RSA NETWITNESS® SUITE

Administración de usuarios y de la seguridad del sistema

para la versión 11.0

Información de contacto

RSA Link en https://community.rsa.com contiene una base de conocimientos que responde a las preguntas comunes y brinda soluciones para problemas conocidos, documentación de productos, análisis de la comunidad y administración de casos.

Marcas comerciales

Para obtener una lista de las marcas comerciales de RSA, visite mexico.emc.com/legal/emc-corporation-trademarks.htm#rsa (visite el sitio web de su país correspondiente).

Acuerdo de licencia

Este software y la documentación asociada son propiedad e información confidencial de EMC, se suministran bajo licencia, y pueden utilizarse y copiarse solamente de acuerdo con los términos de dicha licencia y con el aviso de copyright mencionado a continuación. No se puede suministrar a ninguna persona, ni poner a su disposición de cualquier otra manera, este software ni la documentación, o cualquier copia de estos elementos.

Este documento no constituye ninguna transferencia de titularidad ni propiedad del software, la documentación o cualquier derecho de propiedad intelectual. Cualquier uso o reproducción sin autorización de este software y de la documentación pueden estar sujetos a responsabilidad civil o penal.

Este software está sujeto a cambios sin aviso y no debe considerarse un compromiso asumido por EMC.

Licencias de otros fabricantes

Este producto puede incluir software que ha sido desarrollado por otros fabricantes. El texto de los acuerdos de licencia que se aplican al software de otros fabricantes en este producto puede encontrarse en la página de documentación del producto en RSA Link. Al usar este producto, el usuario acepta regirse totalmente por los términos de los acuerdos de licencia.

Nota sobre tecnologías de cifrado

Es posible que este producto contenga tecnologías de cifrado. Muchos países prohíben o limitan el uso, la importación o la exportación de las tecnologías de cifrado, y las regulaciones actuales de uso, importación y exportación deben cumplirse cuando se use, importe o exporte este producto.

Distribución

EMC considera que la información de esta publicación es precisa en el momento de su publicación. La información está sujeta a cambios sin previo aviso.

febrero 2018

Contenido

Administración de usuarios y de la seguridad del sistema

En esta guía se proporciona información sobre la configuración de la seguridad y el control del acceso de los usuarios. El administrador del sistema debe comprender la configuración de todo el sistema, las cuentas de usuario, las funciones del sistema, los permisos y el acceso a los servicios.

Temas

Configurar la seguridad del sistema

En este tema se presenta un conjunto de procedimientos de punto a punto para implementar la seguridad del sistema. En cada paso de los siguientes temas se explica una configuración en todo el sistema. Siga los pasos en orden para configurar la seguridad en NetWitness Suite.

Temas

Paso 1. Configurar la complejidad de las contraseñas

En este tema se proporcionan instrucciones para configurar requisitos de complejidad de las contraseñas de NetWitness Suite en todo el sistema.

Las contraseñas son una parte importante de la estrategia de seguridad de la red. Proporcionan protección de vanguardia fundamental para los sistemas computacionales y ayudan a impedir ataques y el acceso no autorizado a información privada.

Las políticas de contraseña, diseñadas para mejorar la seguridad de las redes corporativas, varían de acuerdo con el sector, los requisitos corporativos y las normativas. Debido a estas variaciones en las políticas de contraseña, el software NetWitness Suite permite configurar los requisitos de complejidad de las contraseñas para los usuarios internos de NetWitness Suite de modo que se ajusten a las reglas de políticas de contraseña corporativas.

Los requisitos de complejidad de las contraseñas se aplican solo a los usuarios internos y no se imponen a los usuarios externos. Los usuarios externos dependen de sus propios métodos y sistemas para imponer la complejidad de las contraseñas.

Además, puede configurar un período de vencimiento de usuario predeterminado global y determinar si a los usuarios internos se les informa que sus contraseñas están a punto de vencer y cuándo se les informa. La notificación de vencimiento de la contraseña consiste en un mensaje de vencimiento de la contraseña cuando un usuario inicia sesión en NetWitness Suite.

Seguridad de la contraseña

Las contraseñas seguras hacen que los atacantes tengan mayores dificultades para adivinar las contraseñas de los usuarios y ayudan a impedir el acceso no autorizado a la red de la organización. Puede definir el nivel apropiado de seguridad de las contraseñas para los usuarios de NetWitness Suite.Cuando configura los ajustes de seguridad de las contraseñas, estos se aplican a los usuarios internos de NetWitness Suite, incluido el usuario administrador.

Puede optar por imponer cualquier combinación de los siguientes requisitos de seguridad de las contraseñas cuando un usuario de NetWitness Suite crea o cambia su contraseña:

- Longitud mínima de la contraseña
- Cantidad mínima de caracteres en mayúsculas
- Cantidad mínima de caracteres en minúsculas
- Cantidad mínima de decimales (del cero al nueve)
- Cantidad mínima de caracteres especiales
- Cantidad mínima de caracteres alfabéticos no latinos (incluye caracteres Unicode de idiomas

asiáticos)

- Si la contraseña puede o no incluir el nombre de usuario

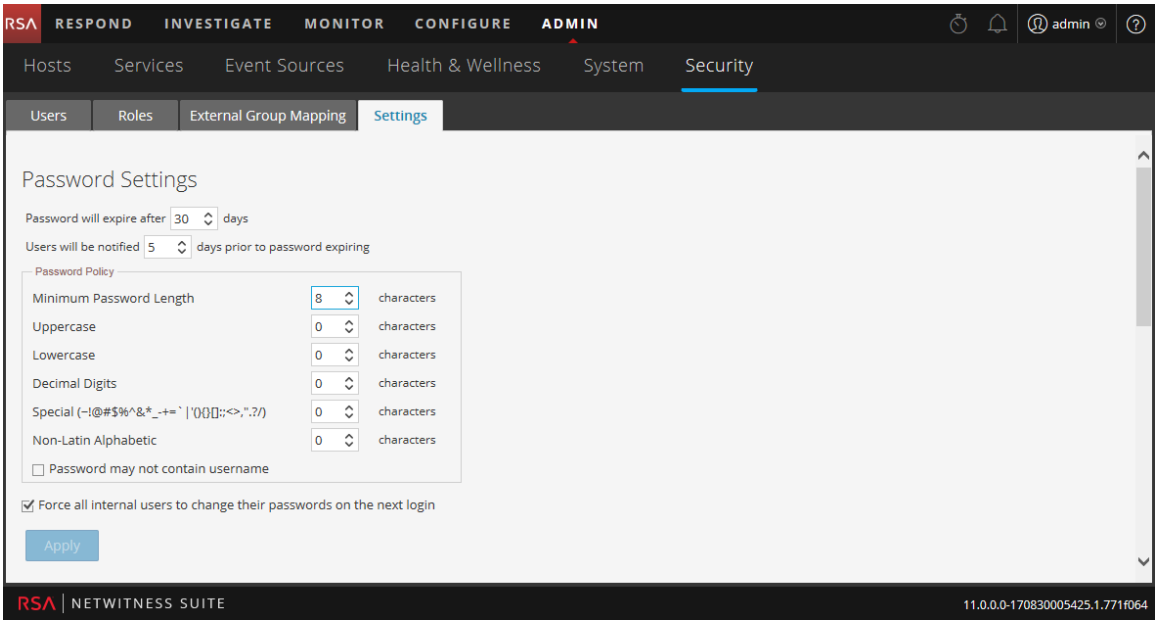
Por ejemplo, puede crear un requisito de contraseñas seguras que tenga un mínimo de ocho caracteres, que no pueda incluir el nombre del usuario y que contenga una combinación de letras en mayúscula y en minúscula, números y caracteres especiales.

Si decide imponer una cantidad mínima de caracteres alfabéticos no latinos, asegúrese de que estos caracteres estén disponibles para los usuarios cuando configuren sus contraseñas.

En el tema "Contraseñas que cumplen con las normas de STIG" de la *Guía de mantenimiento del sistema* se proporciona un ejemplo de una política de contraseñas seguras.

Configurar la seguridad de las contraseñas

1. En NetWitness Suite, vaya a **ADMIN > Seguridad**.
   La vista Seguridad se muestra con la pestaña **Usuarios** abierta.
2. Haga clic en la pestaña **Ajustes de configuración**.



3. En la sección **Configuración de contraseña**, seleccione los requisitos de complejidad de contraseña para imponer cuándo los usuarios de NetWitness Suite configuran sus contraseñas y especifique el mínimo de caracteres requeridos, si corresponde. Configure el valor en 0 para los requisitos que no desea aplicar, a excepción de Longitud mínima de contraseña, que tiene un valor mínimo de 4 caracteres.

Requisito	Descripción
La contraseña vencerá después de <n> días	La cantidad predeterminada de días antes de que venza una contraseña para todos los usuarios internos de NetWitness Suite. Un valor de cero (0) deshabilita el vencimiento de la contraseña. Para instalaciones nuevas, el valor predeterminado es 30. Para las actualizaciones, el valor anterior migra automáticamente a la instalación actualizada.
Se notificará a los usuarios <n> días antes del vencimiento de la contraseña.	La cantidad de días antes de la fecha de vencimiento de la contraseña que se informará a un usuario que su contraseña está a punto de vencer. Los usuarios ven un cuadro de diálogo Mensaje de vencimiento de contraseña cuando inician sesión en NetWitness Suite. El valor mínimo es de 1 día.
Longitud mínima de la contraseña	Especifica una longitud mínima de la contraseña. Una longitud mínima de la contraseña impide que los usuarios usen contraseñas cortas que se pueden adivinar con facilidad. 4 caracteres es el valor predeterminado requerido para la longitud mínima de la contraseña.
Mayúsculas	Especifica una cantidad mínima de caracteres en mayúscula para la contraseña. Esto incluye caracteres del idioma europeo de la A a la Z, con signos diacríticos, caracteres griegos y caracteres cirílicos. Por ejemplo: • Mayúscula cirílica: Д Ц • Mayúscula griega: Π Λ
Minúsculas	Especifica una cantidad mínima de caracteres en minúscula para la contraseña. Esto incluye caracteres del idioma europeo de la a a la z, ese-zeta, con signos diacríticos, caracteres griegos y caracteres cirílicos. Por ejemplo: • Minúscula cirílica: д ц • Minúscula griega: π λ
Números	Especifica una cantidad mínima de caracteres decimales (del cero al nueve) para la contraseña.

Requisito	Descripción
Especial (~!@#$%^&*_ -+=`|'(){} []:;<>,".?/)	Especifica una cantidad mínima de caracteres especiales para la contraseña: ~!@#$%^&*_-+=`|'(){}[]:;<>,".?/
Alfabético no latino	Especifica una cantidad mínima de caracteres alfabéticos Unicode que no correspondan a mayúscula ni minúscula. Esto incluye caracteres Unicode de idiomas asiáticos. Por ejemplo: • Kanji (japonés): 頁 (hoja) 枒 (árbol)
La contraseña no puede contener el nombre de usuario	Especifica que una contraseña no puede contener el nombre del usuario sin distinción de mayúsculas y minúsculas.

4. Si desea que la política de contraseña cambie para que se aplique en el próximo inicio de sesión en lugar del siguiente cambio de contraseña, seleccione **Obligar a todos los usuarios internos a cambiar sus contraseñas en el próximo inicio de sesión**. Tenga en cuenta que esta configuración se selecciona de forma predeterminada.
5. Haga clic en **Aplicar**.
   La configuración de seguridad de las contraseñas se aplica cuando los usuarios internos crean o cambian sus contraseñas. Si seleccionó **Obligar a todos los usuarios internos a cambiar sus contraseñas en el próximo inicio de sesión**, todos los usuarios internos deben cambiar su contraseña la próxima vez que inicien sesión en NetWitness Suite.

Paso 2. Cambiar las contraseñas de administrador predeterminadas

En este tema se proporcionan instrucciones para cambiar la contraseña de administrador del servicio NetWitness Suite y de los servicios principales.

La cuenta de usuario del administrador del sistema se instala con NetWitness Suite. El nombre de usuario es **administrador** y la contraseña predeterminada es aquella que ingresó en la interfaz del usuario basada en texto (TUI) durante el proceso de instalación de NetWitness Suite. La función de los **administradores** se asigna a admin. Esta función cuenta con todos los privilegios del sistema para controlar lo que un usuario puede hacer y los servicios a los cuales puede acceder. La única modificación que puede realizar en esta cuenta es cambiar la contraseña. A diferencia de otros usuarios de NetWitness Suite, los cambios en la contraseña del usuario **administrador** no se propagan automáticamente a los servicios descendentes. Cuando configura los ajustes de seguridad de las contraseñas, estos se aplican a todos los usuarios de NetWitness Suite, incluido el usuario administrador.

Las contraseñas, un importante aspecto de la seguridad de cómputo, están al frente de la protección para su sistema. El usuario **administrador** está preinstalado en NetWitness Suite y en cada servicio principal. Como medida de seguridad, cree los usuarios y las funciones para su organización en NetWitness Suite y en cada servicio principal.

Mejores prácticas

RSA recomienda las siguientes mejores prácticas:

- Cambiar la contraseña de **administrador** predeterminada de cada servicio.
- Crear una contraseña distinta para la cuenta de **administrador** en cada servicio.

Cambiar la contraseña de administrador de NetWitness Suite

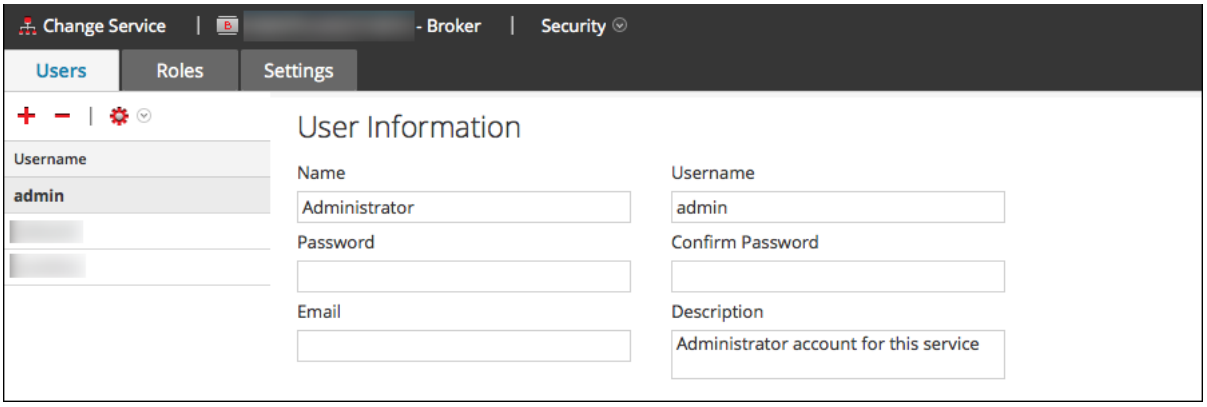
Cambie la contraseña de **administrador** de NetWitness Suite en la vista Perfil. Consulte "Cambiar contraseña" en la *Guía de introducción de NetWitness Suite*. La contraseña del usuario **administrador** no se propaga a los servicios principales.

Nota: Después de cambiar la contraseña de administrador, debe eliminar y volver a agregar un origen de datos en Reporting Engine. Para obtener más información, consulte la sección **Eliminar y volver a agregar un origen de datos en Reporting Engine** a continuación.

Cambiar la contraseña de administrador de los servicios de Core

Para cambiar la contraseña de administrador de un servicio principal:

1. En NetWitness Suite, vaya a **ADMIN > Servicios.**
2. Seleccione un servicio y elija > **Ver** > **Seguridad**.
3. En la pestaña **Usuarios**, seleccione el usuario **administrador**.



4. En el campo **Contraseña**, ingrese una nueva contraseña de administrador para el servicio seleccionado.
5. En el campo **Confirmar contraseña**, vuelva a escribir la nueva contraseña.
6. Haga clic en **Aplicar**.

Nota: Después de cambiar la contraseña de administrador, debe eliminar y volver a agregar un origen de datos en Reporting Engine. Para obtener más información, consulte **Eliminar y volver a agregar un origen de datos en Reporting Engine** a continuación.

Eliminar y volver a agregar un origen de datos en Reporting Engine

Reporting Engine valida un origen de datos mediante el uso del nombre de usuario y la contraseña del origen de datos. Si cambia el nombre de usuario o la contraseña de un origen de datos, debe eliminar y volver a agregar el origen de datos.

Para eliminar y volver a agregar un origen de datos en Reporting Engine:

1. En NetWitness Suite, vaya a **ADMIN > Servicios**.
2. En la vista Servicios, seleccione Reporting Engine y **Ver > Configurar**.
3. Haga clic en la pestaña **Orígenes**.
4. Seleccione un servicio que desee quitar y haga clic en −
5. Haga clic en + y seleccione **Servicios disponibles**.

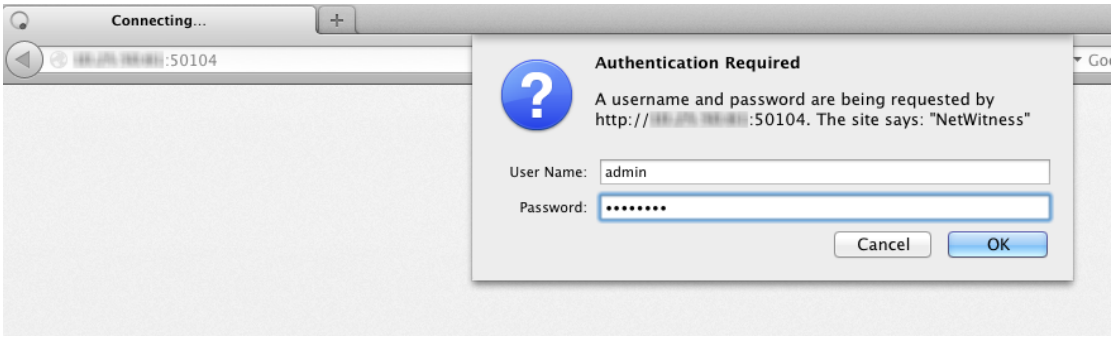
6. Seleccione el servicio que eliminó en el paso 4 y haga clic en **Aceptar**.
7. Cuando se le solicite, ingrese el nombre de usuario y la contraseña nuevos para el servicio.

Cambie la contraseña de administrador para un servicio utilizando el API de REST

En raras circunstancias, es posible que deba cambiar la contraseña de administrador de un servicio principal fuera de la interfaz del usuario de NetWitness Suite. Esta es simplemente otra manera de realizar el cambio de contraseña del servicio principal y no es el método recomendado.

