Konfigurieren von ISE 3.2 zum Zuweisen von Sicherheitsgruppen-Tags für PassiveID-Sitzungen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sicherheitsgruppen-Tags (SGTs) konfiguriert und passiven ID-Sitzungen über Autorisierungsrichtlinien in ISE 3.2 zugewiesen werden.

Voraussetzungen

Anforderungen

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

- Cisco ISE 3.2
- Passive ID, TrustSec und PxGrid

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ISE 3.2
- FMC 7.0.1
- WS-C3850-24P mit 16.12.1

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.

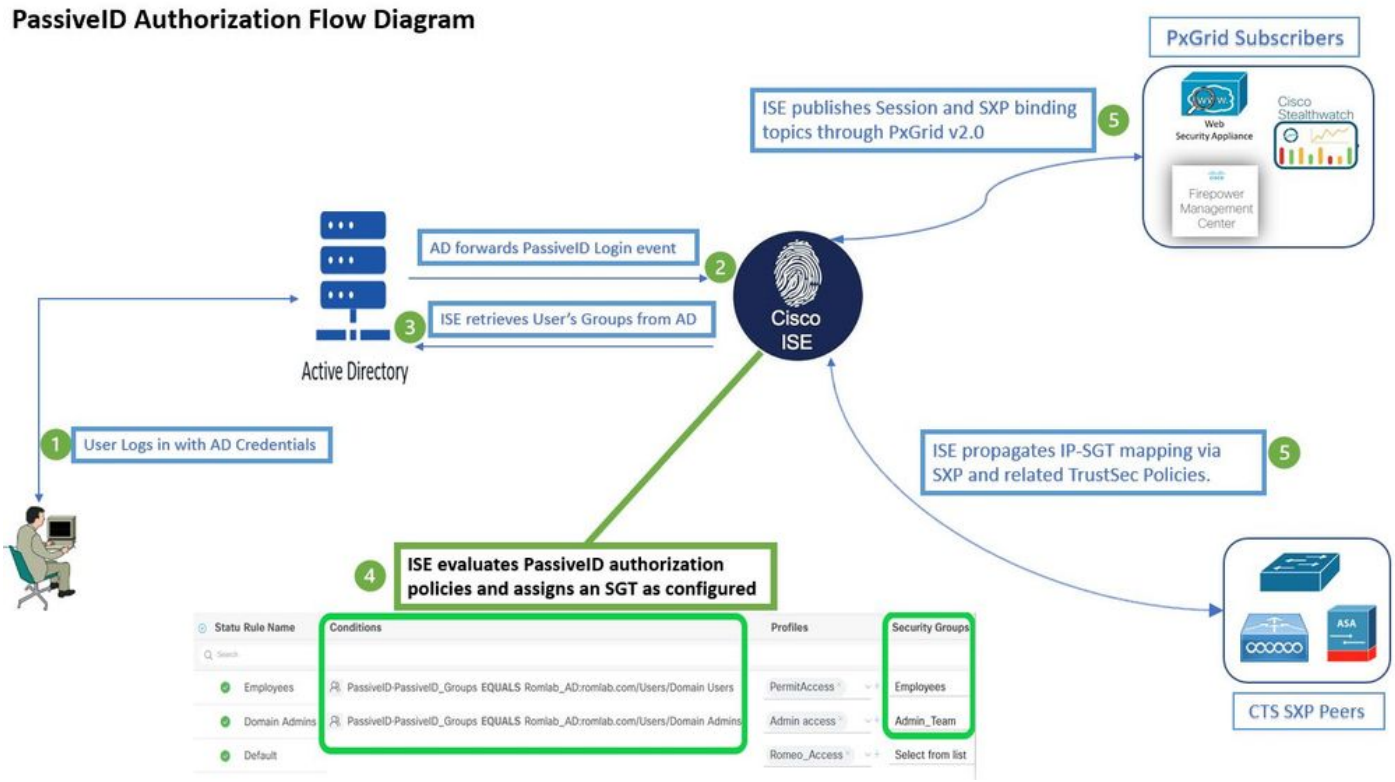
Hintergrundinformationen

Die Cisco Identity Services Engine (ISE) 3.2 ist die Mindestversion, die diese Funktion unterstützt. In diesem Dokument wird nicht auf die Konfiguration von PassiveID, PxGrid und SXP eingegangen. Weitere Informationen finden Sie im Administratorhandbuch.

