Integración del sistema de FireSIGHT con el ISE para la autenticación de usuario de RADIUS

Contenido

Introducción

Este documento describe los pasos para la configuración requeridos para integrar un centro de administración de Cisco FireSIGHT (FMC) o el dispositivo administrado de FirePOWER con el Cisco Identity Services Engine (ISE) para la autenticación de usuario del Remote Authentication Dial In User Service (RADIUS).

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración inicial del sistema y del dispositivo administrado de FireSIGHT vía el GUI y/o el shell
- Configurar las directivas de la autenticación y autorización en el ISE
- Conocimiento del RADIUS básico

Componentes Utilizados

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

- Cisco ASA v9.2.1
- Módulo v5.3.1 ASA FirePOWER
- ISE 1.2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Configuración ISE

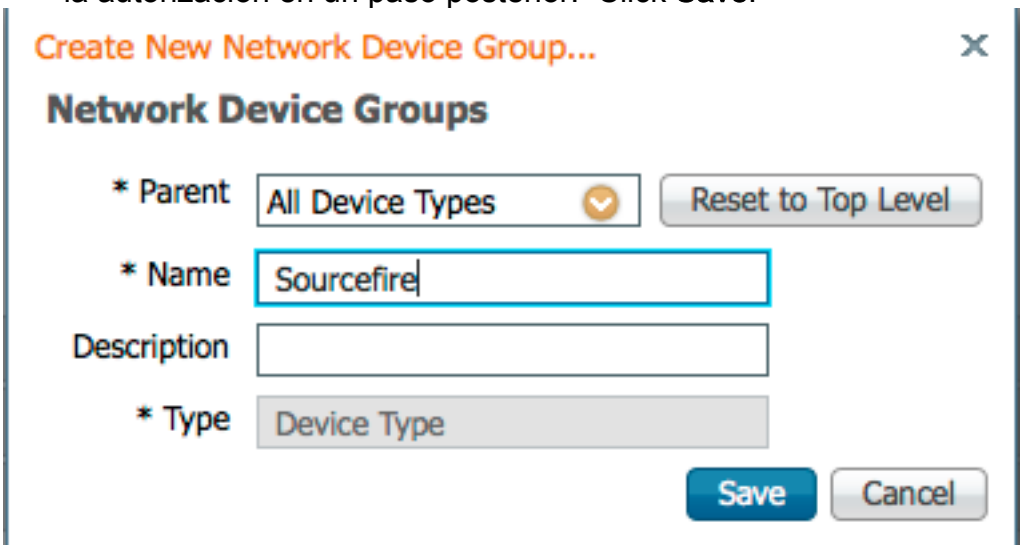
> **Tip**: Hay diferentes formas de configurar las directivas de la autenticación y autorización ISE para soportar la integración con los dispositivos de acceso a la red (NAD) tales como Sourcefire. El ejemplo abajo es una manera de configurar el intregration. La configuración de muestra es un punto de referencia y se puede adaptar para adaptarse a las necesidades del despliegue específico. Observe que la configuración de la autorización es un proceso de dos pasos. Una o más directivas de la autorización serán definidas en el ISE con los pares de vuelta del valor de atributo de RADIUS ISE (AV-pares) al FMC o al dispositivo administrado. Estos AV-pares entonces se asocian a un grupo de usuario local definido en la configuración de la política del sistema FMC.

Configurar los dispositivos de red y a los grupos de dispositivos de red

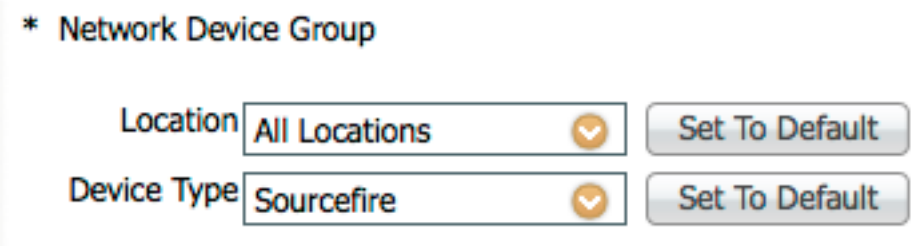
- Del ISE GUI, navegue a la **administración > a los recursos de red > a los dispositivos de red**. Haga clic **+Add** para agregar un nuevo dispositivo de acceso a la red (NAD). Proporcione un nombre y una dirección IP descriptivos del dispositivo. El FMC se define en el ejemplo abajo.

- Bajo **grupo de dispositivos de red**, haga clic en la flecha anaranjada al lado de **todos los tipos de dispositivo.** Haga clic en el icono y selecto **cree al nuevo grupo de dispositivos de red**. En el tiro de pantalla del ejemplo que sigue, han configurado al tipo de dispositivo Sourcefire. Este tipo de dispositivo será referido a la definición de la regla de la directiva de

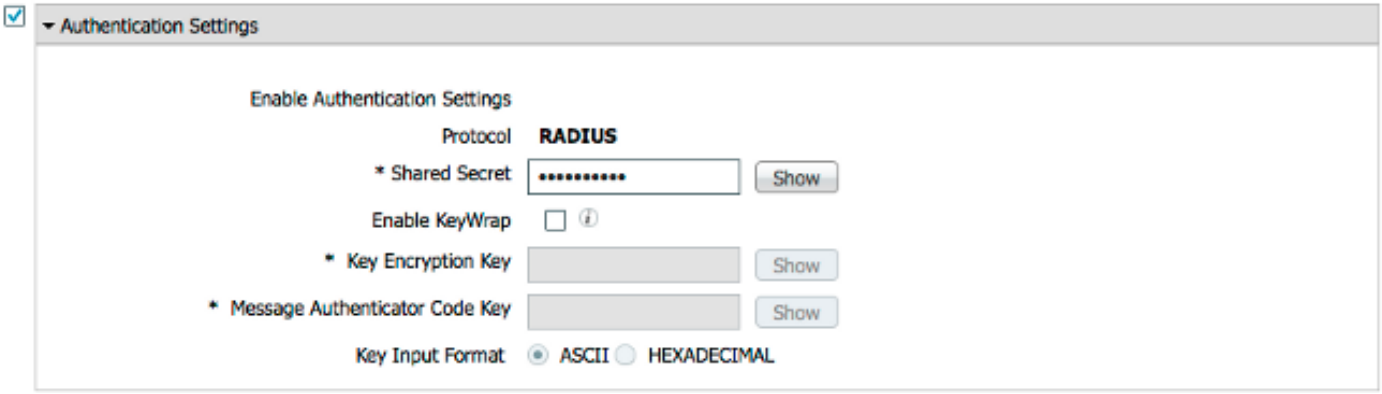
la autorización en un paso posterior. Click **Save**.



