Autenticazione esterna AsyncOS con Cisco Identity Service Engine (Radius)

Sommario

Introduzione

In questo documento viene descritta la configurazione richiesta tra Email Security Appliance (ESA) / Security Management Appliance (SMA) e Cisco Identity Services Engine (ISE) per la corretta implementazione dell'autenticazione esterna con RADIUS.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Autenticazione, autorizzazione e accounting (AAA)
- Attributo RADIUS CLASS.
- Cisco ISE Identity Management and Authorization Policies.
- Ruoli utente Cisco ESA/SMA.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE 2.4
- Cisco ESA 13.5.1, 13.7.0

- Cisco SMA 13.6.2

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.

Prodotti correlati

La versione non compresa tra quelle elencate nella sezione Componenti usati non è stata testata.

Premesse

Attributo Radius CLASS

Utilizzato per l'accounting, è un valore arbitrario che il server RADIUS include in tutti i pacchetti di accounting.

L'attributo class viene configurato in ISE (RADIUS) per ogni gruppo.

Quando un utente viene considerato parte del gruppo ISE/VPN a cui è associato l'attributo 25, il NAC applica la policy in base alle regole di mappatura configurate nel server Identity Services Engine (ISE).

Configurazione

Esempio di rete

Identity Service Engine accetta le richieste di autenticazione da ESA/SMA e le confronta con l'identità e il gruppo di un utente.

Passaggio 1. Creare un gruppo di identità per l'autenticazione.

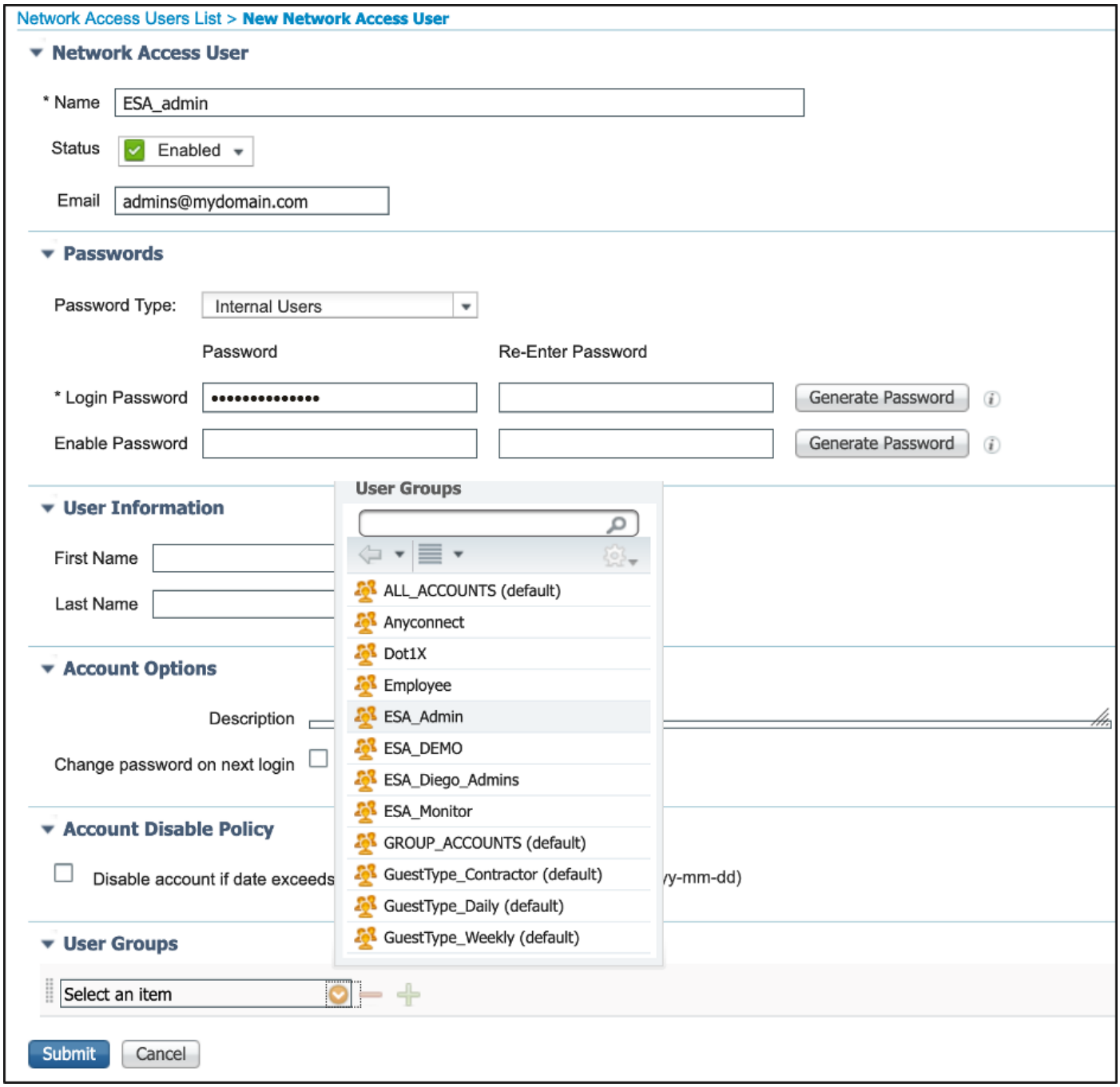
Accedere al server ISE e creare un gruppo di identità:

Passare a Amministrazione->Gestione identità->Gruppi->Gruppo identità utente. Come mostrato nell'immagine.

Nota: Cisco consiglia un Identity Group in ISE per ciascun ruolo ESA/SMA assegnato.

Passaggio 2. Creare utenti locali per l'autenticazione.

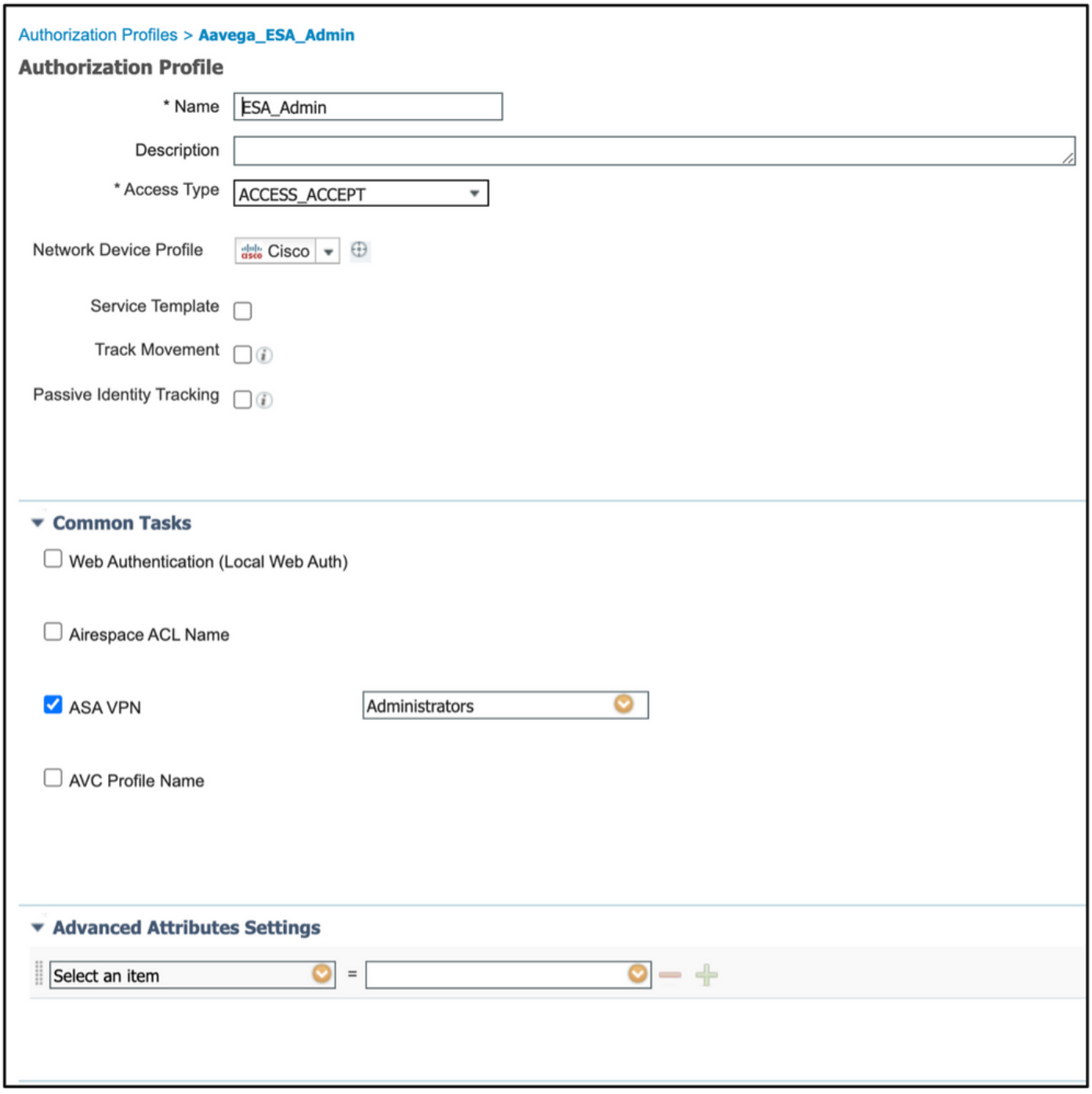
In questo passo, creare nuovi utenti o assegnare utenti già esistenti al gruppo di identità creato nel passo 1. Accedere ad ISE e **selezionare Amministrazione->Gestione delle identità->Identità** e creare nuovi utenti o assegnarli agli utenti nei gruppi creati. Come mostrato nell'immagine.



