Configurare il flusso di autorizzazione per le sessioni ID passive in ISE 3.2

Sommario

Introduzione

In questo documento viene descritto come configurare le regole di autorizzazione per gli eventi di ID passivo per assegnare i servizi SGT alle sessioni.

Premesse

I servizi di identità passiva (ID passivo) non autenticano direttamente gli utenti, ma raccolgono le identità e gli indirizzi IP degli utenti dai server di autenticazione esterni, ad esempio Active Directory (AD), noti come provider, e quindi condividono tali informazioni con i sottoscrittori.

ISE 3.2 introduce una nuova funzionalità che consente di configurare un criterio di autorizzazione per assegnare un tag del gruppo di sicurezza (SGT) a un utente in base all'appartenenza al gruppo Active Directory.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco ISE 3.X
- Integrazione passiva di ID con qualsiasi provider
- Amministrazione di Active Directory (AD)
- Segmentazione (Trustsec)
- PxGrid (griglia di scambio piattaforma)

Componenti usati

- Software Identity Service Engine (ISE) versione 3.2
- Microsoft Active Directory

- Syslog

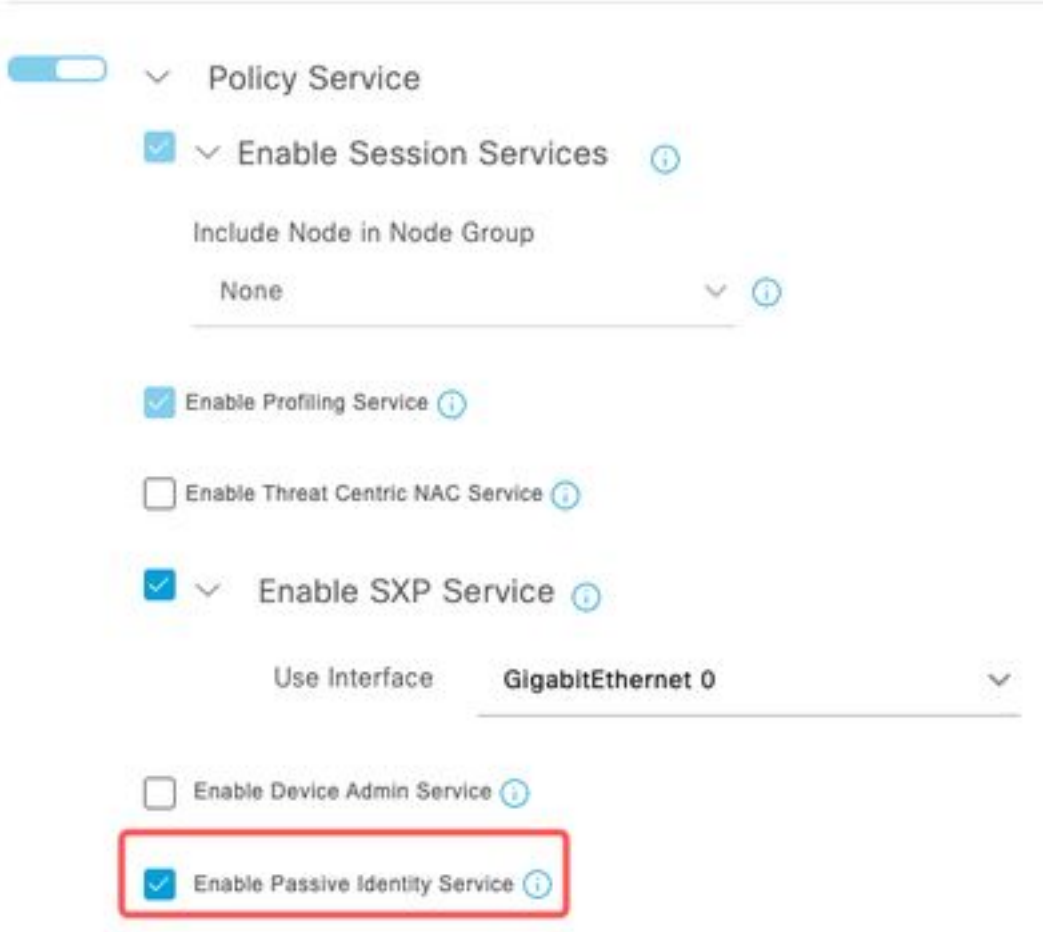
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Passaggio 1. Abilitare i servizi ISE.