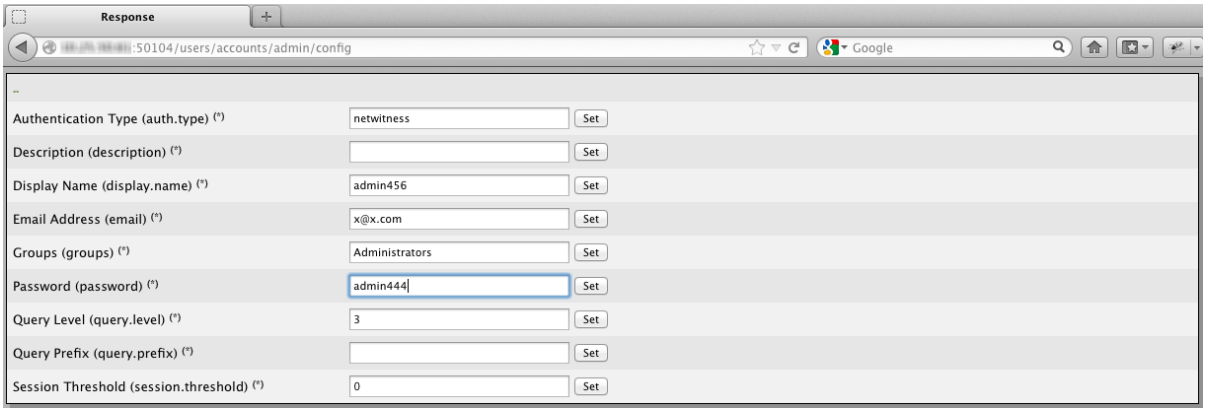
Para cambiar la contraseña de administrador para el servicio utilizando la interfaz del usuario de REST:

1. Abra un navegador web y vaya a la siguiente URL:
   <nombre de host>:<puerto>
   donde el **nombre de host** es el nombre de un servicio principal de NetWitness Suite y **puerto** es el puerto que se usa para comunicación de REST. Este es un ejemplo de un Decoder: `http://10.20.30.40:50104`
   Se muestra el cuadro de diálogo de autenticación.



2. En el cuadro de diálogo, ingrese el nombre de usuario y la contraseña que se usan para la autenticación como administrador en el servicio y haga clic en **Aceptar**. El nombre de usuario predeterminado es **administrador** y la contraseña predeterminada es **netwitness**.
   Aparece la ventana REST del servicio.
3. Navegue por la estructura de nodo a **usuarios/cuentas/administrador/configuración**.
   Los campos de configuración de usuario para administrador aparecen en la ventana del

navegador.



4. En el campo Contraseña, ingrese una nueva contraseña de administrador y haga clic en **Configurar**.

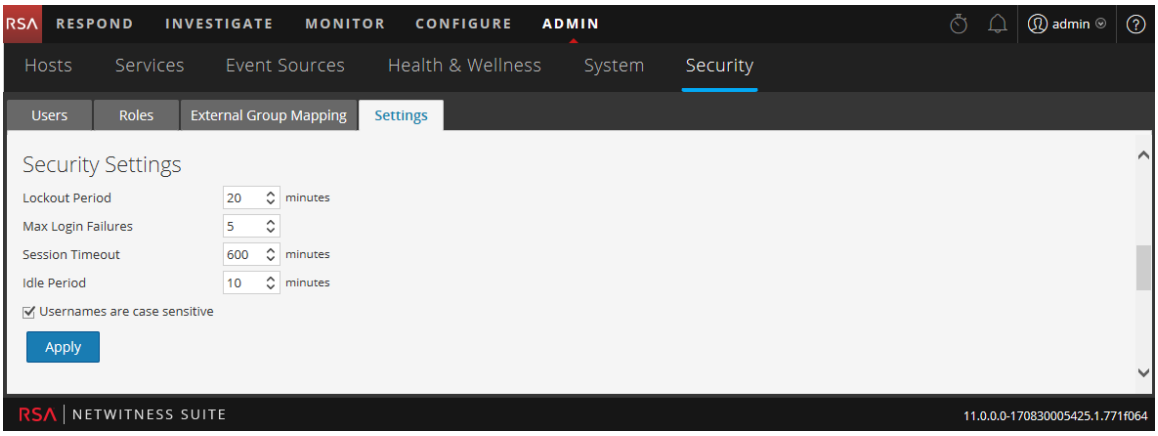
Paso 3. Configurar ajustes de seguridad en el nivel del sistema

En este tema se explica cómo configurar parámetros de seguridad para todo el sistema.

La mayoría de las configuraciones de seguridad global, como la cantidad máxima de intentos de inicio de sesión fallidos, se aplica a todos los usuarios y las sesiones de NetWitness Suite. La configuración relacionada con contraseñas en la sección Seguridad de las contraseñas, como el período de vencimiento de la contraseña y el la cantidad predeterminada de días antes de que venzan las contraseñas de usuario, se aplican a los usuarios internos de NetWitness Suite, pero no a los usuarios externos.

Configurar ajustes de seguridad

1. En NetWitness Suite, vaya a **ADMIN > Seguridad**.
   La vista Seguridad se muestra con la pestaña **Usuarios** abierta.
2. Haga clic en la pestaña **Ajustes de configuración**.



3. En la sección **Configuración de seguridad**, especifique valores para los campos como se describe en la siguiente tabla.

Campo	Descripción
Periodo de bloqueo	La cantidad de minutos para bloquear a un usuario de NetWitness Suite después de que se haya excedido la cantidad configurada de inicios de sesión fallidos. El valor predeterminado es 20 minutos.

Campo	Descripción
Número máximo de errores al iniciar sesión	La cantidad máxima de intentos de inicio de sesión fallidos antes de que un usuario se bloquee. El valor predeterminado es 5.
Tiempo de espera de sesión agotado	La duración máxima de una sesión de usuario antes de que se agote el tiempo de espera en minutos. El valor predeterminado es 600. Se agota el tiempo de espera de la sesión cuando transcurre el tiempo configurado, después del cual el usuario debe iniciar sesión nuevamente. El valor máximo permitido es 30,000. **Nota:** Si migró a NetWitness Suite 11.0 desde la versión 10.6.x y antes usaba un valor de 0 para un tiempo de espera de sesión ilimitado, el valor se restablece automáticamente a 30,000 minutos, puesto que ya no se admite un valor de 0.
Periodo de inactividad	La cantidad de minutos de inactividad antes de que se agote el tiempo de espera de una sesión. El valor predeterminado es 10. El valor máximo permitido es 30,000. **Nota:** Si migró a NetWitness Suite 11.0 desde la versión 10.6.x y antes usaba un valor de 0 para un período inactivo ilimitado, el valor se restablece automáticamente al valor predeterminado de 10, puesto que ya no se admite un valor de 0.
Los nombres de usuario distinguen mayúsculas de minúsculas	Seleccione esta opción si desea que el campo Nombre de usuario en la pantalla de inicio de sesión de NetWitness Suite distinga mayúsculas de minúsculas. Por ejemplo, si los nombres de usuario distinguen mayúsculas de minúsculas, podría usar admin para iniciar sesión en NetWitness Suite, pero no podría usar Admin.

4. Haga clic en **Aplicar**. Los ajustes de seguridad se aplican de inmediato. Si una contraseña vence, el usuario recibe un indicador que le solicita cambiar la contraseña cuando inicia sesión en NetWitness Suite.

Paso 4. (Opcional) Configurar la autenticación externa

En este tema se describen los métodos de autenticación externa compatibles con NetWitness Suite.

Cuando un usuario inicia sesión, NetWitness Suite primero trata de realizar la autenticación localmente. Si no se encuentra un usuario local y la configuración de autenticación externa está habilitada, se hace un intento de autenticar de forma externa.

La autenticación externa permite a los usuarios que no tienen una cuenta de usuario de NetWitness Suite interna iniciar sesión en NetWitness Suite y recibir permisos basados en funciones.

NetWitness Suite admite dos métodos de autenticación externa, Active Directory y módulos de autenticación con capacidad para conectarse (PAM). En los temas de esta sección se describe cómo configurar y probar cada método.

Temas

- Configurar Active Directory
- Configurar la funcionalidad de inicio de sesión PAM

Configurar Active Directory

En este tema se explica cómo configurar NetWitness Suite para usar Active Directory con el fin de autenticar nombres de inicio de sesión del usuario externos.

Cuando un usuario inicia sesión, NetWitness Suite primero trata de realizar la autenticación localmente. Si no se encuentra ningún usuario local y la configuración de Active Directory está activada, se realiza un intento de autenticación con Active Directory Service. Puede configurar los ajustes de Active Directory para habilitar la autenticación de grupos externos en Admin > vista Seguridad > pestaña Ajustes de configuración.

En un ambiente con múltiples servidores de autenticación, el reenvío de LDAP permite el seguimiento de referencias de LDAP para búsquedas de grupos de AD. El reenvío de LDAP puede aumentar el tiempo requerido para iniciar sesión, ya que las búsquedas de grupos de AD se extienden a servidores de autenticación conectados. Cuando su instancia de AD intenta ponerse en contacto con las controladoras de dominio que su firewall bloqueó, los usuarios pueden experimentar un retraso de varios minutos cuando inician sesión en NetWitness Suite. NetWitness Suite tiene una opción de configuración que especifica si se produce el reenvío de LDAP; de manera predeterminada, las referencias de LDAP están deshabilitadas. Cuando están deshabilitadas, la instancia de AD no intenta ponerse en contacto con las controladoras de dominio de referencia.

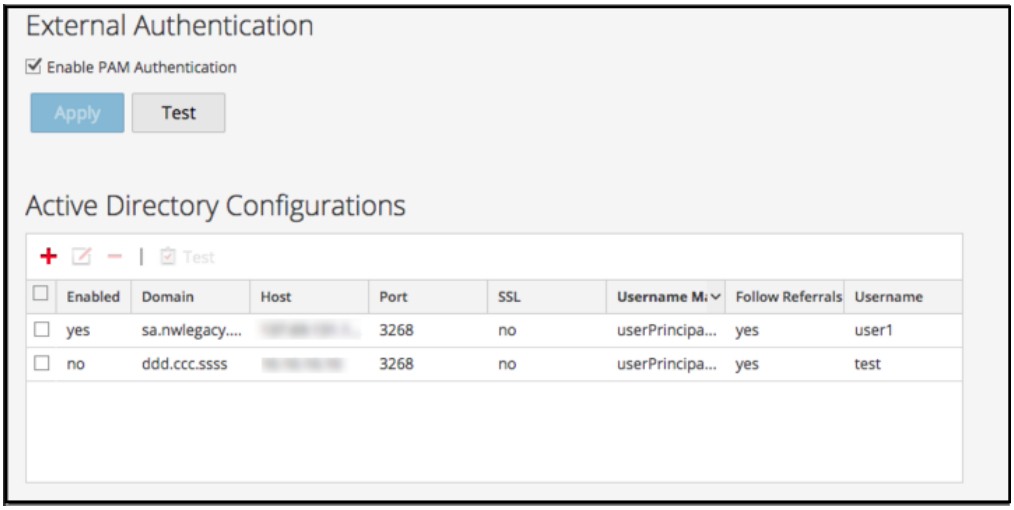
Nota: La pestaña Ajustes de configuración también ofrece la opción para permitir la configuración de PAM, que se puede usar simultáneamente con configuraciones de Active Directory. Para obtener información sobre cómo habilitar y configurar la autenticación de PAM, consulte Configurar la funcionalidad de inicio de sesión PAM.

Procedimientos

Configurar la autenticación de Active Directory

1. Vaya a **ADMIN > Seguridad**.
   La vista Seguridad se muestra con la pestaña **Usuarios** abierta.
2. Haga clic en la pestaña **Ajustes de configuración**.
   Se muestra la lista Configuraciones de Active Directory en el panel para que pueda agregar

o editar una configuración.



3. Agregue, edite o elimine dominios de ser necesario, como se describe en las siguientes secciones.

   Los dominios que se agregan en esta lista se completan automáticamente en la pestaña Mapeo de grupo externo para que pueda mapear funciones de seguridad a cada grupo.

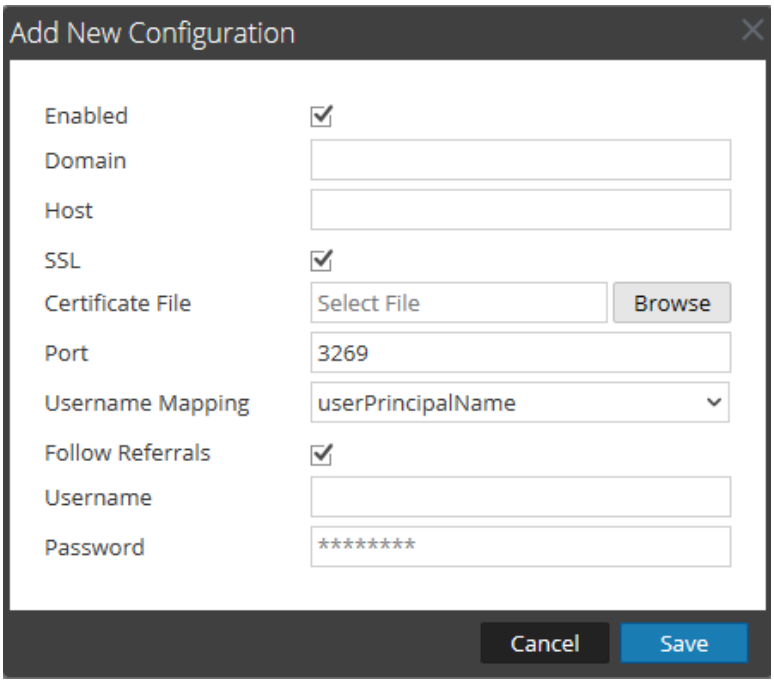
Nota: Para configurar las funciones de seguridad que se usan para el acceso de Active Directory, consulte Paso 5. (Opcional) Mapear funciones de usuario a grupos externos.

Agregar una nueva configuración de Active Directory

Para agregar una nueva configuración de Active Directory en la lista Configuraciones de Active Directory Configurations:

1. En Configuraciones de Active Directory, haga clic en +.

   Se muestra el cuadro de diálogo Agregar nueva configuración.



2. Haga clic en la casilla de verificación **Activado**.
3. Ingrese la información de **Dominio**, **Host** y **Puerto** para el servicio de Active Directory.
4. (Opcional) Para seleccionar SSL para esta configuración, seleccione la casilla de verificación **Usar SSL**. A continuación, debe ingresar un archivo de certificado. Para ello, haga clic en **Navegar** y seleccione el archivo de su preferencia para cargar. Si el servidor de AD usa un certificado público con la firma de CA, no es necesario cargar un certificado. Si el servidor de AD utiliza un certificado autofirmado, debe cargar el certificado de CA o el certificado autofirmado
5. En el campo **Mapeo de nombres de usuario**, seleccione el campo de búsqueda de Active Directory que se usará para el mapeo de nombre de usuario. Puede seleccionar userPrincipalName (UPN) o sAMAccountName.
6. Para sitios que tengan múltiples servidores de autenticación, haga clic en **Seguir referencias** para activar o desactivar el seguimiento de referencias de LDAP para búsquedas de grupos de AD.
7. Para proporcionar credenciales para vincular al servicio Active Directory mientras busca un grupo de Active Directory, ingrese las credenciales en los campos **Nombre de usuario** y **Contraseña**.

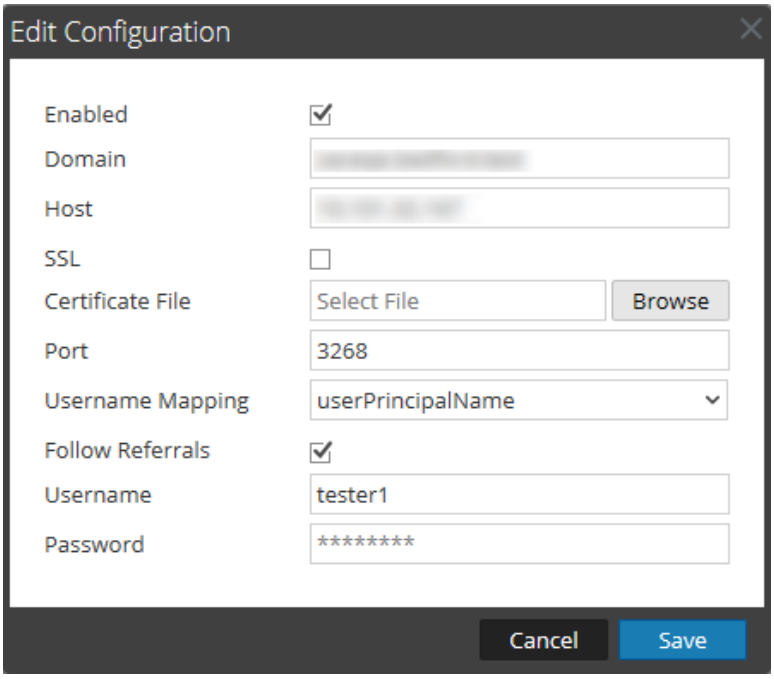
Nota: Si seleccionó sAMAccountName en el campo **Mapeo de nombres de usuario**, debe ingresar el nombre de usuario en el formato “dominio\usuario” para autenticar.

8. Haga clic en **Guardar**.
   La nueva configuración aparece en la lista Configuraciones de Active Directory.

Editar una configuración de Active Directory

Para editar una configuración de Active Directory en la lista Configuraciones de Active Directory:

1. En **Configuraciones de Active Directory**, seleccione la configuración que desea editar y haga clic en .
   Se muestra el cuadro de diálogo Editar configuración.



2. (Opcional) Ingrese la información de **Dominio**, **Host** y **Puerto** para el servicio de Active Directory.
3. (Opcional) Para seleccionar SSL para esta configuración, seleccione la casilla de verificación **Usar SSL**. A continuación, debe ingresar un archivo de certificado. Para ello, haga clic en **Navegar** y seleccione el archivo de su preferencia.
4. (Opcional) En el campo **Mapeo de nombres de usuario**, seleccione el campo de búsqueda de Active Directory que se usará para el mapeo de nombre de usuario.
5. Para especificar el comportamiento de Seguir referencias de LDAP en ambientes con múltiples servidores de autenticación, haga clic en la casilla de verificación **Seguir referencias**.

a. Si desea desactivar el reenvío de LDAP, deseleccione la casilla.

b. Si desea activar el reenvío de LDAP, marque la casilla de verificación.

6. Para proporcionar credenciales para vincular al servicio Active Directory mientras busca un grupo de Active Directory, ingrese las credenciales en los campos **Nombre de usuario** y **Contraseña**.