- Haga clic la flecha anaranjada otra vez y seleccione al grupo de dispositivos de red configurado en el paso arriba



- Marque el cuadro al lado de las **configuraciones de la autenticación**. Ingrese la clave secreta compartida RADIO que será utilizada para este NAD. Observe la misma clave secreta compartida será utilizado otra vez más adelante al configurar al servidor de RADIUS en FireSIGHT MC. Para revisar el valor de la clave del sólo texto, haga clic el botón de la **demostración**. Click **Save**.



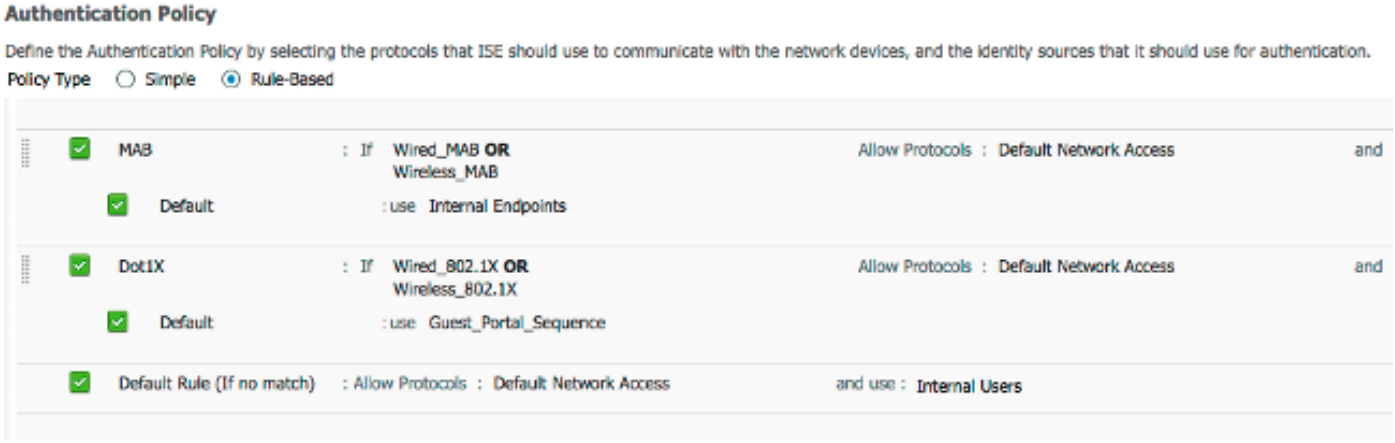
- Relance los pasos antedichos para todo el FireSIGHT los MC y los dispositivos administrados que requerirán la autenticación de usuario de RADIUS/la autorización para el GUI y/o el acceso del shell.

Configurar la política de autenticación ISE:

- Del ISE GUI, navegue a la **directiva > a la autenticación**. Si usa los conjuntos de la directiva, navegue a la **directiva > a los conjuntos de la directiva**. El ejemplo abajo se toma de un despliegue ISE que utilice las interfaces de la política de la autenticación predeterminada y de

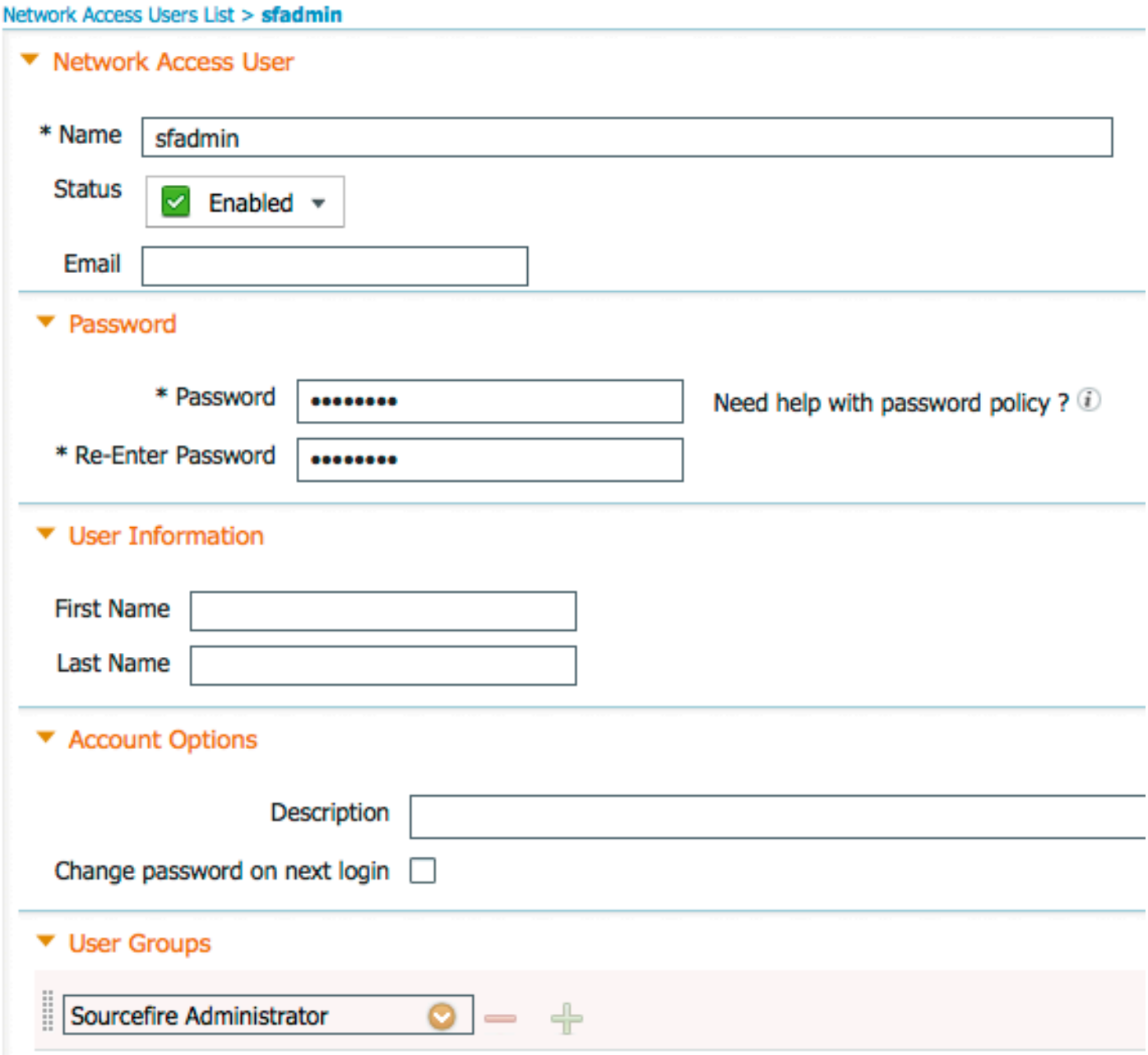
la autorización. La lógica de la regla de la autenticación y autorización es lo mismo sin importar el acercamiento de la configuración.

