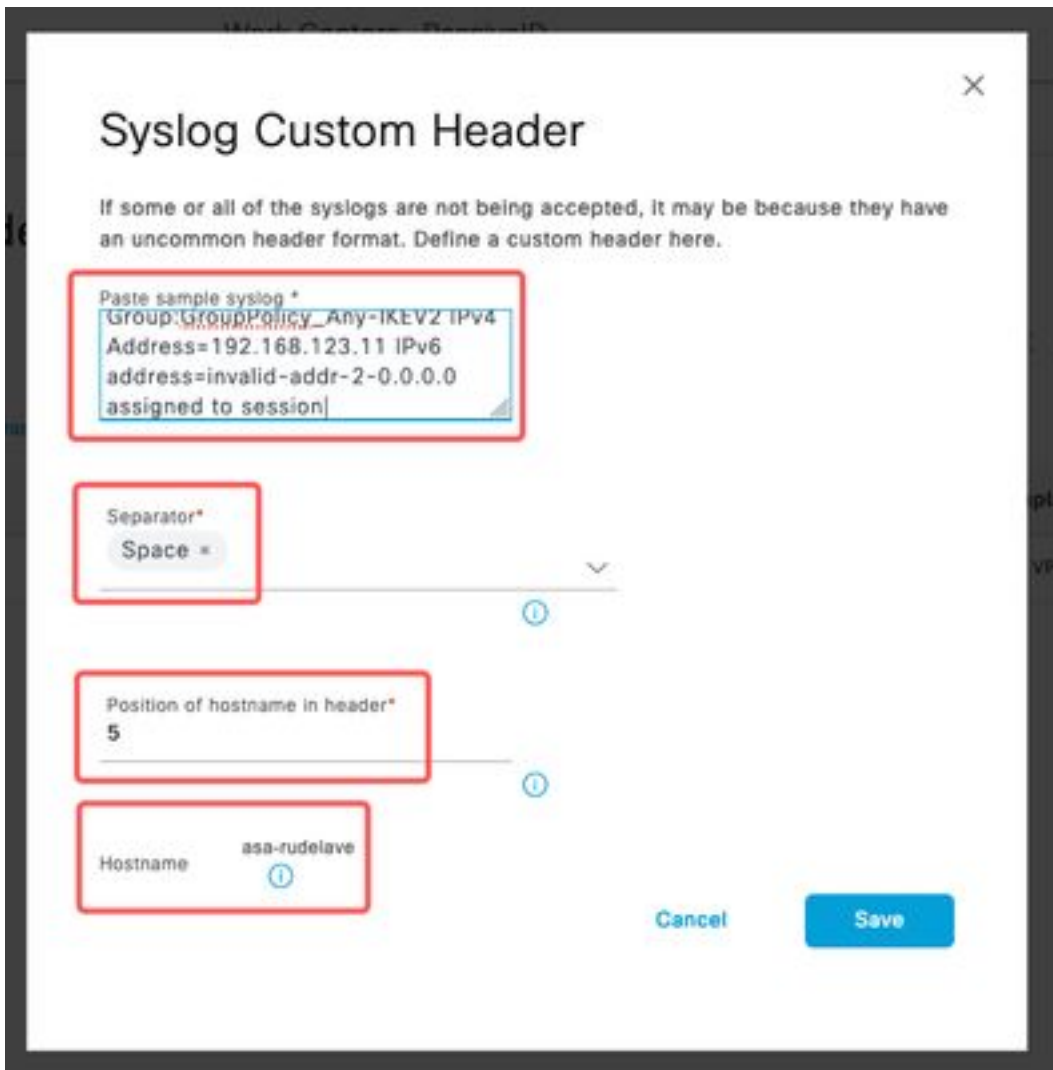
Template* ASA VPN [View](#) [New](#)

Default Domain
aaamexrub.com



Syslog-Anbieter konfigurieren

2. Klicken Sie auf **Benutzerdefinierter Header**. Fügen Sie das Beispiel-Syslog ein, und suchen Sie mit einem Trennzeichen oder einer Registerkarte nach dem Hostnamen des Geräts. Wenn dies der Fall ist, wird der Hostname angezeigt. Klicken Sie auf **Speichern**