Passaggio 3. Creazione dei profili di autorizzazione.

L'autenticazione RADIUS può essere completata senza profili di autorizzazione, tuttavia non è possibile assegnare ruoli. Per completare l'installazione, **passare a Criterio->Elementi criteri->Risultati->Autorizzazione->Profilo di autorizzazione.**

Nota: Creare un profilo di autorizzazione per ruolo da assegnare.



Nota: Assicurarsi di utilizzare l'attributo 25 della classe radius e assegnare un nome. Questo nome deve corrispondere alla configurazione su AsyncOS (ESA/SMA). Nella Figura 3 Amministratori è riportato il nome dell'attributo CLASS.

Passaggio 4. Creare un criterio di autorizzazione.

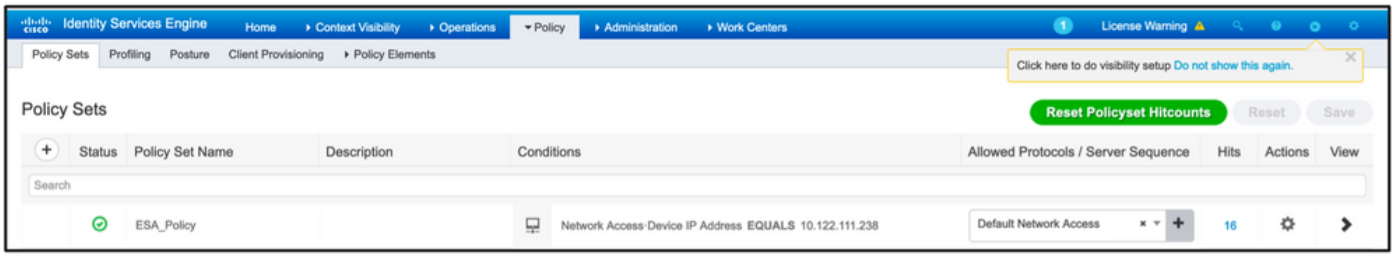
Quest'ultimo passaggio consente al server ISE di identificare gli utenti che tentano di effettuare

l'accesso e di mappare il proprio profilo di autorizzazione.