7. Haga clic en **Guardar**.
   La configuración aparece en la lista Configuraciones de Active Directory.

Probar una configuración de Active Directory

Para probar una configuración de Active Directory:

1. Seleccione la configuración que desea probar desde la lista Configuraciones de Active Directory.

2. En la barra de herramientas, haga clic en Test.
   Se muestra un mensaje que indica que la prueba fue exitosa.

3. Si la prueba no se realiza correctamente, revise y edite la configuración.

Elimina una configuración de Active Directory

Para eliminar una configuración de Active Directory:

1. En Configuraciones de Active Directory, seleccione la configuración que desea eliminar desde la lista Configuraciones de Active Directory.

2. En la barra de herramientas, haga clic en −.
   Se muestra un mensaje que advierte que todos los usuarios en la configuración de Active Directory seleccionada no podrán iniciar sesión en NetWitness Suite si esta se elimina.

3. Realice una de las siguientes acciones:

   a. Para confirmar la eliminación, haga clic en **Sí**.

   b. Para cancelar la eliminación, haga clic en **No**.

Configurar la funcionalidad de inicio de sesión PAM

En este tema se explica cómo configurar NetWitness Suite para usar módulos de autenticación con capacidad para conectarse (PAM) con el fin de autenticar nombres de inicio de sesión del usuario externos.

La funcionalidad de inicio de sesión PAM implica dos componentes por separado:

- PAM para la autenticación de usuarios
- NSS para la autorización de grupos

En conjunto, proporcionan a los usuarios externos la funcionalidad de iniciar de sesión en NetWitness Suite sin disponer de una cuenta interna de NetWitness Suite y de recibir permisos o funciones según el mapeo del grupo externo a una función de seguridad de NetWitness Suite. Se requieren ambos componentes para que un inicio de sesión se realice correctamente.

La autenticación externa es una configuración en el nivel del sistema. Antes de configurar PAM, revise cuidadosamente toda la información que se presenta aquí.

Pluggable Authentication Modules

PAM es una biblioteca que proporciona Linux, cuyo objetivo es autenticar usuarios en proveedores de autenticación, como RADIUS, Kerberos o LDAP. Para su implementación, cada proveedor de autenticación usa un módulo propio, el cual tiene la forma de un paquete del sistema operativo (SO), como pam_ldap. Para autenticar usuarios, NetWitness Suite usa la biblioteca de PAM que proporciona el SO y el módulo que la biblioteca de PAM está configurada para usar.

Nota: PAM solo proporciona la capacidad de autenticar.

Name Service Switch

NSS es una función de Linux que proporciona bases de datos que usan el SO y las aplicaciones para descubrir información, como nombres de host, y atributos de usuario, como el directorio principal, el grupo primario y el shell de inicio de sesión, y para enumerar a los usuarios que pertenecen a un determinado grupo. De forma similar a PAM, NSS se puede configurar y usa módulos para interactuar con distintos tipos de proveedores. NetWitness Suite usa funcionalidades de NSS que proporciona el SO para autorizar a usuarios externos de PAM, para lo cual consulta si NSS conoce a un usuario y después solicita a NSS los grupos de los cuales ese usuario es miembro. NetWitness Suitecompara los resultados de la solicitud con el mapeo de grupo externo de NetWitness Suite y, si se encuentra un grupo coincidente, se otorga acceso al usuario para iniciar sesión en NW con el nivel de seguridad definido en el mapeo de grupo externo.

Nota: NSS no proporciona autenticación.

Combinación de PAM y NSS

Tanto PAM (autenticación) como NSS (autorización) deben ejecutarse correctamente para que un usuario externo reciba autorización para iniciar sesión en NetWitness Suite. El procedimiento para configurar y solucionar problemas de PAM es diferente del procedimiento para configurar y solucionar problemas de NSS. Los ejemplos de PAM de esta guía incluyen Kerberos, LDAP y Radius. Los ejemplos de NSS incluyen Samba, LDAP y UNIX. Las necesidades del sitio determinan la combinación de módulos PAM y NSS que se usa.

Descripción general del proceso

Para configurar la funcionalidad de inicio de sesión PAM, siga las instrucciones de este documento para realizar cada paso:

1. Configurar y probar el módulo PAM.
2. Configurar y probar el servicio NSS.
3. Habilitar PAM en Servidor de NetWitness.
4. Crear mapeos de grupo en Servidor de NetWitness.

Requisitos previos

Antes de comenzar con la configuración de PAM, revise el procedimiento y recopile detalles del servidor de autenticación externa según el módulo PAM que desea implementar.

Antes de comenzar con la configuración de NSS, revise el procedimiento, identifique los nombres de grupo que usará en el mapeo de grupo externo y recopile detalles del servidor de autenticación externa según el servicio NSS que está en uso.

Antes de comenzar con la configuración de PAM en NetWitness Suite, identifique los nombres de grupo que usará en el mapeo de grupo externo. Cuando se mapean funciones, la función en NetWitness Suite debe coincidir con un nombre de grupo existente en el servidor de autenticación externa.

Configurar y probar el módulo PAM

Elija una de las siguientes secciones para configurar el componente PAM:

- Kerberos en PAM
- LDAP en PAM
- RADIUS en PAM
- SecurID

Kerberos en PAM

Puertos de comunicación Kerberos: TCP 88

Para configurar la autenticación PAM mediante Kerberos:

1. Ejecute el siguiente comando (pero primero, verifique que el paquete `krb5-workstation` esté instalado en su ambiente):
   `yum install krb5-workstation pam_krb5`
2. Edite las siguientes líneas del archivo de configuración de Kerberos `/etc/krb5.conf`. Reemplace las variables, delimitadas por <paréntesis angulares> por sus valores y omita los paréntesis angulares. Ponga atención al requisito de mayúsculas/minúsculas donde se indica.

```
# Configuration snippets may be placed in this directory as well
includedir /etc/krb5.conf.d/

[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 dns_lookup_realm = false
 ticket_lifetime = 24h
 dns_lookup_kdc = true
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = <DOMAIN.COM>
 default_ccache_name = KEYRING:persistent:%{uid}

[realms]
 <DOMAIN.COM> = {
 kdc = <SERVER.DOMAIN.COM>
 admin_server = <SERVER.DOMAIN.COM>
 }

 [domain_realm]
 <domain.com> = <DOMAIN.COM>
 <.domain.com> = <DOMAIN.COM>
```

3. Pruebe la configuración de Kerberos con el comando:
   `kinit <user>@<DOMAIN.COM>`

Si no hay ninguna salida después de ingresar la contraseña, la operación se realizó correctamente.

4. Edite el archivo de configuración de Servidor de NetWitness PAM, `/etc/pam.d/securityanalytics`, para agregar la siguiente línea. Si el archivo no existe, créelo y agregue la siguiente línea:
   `auth sufficient pam_krb5.so no_user_check`

Con esto finaliza la configuración de Kerberos en PAM. Ahora, continúe con la sección siguiente, *Configurar y probar el servicio NSS*.

LDAP en PAM

Puertos de comunicación de LDAP: TCP 389 o TCP 636

TCP 389 se puede usar para el tráfico no cifrado y, en la mayoría de los casos, cifrado y generalmente es suficiente. La mayoría de las implementaciones de LDAP modernas son compatibles con el comando `start_tls` una vez que se conectan al puerto 389, lo cual actualiza la conexión de un estado no cifrado a uno cifrado. En esta instancia, las URI de LDAP comienzan con `ldap://`, incluso cuando se usa `start_tls`.

TCP 636 se usa solo en instancias donde el servidor de LDAP no es compatible con el comando `start_tls`. En este caso, las URI de LDAP comienzan con `ldaps://` y el comando `start_tls` no se usa.

Para configurar la autenticación PAM mediante LDAP:

1. Ejecute el siguiente comando (pero primero, verifique que el paquete `openldap-clients` esté instalado en su ambiente):
   `yum install nss-pam-ldapd openldap-clients`
2. Edite el archivo de configuración de LDAP, `/etc/nslcd.conf`, como se muestra en el siguiente ejemplo:

Nota: Reemplace las variables, delimitadas por <paréntesis angulares> por sus valores y omita los paréntesis angulares. Ponga atención al requisito de mayúsculas/minúsculas donde se indica.

Ejemplo de entradas del archivo `/etc/nslcd.conf`:

```
uri ldap://<server.domain.com>
 base <dc=domain,dc=com>
 binddn <cn=bineuser,dc=domain,dc=com>
 bindpw <secret>
```

3. Después de modificar el archivo `/etc/nslcd.conf`, ejecute el siguiente comando:
   `systemctl restart nslcd`

4. (Opcional) Para habilitar el transporte seguro para la comunicación LDAP con verificación de certificado de par (más segura), consulte la página de manuales de Linux de nslcd para obtener la modificación del código correcta para el archivo `/etc/nslcd.conf`.

   Nota: de manera predeterminada, el transporte de LDAP seguro no está activado en los controladores de dominio de Windows. Requieren la instalación de un certificado de servidor para la autenticación del servidor. La obtención y la instalación de este certificado en los DC están fuera del alcance de este documento. En https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx encontrará orientación relacionada con este tema.

5. (Opcional) Para habilitar el transporte seguro para la comunicación LDAP sin certificado de par, consulte la página de manuales de Linux de nslcd para obtener la modificación del código correcta para el archivo `/etc/nslcd.conf`.

6. Para solucionar problemas de configuración de LDAP, primero detenga el servicio `nslcd` mediante el ingreso del siguiente comando:
   ```
   systemctl stop nlscd
   ```

7. Para enviar información de solución de problemas y estado como salida desde el servicio a la consola, ejecute el servicio `nslcd` en modo de depuración desde la línea de comandos:
   ```
   nslcd -d
   ```

8. Edite el archivo de configuración de Servidor de NetWitness PAM, `/etc/pam.d/securityanalytics`, para agregar la siguiente línea. Si el archivo no existe, créelo y agregue la siguiente línea:
   ```
   auth sufficient pam_ldap.so
   ```

Con esto finaliza la configuración de LDAP en PAM. Ahora, continúe con la sección siguiente, *Configurar y probar el servicio NSS*.

RADIUS en PAM

Puertos de comunicación de Radius: UDP 1812 o UDP 1813

Para configurar la autenticación de PAM mediante Radius, debe agregar el servidor Servidor de NetWitness a la lista de clientes del servidor de Radius y configurar una seña secreta compartida. Póngase en contacto con el administrador del servidor de Radius para este procedimiento.

Para configurar la autenticación de PAM para RADIUS mediante LDAP:

1. Ejecute el siguiente comando (pero primero, verifique que el paquete `pam_radius` esté instalado en su ambiente):
   ```
   yum install pam_radius
   ```

2. Edite el archivo de configuración de RADIUS, `/etc/raddb/server`, de la siguiente manera:

```
# server[:port] shared_secret  timeout (s)
server    secret     3
```

3. Edite el archivo de configuración de Servidor de NetWitness PAM, `/etc/pam.d/securityanalytics`, para agregar la siguiente línea. Si el archivo no existe, créelo y agregue la siguiente línea:

```
auth sufficient pam_radius_auth.so
```

Precaución: Para que RADIUS en PAM funcione, los archivos `/etc/raddb/server` deben tener permiso de escritura. El comando necesario para esto es: `chown netwitness:netwitness /etc/raddb/server`.

Los módulos de PAM y los servicios asociados envían información como salida a `/var/log/messages` y `/var/log/secure`. Estas salidas se pueden usar como ayuda en la solución de problemas de configuración.

El siguiente procedimiento es un ejemplo de los pasos para configurar la autenticación de PAM para RADIUS mediante SecurID:

Nota: Los ejemplos de estas tareas usan RSA Authentication Manager como el servidor RADIUS.

1. Ejecute el siguiente comando (pero primero, verifique que el paquete `pam_radius` esté instalado en su ambiente):

```
yum install pam_radius
```

2. Edite el archivo de configuración de RADIUS, `/etc/raddb/server`, y actualícelo con el nombre de host de instancia del Authentication Manager, la seña secreta compartida y el valor de tiempo de espera agotado:

```
# server[:port] shared_secret timeout (s)

 111.222.33.44         secret        1

 #other-server        other-secret  3

 192.168.12.200:6369  securid       10
```

Nota: Debe comentar las líneas `127.0.0.1` y `other-server`, y agregar la dirección IP de la instancia primaria de Authentication Manager con el número de puerto de RADIUS (por ejemplo, `192.168.12.200:1812`), la seña secreta compartida de RADIUS y un valor de tiempo de espera agotado de 10.

3. Edite el archivo de configuración de Servidor de NetWitness PAM, `/etc/pam.d/securityanalytics`, para agregar la siguiente línea. Si el archivo no

existe, créelo y agregue la siguiente línea:

```
auth sufficient pam_radius_auth.so
```

Nota: Puede agregar `debug` al final de la línea anterior en el archivo `/etc/pam.d/securityanalytics` para habilitar la depuración de PAM (por ejemplo, `auth sufficient pam_radius_auth.so debug`)

Los módulos de PAM y los servicios asociados envían información como salida a `/var/log/messages` y `/var/log/secure`. Estas salidas se pueden usar para ayudar a solucionar problemas de configuración.

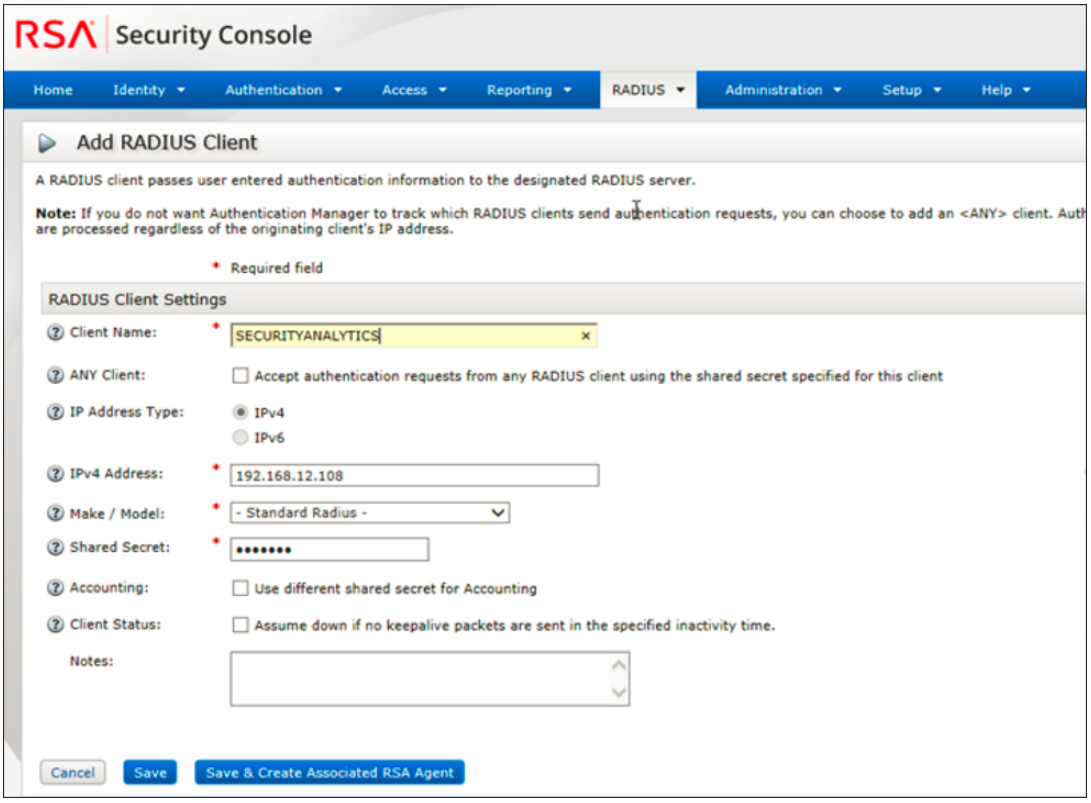
Agregar un cliente de RADIUS y un agente asociado

Nota: Los ejemplos de estas tareas usan RSA Authentication Manager como el servidor RADIUS.
Debe usar las credenciales de cuenta administrativa para iniciar sesión en la consola de seguridad de RSA Authentication Manager.

Para agregar un cliente de RADIUS y un agente asociado:

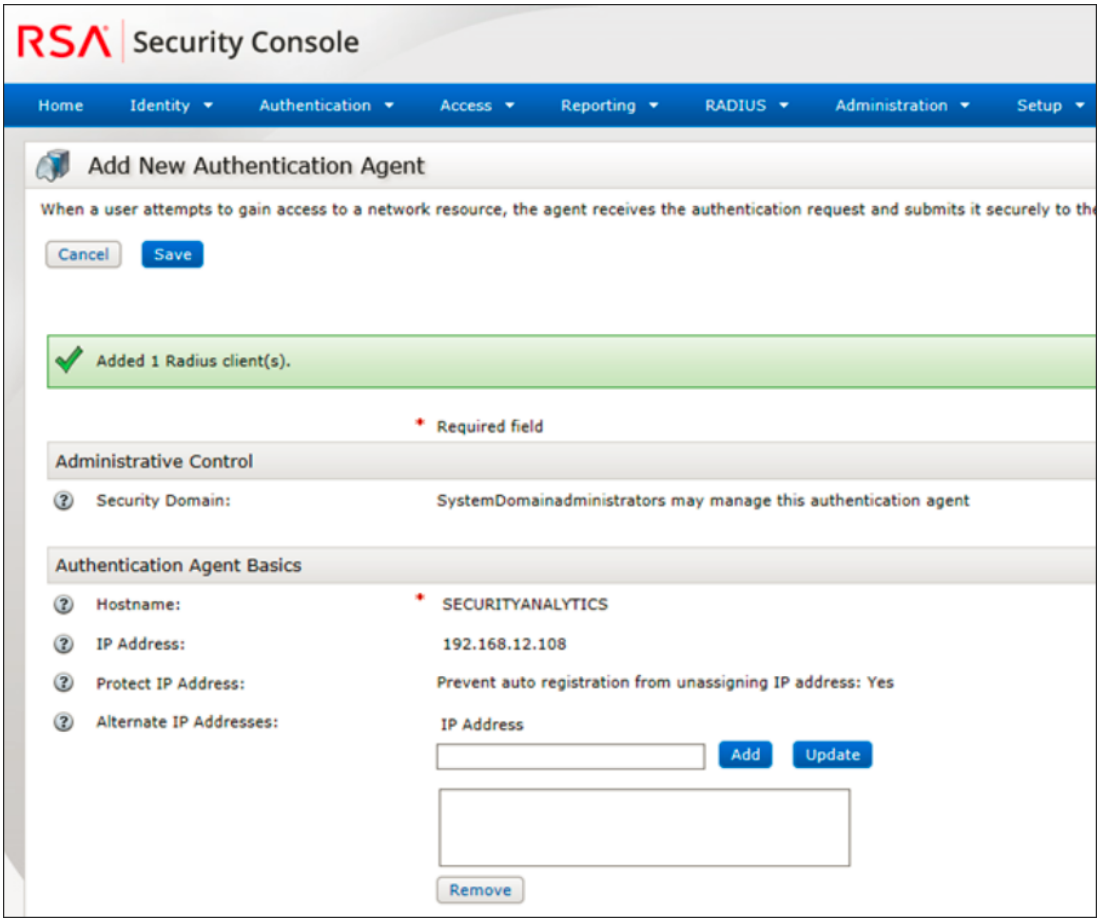
1. Inicie sesión en RSA Authentication Manager.
   Se muestra la consola de seguridad.
2. En la Consola de seguridad, haga clic en **RADIUS > Cliente de RADIUS > Agregar nuevo**.