In ISE 3.1 oder älteren Versionen kann ein Security Group Tag (SGT) nur einer Radius-Sitzung oder einer aktiven Authentifizierung (z. B. 802.1x und MAB) zugewiesen werden. Mit ISE 3.2 können Autorisierungsrichtlinien für PassiveID-Sitzungen konfiguriert werden. Wenn Identity Services Engine (ISE) Benutzeranmeldeereignisse von einem Anbieter wie Active Directory Domain Controllers (AD DC) WMI oder AD Agent empfängt, weist sie der PassiveID-Sitzung ein Security Group Tag (SGT) zu, das auf der Active Directory-Gruppenmitgliedschaft des Benutzers basiert. Die IP-SGT-Zuordnung und die AD-Gruppendetails für die PassiveID können über das SGT Exchange Protocol (SXP) und/oder an Abonnenten von Platform Exchange Grid (pxGrid) wie Cisco FirePOWER MANAGEMENT CENTER (FMC) und Cisco Secure Network Analytics (Stealthwatch) in der TrustSec-Domäne veröffentlicht werden.

Konfigurieren

Flussdiagramm

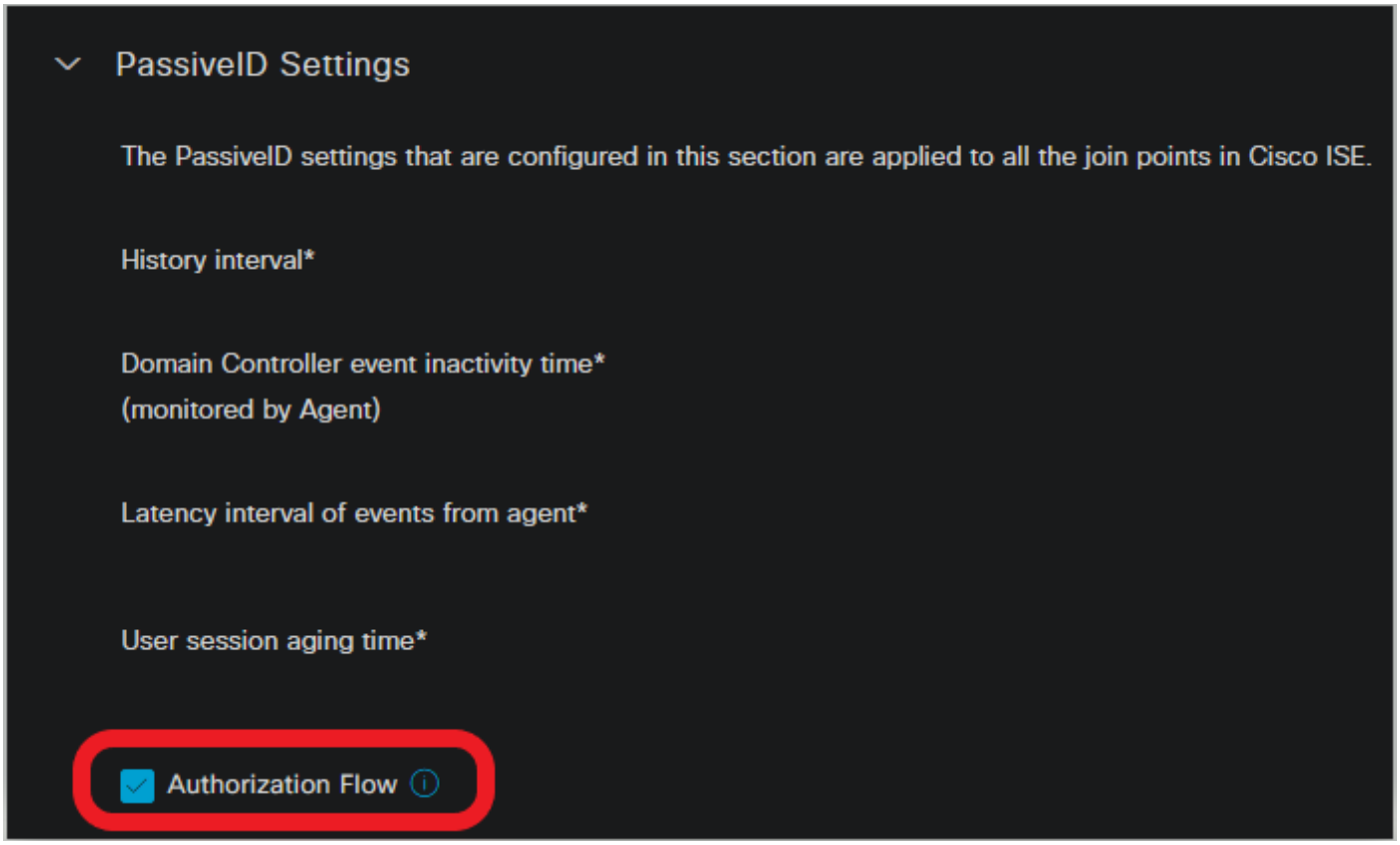


Flussdiagramm

Konfigurationen

Autorisierungsablauf aktivieren:

Navigieren Sie zu **Active Directory >Advanced Settings > PassiveID Settings** und überprüfen Sie **Authorization Flow** Kontrollkästchen, um Autorisierungsrichtlinien für Benutzer mit PassiveID-Anmeldung zu konfigurieren. Diese Option ist standardmäßig deaktiviert.

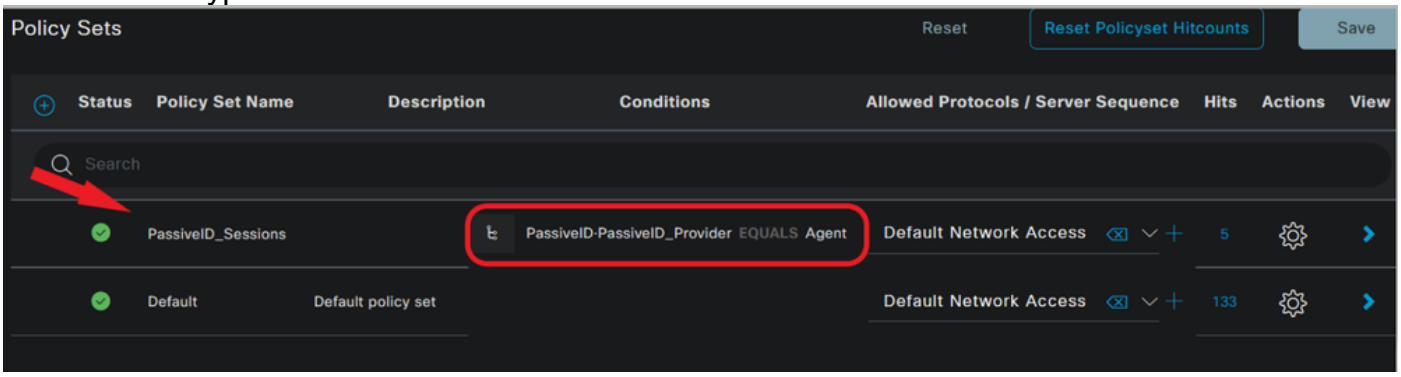


Freigabe des Autorisierungsflusses

> **Hinweis**: Damit diese Funktion funktioniert, stellen Sie sicher, dass Sie PassiveID-, PxGrid- und SXP-Dienste in Ihrer Bereitstellung ausführen. Sie können dies überprüfen unter **Administration > System > Deployment** .

