Autenticación externa AsyncOS con Cisco Identity Service Engine (Radius)

Contenido

Introducción

Este documento describe la configuración requerida entre el dispositivo de seguridad Email Security Appliance (ESA) / Security Management Appliance (SMA) y Cisco Identity Services Engine (ISE) para una implementación exitosa de la autenticación externa con RADIUS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Autenticación, autorización y administración (AAA)
- Atributo RADIUS CLASS.
- Políticas de autorización y gestión de identidades de Cisco ISE.
- Funciones de usuario de Cisco ESA/SMA.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ISE 2.4
- Cisco ESA 13.5.1, 13.7.0

- Cisco SMA 13.6.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

No se probó la versión fuera de las enumeradas en la sección de componentes utilizados.

Antecedentes

Atributo Radius CLASS

Utilizado para la contabilidad, es un valor arbitrario que el servidor RADIUS incluye en todos los paquetes de contabilización.

El atributo class se configura en ISE (RADIUS) por grupo.

Cuando se considera que un usuario forma parte del grupo ISE/VPN que tiene el atributo 25 vinculado a él, el NAC aplica la política basándose en las reglas de asignación configuradas en el servidor de Identity Services Engine (ISE).

Configurar

Diagrama de la red

Identity Service Engine acepta las solicitudes de autenticación de ESA/SMA y las compara con una identidad de usuario y un grupo.

Paso 1. Cree un grupo de identidad para la autenticación.

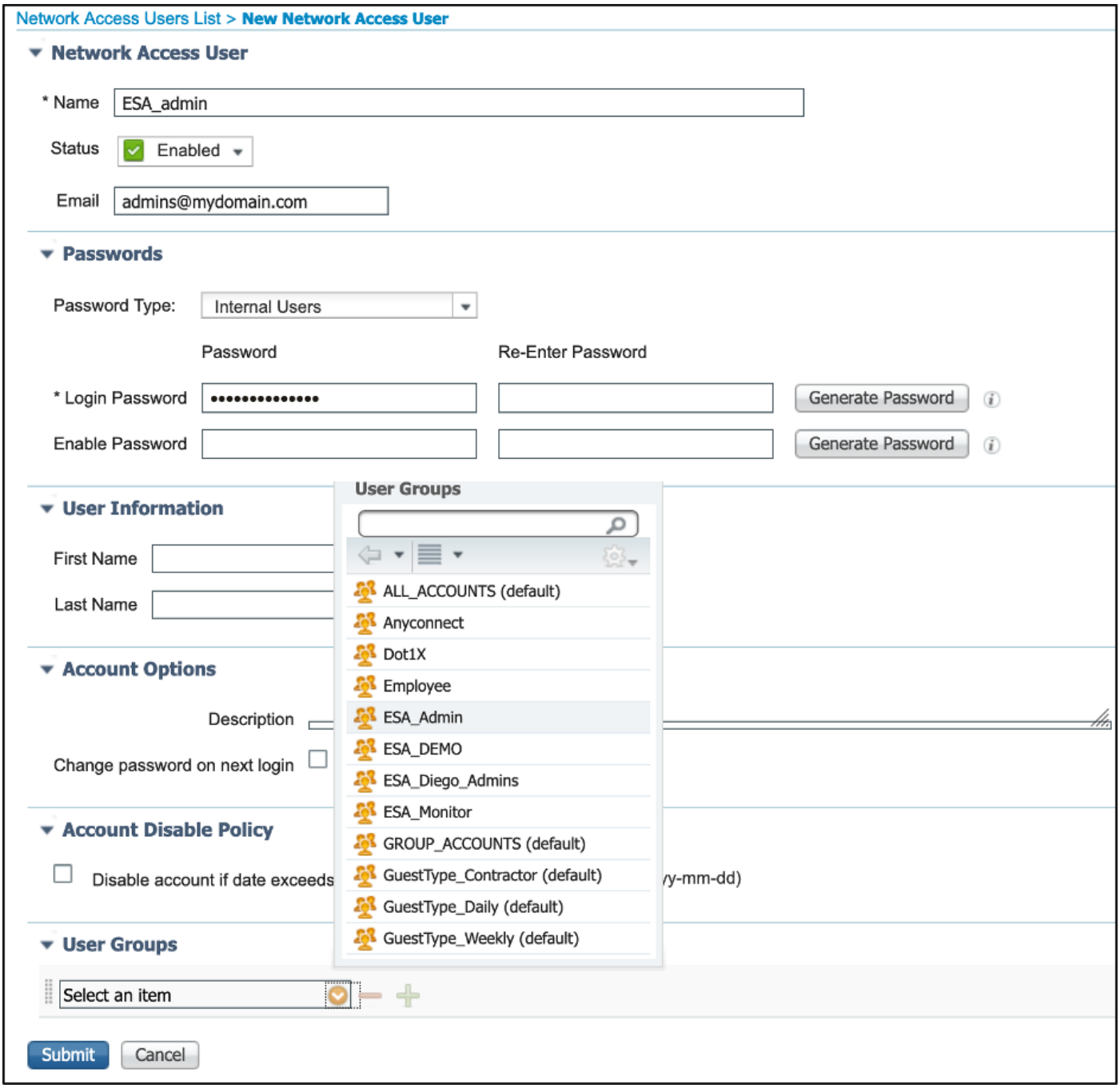
Inicie sesión en el servidor ISE y Crear un grupo de identidades:

Vaya a Administration->Identity Management->Groups->User Identity Group. Como se muestra en la imagen.

Nota: Cisco recomienda un grupo de identidad en ISE para cada función ESA/SMA asignada.

Paso 2. Crear usuarios locales para autenticación.

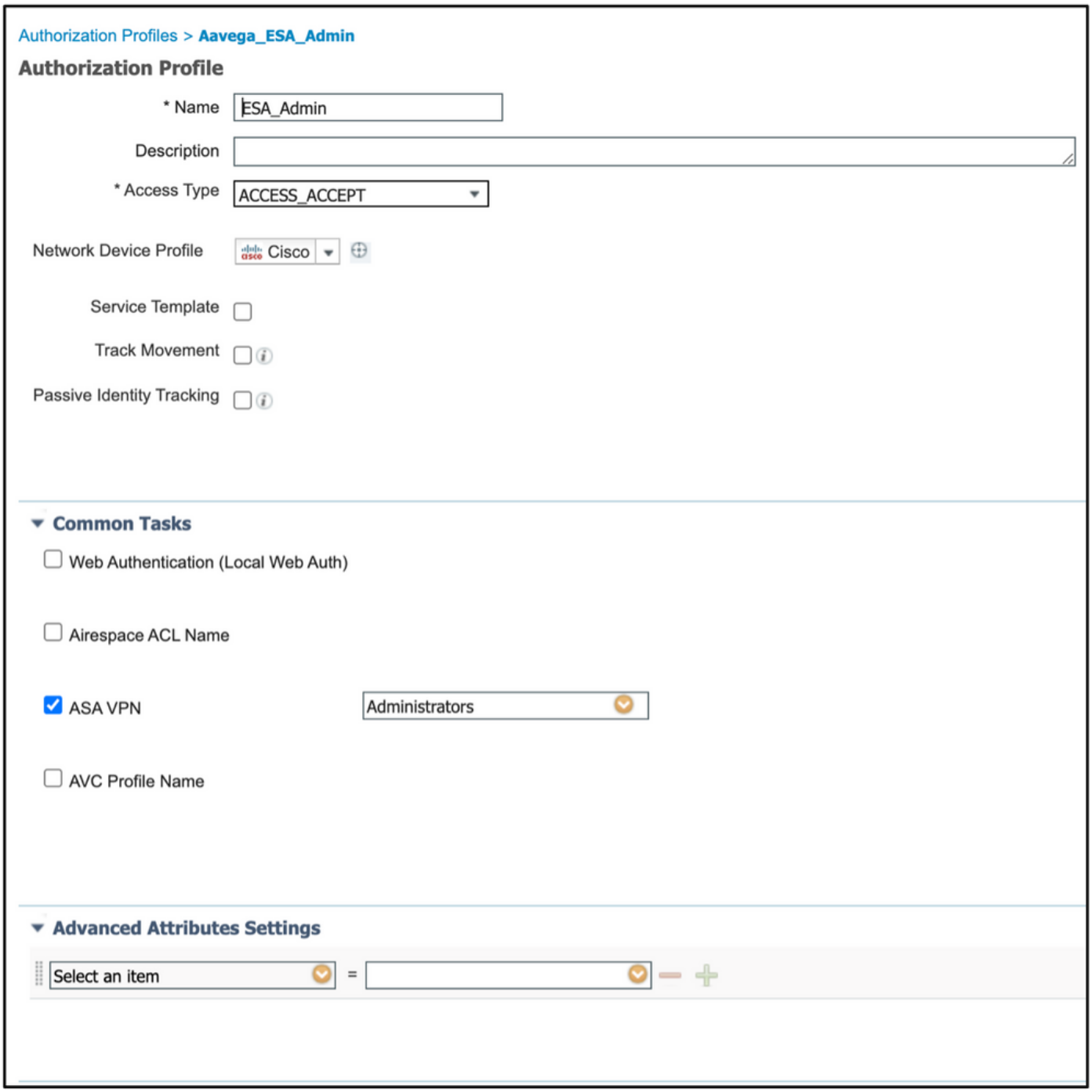
En este paso, cree nuevos usuarios o asigne usuarios que ya existan al grupo de identidad que creamos en el paso 1. Inicie sesión en ISE y **navegue hasta Administration->Identity Management->Identities** y cree nuevos usuarios o asígneles a los usuarios de los grupos que ha creado. Como se muestra en la imagen.