- **La regla predeterminada (si ninguna coincidencia)** será utilizada para autenticar los pedidos de RADIUS de los NAD donde no está puente de la autenticación de MAC (MAB) o 802.1x el método funcionando. Según lo configurado por abandono, esta regla buscará las cuentas de usuario en la fuente local de la identidad de los **usuarios internos** ISE. Esta configuración se puede modificar para referir a una fuente externa de la identidad tal como Active Directory, LDAP, etc según lo definido bajo la **administración > Administración de la identidad > las fuentes externas de la identidad**. Para el motivo del simplciity, este ejemplo definirá las cuentas de usuario localmente en el ISE así que no se requiere ningunas otras modificaciones a la política de autenticación.



Agregar a un usuario local al ISE

- Navegue a la **administración > a la Administración de la identidad > a las identidades > Users**. Haga clic en Add (Agregar). Ingrese un nombre de usuario y contraseña significativo. Bajo selección de **grupos de usuarios**, seleccione un nombre de grupo existente o haga clic el verde + muestra de agregar a un nuevo grupo. En este ejemplo, asignan el usuario “sfadmin” al grupo de encargo “administrador de Sourcefire”. Conectarán a este grupo de usuarios al perfil de la autorización definido en el paso de la **directiva de la autorización ISE que configura** abajo. Click **Save**.



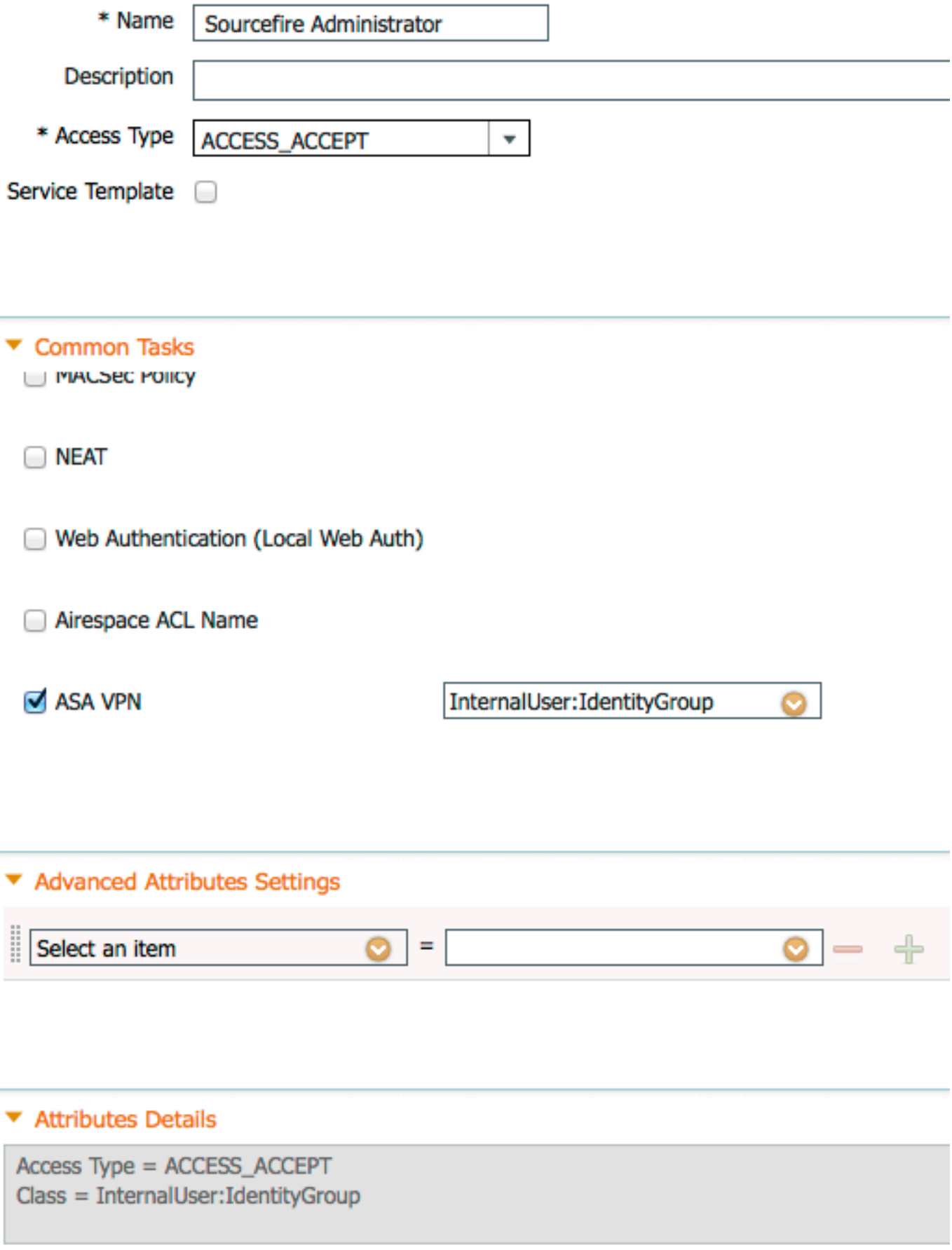
Configurar la directiva de la autorización ISE