Policy Set-Konfiguration:

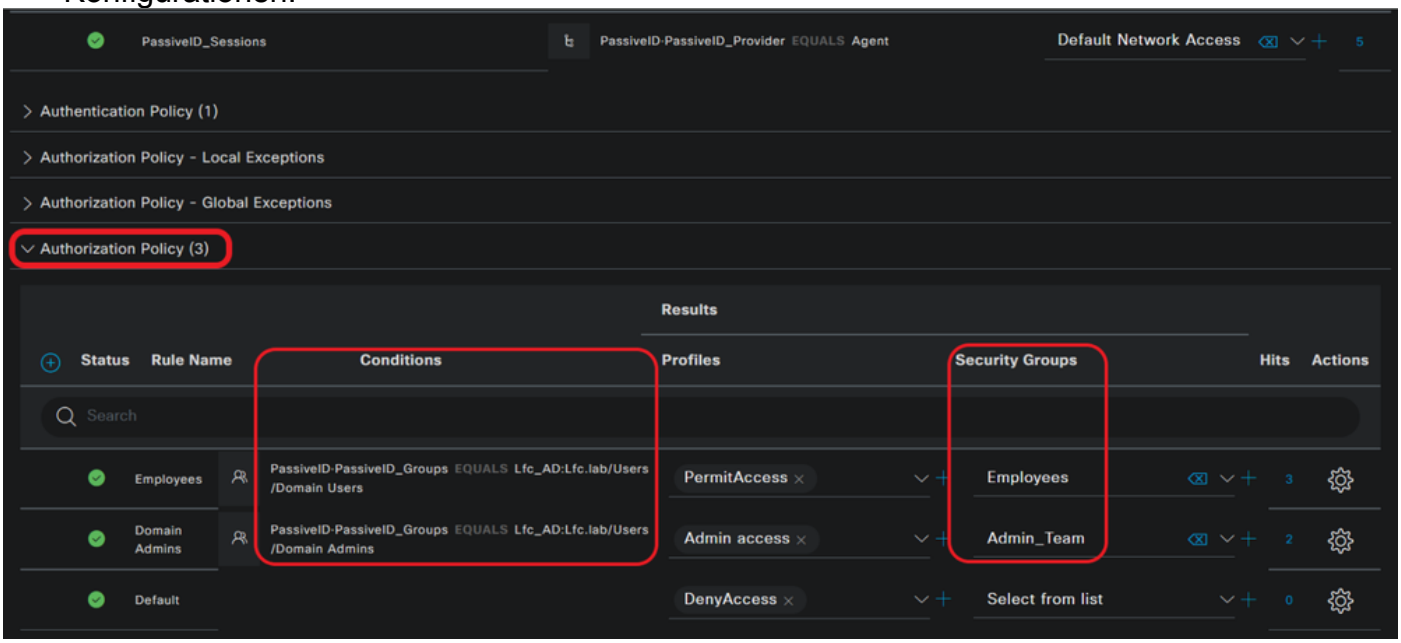
1. Erstellen Sie einen separaten Policy Set für PassiveID (empfohlen).
2. Verwenden Sie unter Bedingungen das Attribut **PassiveID·PassiveID_Provider** und wählen Sie den Anbietertyp aus.



Policy Sets

3. Autorisierungsregeln für den in Schritt 1 erstellten Richtliniensatz konfigurieren

- Erstellen Sie eine Bedingung für jede Regel, und verwenden Sie das Dictionary PassiveID auf der Grundlage von AD-Gruppen, Benutzernamen oder Beide.
- Weisen Sie jeder Regel eine Sicherheitsgruppen-Tag zu, und speichern Sie die Konfigurationen.