Se muestra la página Agregar cliente de RADIUS.



3. En Configuración del cliente de RADIUS, proporcione la siguiente información:
   a. En el campo **Nombre de cliente**, escriba el nombre del cliente, por ejemplo, NetWitness Suite.
   b. En el campo **Dirección IPv4**, ingrese la dirección IPv4 del cliente de RADIUS, por ejemplo, 192.168.12.108.
   c. En la lista desplegable **Marca/modelo**, seleccione el tipo de cliente de RADIUS, por ejemplo, Fortinet.
   d. En el campo **Seña secreta compartida**, ingrese la seña secreta compartida de autenticación.

4. Haga clic en **Guardar y crear agente de RSA asociado**.



5. Haga clic en **Guardar**.

Si la instancia de Authentication Manager no puede encontrar el agente de autenticación en la red, se muestra una página de advertencia. Haga clic en **Sí, guardar agente**.

Para obtener más información, consulte el tema Agregar un cliente de RADIUS en *Guía del Administrador de RSA Authentication Manager 8.2*.

Con esto finaliza la configuración de RADIUS en PAM. Ahora, continúe con la sección siguiente, *Configurar y probar el servicio NSS*.

Agente PAM para SecurID

Puerto de comunicación de PAM: UDP 5500

Requisitos previos
El módulo PAM de RSA SecurID solo es compatible en las siguientes condiciones:

1. Las conexiones de confianza deben estar habilitadas y en funcionamiento entre NetWitness Suite y los servicios principales.

Descripción general del proceso

Los pasos generales para configurar el módulo PAM de SecurID son:

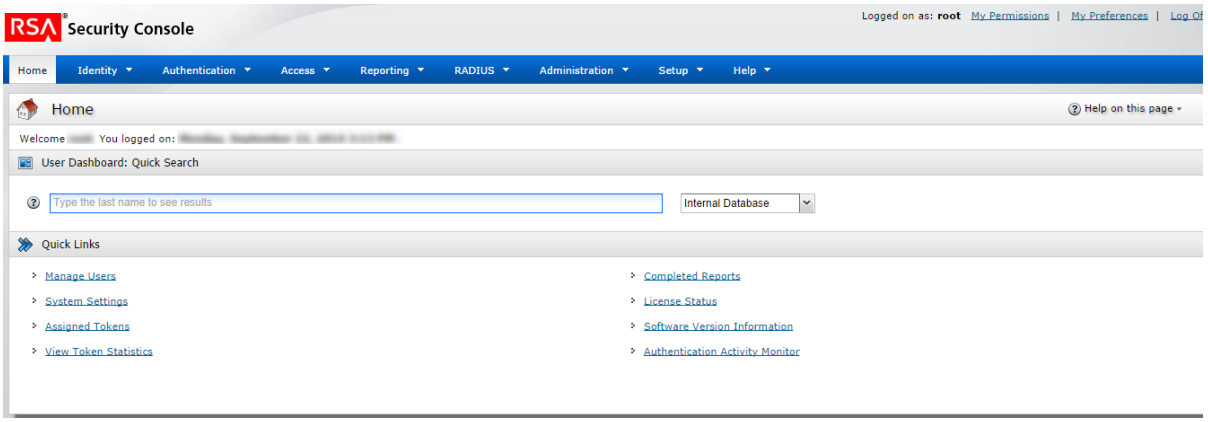
1. Configurar **Authentication Manager**:
   a. Agregar el agente de autenticación.
   b. Descargar el archivo de configuración.
2. Configurar **Servidor de NetWitness**:
   a. Copiar el archivo de configuración desde Authentication Manager y personalizarlo.
   b. Instalar el módulo SecurID en PAM.
3. Probar la conectividad y la autenticación.

Posteriormente, siga los procedimientos restantes de las secciones que se indican a continuación:

- Configurar NSS.
- Habilitar PAM en Servidor de NetWitness.
- Configurar mapeos de grupo en Servidor de NetWitness.

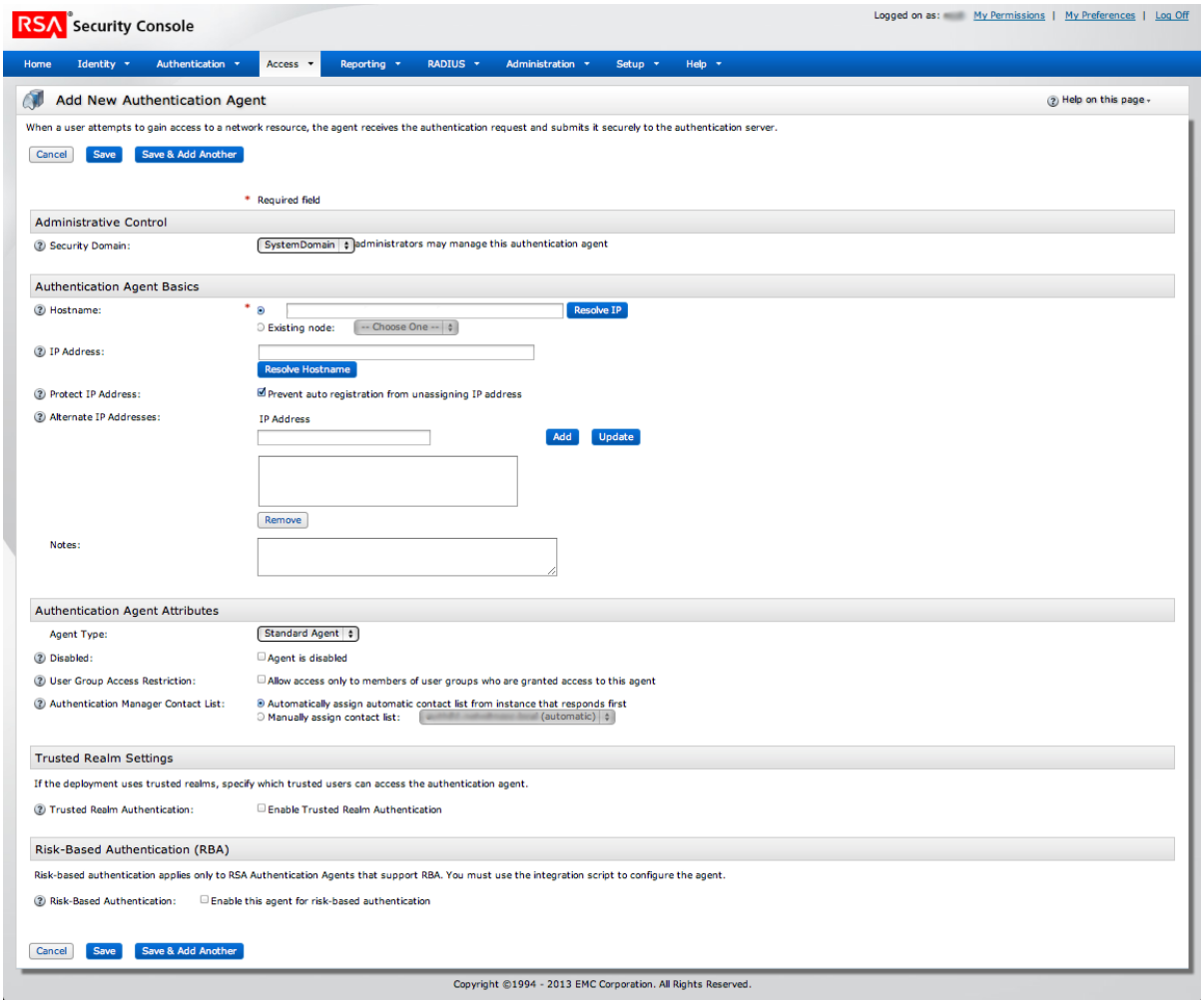
Para configurar Authentication Manager:

1. Inicie sesión en RSA Authentication Manager.
   Se muestra la Consola de seguridad.

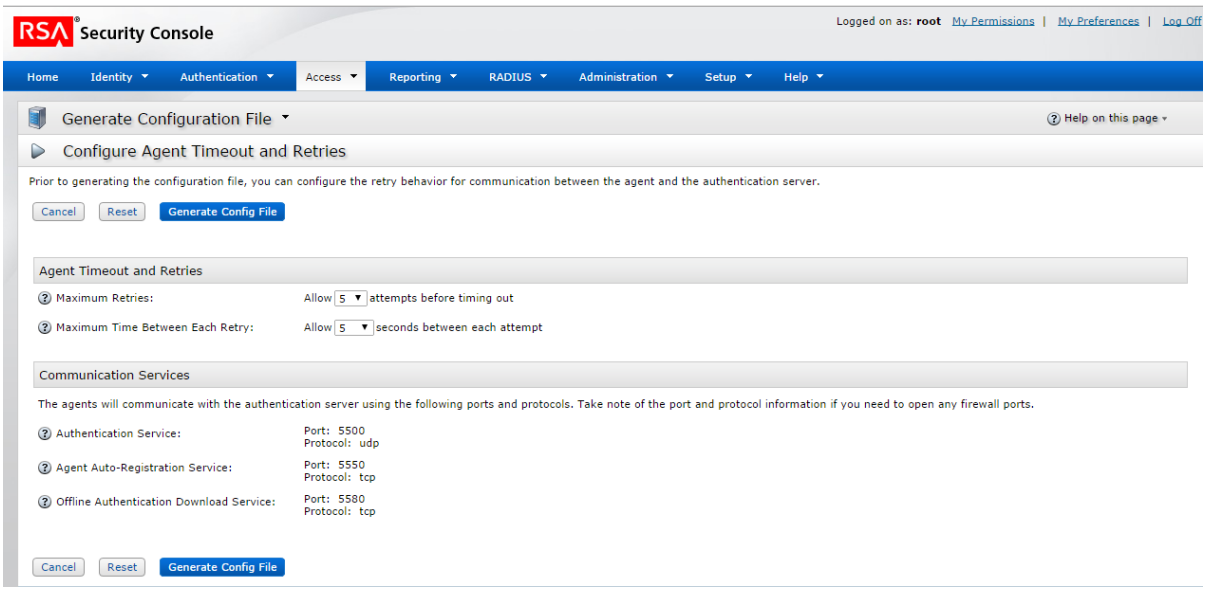


2. En la Consola de seguridad, agregue un nuevo agente de autenticación.
   Haga clic en **Acceso > Agentes de autenticación > Agregar nuevo.**

Se muestra la página Agregar nuevo agente de autenticación.



3. En el campo **Nombre de host**, escriba el nombre de host del Servidor de NetWitness.
4. Haga clic en **Resolver dirección IP**.
   La dirección IP del Servidor de NetWitness se muestra automáticamente en el campo **Dirección IP**.
5. Conserve la configuración predeterminada y haga clic en **Guardar**.
6. Genere un archivo de configuración.
   Vaya a **Acceso > Agentes de autenticación > Generar archivo de configuración**.
   Se muestra la página Generar archivo de configuración.



7. Conserve los valores predeterminados y haga clic en **Generar archivo de configuración**. Esto crea **AM_Config.zip**, el cual contiene dos archivos.
8. Haga clic en **Descargar ahora**.

Para instalar y configurar el módulo SecurID en PAM:

1. En el Servidor de NetWitness, cree un directorio:
   `mkdir /var/ace`
2. En el Servidor de NetWitness, copie `sdconf.rec` desde el archivo .zip a `/var/ace`.
3. Cree un archivo de texto `sdopts.rec` en el directorio `/var/ace`.
4. Inserte la siguiente línea:
   `CLIENT_IP=<IP address of Servidor de NetWitness>`
5. Instale el agente de autorización de SecurID para PAM, el cual está disponible en el repositorio YUM:
   `yum install sid-pam-installer`
6. Ejecute el script de instalación:
   `/opt/rsa/pam-agent-installer/install_pam.sh`
7. Siga los indicadores para aceptar o cambiar los valores predeterminados.
8. Edite el archivo de configuración de Servidor de NetWitness PAM, `/etc/pam.d/securityanalytics`, para agregar la siguiente línea. Si el archivo no existe, créelo y agregue la siguiente línea:
   `auth sufficient pam_securid.so`

Con esto finaliza la instalación del módulo SecurID en PAM. A continuación, pruebe la conectividad y la autenticación. Posteriormente, siga los procedimientos que se indican en Configurar y probar el servicio NSS.

Nota: Si la configuración de PAM SecurID no está completa, puede bloquearse el servidor Jetty y la interfaz del usuario de NetWitness Suite no se mostrará. Debe esperar hasta que finalice la configuración de autenticación de PAM y, a continuación, reinicie el servidor Jetty.

Para probar la conectividad y la autenticación:

1. Ejecute `/opt/pam/bin/64bit/acetest` e ingrese **username** y **passcode**.
2. (Opcional) Si acetest falla, active la depuración:
   ```
   vi/etc/sd_pam.conf
   RSATRACELEVEL=15
   ```
3. Ejecute `/opt/pam/bin/64bit/acestatus`. La salida es la siguiente
   ```
   RSA ACE/Server Limits
    ---------------------
    Configuration Version : 15 Client Retries : 5
    Client Timeout : 5 DES Enabled : Yes

   RSA ACE/Static Information
    -------------------------
    Service : securid Protocol : udp Port Number : 5500

   RSA ACE/Dynamic Information
    --------------------------
    Server Release : 8.1.0.0 Communication : 5

   RSA ACE/Server List
    ------------------
    Server Name :  auth81.netwitness.local
    Server Address :  192.168.100.10
    Server Active Address : 192.168.100.10
    Master : Yes Slave : No Primary : Yes
    Usage : Available for Authentications
   ```
4. (Opcional) Para solucionar problemas del servidor de Authentication Manager, vaya a **Reporting > Monitores de actividad en tiempo real > Monitor de actividad de autenticación.**
   A continuación, haga clic en **Iniciar monitor**.
5. Si cambió la configuración, restablezca RSATRACELEVEL a 0:
   ```
   vi/etc/sd_pam.conf
   RSATRACELEVEL=0
   ```

Precaución: Después de la instalación, verifique que VAR_ACE en el archivo `/etc/sd_pam.conf` señale la ubicación correcta del archivo sdconf.rec. Esta es la ruta a los archivos de configuración. El comando necesario para esto es: `chown -R netwitness:netwitness /var/ace`.

Con esto finaliza la configuración de Agente PAM para SecurID. Ahora, continúe con la sección siguiente, *Configurar y probar el servicio NSS*.

Configurar y probar el servicio NSS

Elegir un servicio NSS

Existen tres opciones para el servicio NSS: Samba, LDAP y UNIX. Las tres tienen ventajas y desventajas.

Ventajas de Samba en NSS	Desventajas de Samba en NSS
Especialmente diseñado para Active Directory	No se puede usar con back-ends que no pertenecen a AD
Requiere configuración mínima en Active Directory o no la requiere en absoluto	La configuración y la solución de problemas pueden ser más difíciles
No se requieren cuentas de usuario especiales	Requiere que la máquina de Servidor de NW esté unida al dominio de Active Directory
	Usa muchos puertos para comunicarse con Active Directory; la implementación es más difícil a través de firewalls y proxies

Ventajas de LDAP en NSS	Desventajas de LDAP en NSS
La configuración básica es más simple	Puede requerir configuración y funciones adicionales dentro de Active Directory
Puede comunicarse con cualquier implementación de LDAP	Requiere la configuración de una cuenta de vinculación de LDAP

Ventajas de LDAP en NSS	Desventajas de LDAP en NSS
Usa un único puerto TCP para la comunicación; es más fácil trabajar con firewalls y proxies	El transporte seguro es más difícil de habilitar a menos que esté configurado para no validar los certificados del servidor
No requiere la unión del host de NW a un dominio de AD	

UNIX en NSS

No se requiere configuración para habilitar el módulo UNIX en NSS; está habilitado de manera predeterminada en el sistema operativo del host. Para autorizar a un usuario para un grupo específico, agréguelo simplemente al sistema operativo y a un grupo:

1. Cree el grupo del SO que usará y agregue el usuario externo con este comando:
   `groupadd <groupname>`
2. Agregue el usuario externo al SO con este comando:
   `adduser -G <groupname> -M -N <externalusername>`

Nota: Observe que esto NO permite ni autoriza el acceso a la consola del Servidor de NW.

Con esto finaliza la configuración de UNIX en NSS. A continuación, vaya a Probar la funcionalidad de NSS.

Samba en NSS

Puertos de comunicación de AD Winbind

Los siguientes puertos corresponden al mínimo que debe estar abierto según las pruebas internas para permitir la funcionalidad Samba en NSS. Estos se proporcionan solo como referencia.