- Navegue a la **directiva > a los elementos de la directiva > a los resultados > a la autorización > a los perfiles de la autorización**. Haga clic el verde + muestra de agregar un nuevo perfil de la autorización.
- Proporcione un nombre descriptivo tal como administrador de Sourcefire. Seleccione **ACCESS_ACCEPT** para el **tipo de acceso**. Bajo **tareas comunes**, navegue a la parte inferior y marque el rectángulo al lado de **ASA VPN**. Haga clic la flecha anaranjada y seleccione **InternalUser: IdentityGroup**. Click **Save**.

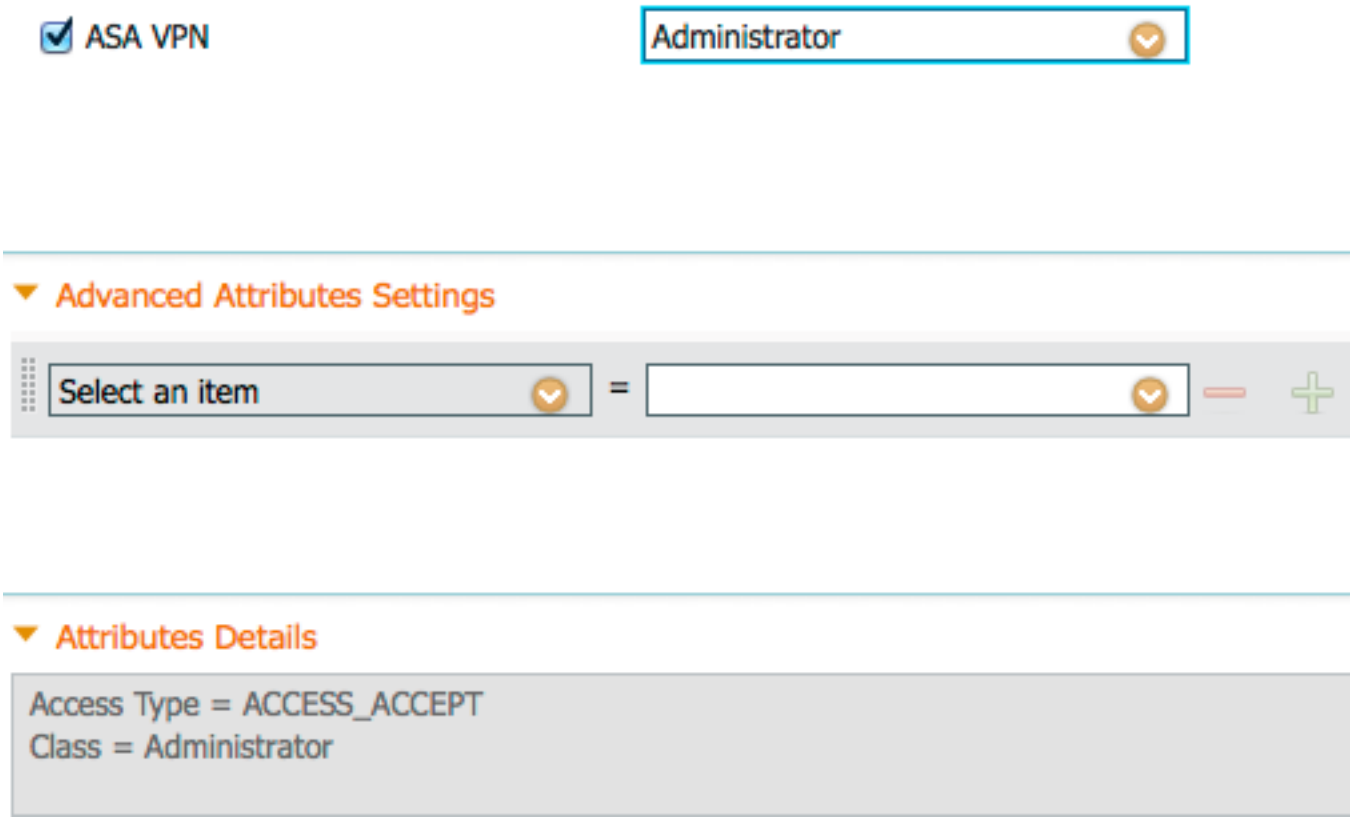
  Tip: Porque este ejemplo utiliza el almacén de la identidad del usuario local ISE, el InternalUser: La opción del grupo de IdentityGroup se utiliza para simplificar la configuración. Si usa un almacén externo de la identidad, el atributo de la autorización ASA VPN todavía se utiliza, sin embargo, el valor que se volverá al dispositivo de Sourcefire se configura manualmente. Por ejemplo, manualmente tecleando al administrador en el ASA VPN caiga abajo el cuadro dará lugar a un valor de los AV-pares Class-25 de la clase = del administrador que son enviados al dispositivo de Sourcefire. Este valor se puede entonces

asociar a un grupo de usuarios del sourcefire como parte de la configuración de la política del sistema. Para los usuarios internos, cualquier método de configuración es aceptable.