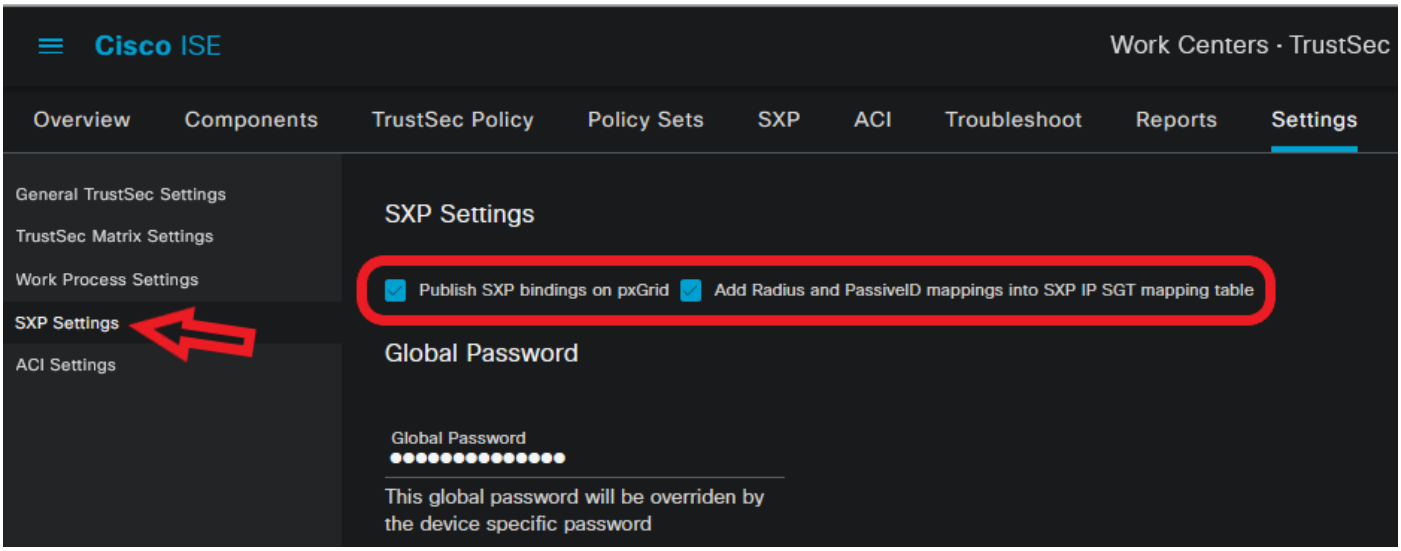


Autorisierungsrichtlinie

Hinweis: Die Authentifizierungsrichtlinie ist irrelevant, da sie in diesem Fluss nicht verwendet wird.

Hinweis: Sie können **PassiveID_Username, PassiveID_Groups**,Oder **PassiveID_Provider** -Attribute, um die Autorisierungsregeln zu erstellen.

4. Navigieren Sie zu **Work Centers > TrustSec > Settings > SXP Settings** aktivieren **Publish SXP bindings on pxGrid** und **Add RADIUS and PassiveID Mappings into SXP IP SGT Mapping Table** um PassiveID-Zuordnungen mit PxGrid-Abonnenten gemeinsam zu nutzen und sie in die SXP-Zuordnungstabelle auf der ISE aufzunehmen.



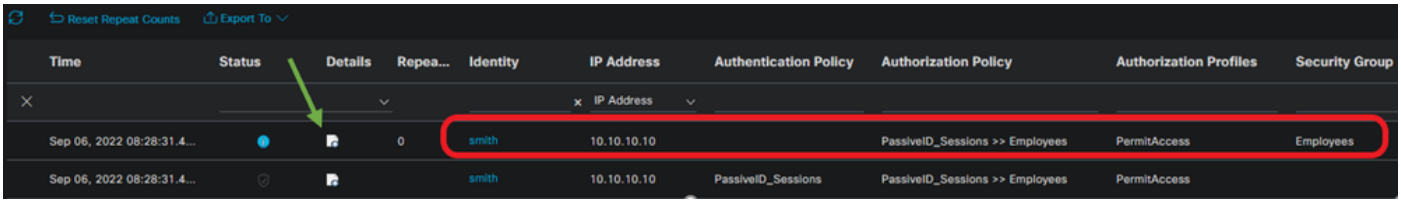
SXP-Einstellungen

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

ISE-Verifizierung

Sobald die Benutzeranmeldeereignisse von einem Anbieter wie Active Directory Domain Controllers (AD DC) WMI oder AD Agent an die ISE gesendet wurden, fahren Sie mit der Überprüfung der Live-Protokolle fort. Navigieren Sie zu **Operations > Radius > Live Logs**.



Radius-LiveProtokolle

Klicken Sie in der Spalte Details auf das Lupensymbol, um einen detaillierten Bericht für einen Benutzer anzuzeigen, in diesem Beispiel Smith (Domain Users), wie hier gezeigt.

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.