1. Su ISE, selezionare Amministrazione > **Distribuzione**, scegliere il nodo ISE e fare clic su **Modifica**, abilita **Policy Service** e scegliere **Abilita Passive Identity Service**. Facoltativamente, è possibile abilitare SXP e PxGrid se le sessioni di ID passivo devono essere pubblicate tramite ognuna di esse. Fare clic su **Salva**.

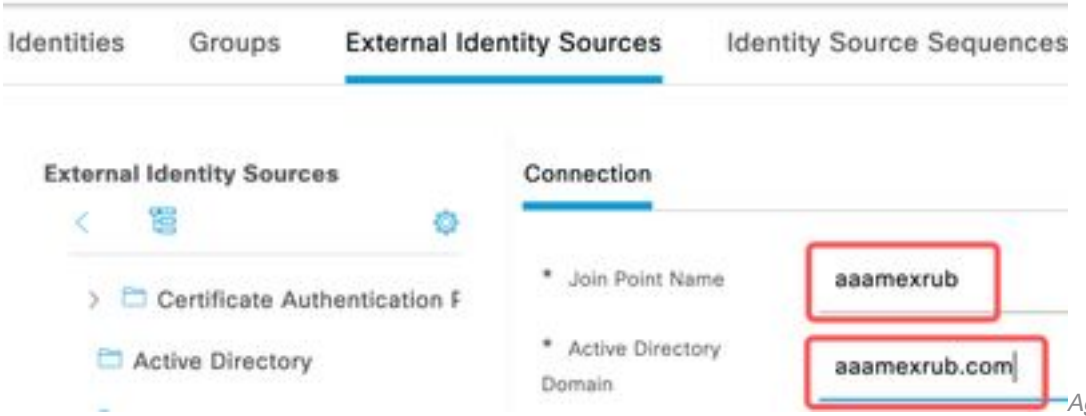
   Avviso: impossibile pubblicare in SXP i dettagli SGT degli utenti di accesso con ID passivo autenticati dal provider API. Tuttavia, i dettagli SGT di questi utenti possono essere pubblicati attraverso pxGrid e pxGrid Cloud.



Servizi attivati

Passaggio 2. Configurare Active Directory.

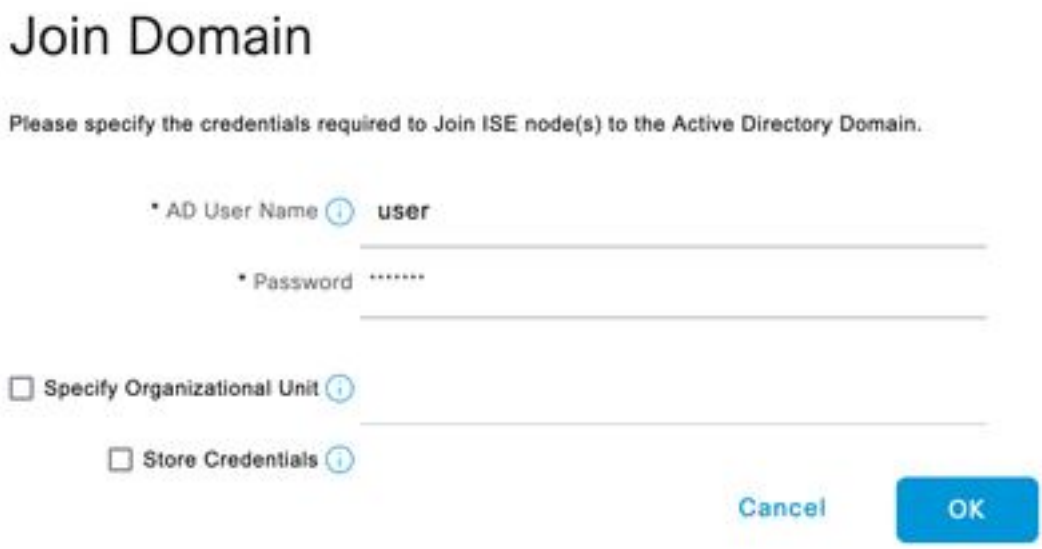
1. Passare a Amministrazione > **Gestione identità** > **Origini identità esterne** e scegliere **Active Directory,** quindi fare clic sul **pulsante Aggiungi**.
2. Immettere il **nome** del **punto di join** e il **dominio di Active Directory**. Fare clic su **Invia**.