Se l'autorizzazione ha esito positivo, ISE restituisce un valore access-accept insieme al valore CLASS definito nel profilo di autorizzazione.

Passare a Criterio > Set di criteri > Aggiungi (+ simbolo)

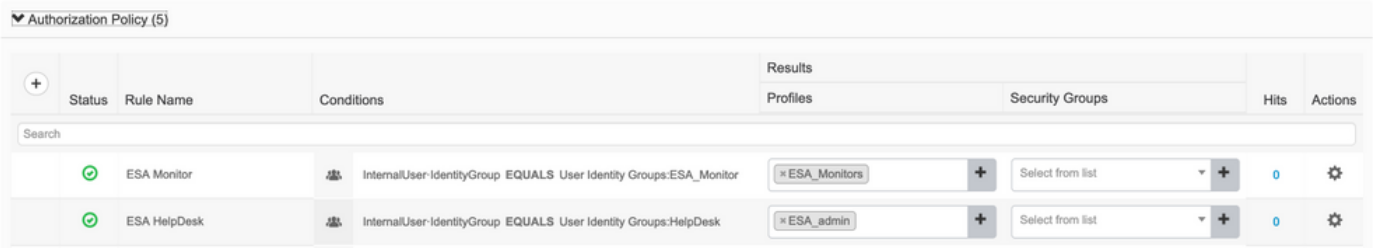
Assegnate un nome e selezionate il simbolo più per aggiungere le condizioni richieste. Questo ambiente lab utilizza un raggio. Indirizzo IP-NAS. Salvare il nuovo criterio.



Per soddisfare correttamente le richieste di autorizzazione, è necessario aggiungere le condizioni.

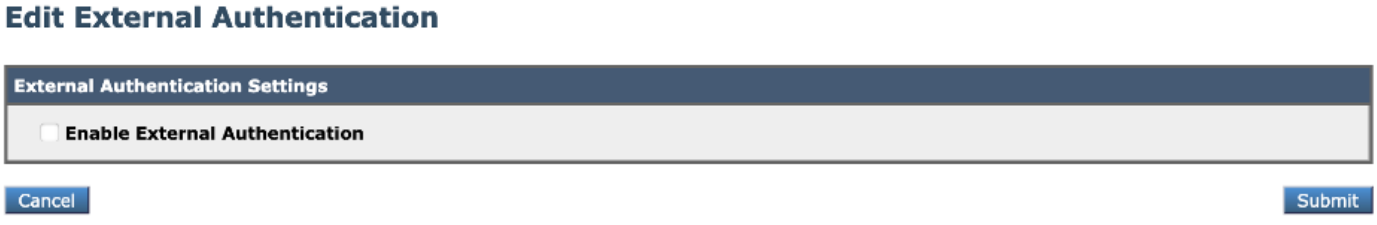
Seleziona e aggiungere condizioni.

L'ambiente lab utilizza InternalUser-IdentityGroup e corrisponde a ciascun profilo di autorizzazione.



Passaggio 5. Abilitare l'autenticazione esterna in AsyncOS ESA/SMA.

Collegarsi all'appliance AsyncOS (ESA/SMA/WSA). E **passare ad Amministrazione di sistema > Utenti > Autenticazione esterna > Abilita autenticazione esterna** su ESA.