Ejemplo del usuario interno



Ejemplo del usuario externo



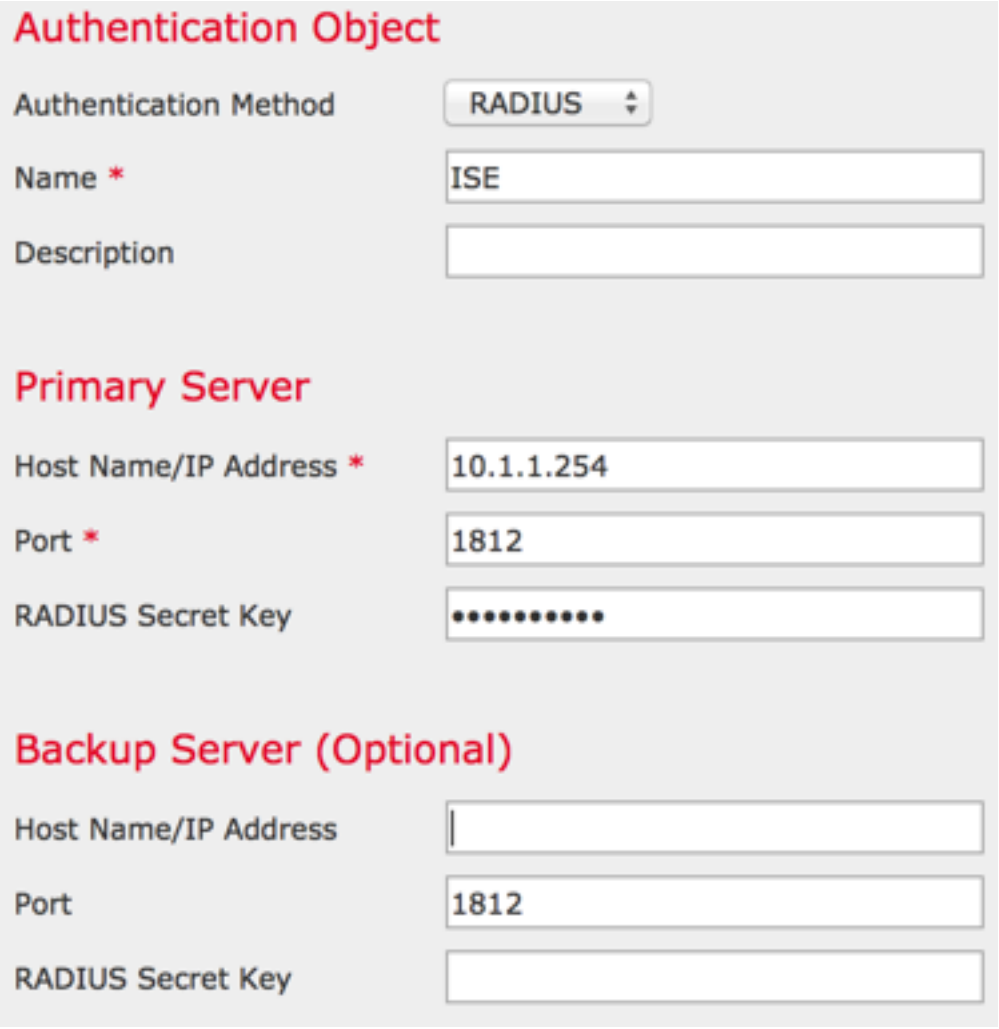
- Navegue a la **directiva > a la autorización** y configure una nueva directiva de la autorización para las sesiones de la administración de Sourcefire. El ejemplo abajo utiliza el **DISPOSITIVO:** Condición del **tipo de dispositivo** para hacer juego el tipo de dispositivo configurado en **Configurando la** sección de los **dispositivos de red y de los grupos de dispositivos de red** arriba. Esta directiva entonces se asocia al perfil de la autorización del administrador de Sourcefire configurado arriba. Click **Save**.

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones
✓	Sourcefire Administrator	if	DEVICE:Device Type EQUALS All Device Types#Sourcefire	then	Sourcefire Administrator
✓	CWA-PSN1	if	Network Access:ISE Host Name EQUALS ise12-psn1	then	CWA-PSN1
✓	CWA-PSN2	if	Network Access:ISE Host Name EQUALS ise12-psn2	then	CWA-PSN2