Aggiungi Active Directory

3. Viene visualizzata una schermata di popup per unire ISE ad AD. Fare clic su **Sì**. Immettere il **nome utente** e la **password**. Fare clic su OK.

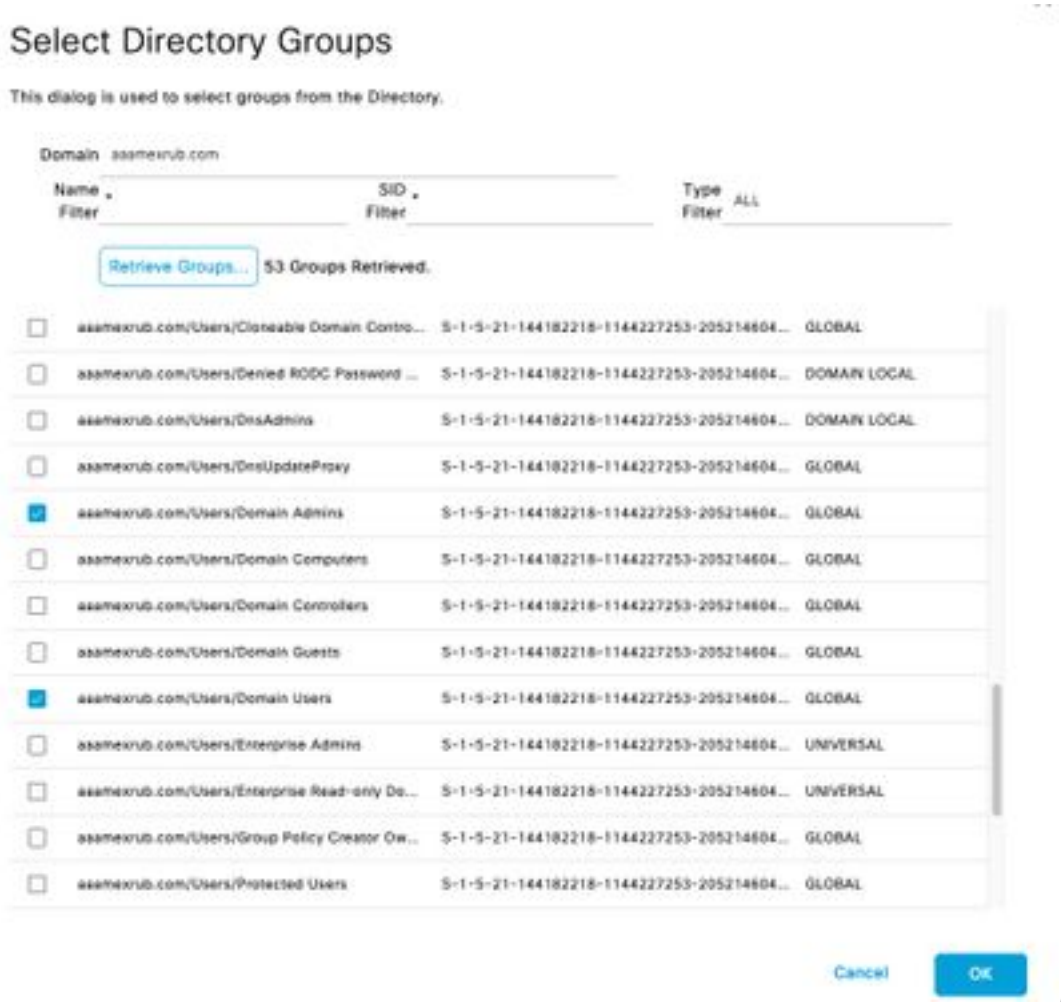
Partecipate anche voi ad



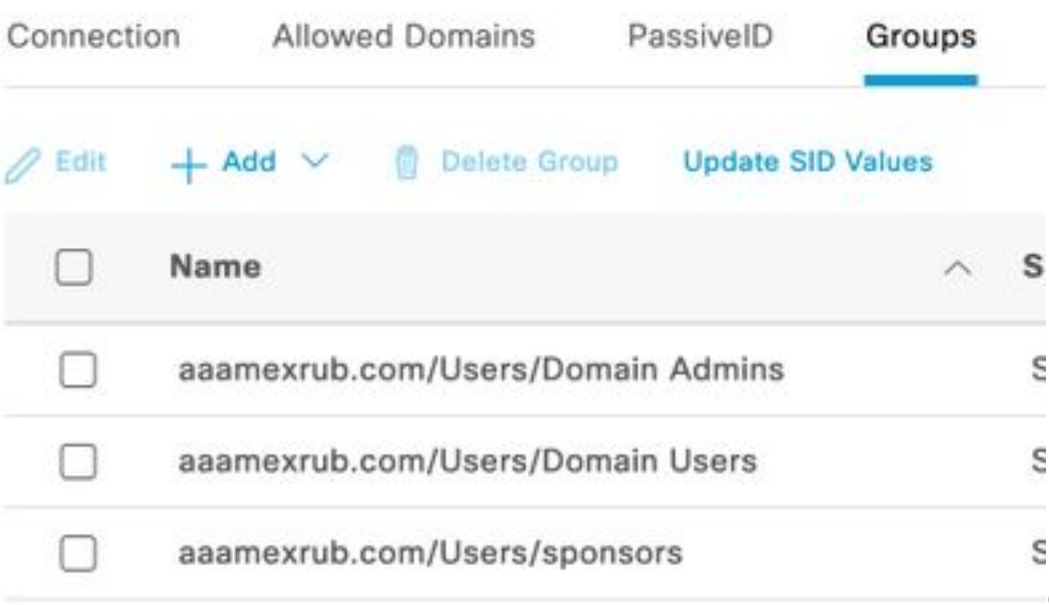
ISE

Aggiungi ad Active Directory

4. Recuperare i gruppi AD. Passare a **Gruppi**, fare clic su **Aggiungi**, quindi