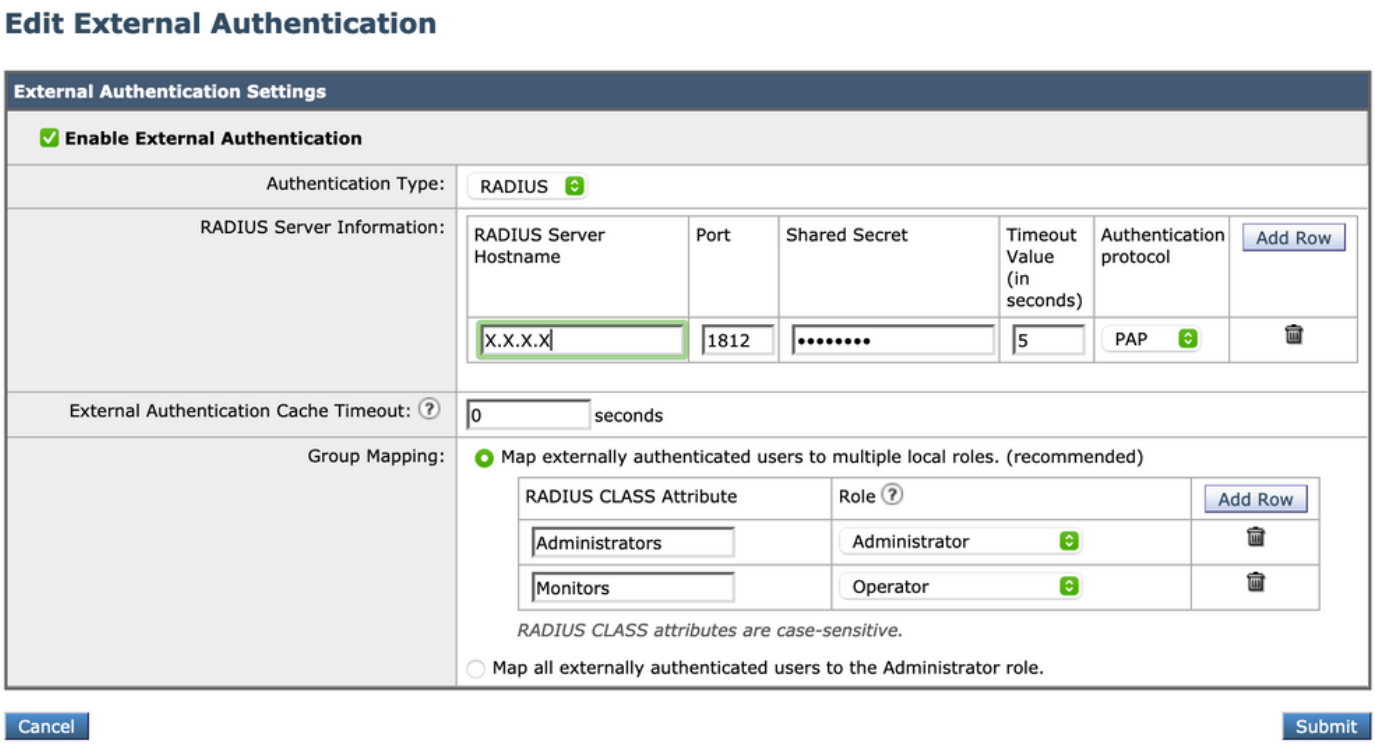


Fornire i seguenti valori:

- Nome host server RADIUS
- Port
- Segreto condiviso

- Valore timeout (in secondi)
- Protocollo di autenticazione

Selezionare **Esegui mapping degli utenti autenticati esternamente a più ruoli locali (scelta consigliata)**. Come mostrato nell'immagine.