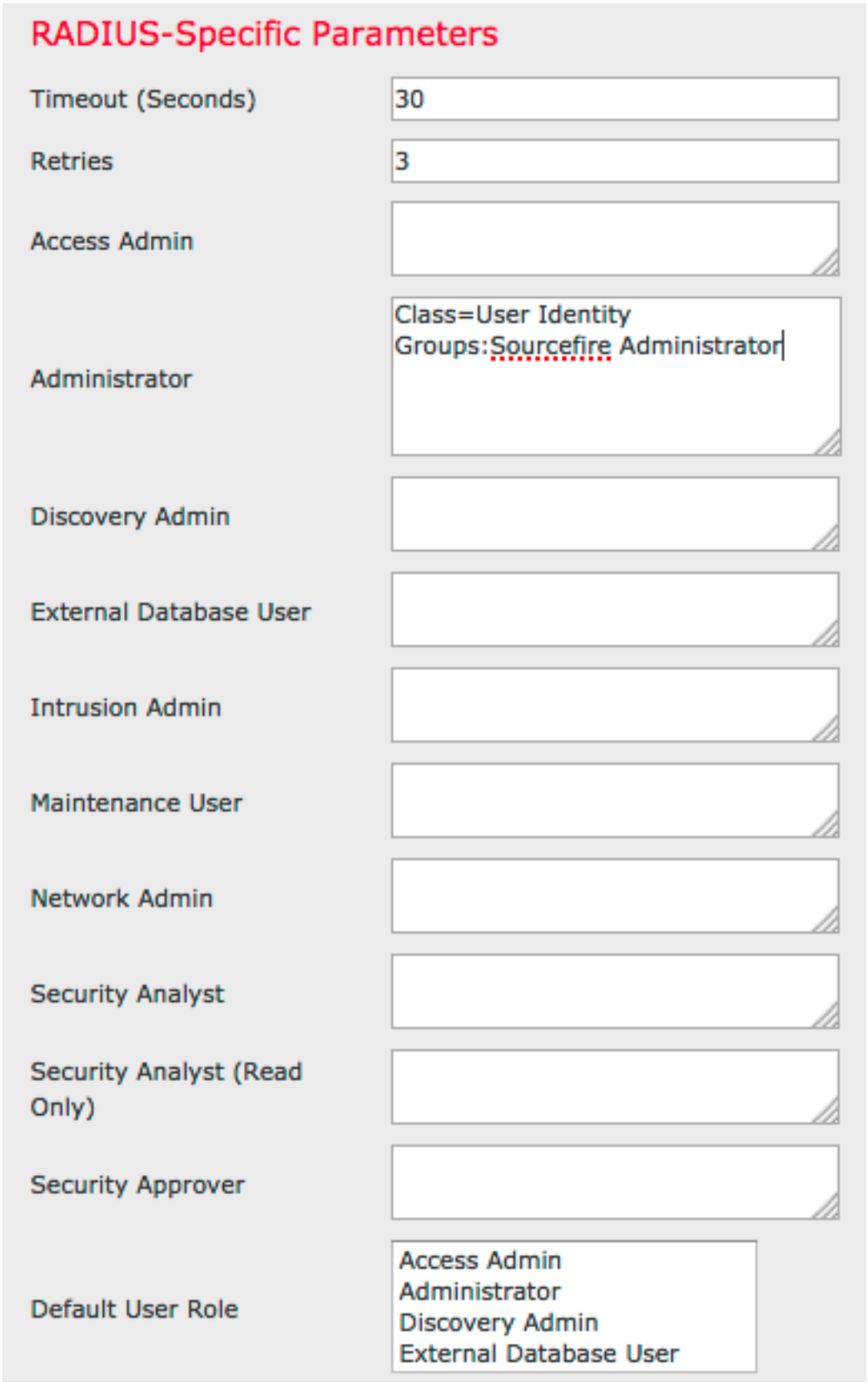
Configuración de la política del sistema de Sourcefire

- Inicie sesión a FireSIGHT MC y navegue al **sistema > al Local > User Management (Administración de usuario)**. Haga clic en el tecleo de cuadro de la **autenticación de inicio de sesión** + crean el botón del objeto de la autenticación para agregar a un nuevo servidor de RADIUS para la autenticación de usuario/la autorización.
- Seleccione el **RADIUS** para el **método de autentificación**. Ingrese un nombre descriptivo para el servidor de RADIUS. Ingrese el **nombre del host/el IP Address** y la **clave secreta del**

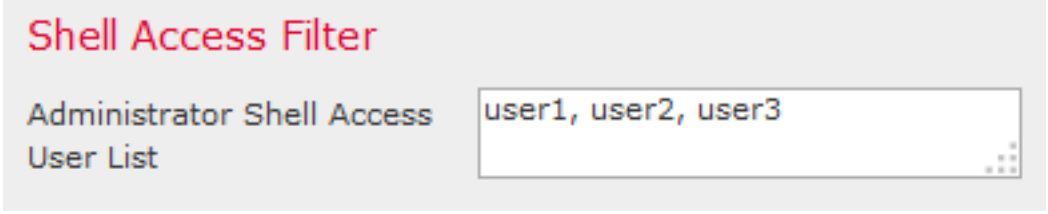
RADIO. La clave secreta debe hacer juego la clave configurada previamente en el ISE. Ingrese opcionalmente un **nombre de** host servidor del respaldo ISE**/un IP Address** si existe uno.



- Bajo **parámetros RADIUS-específicos** seccione, ingrese la cadena de los AV-pares Class-25 en el cuadro de texto al lado del nombre de grupo local de Sourcefire que se corresponderá con para el acceso a GUI. En este ejemplo, la identidad de Class=User agrupa: El valor del administrador de Sourcefire se asocia al Grupo del administrador de Sourcefire. Éste es el valor las devoluciones ese ISE como parte del ACCESS-ACCEPT. Opcionalmente, seleccione un **papel de usuario predeterminado** para los usuarios autenticados que no hacen los grupos Class-25 asignar. Haga clic la **salvaguardia** para salvar la configuración o para proceder a la sección del verificar abajo a la prueba de la autentificación con el ISE.