su **Recupera gruppi** e scegliere tutti i gruppi interessati, quindi fare clic su **OK**.

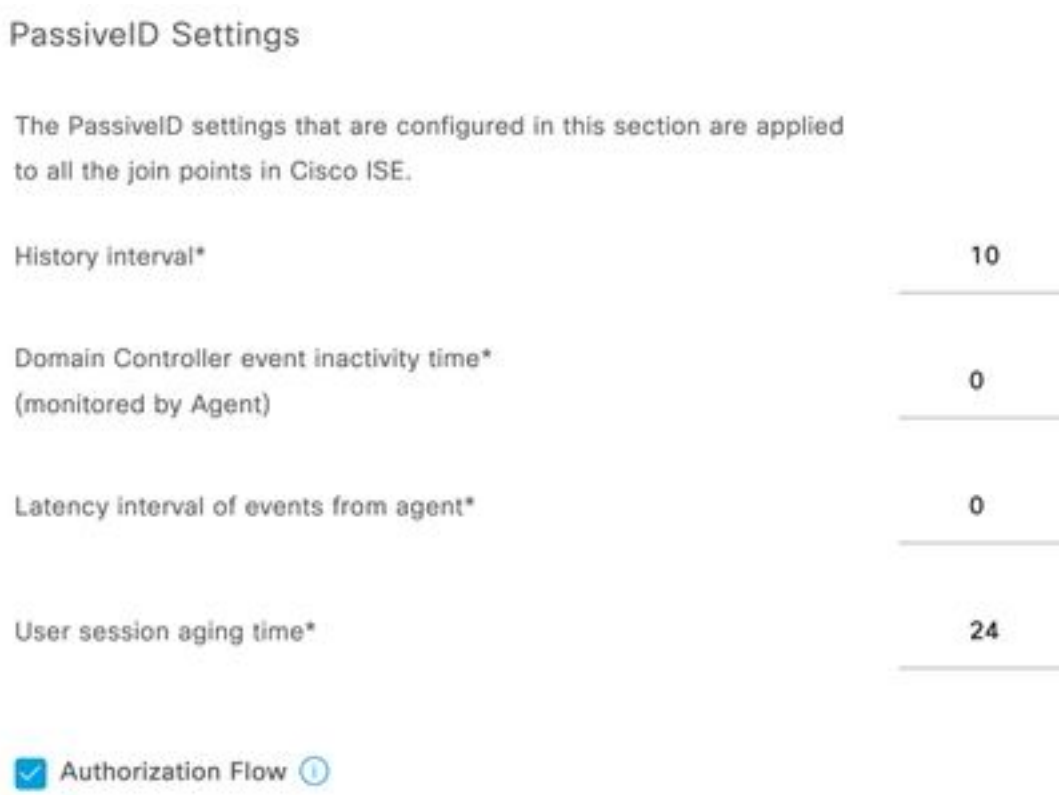


Recupera gruppi AD



Gruppi recuperati

5. Abilitare il flusso di autorizzazione. Passare a **Impostazioni avanzate** e nella sezione **Impostazioni ID passivo** selezionare la casella di controllo **Flusso di autorizzazione**. Fare clic su **Salva**.