TCP 88: Kerberos
TCP 139: Netbios
TCP 389: LDAP
UDP 53: DNS
UDP 88: Kerberos
UDP 389: LDAP

Pueden ser necesarios puertos adicionales, según los requisitos de implementación específicos del sitio. Consulte el siguiente artículo para obtener información sobre todos los puertos que puede requerir la comunicación de Active Directory: http://technet.microsoft.com/en-us/library/dd772723%28ws.10%29.aspx

Para configurar Samba en NSS:

1. Edite el archivo de configuración de Samba, `/etc/samba/smb.conf`, de la siguiente manera. Reemplace las variables, delimitadas por <paréntesis angulares> por sus valores y omita los paréntesis angulares. Ponga atención al requisito de mayúsculas/minúsculas donde se indica.

```
[global]
 workgroup = domain
 netbios name = <NW_APPLIANCE_HOSTNAME>
 password server = <ADSERVER.DOMAIN.COM>
 realm = <DOMAIN.COM>

 local master = no
 security = ads
 syslog only = yes
 log file = /var/log/samba/log.%m
 max log size = 5120
 idmap config * : range = 16777216-33554431
 template shell = /bin/bash
 winbind use default domain = true
 winbind offline logon = false
 winbind enum groups = yes
```

2. Para habilitar e iniciar el servicio de vinculación de Windows, `winbind`, escriba los siguientes comandos:

```
systemctl enable winbind
systemctl start winbind
```

3. Edite el archivo de configuración de NSS, `/etc/nsswitch.conf`. Actualice solo las 2 entradas siguientes y conserve todos los demás valores predeterminados:

```
passwd:     files winbind
group:      files winbind
```

4. Para unirse al dominio, escriba el siguiente comando:

```
net ads join -U <DomainAdminUser>
```

5. Para almacenar el SID del controlador de dominio, escriba el siguiente comando:

```
net rpc getsid -S <SERVER.DOMAIN.COM>
```

6. Pruebe la funcionalidad de NSS como se describe en la sección *Probar la funcionalidad de NSS*.

7. Cuando haya confirmado que NSS funciona correctamente desde la línea de comandos, para reiniciar el host de modo que se apliquen los cambios en NSS, escriba el siguiente comando.
   `reboot`

Para solucionar problemas de Samba en NSS:

Para comprobar si Winbind en NSS puede comunicarse correctamente con Active Directory:

1. Escriba los siguientes comandos:
   `wbinfo -u` para obtener una lista de usuarios de AD
   `wbinfo -g` para obtener una lista de grupos de AD
2. Si ninguno de los comandos se ejecuta correctamente, ejecute `winbind` en el modo de depuración de la consola mediante el ingreso de los siguientes comandos:
   ```
   systemctl stop winbind
   winbindd -S -F -d <optional debugleve 0-10>
   ```
3. Desde una sesión del protocolo SSH por separado, repita el paso 1 y observe la salida de `winbindd` para ver si hay alguna señal del problema.
   Aumente el detalle de la depuración de `winbindd` según sea necesario.
4. Realice los ajustes necesarios en `/etc/samba/smb.conf`.
5. En la ventana de depuración de `winbindd` del paso 2, detenga `winbindd` mediante el ingreso de `CTRL-C`.
   Repita los pasos 1 y 2 y continúe con la solución de problemas hasta que los comandos `wbinfo` se ejecuten correctamente.
6. Cuando los comandos `wbinfo` se hayan ejecutado correctamente, use los comandos `getent` de la sección Probar la funcionalidad de NSS de esta guía para probar NSS.
   ```
   getent passwd <pamUser>
   getent group <groupOfPamUser>
   ```
7. Cuando `getent` se haya ejecutado correctamente, detenga la línea de comandos `winbindd` mediante el ingreso de `CTRL-C` y escriba el siguiente comando para iniciar el demonio del servicio:
   ```
   systemctl start winbind
   ```

Si `wbinfo -g` se ejecuta correctamente desde la línea de comandos, pero la búsqueda del mapeo de grupo externo no muestra ningún grupo de Active Directory:

1. Agregue la siguiente línea a `/etc/samba/smb.conf`:
   ```
   allow trusted domains = no
   ```
2. Escriba `systemctl restart winbind .`

Con esto finaliza la configuración de Samba en NSS. A continuación, vaya a Probar la funcionalidad de NSS.

LDAP en NSS

Nota: Estas instrucciones requieren que todos los objetos de usuario de PAM y de grupo de NSS de Active Directory tengan sus atributos `uidNumber` y `gidNumber` configurados en números de UID y GID estilo UNIX para que LDAP en NSS pueda usarlos. Es posible que esquemas de Active Directory más antiguos no tengan estos atributos de manera predeterminada. Los esquemas de AD más nuevos pueden tener estos atributos, pero puede que no estén definidos en cada objeto. La configuración correcta de estos atributos escapa del alcance de este documento. Póngase en contacto con el administrador de Active Directory para que defina estos atributos para los usuarios de PAM y los grupos de NSS.

Para usar NSS, se debe crear un usuario de vinculación de LDAP en Active Directory. Este usuario se debe configurar de modo que su contraseña no venza. Debido a que estas credenciales se deben especificar en texto sin formato para el servicio LDAP en NSS, los permisos de `/etc/nslcd.conf` se deben dejar en su valor predeterminado de 600 de modo que los usuarios del sistema, con excepción del usuario raíz, no puedan leer el archivo.

Puertos de comunicación de LDAP: TCP 389 o TCP 636

TCP 389 se puede usar para el tráfico no cifrado y, en la mayoría de los casos, cifrado y generalmente es suficiente. La mayoría de las implementaciones de LDAP modernas son compatibles con el comando `start_tls` una vez que se conectan al puerto 389, lo cual actualiza la conexión de un estado no cifrado a uno cifrado. En esta instancia, las URI de LDAP comienzan con `ldap://`, incluso cuando se usa `start_tls`.

TCP 636 se usa solo en instancias donde el servidor de LDAP no es compatible con el comando `start_tls`. En esta instancia, las URI de LDAP comienzan con `ldaps://` y el comando `start_tls` no se usa.

Para configurar el módulo NSS para LDAP con Active Directory:

1. Obtenga el paquete `nss-pam-ldapd` del repositorio SMCUPDATE o del repositorio de actualización de Servidor de NetWitness si el servidor está sincronizado con SMCUPDATE. Esto requiere una cuenta de Live configurada en NetWitness Suite.
2. Ejecute el siguiente comando para instalar el paquete:
   ```
   yum install nss-pam-ldapd
   ```
3. Edite `/etc/nslcd.conf` para incluir las siguientes líneas y asegúrese de dejar como comentario todas las líneas existentes en el archivo mediante una marca hash # en el comienzo de la línea:
   ```
   uid nslcd
   gid ldap
   uri ldap://<server.domain.com>
   base <dc=domain,dc=com>
   binddn <cn=binduser,dc=domain,dc=com
   bindpw <secret>
   ```
   Nota: Debe agregar mapeos adicionales entre las búsquedas de NSS y las búsquedas de LDAP para su ambiente específico. Consulte la página de los manuales Linux para nslcd para obtener detalles específicos.
4. (Opcional) Para habilitar el transporte seguro para la comunicación LDAP con verificación de certificado de par (más segura), consulte la página de manuales de Linux de nslcd para obtener la modificación del código correcta para el archivo `/etc/nslcd.conf`.

Nota: de manera predeterminada, el transporte de LDAP seguro no está activado en los controladores de dominio de Windows. Requieren la instalación de un certificado de servidor para la autenticación del servidor. La obtención y la instalación de este certificado en los DC están fuera del alcance de este documento. Encontrará orientación relacionada con este tema en la siguiente URL: https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx

5. (Opcional) Para habilitar el transporte seguro para la comunicación LDAP sin certificado de par, consulte la página de manuales de Linux de nslcd para obtener la modificación del código correcta para el archivo `/etc/nslcd.conf`.
6. Edite el archivo de configuración de NSS, `/etc/nsswitch.conf`. Actualice solo las dos entradas siguientes y deje las demás en sus valores predeterminados:
   ```
   passwd:files ldap
   group:files ldap
   ```

7. Para habilitar e iniciar el servicio NSLCD, escriba estos comandos:
   ```
   systemctl enable nslcd
   systemctl start nslcd
   ```
8. Pruebe la funcionalidad de NSS de acuerdo con lo que se indica en la sección *Probar la funcionalidad de NSS*. Si las pruebas de NSS fallan, solucione problemas de LDAP en NSS, como se describe en *Solucionar problemas de LDAP en NSS*.
9. Cuando haya confirmado que NSS funciona correctamente desde la línea de comandos, reinicie el host de modo que se apliquen los cambios en NSS.
   ```
   reboot
   ```

Para solucionar problemas de LDAP en NSS:

1. Para solucionar problemas de LDAP en NSS, primero detenga el servicio nslcd mediante el ingreso del siguiente comando:
   ```
   systemctl stop nslcd
   ```
2. Para enviar información de solución de problemas y estado como salida desde el servicio a la consola, ejecute el servicio nslcd en modo de depuración desde la línea de comandos.
   ```
   nslcd -d
   ```
3. (Opcional) Para aumentar el detalle de la depuración, agregue una d adicional varias veces al final de nslcd -d; por ejemplo, escriba el siguiente comando:
   ```
   nslcd -ddd
   ```
4. Desde una sesión del protocolo SSH por separado, use los comandos `getent` de la sección Probar la funcionalidad de NSS de esta guía para probar NSS. Observe alguna indicación de dónde se está produciendo la falla en la salida de depuración de nslcd. Aumente el detalle de la depuración de nslcd según sea necesario.
   ```
   getent passwd <pamUser>
   getent group <groupOfPamUser>
   ```
5. Realice los ajustes necesarios en `/etc/nslcd.conf` de acuerdo con la salida del paso 2 o 3.
6. En la ventana de depuración de nslcd del paso 2 o 3, detenga `nslcd` con `CTRL-C`. Repita el paso 2 o 3 y continúe con la solución de problemas hasta que el comando `getent` se ejecute correctamente.
7. Cuando `getent` se haya ejecutado correctamente, detenga la línea de comandos `nslcd` e inicie el demonio del servicio:
   ```
   systemctl start nslcd
   ```

Entre los problemas comunes se pueden incluir:

- Certificado SSL de transporte seguro de LDAP no instalado en el servidor de LDAP/AD.
- Verificación del certificado de CA fallida: deje como comentario la línea `tls_cacert` en `/etc/nslcd.conf` e intente con `tls_reqcert never`. Una ejecución correcta demuestra que la verificación del certificado está fallando.
  - El certificado de CA raíz no está en el formato PEM.
  - Se usa el certificado de la CA emisora en lugar del certificado de CA raíz.
  - El nombre del certificado SSL del servidor de LDAP no coincide con su nombre de host.
- DN base incorrecto.
- El usuario de vinculación o la contraseña de LDAP no se especificaron correctamente.
- Especificación incorrecta de `ldaps://` en lugar de `ldap://` en la línea `uri` de `/etc/nslcd.conf`. `ldaps://` solo se debe utilizar cuando se usa LDAPS y no se usa el comando `start_tls`.
- Los usuarios y los grupos de Active Directory no tienen los atributos `uidNumber` ni `gidNumber` configurados.
- El firewall de la red está bloqueando las comunicaciones.
- El nombre de host del servidor de LDAP especificado no se puede resolver.
  - Configuración incorrecta de DNS en `/etc/resolv.conf`.
  - Se especificó un nombre de host incorrecto en la línea `uri` de `/etc/nslcd.conf`.

Con esto finaliza la configuración de LDAP en NSS. A continuación, vaya a Probar la funcionalidad de NSS.

Probar la funcionalidad de NSS

Para probar si NSS está funcionando con cualquiera de los servicios NSS anteriores, use los siguientes comandos:

```
getent passwd <pamUser>
 getent group <groupOfPamUser>
```

La salida debe ser similar a:

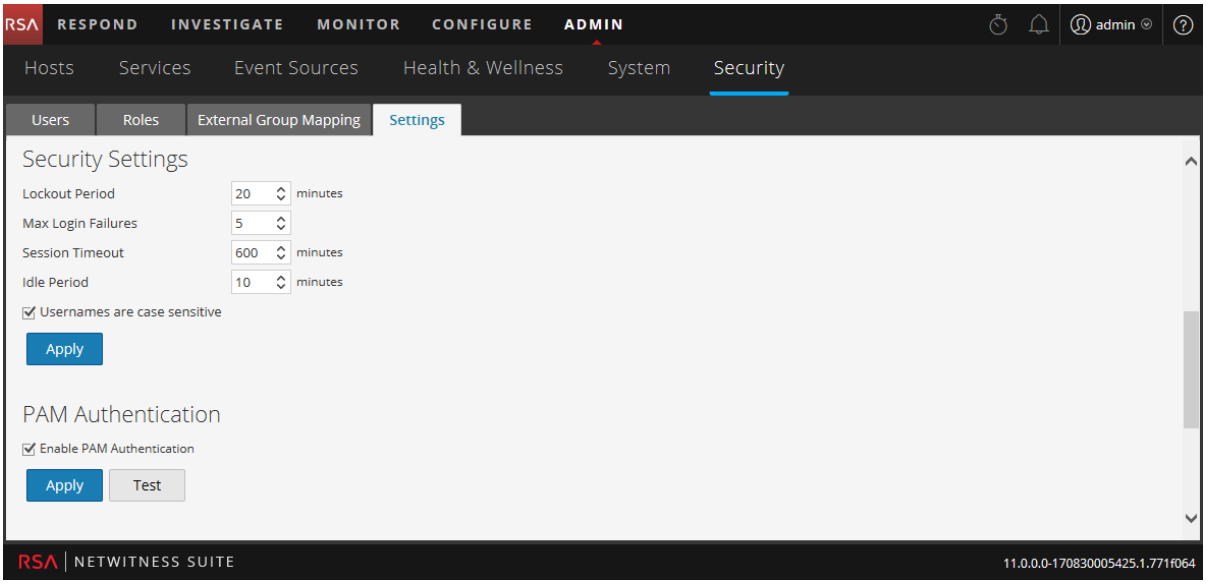
```
[root@~]# getent passwd myuser
 myuser:*:10000:10000::/home/myuser:/bin/sh
[root@~]# getent group mygroup
 mygroup:*:10000:myuser3
```

- Si ninguno de los comandos produce salida, NSS no está funcionando correctamente para la autorización externa. Consulte la orientación sobre la solución de problemas correspondiente a su módulo NSS que se proporciona en este documento.
- Si los comandos `getent` se ejecutan correctamente y la autenticación correcta se confirma en `/var/log/secure`, pero NetWitness Suite continúa sin permitir el inicio de sesión de usuarios externos:
  - ¿Se especificó el nombre de grupo correcto para el grupo NSS en el mapeo de grupo externo de NW? Consulte Activar PAM y crear mapeos de grupo a continuación.
  - Es posible que la configuración de NSS haya cambiado y que NetWitness Suite no haya reconocido el cambio. Un reinicio del host de NetWitness Suite hará que NetWitness Suite reconozca los cambios en la configuración de NSS. Un reinicio de `jetty` no es suficiente.

Continúe con la sección siguiente, Habilitar PAM en Servidor de NetWitness.

Habilitar PAM en Servidor de NetWitness

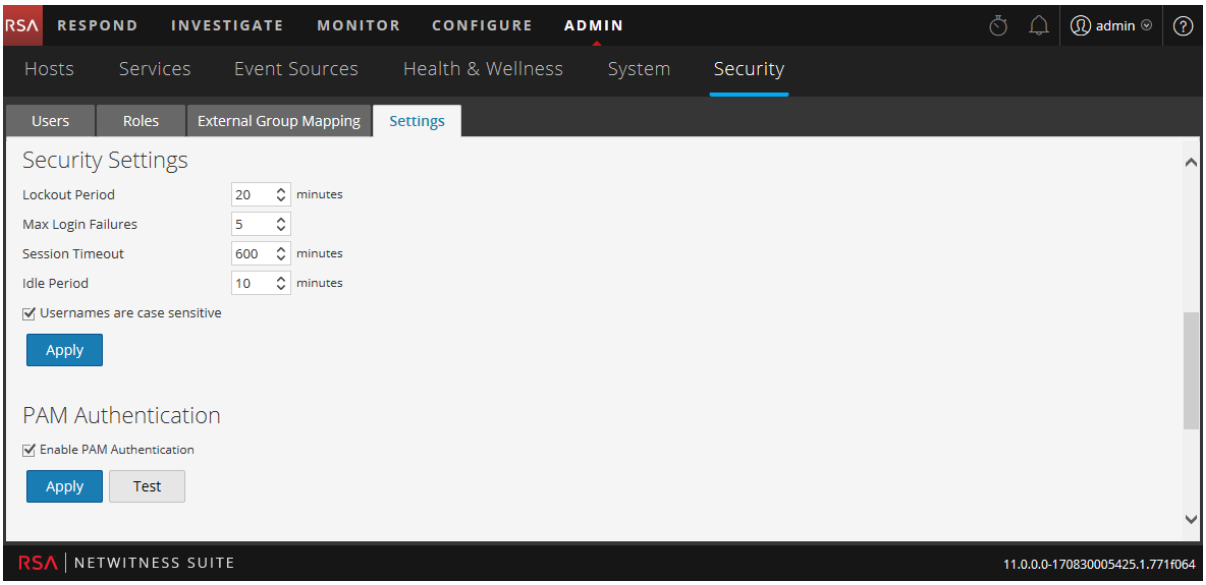
1. En NetWitness Suite, vaya a **ADMIN > Seguridad**.
   La vista Admin > Seguridad se muestra con la pestaña Usuarios abierta.
2. Haga clic en la pestaña **Ajustes de configuración**.
3. En **Autenticación de PAM**, seleccione **Habilitar autenticación de PAM** y haga clic en **Aplicar**.



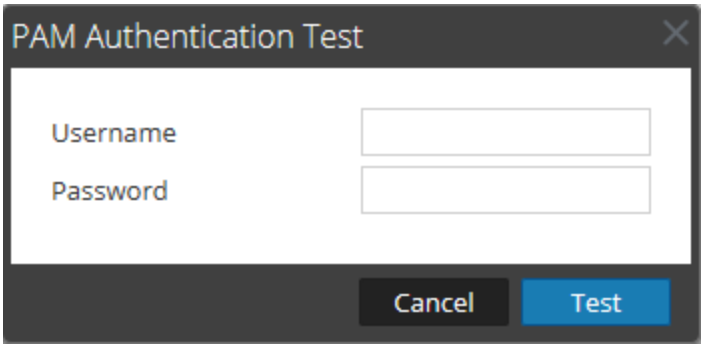
Probar la autenticación de PAM

Para probar la autenticación externa de PAM:

1. Vaya a **ADMIN > Seguridad**.
   La vista Seguridad se muestra con la pestaña **Usuarios** abierta.
2. Haga clic en la pestaña **Ajustes de configuración**.
3. En **Autenticación de PAM**, seleccione **Habilitar autenticación de PAM**.



4. En las opciones de **Autenticación de PAM**, haga clic en **Probar.**
   Se muestra el cuadro de diálogo **Prueba de autenticación de PAM**.



5. Escriba un nombre de usuario y una contraseña para los que desee probar su autenticación mediante la configuración actual de PAM.
6. Haga clic en **Probar**.
   Se prueba el método de autenticación externa para garantizar la conectividad.
7. Si la prueba no se realiza correctamente, revise y edite la configuración.

PAM se habilita y las configuraciones de Active Directory también permanecen habilitadas. Las configuraciones de PAM se completan automáticamente en la pestaña Mapeo de grupo externo, de modo que pueda mapear las funciones de seguridad a cada grupo. Para configurar las funciones de seguridad que se usan para el acceso de PAM, consulte el Paso 5. (Opcional) Mapear funciones de usuario a grupos externos.