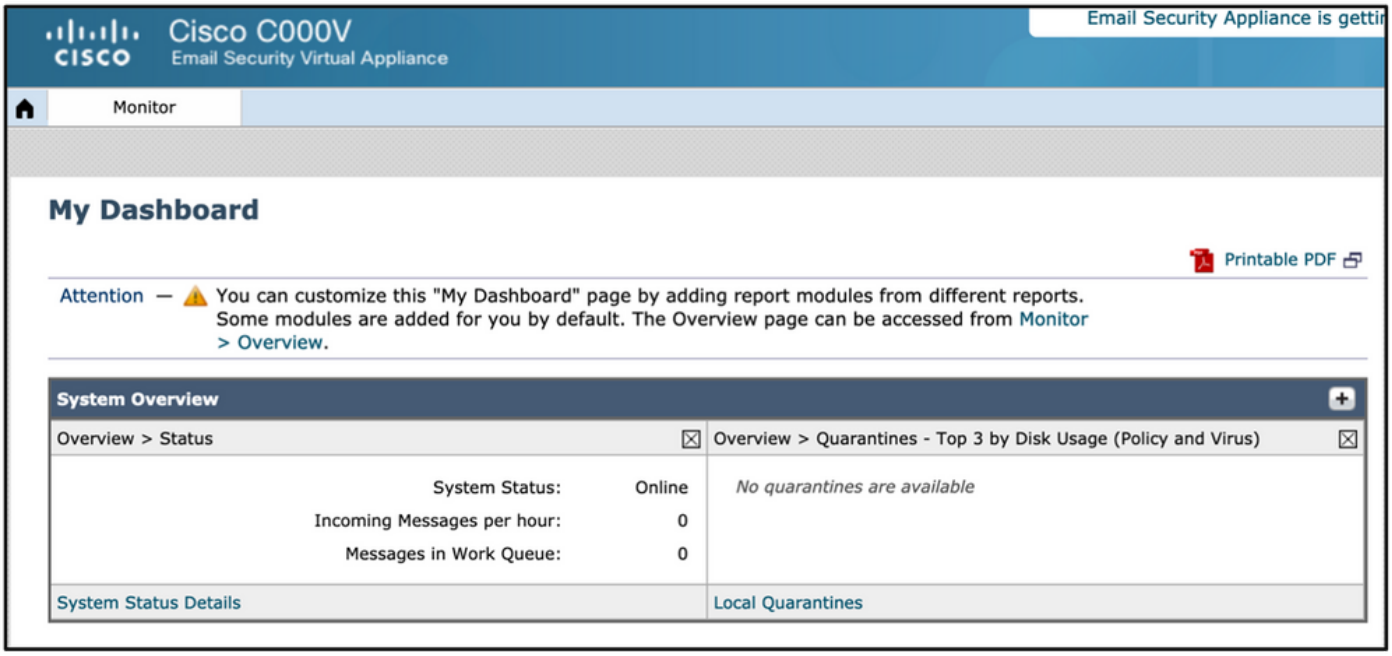


Nota: L'attributo RADIUS CLASS DEVE corrispondere all'attributo Name definito nel passo 3 (per le attività comuni mappate come VPN ASA).

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Accedere all'accessorio AsyncOS e verificare che l'accesso sia stato concesso e che il ruolo assegnato sia stato assegnato correttamente. Come mostrato nell'immagine con il ruolo utente guest.

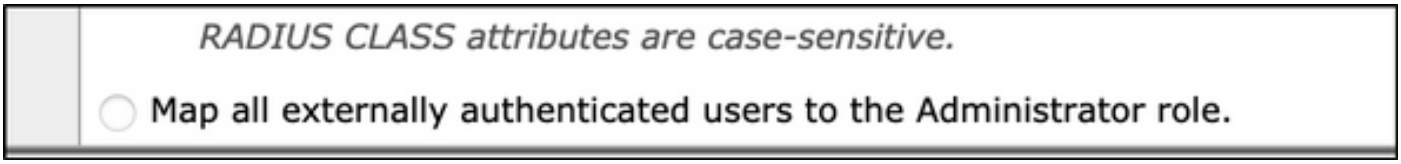


Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Se il tentativo di login non riesce a funzionare su ESA con il messaggio "Nome utente o password non valida". Il problema potrebbe essere relativo ai criteri di autorizzazione.

Accedere a ESA e da Autenticazione esterna selezionare Mapping di tutti gli utenti autenticati esternamente al ruolo Administrator.



Inviare e confermare le modifiche. Eseguire un nuovo tentativo di accesso. Se l'accesso ha esito positivo, verificare due volte il profilo di autorizzazione ISE Radius (attributo CLASS 25) e l'impostazione dei criteri di autorizzazione.

Informazioni correlate

- **Guida per l'utente di ISE 2.4**
- **Guida per l'utente di AsyncOS**