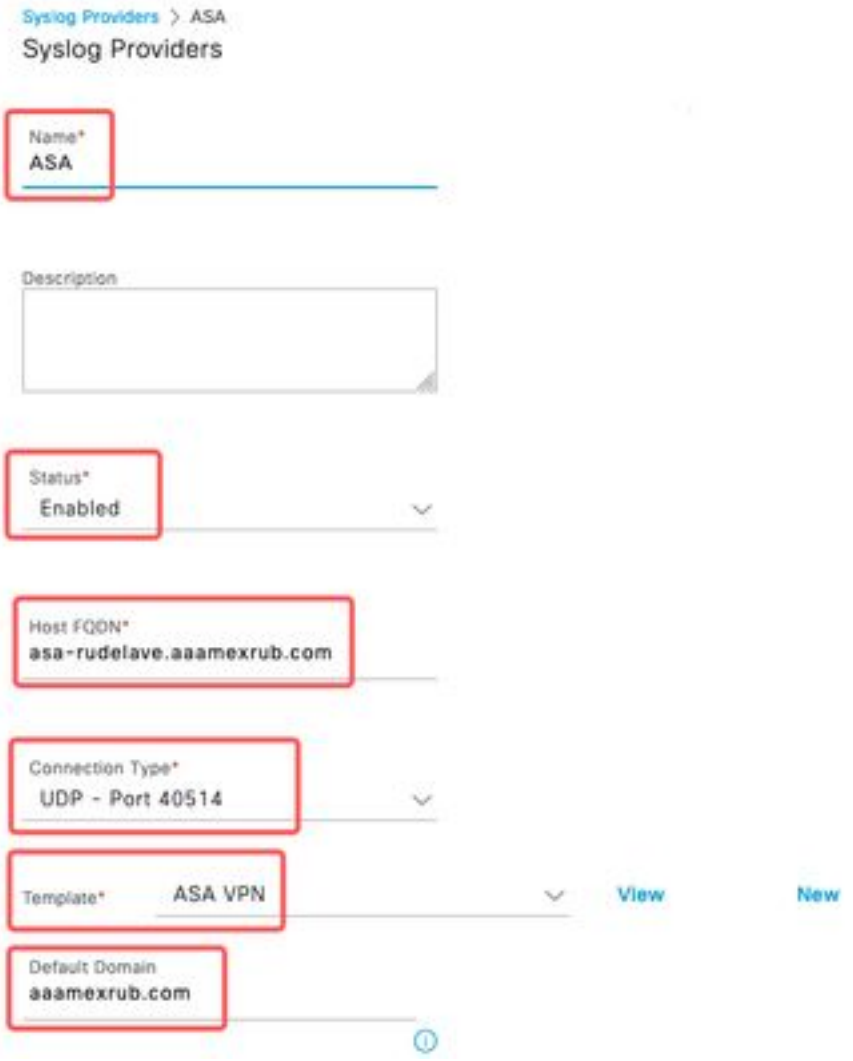


Abilita flusso di autorizzazione

Passaggio 3. Configurare il provider Syslog.