Paso 3. Crear perfiles de autorización.

La autenticación RADIUS se puede completar correctamente sin perfiles de autorización; sin embargo, no se asignaron roles. Para una configuración completa, **navegue hasta Política->Elementos de política->Resultados->Autorización->Perfil de autorización.**

Nota: Cree un perfil de autorización por función que se va a asignar.



Nota: Asegúrese de utilizar el atributo de clase radius 25 y proporcione un nombre. Este nombre debe coincidir con la configuración de AsyncOS (ESA/SMA). En la figura 3, Administradores es el nombre del atributo CLASS.

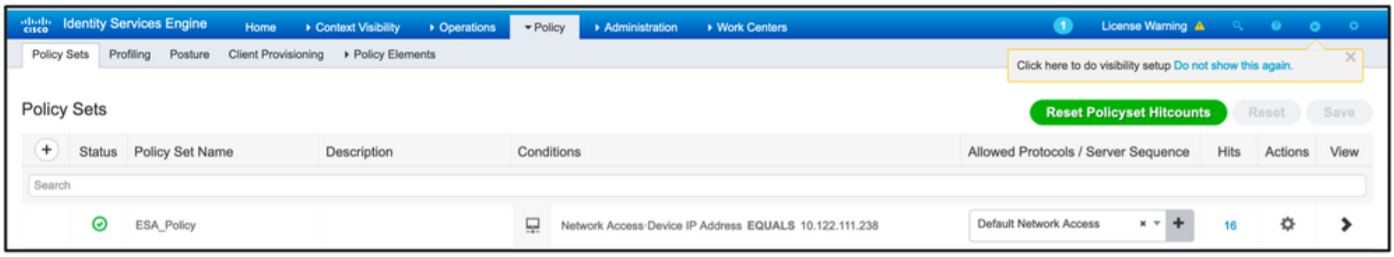
Paso 4. Cree una política de autorización.