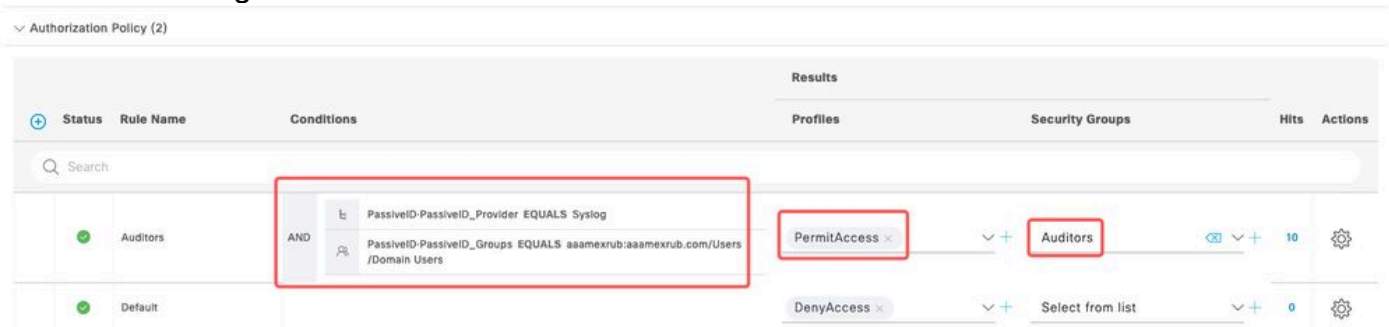


Benutzerdefinierten Header

konfigurieren

Schritt 4: Konfiguration der Authentifizierungsregeln

1. Navigieren Sie zu Policy > Policy Sets (Richtlinie > Richtlinienätze). In diesem Fall wird die Standardrichtlinie verwendet. Klicken Sie auf die **Standard**-Richtlinie. Fügen Sie in der **Autorisierungsrichtlinie** eine neue Regel hinzu. In den PassiveID-Richtlinien hat die ISE alle Anbieter. Sie können diese mit einer PassiveID-Gruppe kombinieren. Wählen Sie **Zugriffsberechtigung** als Profil aus, und wählen Sie in **Sicherheitsgruppen** die SGT-Anforderung aus.



Konfiguration der Authentifizierungsregeln

Überprüfung

Sobald die ISE das Syslog empfängt, können Sie die Radius Live Logs überprüfen, um den

Autorisierungsfluss anzuzeigen. Navigieren Sie zu **Operationen > Radius > Live-Protokolle**.

In den Protokollen wird das Authorization-Ereignis angezeigt. Dieser enthält den Benutzernamen, die Autorisierungsrichtlinie und das zugehörige Security Group Tag.

Time	Status	Details	Repea...	Identity	Endpoint ID	Authenticatio...	Authorization Policy	Authorization ...	Security ...	IP Address
Jan 31, ...	●		0	test	192.168.123.10	PassiveID provider	PassiveID provider >> Auditors	PermitAccess	Auditors	192.168.123.10
Jan 31, ...	●			test	192.168.123.10	PassiveID provider	PassiveID provider >> Auditors	PermitAccess		192.168.123.10

Radius-Live-Protokoll

Klicken Sie auf den **Detailbericht**, um weitere Details zu überprüfen. Hier sehen Sie den Nur-Autorisieren-Fluss, der die Richtlinien für die Zuweisung des SGT auswertet.

Overview

Event	5236 Authorize-Only succeeded
Username	test
Endpoint Id	192.168.123.10
Endpoint Profile	
Authentication Policy	PassiveID provider
Authorization Policy	PassiveID provider >> Auditors
Authorization Result	PermitAccess

Steps

- 15041 Evaluating Identity Policy
- 15013 Selected Identity Source - All_AD_Join_Points
- 24432 Looking up user in Active Directory - All_AD_Join_Points
- 24325 Resolving identity - test@aaamexrub.com
- 24313 Search for matching accounts at join point - aaamexrub.com
- 24319 Single matching account found in forest - aaamexrub.com
- 24323 Identity resolution detected single matching account
- 24355 LDAP fetch succeeded - aaamexrub.com
- 24416 User's Groups retrieval from Active Directory succeeded - All_AD_Join_Points
- 22037 Authentication Passed
- 90506 Running Authorize Only Flow for Passive ID - Provider Syslog
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15036 Evaluating Authorization Policy
- 90500 New Identity Mapping
- 5236 Authorize-Only succeeded

Authentication Details

Source Timestamp	2023-01-31 16:15:04.507
Received Timestamp	2023-01-31 16:15:04.507
Policy Server	asc-ise32-726
Event	5236 Authorize-Only succeeded
Username	test
Endpoint Id	192.168.123.10
Calling Station Id	192.168.123.10
IPv4 Address	192.168.123.10
Authorization Profile	PermitAccess

Radius Live-Protokollbericht

Fehlerbehebung

In diesem Fall werden zwei Flows verwendet: die passiveID-Sitzung und der Autorisierungsfluss. Um das Debugging zu aktivieren, navigieren Sie zu **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration**, und wählen Sie den ISE-Knoten aus.

Aktivieren Sie für die PassiveID die nächsten Komponenten auf der **DEBUG**-Ebene:

- PassiveID

Um die Protokolle anhand des Anbieters der passiven ID, der Datei, die für dieses Szenario geprüft werden soll, zu überprüfen, müssen Sie die **Datei** passiveid-syslog.log für die anderen

Anbieter überprüfen:

- passiveid-agent.log
- passiveid-api.log
- passiveid-endpoint.log
- passiveid-span.log
- Passiveid-Wmilog

Aktivieren Sie für den Autorisierungsablauf die nächsten Komponenten auf der **DEBUG**-Ebene:

- Policy-Engine
- Port-JNI

Beispiel:

Diagnostic Tools Download Logs **Debug Wizard**

Debug Profile Configuration
Debug Log Configuration

Node List > asc-ise32-726.aamexrub.com

Debug Level Configuration

[Edit](#) [Reset to Default](#)

Component Name	Log Level	Description	Log file Name
<input type="radio"/> PassiveID	DEBUG	PassiveID events and messages	passiveid-wmi.log
<input type="radio"/> policy-engine	DEBUG	Policy Engine 2.0 related messages	ise-psc.log
<input type="radio"/> prrt-JNI	DEBUG	prrt policy decision request processing layer related ...	prrt-management.log

Debugging aktiviert

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.