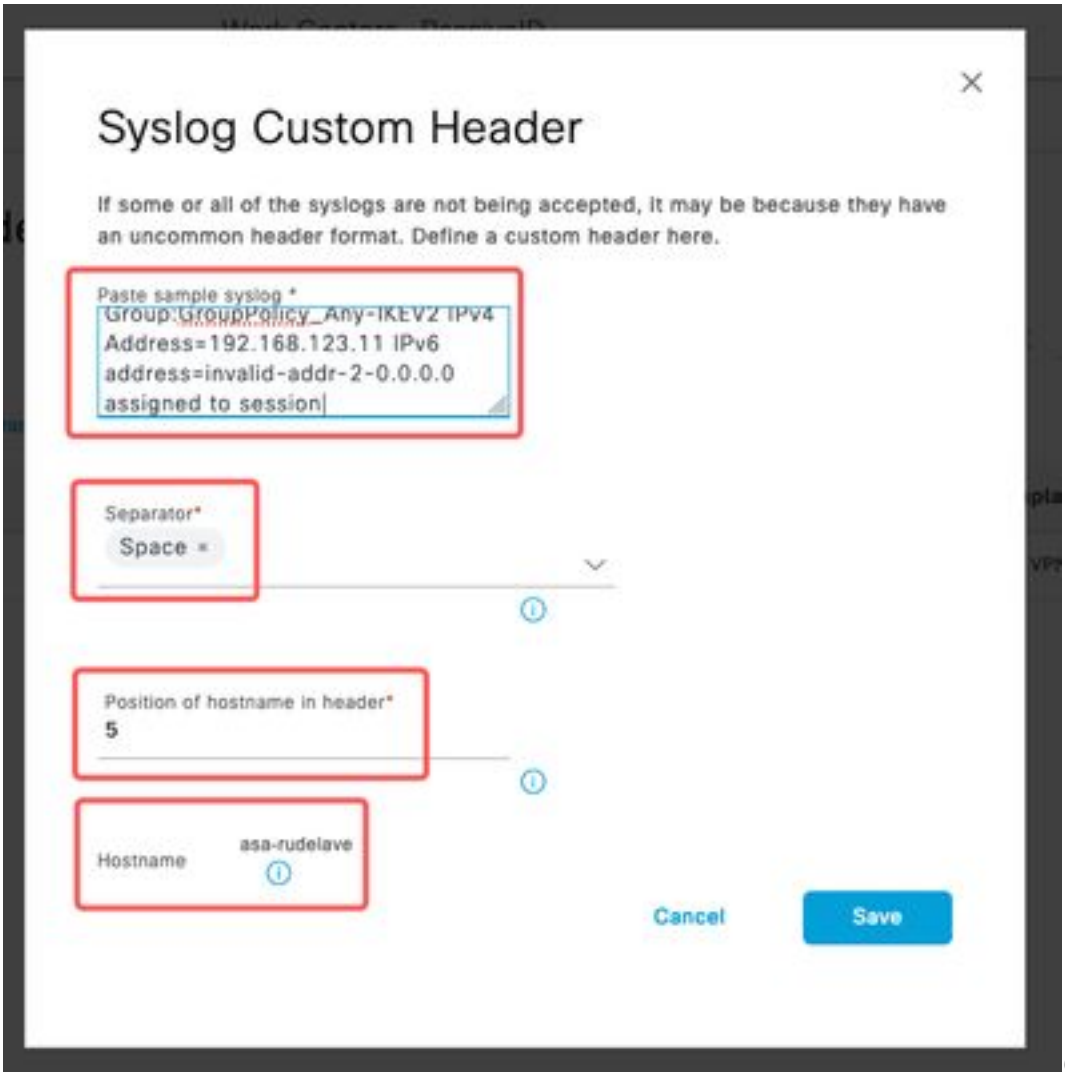
1. Passare a Centri di lavoro **> ID passivo > Provider**, scegliere **Provider di syslog**, fare clic su **Aggiungi** e completare le informazioni. Fare clic su Salva.

   Attenzione: in questo caso, ISE riceve il messaggio syslog da una connessione VPN riuscita in un'appliance ASA, ma questo documento non descrive la configurazione.



Configura provider Syslog

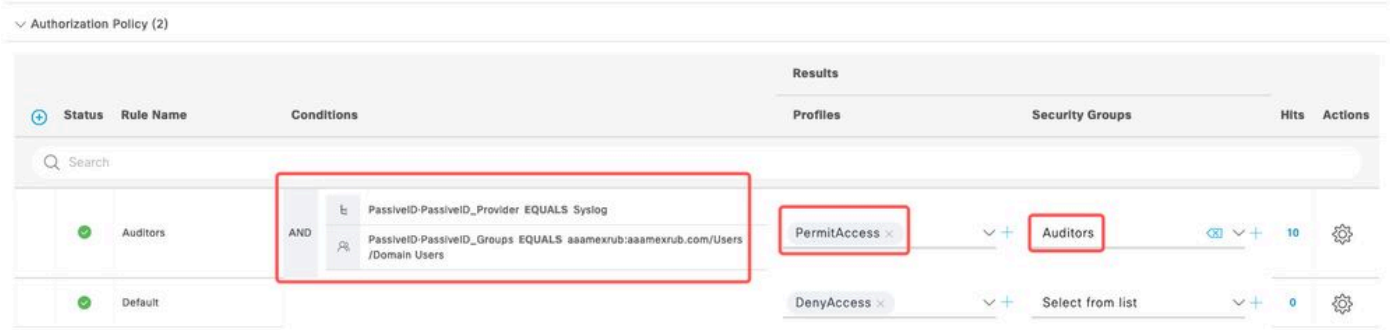
2. Fare clic su **Intestazione personalizzata**. Incollare il syslog di esempio e utilizzare un separatore o una tabulazione per trovare il nome host del dispositivo. Se è corretto, viene visualizzato il nome host. Fare clic su Salva.