Este último paso permite al servidor ISE identificar los intentos de inicio de sesión del usuario y asignar al perfil de autorización correcto.

En el caso de una autorización correcta, ISE devuelve un access-accept junto con el valor CLASS definido en el perfil de autorización.

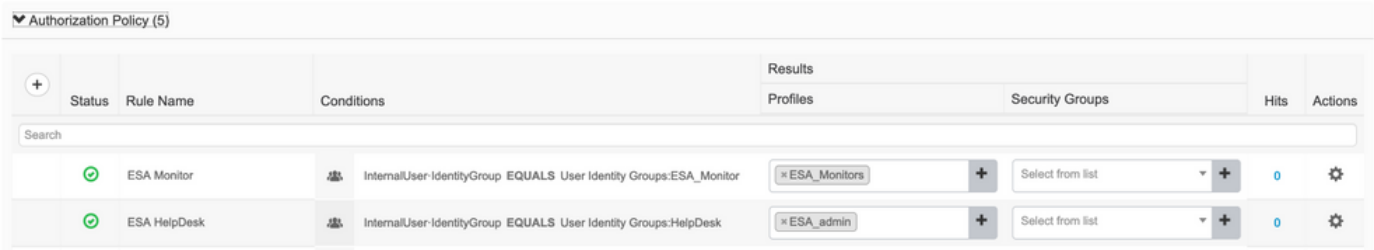
Vaya a Política > Conjuntos de políticas > Agregar (+ símbolo)

Asigne un nombre y seleccione el símbolo más para agregar las condiciones necesarias. Este entorno de laboratorio utiliza un Radius. NAS-IP-Address. Guarde la nueva política.



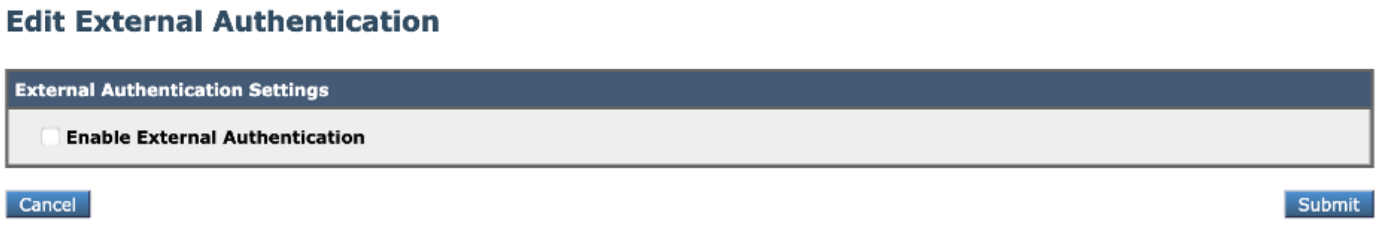
Para que las solicitudes de autorización coincidan correctamente, se deben agregar las condiciones. **Seleccionar** > y agregar condiciones.

El entorno de laboratorio utiliza InternalUser-IdentityGroup y coincide con cada perfil de autorización.



Paso 5. Habilite la autenticación externa en AsyncOS ESA/ SMA.