Cómo funciona el control de acceso basado en funciones

En este tema se explica el control de acceso basado en funciones (RBAC) cuando hay una conexión de confianza entre el servidor de Servidor de NetWitness y un servicio principal.

En RSA NetWitness® Suite, las funciones determinan lo que pueden hacer los usuarios. Una función tiene permisos asignados y se debe asignar una función a cada usuario. El usuario tiene entonces permiso para hacer lo que la función le permite.

Funciones preconfiguradas

Para simplificar el proceso de creación de funciones y asignación de permisos, existen funciones preconfiguradas en NetWitness Suite. También puede agregar funciones personalizadas para su organización.

En la siguiente tabla se indica cada función preconfigurada y sus permisos asignados. La función Administradores tiene asignados todos los permisos. Un subconjunto de permisos está asignado a cada una de las otras funciones.

Función	Permiso
Administradores	Acceso completo al sistema. El perfil Administradores del sistema cuenta con todos los permisos de forma predeterminada.
Operadores	Acceso a configuraciones, pero no a metadatos ni a contenido de sesiones. El perfil Operadores del sistema se centra en la configuración del sistema, pero no en Investigation, ESA, Alerting, Reporting y Respond.
Analistas	Acceso a metadatos y contenido de sesiones, pero no a configuraciones. El perfil Analistas del centro de operaciones de seguridad (SOC) se centra en Investigation, ESA, Alerting, Reporting y Respond, pero no en la configuración del sistema.
Respond_ Administrator	Acceda a todos los permisos de Respond.

Función	Permiso
SOC_Managers	El mismo acceso que poseen los analistas, además del permiso adicional para manejar incidentes. El perfil Administradores del SOC es idéntico al de los Analistas, pero tiene los permisos necesarios para configurar Respond.
Malware_ Analysts	Acceso a investigaciones y eventos de malware. El único acceso que se otorga al perfil Analistas de malware es almódulo Malware Analysis.
Data_Privacy_ Officers	El perfil Encargado de la privacidad de datos (DPO) es similar al de los Administradores, pero tiene un enfoque adicional en opciones de configuración que administran el ocultamiento y la visualización de datos confidenciales dentro del sistema (consulte *Administración de la privacidad de datos*). Los usuarios a los cuales se asigna la función DPO pueden ver qué claves de metadatos están marcadas para ocultamiento y también ven claves de metadatos y valores ocultos creados para las claves de metadatos marcadas.

Conexiones de confianza entre el servidor y un servicio

En una conexión de confianza, un servicio confía explícitamente en el servidor de Servidor de NetWitness para administrar y autenticar usuarios. Esto disminuye la administración en cada servicio, ya que los usuarios autenticados no se deben definir localmente en cada servicio principal.

Como indica la siguiente tabla, se realizan todas las tareas de administración de usuarios en el servidor.

Tarea	Ubicación
Agregar un usuario	Servidor
Mantener nombres de usuario	Servidor
Mantener contraseñas	Servidor
Autenticar usuarios de NetWitness Suite internos	Servidor

Tarea	Ubicación
(Opcional) Autenticar usuarios externos con:	
- Active Directory	Servidor
- PAM	Servidor
Instalar y configurar PAM	Servidor

Los beneficios de una conexión de confianza y de la administración de usuarios centralizada son:

- Todas las tareas de administración de usuarios se realizan una vez, solo en el servidor de Servidor de NetWitness.
- Puede controlar el acceso a los servicios, pero no tiene que configurar y autenticar usuarios en los servicios.
- Los usuarios ingresan contraseñas una vez en el inicio de sesión de NetWitness Suite y el servidor los autentica.
- Los usuarios, que el servidor ya autenticó, acceden a cada servicio principal en ADMIN > Servicios sin ingresar una contraseña.

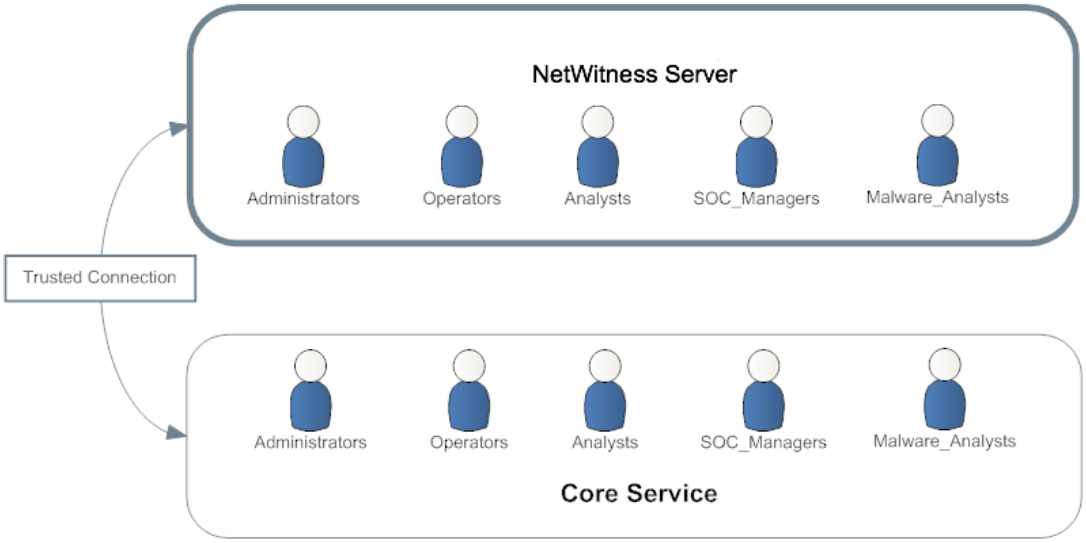
Cómo se establecen conexiones de confianza

Cuando instala o realiza una actualización a 11.0, las conexiones de confianza se establecen de manera predeterminada con dos configuraciones:

1. SSL está activado.
2. El servicio principal está conectado a un puerto SSL cifrado.

Nombres de función comunes en el servidor y los servicios

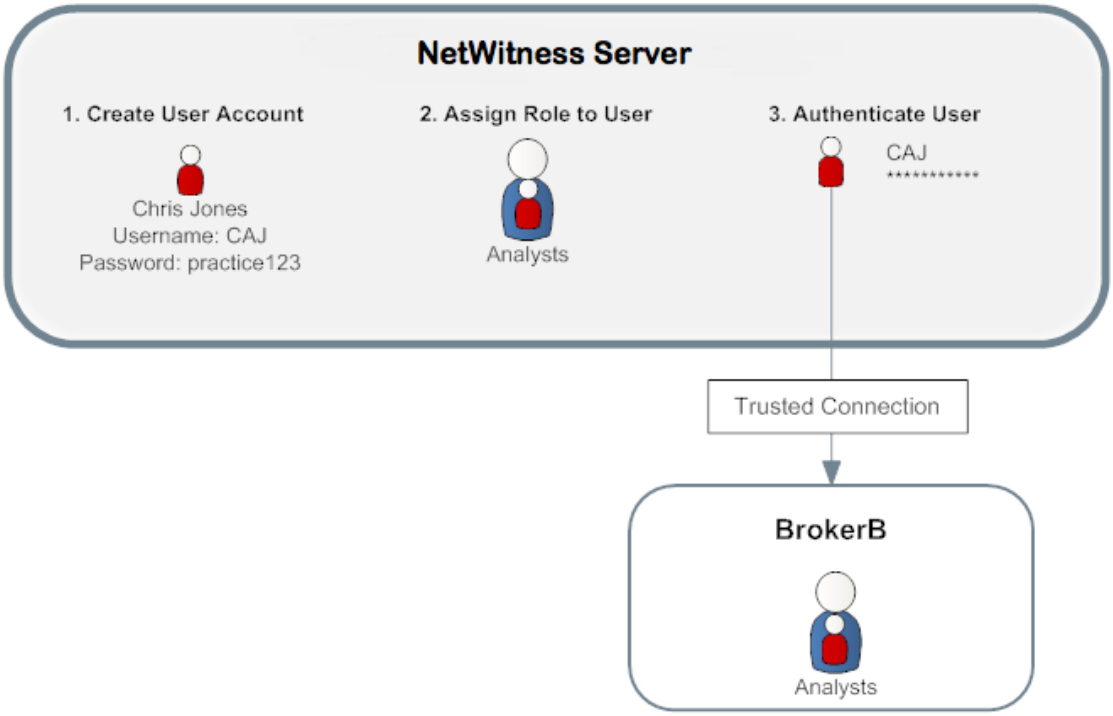
Las conexiones de confianza dependen de los nombres de función comunes en el servidor y los servicios. En una instalación nueva, NetWitness Suite instala las cinco funciones preconfiguradas en el servidor y cada servicio principal.



Si agrega una función personalizada, como JuniorAnalysts, debe agregarla a cada servicio, como ArchiverA y BrokerB. Los nombres de función distinguen mayúsculas de minúsculas, no pueden incluir espacios y deben ser idénticos. Por ejemplo, JuniorAnalyst (singular) y JuniorAnalysts (plural) no coinciden con los requisitos de nombres de función comunes.

Flujo de trabajo de punto a punto para la configuración de usuarios y acceso a servicios

Este flujo de trabajo muestra cómo funciona el control de acceso basado en funciones cuando hay una conexión de confianza entre Servidor de NetWitness y el BrokerB de servicio.



1. En Servidor de NetWitness, cree una cuenta para un nuevo usuario:
   Nombre: Chris Jones
   Nombre de usuario: CAJ
   Contraseña: practice123
2. Determine si desea asignar una función preconfigurada o personalizada a Chris Jones:
   - **Función preconfigurada**
     a. Mantenga o modifique los permisos predeterminados asignados a la **función Analistas**, que incluye permisos como acceso a los módulos Alerting, Investigation y Malware,
     b. Asigne la función Analistas a Chris Jones.
   - **Función personalizada**
     a. Cree la función personalizada, como JuniorAnalysts.
     b. Asigne permisos a la **función JuniorAnalysts**.
     c. Asigne la función JuniorAnalysts a Chris Jones.
     d. Agregue la función JuniorAnalysts al servicio, como BrokerB.
3. El usuario, Chris Jones, inicia sesión en Servidor de NetWitness:
   Nombre de usuario: CAJ

Contraseña: practice123

4. El servidor autentifica a Chris.
5. La conexión de confianza permite que el usuario autenticado, Chris, acceda a BrokerB sin ingresar otra contraseña.

Para obtener descripciones y procedimientos más detallados, consulte Administrar usuarios con funciones y permisos.

Tema relacionado

- Permisos de función

Permisos de función

En este tema se describe el acceso a la interfaz del usuario que tienen de manera predeterminada los usuarios asignados a las funciones incorporadas de NetWitness Suite.

En NetWitness Suite, el acceso de los usuarios a cada módulo, dashlet y vista está restringido según los permisos asignados que se describen en este tema. Puede encontrar estos permisos de funciones en los cuadros de diálogo Agregar función o Editar función, accesibles en la pestaña Admin > Seguridad > Funciones.

En los cuadros de diálogo Agregar función o Editar función, las pestañas de la sección Permisos representan diferentes áreas de la NetWitness Suite y muestran los permisos disponibles para esas áreas. Por ejemplo, la pestaña Administration muestra los permisos disponibles en la vista Admin.

Nota: No hay ninguna pestaña Configurar en los cuadros de diálogo Agregar función/Editar función que corresponda a la vista Configurar. Para asignar permisos en la vista Configurar, asigne permisos a las vistas que incluye la vista Configurar: Contenido de Live (Live), Reglas de incidentes (Incidents), Reglas de ESA (Alerting), Suscripciones (Live) y Feeds personalizados (Live).

Nota: A la izquierda de la pestaña Administration hay una pestaña marcada con un asterisco (*). Esta pestaña indica acceso a la administración de los servicios de back-end solamente.

Las tablas siguientes muestran los permisos predeterminados asignados a cada función de usuario de NetWitness Suite:

- Administradores
- Operadores
- Analistas
- Administrador de Respond
- Administradores del SOC (Admin. del SOC)
- Analistas de Malware (MA)
- Encargados de la privacidad de datos (DPO)

Dado que la función Administradores tiene todos los permisos de forma predeterminada, no se incluye en las tablas.

Formato de los permisos de servicios para servicios nuevos

Los permisos de servicios para algunos servicios NetWitness Suite nuevos contienen tres partes en el siguiente formato:

<service name>.<resource>.<action>

Por ejemplo, para el permiso **investigate-server.metrics.read**:

- nombre del servicio = **investigate-server**
- recurso = **metrics**
- acción = **read**

Los usuarios que tienen asignado este permiso pueden leer cualquier métrica que exponga el servicio Servidor de Investigate.

Administration

En la siguiente tabla se indican los permisos de la pestaña Administration asignados a cada función. La función Administradores tiene todos los permisos de forma predeterminada y no se enumera.

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
Acceder al modulo Administration	Sí	Sí	Sí	Sí	Sí
Estado y condición de acceso	Sí	Sí	Sí	Sí	Sí
Aplicar actualizaciones del sistema	Sí				
Puede optar por participar en el uso compartido de inteligencia de Live.	Sí				
Administrar auditoría global	Sí				Sí
Administrar política de estado y condición	Sí				
Administrar configuración avanzada	Sí				
Administrar auditoría	Sí				Sí

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
Administrar correo electrónico	Sí				
Administrar LLS	Sí				
Administrar registros	Sí				Sí
Administrar notificaciones	Sí				
Administrar plug-ins	Sí				
Administrar predicados	Sí				
Administrar reconstrucción	Sí				
Administrar seguridad	Sí				Sí
Administrar servicios	Sí				Sí
Administración de la configuración del sistema	Sí				
Modificar la configuración de ESA	Sí				
Modificar orígenes de eventos	Sí				
Modificar hosts	Sí				
Modificación de servicios	Sí				Sí
Ver orígenes de eventos	Sí		Sí		
Ver política de estado y condición	Sí	Sí	Sí		
Vista del navegador de estadísticas de estado y condición	Sí	Sí	Sí		Sí

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
Ver hosts	Sí				Sí
Vista de servicios	Sí				Sí

Servidor de Admin

En la siguiente tabla se describen los permisos de la pestaña Servidor de Admin. La función Administradores tiene todos los permisos y es la única que otorga permisos de forma predeterminada.

Permiso	Descripción
admin-server.configuration.manage	Permiso para ver y modificar todos los parámetros de configuración de servicios
admin-server.health.read	Permiso para leer las notificaciones de estado que expone el servicio
admin-server.logs.manage	Permiso para cambiar la configuración relacionada con el registro
admin-server.metrics.read	Permiso para leer las métricas que expone el servicio
admin-server.process.manage	Permiso para iniciar y detener el servicio
admin-server.security.manage	Permiso para editar los recursos relacionados con la seguridad (contraseñas, claves, etc.)
admin-server.security.read	Permiso para leer los recursos relacionados con la seguridad

Alertas

En la siguiente tabla se indican los permisos de la pestaña Alerting asignados a cada función. La función Administradores tiene todos los permisos de forma predeterminada y no se enumera.

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
Acceder al módulo Alerting	Sí	Sí	Sí		Sí
Administrar reglas	Sí		Sí		Sí
Ver alertas		Sí	Sí		Sí
Ver reglas	Sí		Sí		Sí

Servidor de Config

En la siguiente tabla se describen los permisos de la pestaña Servidor de Config. La función Administradores tiene todos los permisos y es la única que otorga permisos de forma predeterminada.

Permiso	Descripción
config-server.*	Todos los permisos (todo lo que aparece a continuación)
config-server.configuration.manage	Permiso para ver y modificar todos los parámetros de configuración de servicios
config-server.health.read	Permiso para leer las notificaciones de estado que expone el servicio
config-server.logs.manage	Permiso para cambiar la configuración relacionada con el registro
config-server.metrics.read	Permiso para leer las métricas que expone el servicio
config-server.process.manage	Permiso para iniciar y detener el servicio
config-server.security.manage	Permiso para editar los recursos relacionados con la seguridad (contraseñas, claves, etc.)
config-server.security.read	Permiso para leer los recursos relacionados con la seguridad

Tablero

En la siguiente tabla se indican los permisos de la pestaña Tablero asignados a cada función. La función Administradores tiene todos los permisos de forma predeterminada y no se enumera.

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
Acceso a dashlet: dashlet Lista de dispositivos de administración	Sí	Sí	Sí		Sí
Acceso a dashlet: dashlet Monitor de dispositivo de administración	Sí				Sí
Acceso a dashlet: dashlet Novedades de administración	Sí	Sí	Sí		Sí
Acceso a dashlet: dashlet Diferencia de alertas		Sí	Sí		Sí
Acceso a dashlet: dashlet Alertas recientes de Alerting		Sí	Sí		Sí
Acceso a dashlet: dashlet de trabajos de investigación		Sí	Sí		Sí
Acceso a dashlet: dashlet Valores principales de Investigation		Sí	Sí		Sí
Acceso a dashlet: dashlet Recursos destacados de Live	Sí	Sí	Sí		Sí
Acceso a dashlet: dashlet de recursos nuevos de Live	Sí	Sí	Sí		Sí
Acceso a dashlet: dashlet de suscripciones a Live	Sí	Sí	Sí		Sí

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
Acceso a dashlet: dashlet de recursos actualizados de Live	Sí	Sí	Sí		Sí
Acceso a dashlet: dashlet Trabajos de malware		Sí	Sí		Sí
Accesoa dashlet: dashlet Informe reciente de Reporting		Sí	Sí		Sí
Acceso a dashlet: dashlet Gráficos de Reporting		Sí	Sí		Sí
Acceso a dashlet: dashlet Alertas principales		Sí	Sí		Sí
Acceso a dashlet: dashlet RSA First Watch de Unified	Sí	Sí	Sí		Sí
Acceso a dashlet: dashlet Accesos directos de Unified	Sí	Sí	Sí		Sí

Servidor de ESA Analytics

En la siguiente tabla se describen los permisos de la pestaña Servidor de ESA Analytics. Las funciones Administradores y Operadores tienen todos los permisos y son las únicas a las que se les otorga permisos de forma predeterminada.

Permiso	Descripción
esa-analytics-server.*	Todos los permisos (todo lo que aparece a continuación)
esa-analytics-server.analytics.manage	Permiso para ver y modificar ESA Analytics
esa-analytics-server.analytics.read	Permiso para ver ESA Analytics

Permiso	Descripción
esa-analytics-server.configuration.manage	Permiso para ver y modificar todos los parámetros de configuración de servicios
esa-analytics-server.health.read	Permiso para leer las notificaciones de estado que expone el servicio
esa-analytics-server.logs.manage	Permiso para cambiar la configuración relacionada con el registro
esa-analytics-server.metrics.read	Permiso para leer las métricas que expone el servicio
esa-analytics-server.model.manage	Permiso para ver y modificar modelos ESA
esa-analytics-server.model.read	Permiso para ver modelos ESA
esa-analytics-server.process.manage	Permiso para iniciar y detener el servicio
esa-analytics-server.security.read	Permiso para leer los recursos relacionados con la seguridad

Incidentes

En la siguiente tabla se indican los permisos de la pestaña Incidentes asignados a cada función. La función Administradores tiene todos los permisos de forma predeterminada y no se enumera.