Configura intestazione personalizzata

Passaggio 4. Configurazione delle regole di autorizzazione

1. Passare a **Criterio > Set di criteri.** In questo caso, viene utilizzato il criterio Predefinito. Fare clic sul criterio **Predefinito**. Nel **criterio di autorizzazione** aggiungere una nuova regola. Nelle policy PassiveID, ISE ha tutti i provider. È possibile combinare questo gruppo con un gruppo PassiveID. Scegliere **Permit Access** as Profile (Consenti accesso come profilo) e in **Security Groups (Gruppi di sicurezza)** scegliere il tipo di servizio desiderato.



Configurazione delle regole di autorizzazione

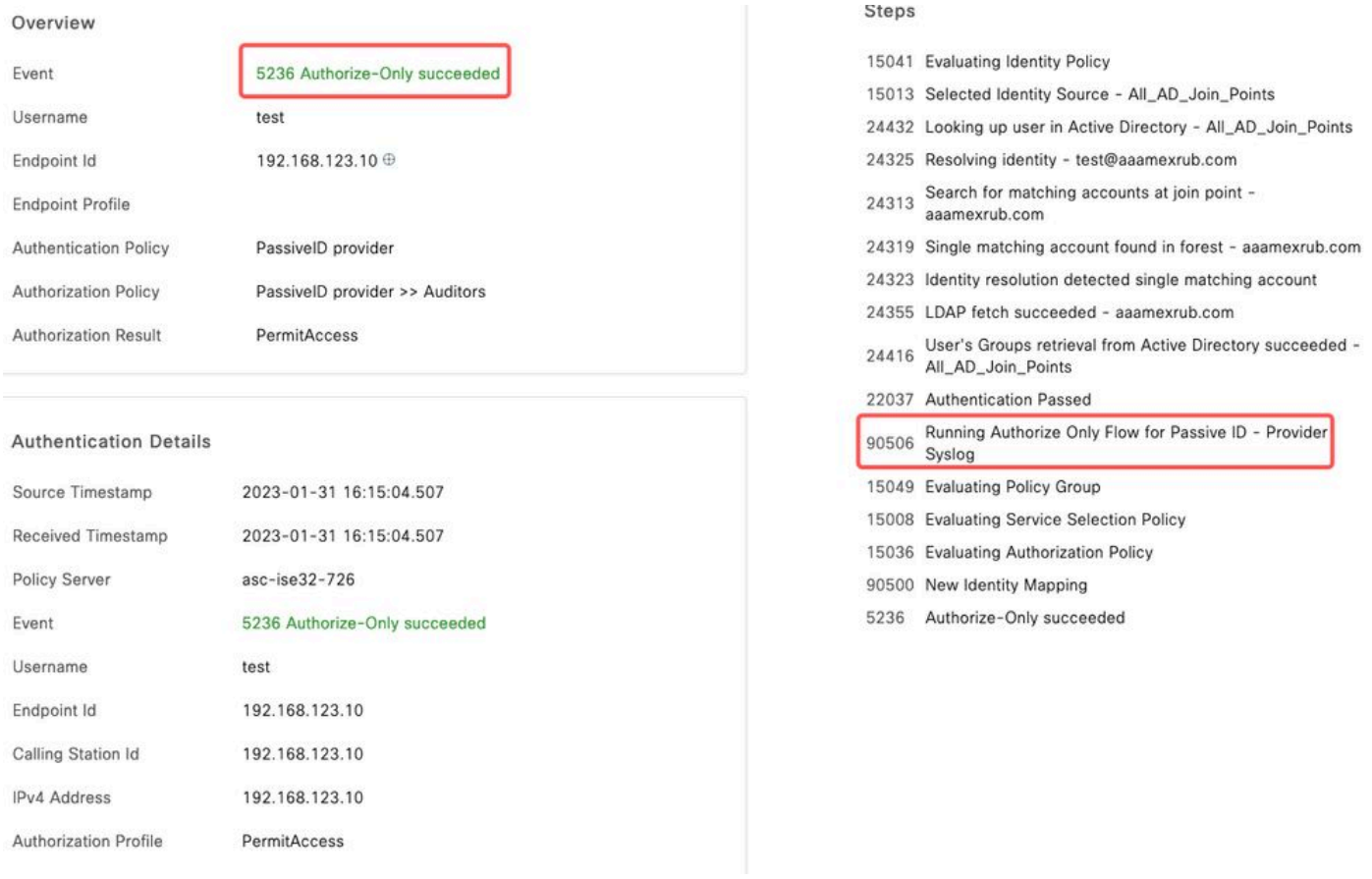
Verifica

Una volta che ISE ha ricevuto il syslog, è possibile controllare i log di Radius Live per verificare il flusso di autorizzazione. Passare a **Operazioni > Raggio > Log attivi**.