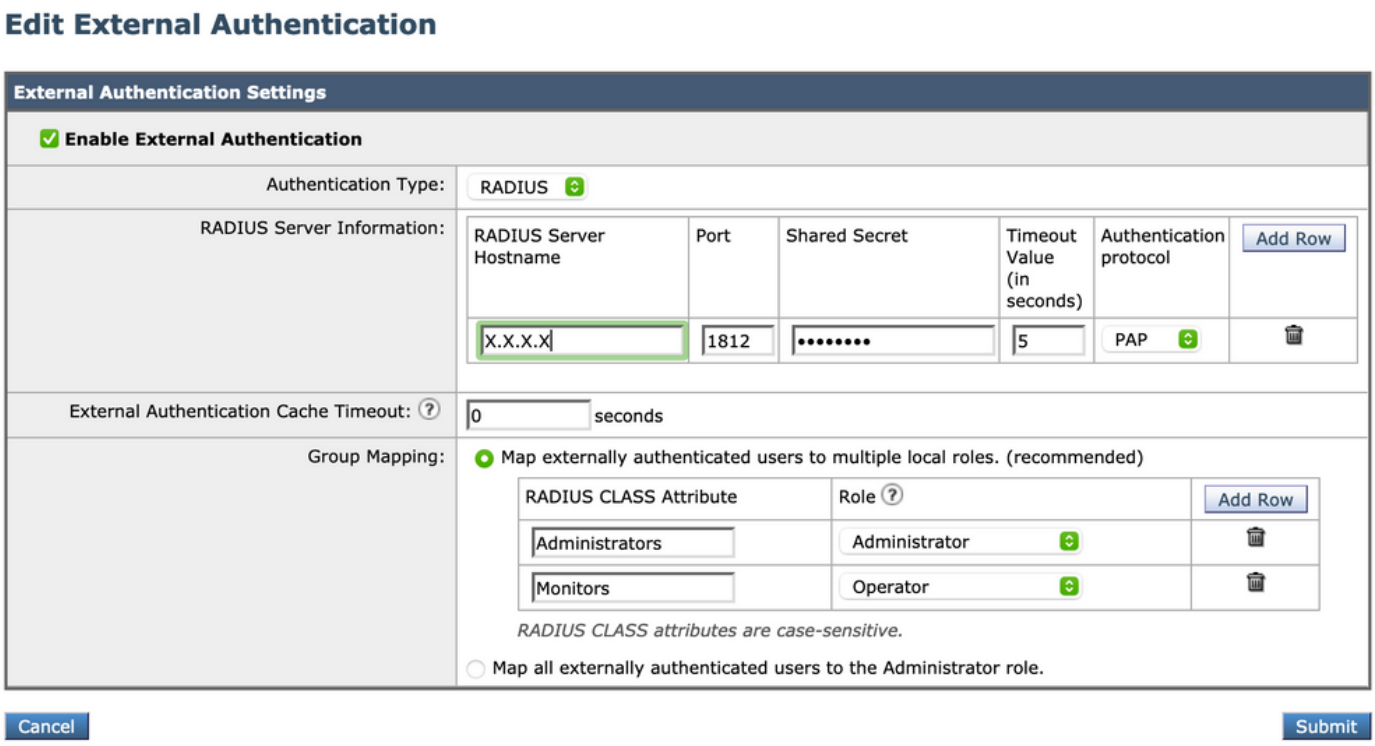
Inicie sesión en el dispositivo AsyncOS (ESA/SMA/WSA). Y **navegue hasta Administración del sistema > Usuarios > Autenticación externa > Habilitar autenticación externa** en ESA.



Proporcione estos valores:

- Nombre de host del servidor RADIUS
- Puerto
- secreto compartido
- Valor de tiempo de espera (en segundos)
- Protocolo de autenticación

Seleccione **Asignar usuarios autenticados externamente a varias funciones locales (recomendado)**. Como se muestra en la imagen.