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
Acceder al módulo Incident		Sí	Sí	Sí	Sí
Configuración de la integración de Incident Management			Sí		Sí

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
Eliminar alertas e incidentes					Sí
Administración de las reglas del manejo de alertas			Sí		Sí
Ver y administrar incidentes		Sí	Sí	Sí	Sí

Investigar

En la siguiente tabla se indican los permisos de la pestaña Investigate asignados a cada función. La función Administradores tiene todos los permisos de forma predeterminada y no se enumera.

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
Acceder al módulo Investigation		Sí	Sí	Sí	Sí
Búsqueda de contexto		Sí	Sí	Sí	
Crear incidentes desde Investigation		Sí	Sí	Sí	
Administrar lista desde Investigation		Sí	Sí	Sí	
Navegar por los eventos		Sí	Sí	Sí	Sí
Navegar por los valores		Sí	Sí	Sí	Sí

Servidor de Investigate

En la siguiente tabla se describen los permisos de la pestaña Servidor de Investigate.

Permiso	Descripción
investigate-server.*	Todos los permisos (todo lo que aparece a continuación)

Permiso	Descripción
investigate-server.configuration.manage	Permiso para cambiar las propiedades de configuración del servidor
investigate-server.health.read	Permiso para leer las notificaciones de estado que expone el servicio
investigate-server.logs.manage	Permiso para cambiar la configuración relacionada con el registro
investigate-server.metrics.read	Permiso para leer las métricas que expone el servicio
Investigate-server.process.manage	Permiso para iniciar y detener el servicio
investigate-server.security.manage	Permiso para editar los recursos relacionados con la seguridad (contraseñas, claves, etc.)
investigate-server.security.read	Permiso para leer los recursos relacionados con la seguridad

En la siguiente tabla se indican los permisos de la pestaña Servidor de Investigate asignados a cada función. La función Administradores tiene todos los permisos de forma predeterminada y no se enumera.

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
investigate-server.*		Sí	Sí	Sí	Sí
investigate-server.configuration.manage					
investigate-server.health.read					
investigate-server.logs.manage					
investigate-server.metrics.read					

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
investigate-server.process.manage					
investigate-server.security.manage					
investigate-server.security.read					

Live

En la siguiente tabla se indican los permisos de la pestaña Live asignados a cada función. La función Administradores tiene todos los permisos de forma predeterminada y no se enumera.

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
Live					
Acceder al módulo Live	Sí	Sí	Sí		Sí
Administración de la configuración del sistema de Live	Sí				
Recursos					
Implementación de recursos de Live	Sí				Sí
Administración de los feeds de Live	Sí				Sí
Administrar de recursos de Live	Sí				Sí
Buscar recursos de Live	Sí	Sí	Sí		Sí

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
Ver detalles de recursos de Live	Sí	Sí	Sí		Sí

Servidor de Orchestration

En la siguiente tabla se describen los permisos de la pestaña Servidor de Orchestration. Las funciones Administradores, Operadores y Encargados de la privacidad de datos tienen todos los permisos y son las únicas a las que se les otorga permisos de forma predeterminada.

Permiso	Descripción
orchestration-server.*	Todos los permisos (todo lo que aparece a continuación)
orchestration-server.configuration.manage	Permiso para ver y modificar todos los parámetros de configuración de servicios
orchestration-server.health.read	Permiso para leer las notificaciones de estado que expone el servicio
orchestration-server.logs.manage	Permiso para cambiar la configuración relacionada con el registro
orchestration-server.metrics.read	Permiso para leer las métricas que expone el servicio
orchestration-server.process.manage	Permiso para iniciar y detener el servicio
orchestration-server.security.manage	Permiso para editar los recursos relacionados con la seguridad (contraseñas, claves, etc.)
orchestration-server.security.read	Permiso para leer los recursos relacionados con la seguridad

Malware

En la siguiente tabla se indican los permisos de la pestaña Malware asignados a cada función. La función Administradores tiene todos los permisos de forma predeterminada y no se enumera.

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
Descarga de archivos de malware		Sí	Sí	Sí	Sí
Inicialización del escaneo de Malware Analysis		Sí	Sí	Sí	Sí
Vista de eventos de Malware Analysis		Sí	Sí	Sí	Sí

Informes

En la siguiente tabla se indican los permisos de la pestaña Informes asignados a cada función. La función Administradores tiene todos los permisos de forma predeterminada y no se enumera.

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
Alerta					
Definición de alertas de RE		Sí	Sí		Sí
Exportación de la definición de alerta de RE		Sí	Sí		Sí
Administración de alertas de RE		Sí	Sí		Sí
Vista de alertas de RE		Sí	Sí		Sí
Vista de alertas calendarizadas de RE		Sí	Sí		Sí

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
Gráfico					
Definición de gráfico		Sí	Sí		Sí
Eliminar un gráfico		Sí	Sí		Sí
Exportación de la definición de gráfico		Sí	Sí		Sí
Administrar gráficos		Sí	Sí		Sí
Vista de gráficos		Sí	Sí		Sí
Lista					
Definición de listas		Sí	Sí		Sí
Eliminar lista		Sí	Sí		Sí
Exportar lista		Sí	Sí		Sí
Administrar listas		Sí	Sí		Sí
Informe					
Definición de informes		Sí	Sí		Sí
Delete Report		Sí	Sí		Sí
Exportar un informe		Sí	Sí		Sí
Administrar informes		Sí	Sí		Sí
Vista de informe		Sí	Sí		Sí
Informes					
Acceder a la configuración		Sí	Sí		Sí
Acceder al módulo Reporter		Sí	Sí		Sí

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
Acceder a la búsqueda en Reporter		Sí	Sí		Sí
Acceder a vista		Sí	Sí		Sí
Regla					
Agregar definición de alerta de RE desde regla		Sí	Sí		Sí
Definición de una regla		Sí	Sí		Sí
Delete Rule		Sí	Sí		Sí
Exportar regla		Sí	Sí		Sí
Administrar reglas		Sí	Sí		Sí
Vista del uso de la regla		Sí	Sí		Sí
Calendarios					
Definición de un calendario		Sí	Sí		Sí
Eliminar calendario		Sí	Sí		Sí
Vista de calendarios		Sí	Sí		Sí
Warehouse Analytics					
Definir trabajos		Sí	Sí		Sí
Eliminar trabajos		Sí	Sí		Sí
Administrar trabajos		Sí	Sí		Sí
Ver trabajos		Sí	Sí		Sí

Servidor de Respond

En la siguiente tabla se describen los permisos de la pestaña Servidor de Respond.

Permiso	Descripción
respond-server.*	Todos los permisos (todo lo que aparece a continuación)
respond-server.alert.delete	Permiso para eliminar alertas
respond-server.alert.manage	Permiso para crear, actualizar o eliminar alertas
respond-server.alert.read	Permiso para ver alertas
respond-server.alertrule.manage	Permiso para crear, actualizar o eliminar reglas de agregación de alertas
respond-server.alertrule.read	Permiso para ver reglas de agregación de alertas
respond-server.configuration.manage	Permiso para cambiar las propiedades de configuración del servicio
respond-server.health.read	Permiso para leer las notificaciones de estado que expone el servicio
respond-server.incident.delete	Permiso para eliminar incidentes
respond-server.incident.manage	Permiso para crear, actualizar o eliminar incidentes
respond-server.incident.read	Permiso para ver incidentes
respond-server.journal.manage	Permiso para crear, actualizar o eliminar entradas del registro de un incidente
respond-server.journal.read	Permiso para ver las entradas del registro de un incidente

Permiso	Descripción
respond-server.logs.manage	Permiso para cambiar la configuración relacionada con el registro
respond-server.metrics.read	Permiso para leer las métricas que expone el servicio
respond-server.process.manage	Permiso para iniciar y detener el servicio
respond-server.remediation.manage	Permiso para crear, actualizar o eliminar tareas de corrección
respond-server.remediation.read	Permiso para ver las tareas de corrección
respond-server.security.manage	Permiso para editar los recursos relacionados con la seguridad (contraseñas, claves, etc.)
respond-server.security.read	Permiso para leer los recursos relacionados con la seguridad

En la siguiente tabla se indican los permisos de la pestaña Servidor de Respond asignados a cada función. Las funciones Administradores y Administrador de Respond tienen todos los permisos de forma predeterminada y no se enumeran.

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
respond-server.*					Sí
respond-server.alert.delete					
respond-server.alert.manage		Sí	Sí	Sí	
respond-server.alert.read		Sí	Sí	Sí	
respond-server.alertrule.manage			Sí		

Permiso	Operadores	Analistas	Admin. del SOC	MA	DPO
respond-server.alertrule.read			Sí		
respond-server.configuration.manage					
respond-server.health.read					
respond-server.incident.delete					
respond-server.incident.manage		Sí	Sí	Sí	
respond-server.incident.read		Sí	Sí	Sí	
respond-server.journal.manage		Sí	Sí	Sí	
respond-server.journal.read		Sí	Sí	Sí	
respond-server.logs.manage					
respond-server.metrics.read					
respond-server.process.manage					
respond-server.remediation.manage		Sí	Sí	Sí	
respond-server.remediation.read		Sí	Sí	Sí	
respond-server.security.manage					
respond-server.security.read					

Servidor de Security

En la siguiente tabla se describen los permisos de la pestaña Servidor de Security. Las funciones Administradores, Operadores y Encargados de la privacidad de datos tienen todos los permisos y son las únicas a las que se les otorga permisos de forma predeterminada.

Permiso	Descripción
security-server.*	Todos los permisos (todo lo que aparece a continuación)
security-server.account.manage	Permiso para ver, crear, modificar o quitar cuentas locales de NetWitness Suite
security-server.account.read	Permiso para ver cuentas locales de NetWitness Suite
security-server.configuration.manage	Permiso para ver y modificar todos los parámetros de configuración de servicios
security-server.health.read	Permiso para leer las notificaciones de estado que expone el servicio
security-server.logs.manage	Permiso para cambiar la configuración relacionada con el registro
security-server.metrics.read	Permiso para leer las métricas que expone el servicio
security-server.permission.manage	Permiso para crear o quitar permisos de NetWitness Suite
security-server.process.manage	Permiso para iniciar y detener el servicio
security-server.role.manage	Permiso para crear, modificar o quitar funciones de NetWitness Suite (por ejemplo, agregar permisos de función)
security-server.role.read	Permiso para ver definiciones de funciones de NetWitness Suite
security-server.security.manage	Permiso para editar los recursos relacionados con la seguridad (contraseñas, claves, etc.)
security-server.security.read	Permiso para leer los recursos relacionados con la seguridad
security-server.user.manage	Permiso para ver, crear, modificar o quitar perfiles de usuario de NetWitness Suite

Permiso	Descripción
security-server.user.read	Permiso para ver detalles de perfil de usuario de NetWitness Suite (por ejemplo, funciones, horas de inicio de sesión, etc.)

Administrar usuarios con funciones y permisos

En este tema se presenta un conjunto de procedimientos de punto a punto para administrar usuarios en NetWitness Suite. En estos pasos se explica cómo agregar un usuario en NetWitness Suite y la forma de controlar lo que el usuario puede hacer.

Temas

Paso 1. Revisar las funciones preconfiguradas de NetWitness

Para simplificar el proceso de creación de funciones y asignación de permisos, existen funciones preconfiguradas en NetWitness Suite.

Función	Permiso
Administradores	Acceso completo al sistema
Operadores	Acceso a configuraciones, pero no a metadatos ni a contenido de sesiones
Analistas	Acceso a metadatos y contenido de sesiones, pero no a configuraciones
Respond_ Administrator	Acceda a todos los permisos de incidentes y del servidor de Respond.
SOC_Managers	El mismo acceso que poseen los analistas, además del permiso adicional para manejar incidentes
Malware_ Analysts	Acceso a eventos de malware y a metadatos y contenido de sesiones
Data_Privacy_ Officers	Acceso a metadatos y contenido de sesiones, así como a opciones de configuración que administran el ocultamiento y la visualización de datos confidenciales en el sistema (consulte Administración de la privacidad de datos).

El administrador también puede agregar funciones personalizadas.

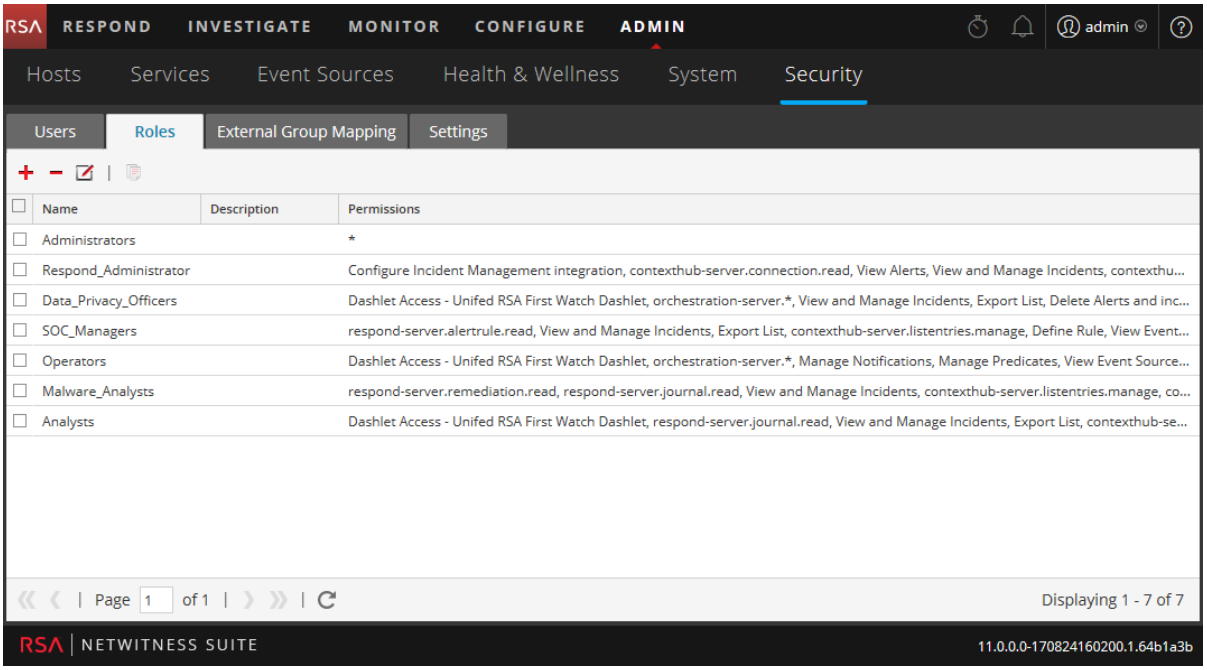
Paso 2. (Opcional) Agregar una función y asignar permisos

Aunque NetWitness Suite tiene funciones preconfiguradas, puede agregar funciones personalizadas. Por ejemplo, además de la función Analistas preconfigurada, podría agregar las funciones personalizadas AnalystsEurope y AnalystsAsia. Para obtener una lista detallada de permisos, consulte Permisos de función.

Cada uno de los siguientes procedimientos comienza en la pestaña **Funciones**.

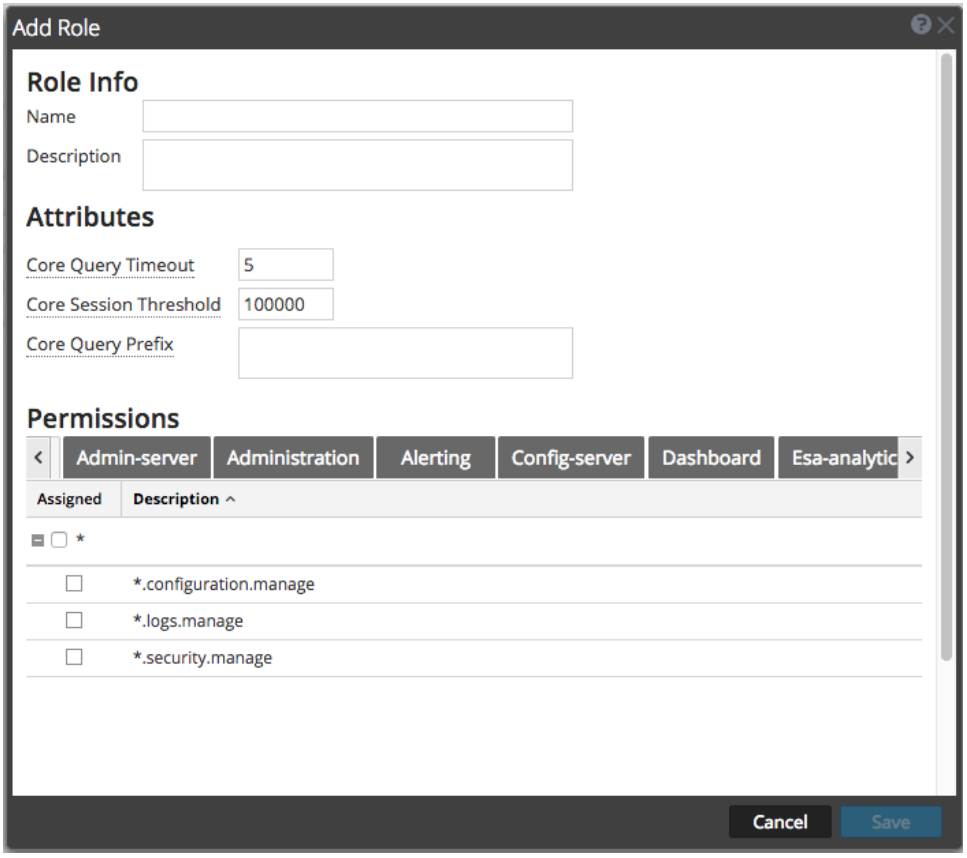
Para navegar a la pestaña Funciones:

1. Vaya a **ADMIN > Seguridad**.
   La vista Seguridad se muestra con la pestaña **Usuarios** abierta.
2. Haga clic en la pestaña **Funciones**.



Agregar una función y asignar permisos

1. En la pestaña **Funciones**, haga clic en ✚ en la barra de herramientas.
2. Se muestra el cuadro de diálogo **Agregar función**.