Nei registri è possibile visualizzare l'evento Authorization. Questo contiene il nome utente, il criterio di autorizzazione e il tag del gruppo di sicurezza associati.

Registro Radius Live

Per controllare ulteriori dettagli, fare clic sul **report dettagliato**. Qui è possibile vedere il flusso di sola autorizzazione che valuta i criteri per assegnare il SGT.



Report registro Radius Live

Risoluzione dei problemi

In questo caso, vengono utilizzati due flussi, ovvero le sessioni passiveID e il flusso di autorizzazione. Per abilitare i debug, selezionare **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration,** quindi scegliere il nodo ISE.

Per l'ID passivo, abilitare i componenti successivi al livello **DEBUG**:

- ID passivo

Per controllare i registri, in base al provider di ID passivo, il file da controllare per questo scenario, è necessario rivedere il **file** passiveid-syslog.log per gli altri provider:

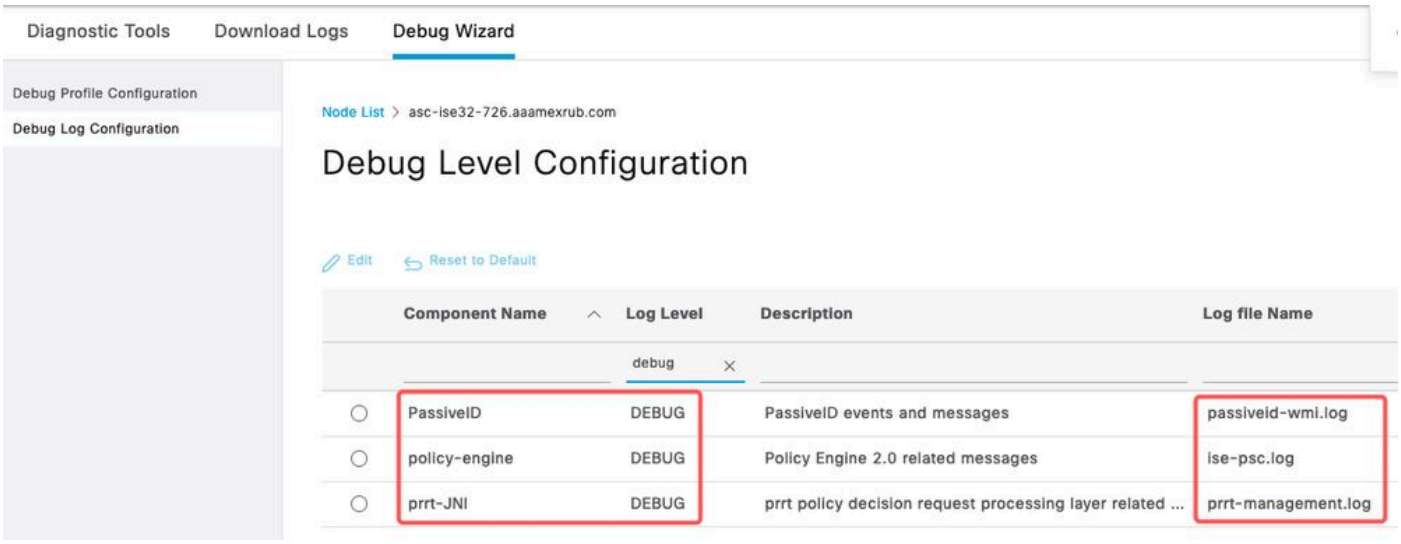
- passiveid-agent.log

- passiveid-api.log
- passiveid-endpoint.log
- passiveid-span.log
- passiveid-wmilog

Per il flusso di autorizzazione, abilitare i componenti successivi al livello **DEBUG**:

- motore delle regole
- prrt-JNI

Esempio:



Debug abilitati

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).