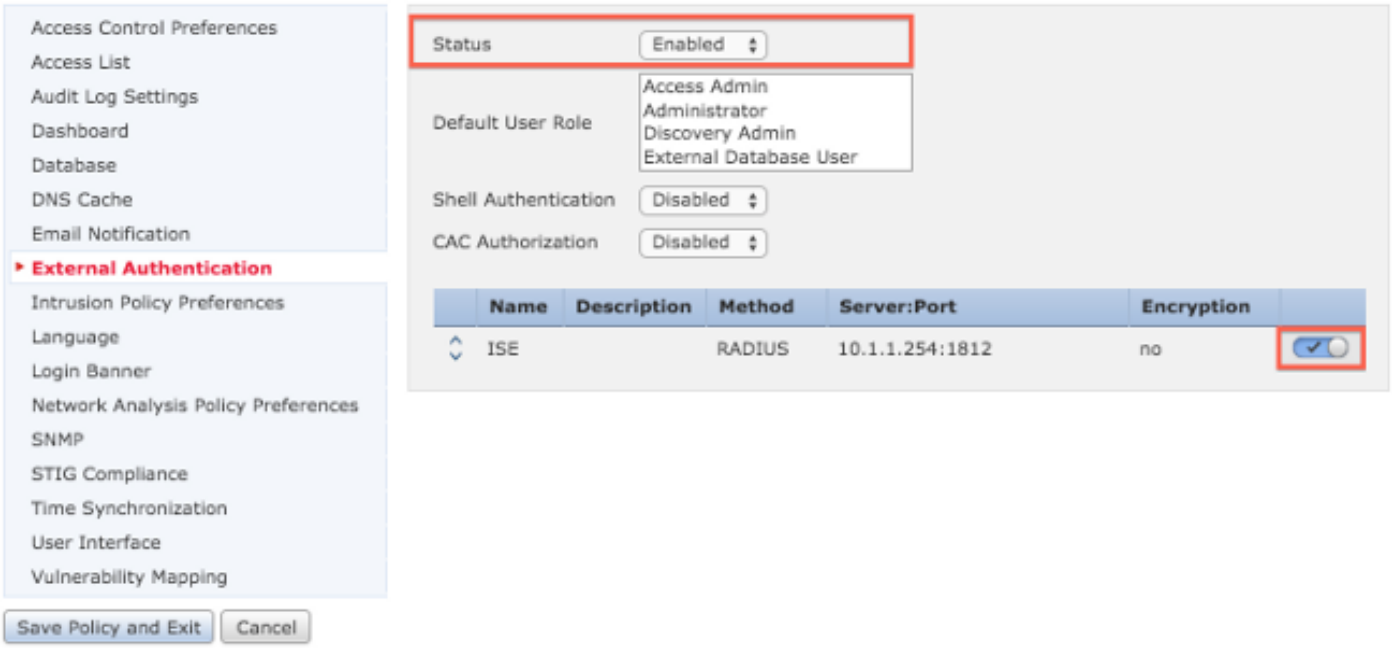
- Bajo el **filtro del acceso del shell**, ingrese una lista separada coma de usuarios para restringir las sesiones shell/SSH.



Habilite la autenticación externa

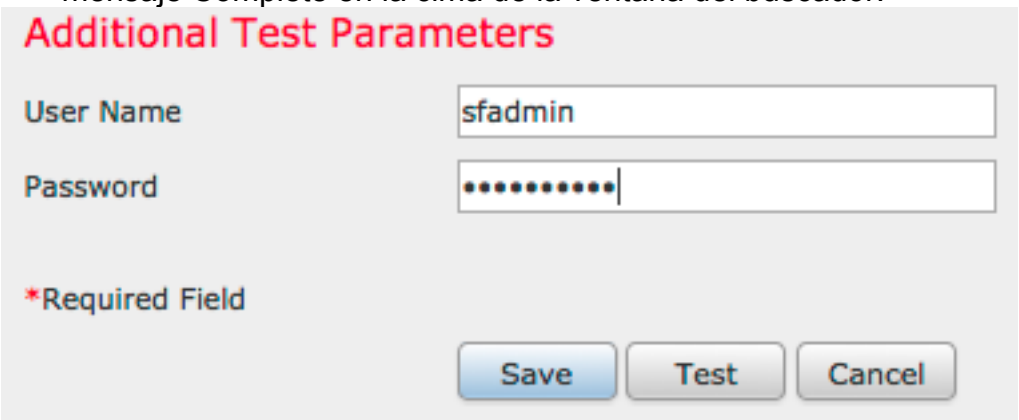
Finalmente, complete estos pasos para habilitar la autenticación externa en el FMC:

1. Navegue al **sistema** > al **Local** > a la **política del sistema**.
2. Seleccione la **autenticación externa** en el panel izquierdo.
3. Cambie el *estatus a* **habilitado** (inhabilitado por abandono).
4. Habilite al servidor de RADIUS agregado ISE.
5. Salve la directiva y reaplique la directiva en el dispositivo.



Verificación

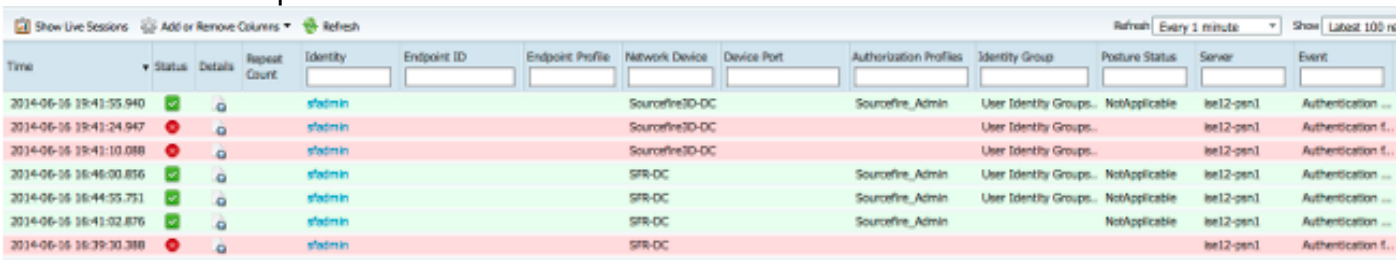
- A la autenticación de usuario a prueba contra el ISE, navegue hacia abajo a los **parámetros de prueba la** sección **adicional** y ingrese un nombre de usuario y contraseña para el usuario ISE. Haga clic la **prueba.** Una prueba satisfactoria dará lugar a un éxito verde: Pruebe el mensaje Complete en la cima de la ventana del buscador.



- Para ver los resultados de la prueba de la autentificación, ir a la **sección de resultados de la prueba** y hacer clic la flecha **negra** al lado de los **detalles de la demostración**. En el tiro de pantalla del ejemplo abajo, observe el “radiusauth - respuesta: |Grupos de la identidad de Class=User: Administrador de Sourcefire|” valor recibido del ISE. Esto debe hacer juego el valor de clase asociado al grupo local de Sourcefire configurado en FireSIGHT MC arriba.