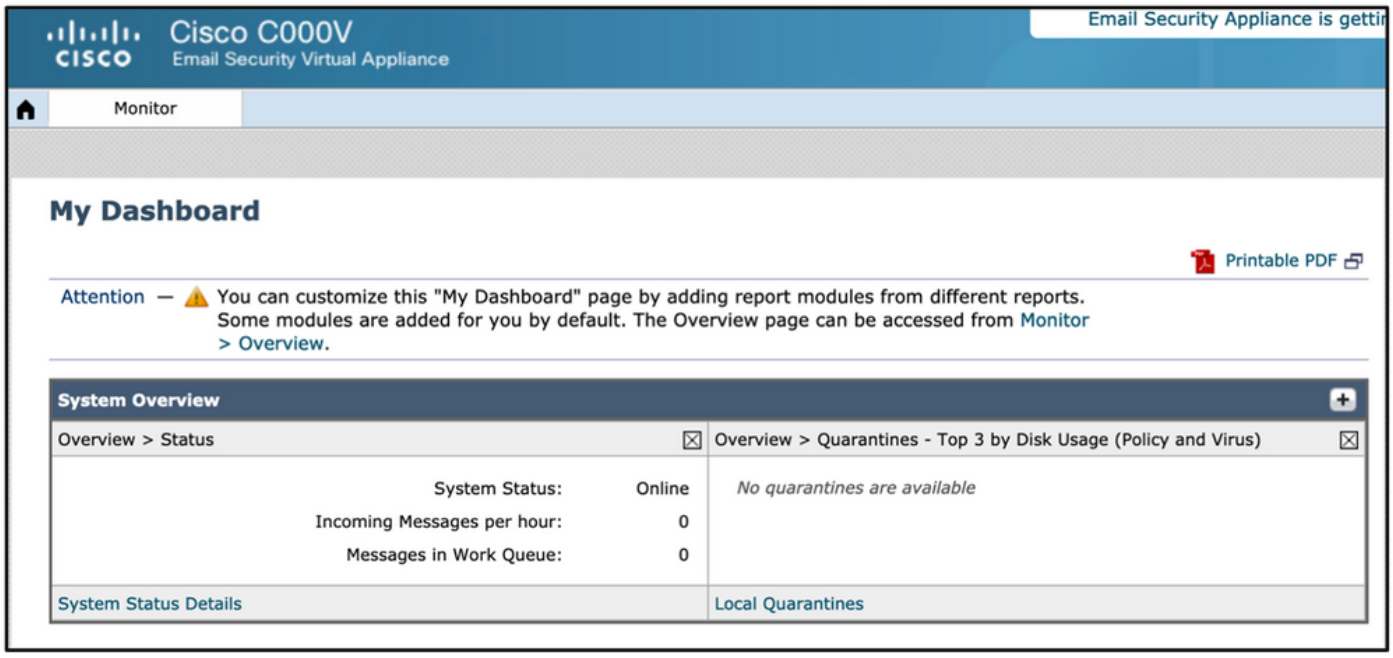


Nota: El atributo de clase Radius DEBE coincidir con el nombre del atributo definido en el paso 3 (en tareas comunes asignadas como VPN ASA).

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Inicie sesión en su dispositivo AsyncOS y confirme que se ha concedido acceso y que la función asignada se ha asignado correctamente. Como se muestra en la imagen con la función de usuario invitado.

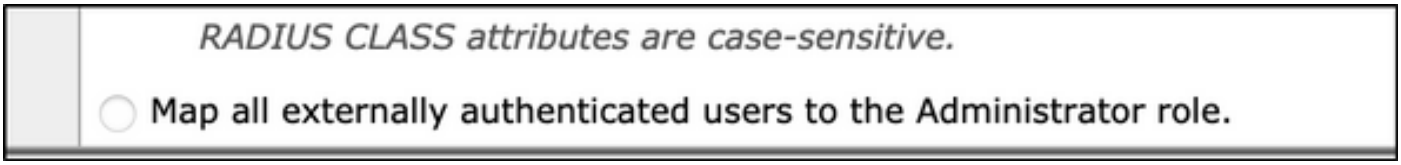


Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Si el intento de inicio de sesión no funciona en el ESA con el mensaje "Nombre de usuario o contraseña no válidos". El problema podría estar en la Política de autorización.

Inicie sesión en ESA y, desde Autenticación externa, seleccione Asignar todos los usuarios autenticados externamente a la función de administrador.



Envíe y confirme los cambios. Realice un nuevo intento de inicio de sesión. En caso de que se inicie sesión correctamente, verifique dos veces el perfil de autorización de ISE Radius (atributo CLASS 25) y la configuración de la política de autorización.

Información Relacionada

- **Guía de usuario de ISE 2.4**
- **Guía de usuario de AsyncOS**