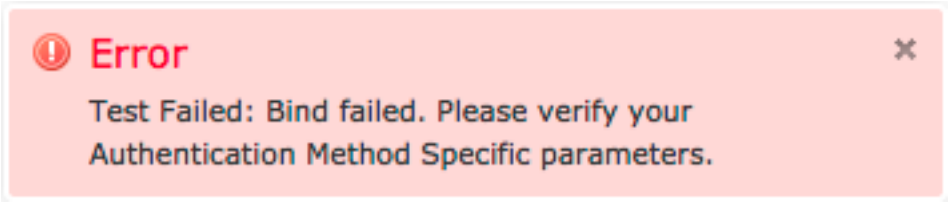
Click **Save**.

- Del ISE Admin GUI, navegue a las **operaciones > a las autenticaciones** para verificar el éxito o el error de la prueba de la autenticación de usuario.

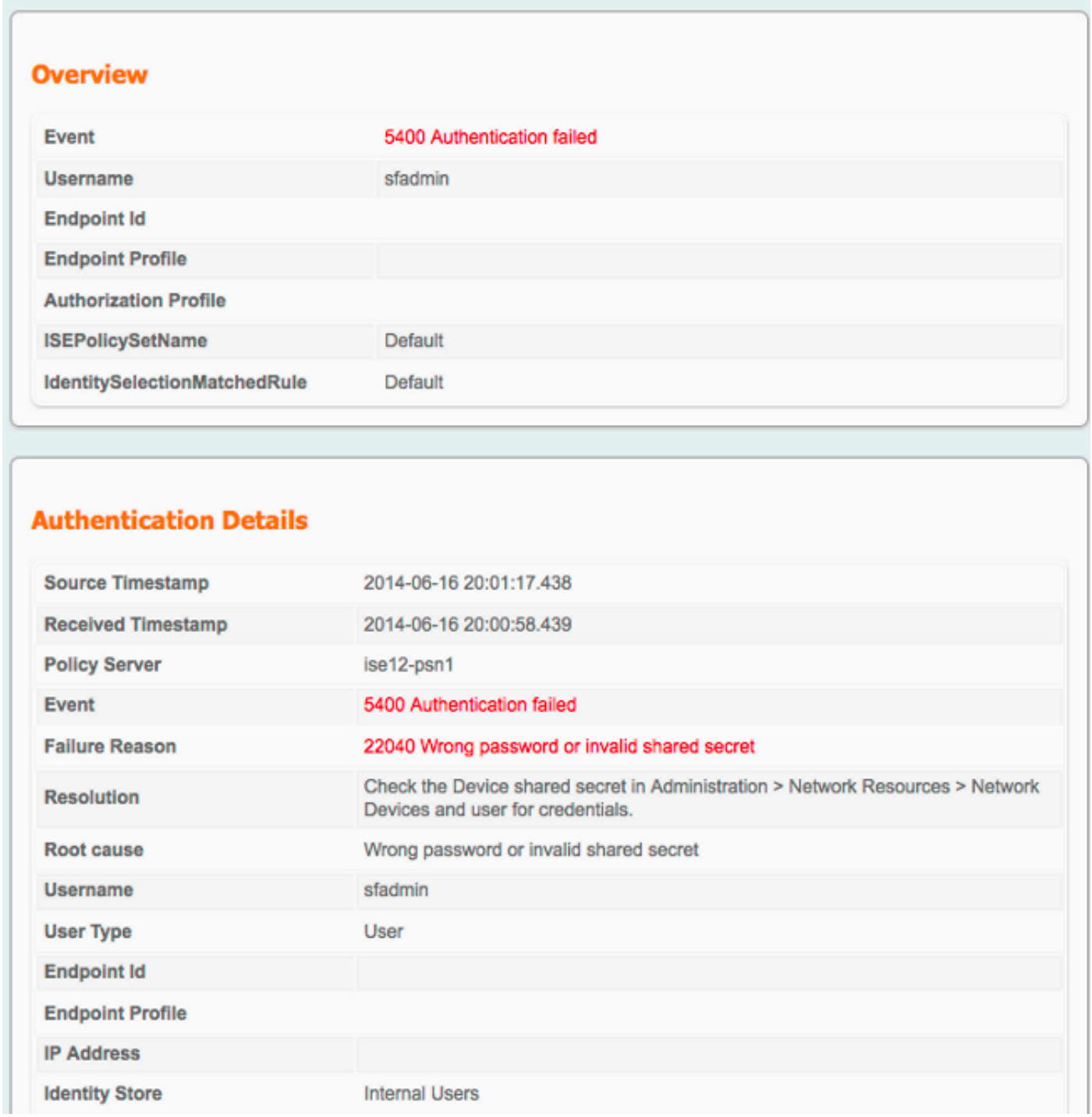


Troubleshooting

- Al probar la autenticación de usuario contra el ISE, el error siguiente es indicativo de una discordancía de clave secreta RADIUS o de un nombre de usuario incorrecto/de una contraseña.



- Del ISE admin GUI, navegue a las **operaciones > a las autenticaciones**. Un evento **rojo** es indicativo de un error mientras que un evento **verde** es indicativo de una autenticación satisfactoria/de una autorización/de un cambio de la autorización. Haga clic en  el icono para revisar los detalles del evento de la autenticación.



Overview

Event	5400 Authentication failed
Username	sfadmin
Endpoint Id	
Endpoint Profile	
Authorization Profile	
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default

Authentication Details

Source Timestamp	2014-06-16 20:01:17.438
Received Timestamp	2014-06-16 20:00:58.439
Policy Server	ise12-psn1
Event	5400 Authentication failed
Failure Reason	22040 Wrong password or invalid shared secret
Resolution	Check the Device shared secret in Administration > Network Resources > Network Devices and user for credentials.
Root cause	Wrong password or invalid shared secret
Username	sfadmin
User Type	User
Endpoint Id	
Endpoint Profile	
IP Address	
Identity Store	Internal Users

Información Relacionada

[Soporte Técnico y Documentación - Cisco Systems]