3. En la sección **Información de función**, escriba la siguiente información para la función:
   - **Nombre**
   - (Opcional) **Descripción**
4. En la sección **Atributos**, ingrese los valores que prefiera para cada atributo. Para obtener más información sobre los atributos, consulte Paso 3. Verificar atributos de consultas y sesiones por función.
5. En la sección **Permisos**:
   - Haga clic en ‹ y › para desplazarse a través de los módulos.
   - Seleccione un módulo al cual accederá la función.
   - Seleccione cada permiso que tendrá la función.

6. Repita el paso anterior hasta que seleccione todos los permisos que asignará a la función.
7. Haga clic en **Guardar** para agregar la nueva función, lo cual se aplica de inmediato. Ahora puede asignar la nueva función a los usuarios.

Duplicar una función

Una forma eficiente de agregar una nueva función es duplicar una función similar, guardarla con un nuevo nombre y revisar los permisos que ya están asignados.

1. En la pestaña **Funciones**, seleccione la función que desea duplicar y haga clic en .
2. Especifique un nuevo nombre de función y haga clic en **Guardar**.
3. Para cambiar los permisos, siga los pasos del siguiente procedimiento.

Cambiar permisos asignados a una función

1. En la pestaña **Funciones**, seleccione la función y haga clic en .
   Se muestra el cuadro de diálogo **Editar función**.
2. En la sección **Permisos**:
   - Haga clic en y para desplazarse a través de los módulos.
   - Seleccione un módulo para revisar sus permisos.
   - Seleccione o deseleccione cada permiso.
3. Repita el paso anterior hasta que la función tenga los permisos requeridos.
4. Haga clic en **Guardar**. Los permisos revisados se aplican de inmediato.

Eliminar una función

Puede eliminar una función si no está asignada a ningún usuario.

1. En la pestaña **Funciones**, seleccione la función y haga clic en .
2. Un cuadro de diálogo solicita confirmar la intención de eliminar la función. Haga clic en **Sí**.

Paso 3. Verificar atributos de consultas y sesiones por función

En este tema se explican los atributos de consultas y sesiones y se proporcionan instrucciones para configurarlos para las funciones de usuario. También se describe cómo estos ajustes de función afectan las configuraciones de usuarios individuales y lo que sucede si un usuario es miembro de varias funciones.

Después de definir las funciones de usuario, es importante verificar los atributos de consultas y sesiones que se configuran para cada función. Puede ajustar esta configuración de acuerdo con los requisitos.

Atributos de consultas y sesiones

Los atributos de consulta y sesión determinan el manejo de las consultas que ejecuta un usuario. Estos atributos permiten controlar la información que los usuarios pueden recuperar. Estos atributos se aplican a todas las sesiones de usuarios asignados a una función.

De acuerdo con los requisitos, puede especificar los siguientes atributos de manejo de consultas para una función de usuario:

- **Tiempo de espera agotado de consulta de Core** es una configuración opcional que se aplica a NetWitness Suite 10.5 y a servicios superiores de Core. Especifica la cantidad máxima de minutos que un usuario puede ejecutar una consulta. Si se configura este valor, debe ser cero (0) o mayor. Un valor de cero especifica que no hay tiempo de espera agotado.
- **Umbral de sesión de Core** es una configuración obligatoria. Este valor debe ser cero (0) o mayor. Si el umbral es mayor de cero, una optimización de consulta extrapolará los conteos de sesiones totales que superen el umbral. Cuando el valor de metadatos que devuelve la consulta alcance el umbral, el sistema:
  - Detendrá su determinación del conteo de sesiones
  - Mostrará el umbral y el porcentaje de tiempo de consulta utilizado para alcanzar el umbral
- **Prefijo de consulta de Core** es un filtro opcional que se aplica a las consultas que ejecuta el usuario. El prefijo restringe los resultados de consulta que ve el usuario. Por ejemplo, se antepone el prefijo de consulta `'service' = 80` a cualquier consulta que ejecute el usuario y este solo puede acceder a metadatos de sesiones HTTP.

La configuración de atributos de manejo de consultas que se aplica a un usuario depende de las membresías en las funciones del usuario. Es importante verificar la configuración de atributos de manejo de consultas para las funciones.

Cómo se aplica la configuración de atributos de manejo de consultas a usuarios individuales

Si un usuario es miembro de varias funciones, se aplica al usuario la siguiente lógica:

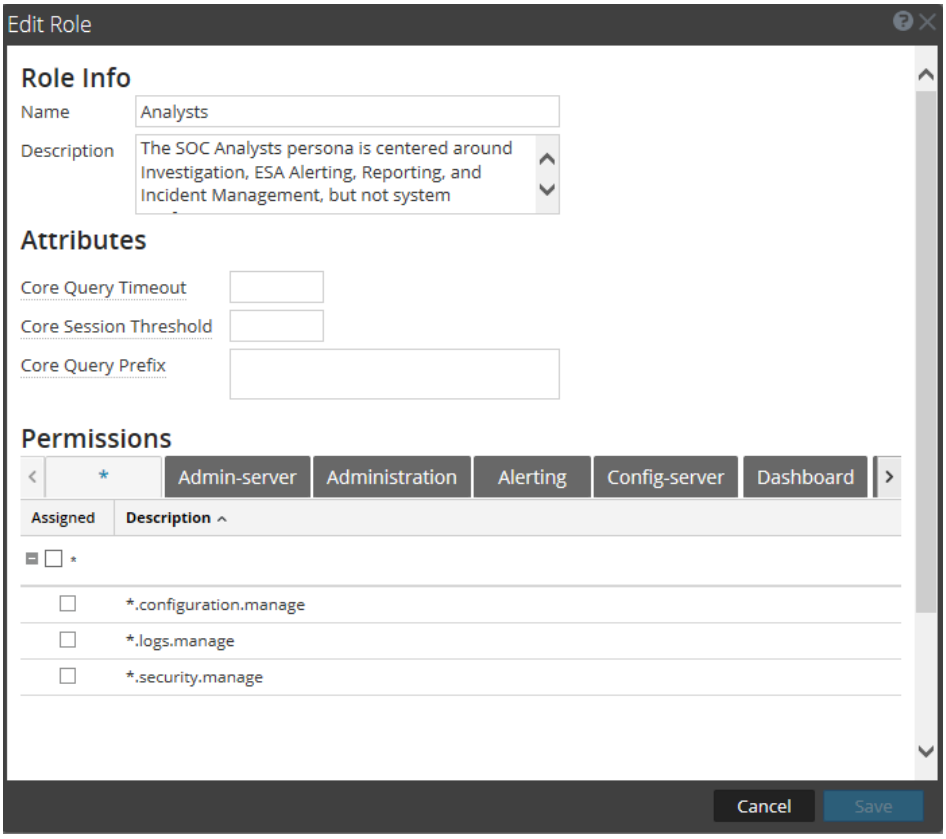
- **Tiempo de espera agotado de consulta:** Se aplica al usuario el valor más permisivo (más alto) de todas las funciones asignadas.
- **Prefijo de consulta:** Los prefijos de consulta de cada una de las funciones de usuario se unen mediante el operador Y.
- **Umbral de sesión:** Se aplica al usuario el valor más alto de todas las funciones asignadas.

Procedimiento

Para establecer los atributos de manejo de consultas de una función de usuario:

1. Vaya a **ADMIN > Seguridad**.
   La vista Seguridad se muestra con la pestaña **Usuarios** abierta.
2. Haga clic en la pestaña **Funciones**. Si va a agregar una función, haga clic en  . Si va a editar una función, seleccione la función y haga clic en  .

Se muestran los cuadros de diálogo Agregar función o Editar función.



3. Para configurar los atributos de la función, en la sección **Atributos**:
   - (Opcional) En el campo **Tiempo de espera agotado de consulta de Core**, escriba la cantidad máxima de minutos que un usuario puede ejecutar una consulta. El valor predeterminado es 5 minutos. Este tiempo de espera agotado solo se aplica a las consultas que se ejecutan desde Investigation. NetWitness Suite 10.5 y los servicios superiores de Core usan este campo.
     Cuando se migra a NetWitness Suite 10.5 y superior, si no hay ningún valor configurado en las funciones, 5 minutos se configura de manera predeterminada.
   - Escriba un **Umbral de sesión** de **Core** para que el sistema detenga su determinación del conteo de sesiones. El valor predeterminado es `100000`. El límite que especifica aquí reemplaza el valor **Máximo de exportación de sesiones** definido en la configuración de la vista INVESTIGATE.
   - (Opcional) Escriba un **Prefijo de consulta de Core** para filtrar los resultados de la consulta que ven los miembros de la función. De forma predeterminada, este valor está en blanco.

> **Nota:** Un valor mostrado en cursiva indica un valor predeterminado; por ejemplo, *5*. Un valor que no se muestra en cursiva indica un cambio respecto del valor predeterminado; por ejemplo, `1200`.

4. Haga clic en **Guardar.**

Paso 4. Configurar un usuario

En este tema se presentan los procedimientos para configurar un usuario nuevo.

Temas

- Agregar un usuario y asignar una función
- Habilitar, desbloquear y eliminar cuentas de usuarios

Agregar un usuario y asignar una función

En este tema se explica cómo agregar un nuevo usuario a cada tipo de cuenta de usuario, local y externa. También se explica cómo asignar una función a un usuario local.

Todos los usuarios de NetWitness Suite deben tener una cuenta de usuario local o externa.

Las siguientes consideraciones son importantes al administrar cuentas de usuario locales y externas.

Cuenta de usuario local	Cuenta de usuario externa
Administrada en NetWitness Suite	Administrada externamente y fuera del alcance de este documento
Funciones asignadas directamente	Funciones asignadas por mapeo de grupo externo
Deriva permisos de cada función asignada al usuario, como se explica en este tema.	Deriva permisos de cada función mapeada al grupo de usuarios externos de la cuenta, como se explica en el Paso 5. (Opcional) Mapear funciones de usuario a grupos externos.
NetWitness Suite administra toda la información del usuario.	NetWitness Suite administra solo la identificación del usuario. Se incluye nombre de usuario, nombre completo y correo electrónico.

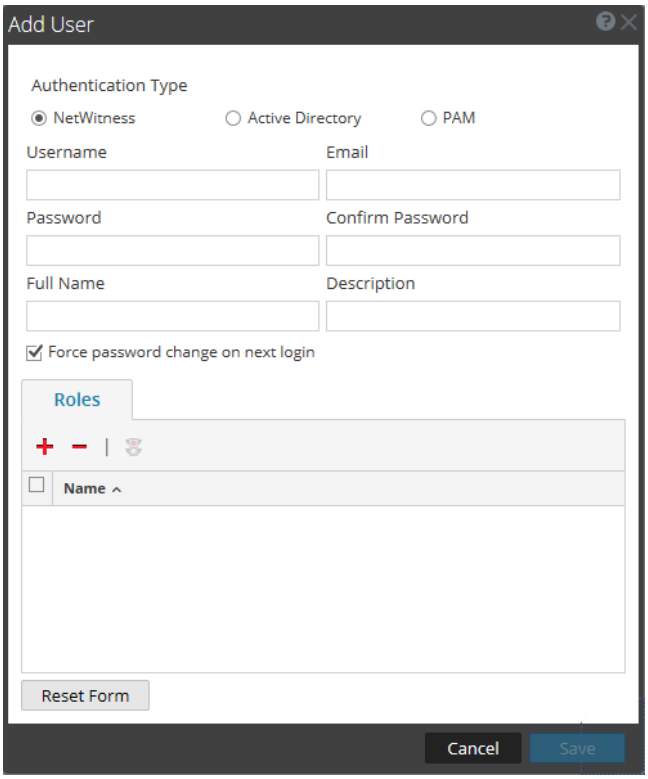
Procedimientos

Cada uno de los siguientes procedimientos comienza en la pestaña Usuarios. Para navegar a la pestaña Usuarios, vaya a**ADMIN > Seguridad**. La vista Seguridad se muestra con la pestaña Usuarios abierta.

Agregar un usuario y asignar una función

Para agregar una cuenta de usuario local y asignar una función al usuario:

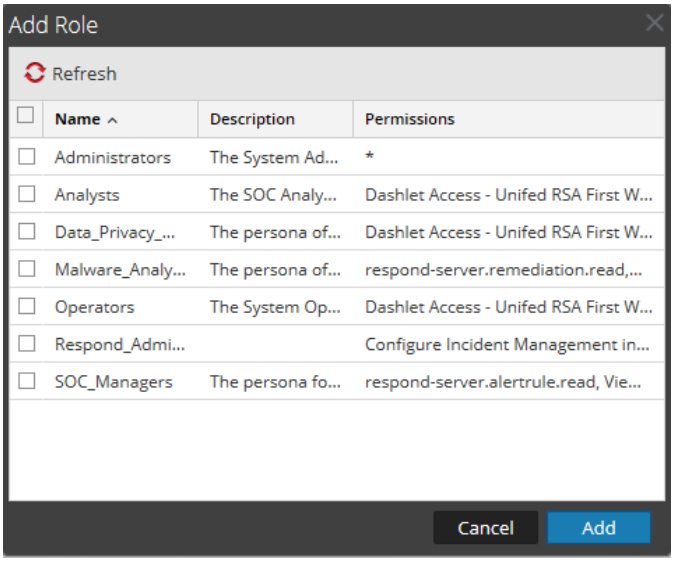
1. En la pestaña **Usuarios**, haga clic en  en la barra de herramientas.
   Se muestra el cuadro de diálogo **Agregar usuario**.



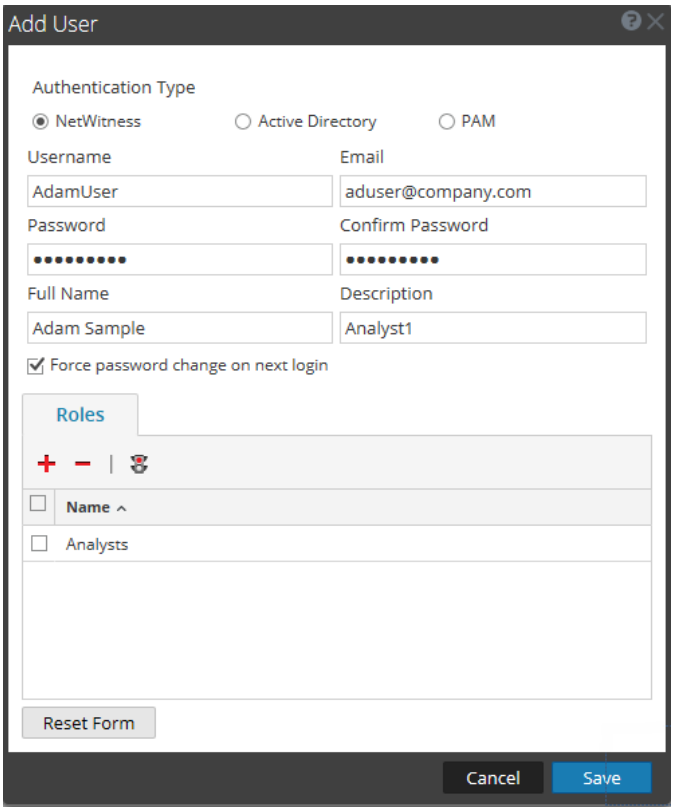
2. Escriba la siguiente información de cuenta para el usuario nuevo:
   - **Tipo de autenticación**: **NetWitness** está seleccionado de forma predeterminada y es la elección correcta cuando se agrega un usuario local. Esta opción solo se muestra cuando hay configuraciones de AD o PAM configuradas para permitir la selección de ese tipo de autenticación. Si no hay ninguna configuración de AD o PAM, el tipo de autenticación se configura automáticamente en NetWitness y no hay otras opciones disponibles.
   - **Nombre de usuario** para iniciar sesión en NetWitness Suite
   - Dirección de **Correo electrónico**
   - Contraseña para iniciar sesión en NetWitness Suite, en los campos **Contraseña** y **Confirmar contraseña**
   - **Nombre completo** del nuevo usuario
   - (Opcional) **Descripción** de la cuenta de usuario
3. Para dar vencimiento a la contraseña del usuario la próxima vez que inicia sesión, seleccione **Forzar cambio de contraseña en el próximo inicio de sesión**.
   Esto no afecta a las sesiones de usuario activas. El ícono  aparece en la fila del usuario para mostrar que su contraseña venció. Una vez que se produce el vencimiento de la

contraseña, no es posible deshacerlo. Esta casilla de verificación se deselecciona la próxima vez que se edita la cuenta de usuario.

4. Para asignar una función al usuario, haga clic en + en la pestaña **Funciones**.
   El cuadro de diálogo de selección **Agregar función** muestra la lista de funciones disponibles.

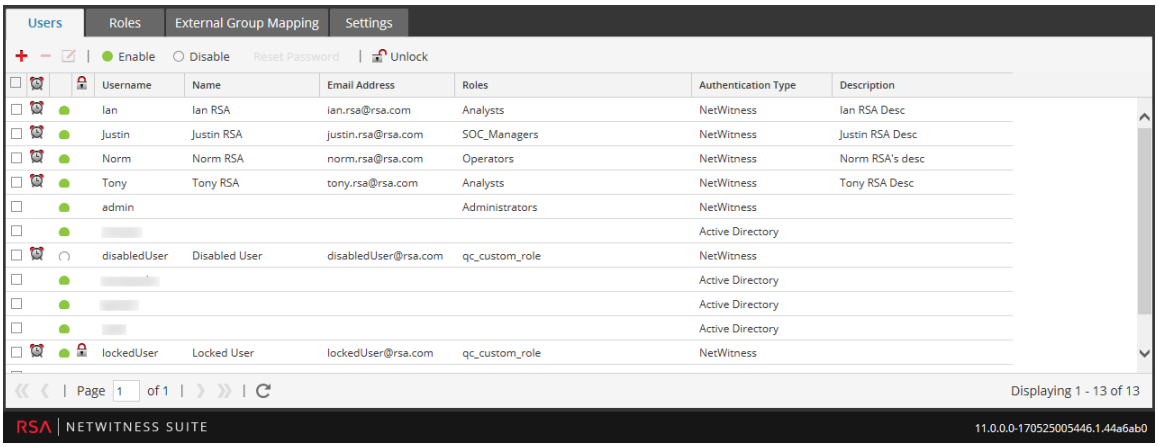


5. Seleccione cada función que desea asignar y haga clic en **Agregar**.
   El cuadro de diálogo **Agregar usuario** muestra cada función asignada al usuario.



6. (Opcional) Seleccione una función y haga clic en para **Mostrar todos los permisos** para la función.

7. Haga clic en **Guardar**.
   La pestaña **Usuarios** muestra el nuevo usuario y cada función asignada al usuario. La cuenta se activa de inmediato.

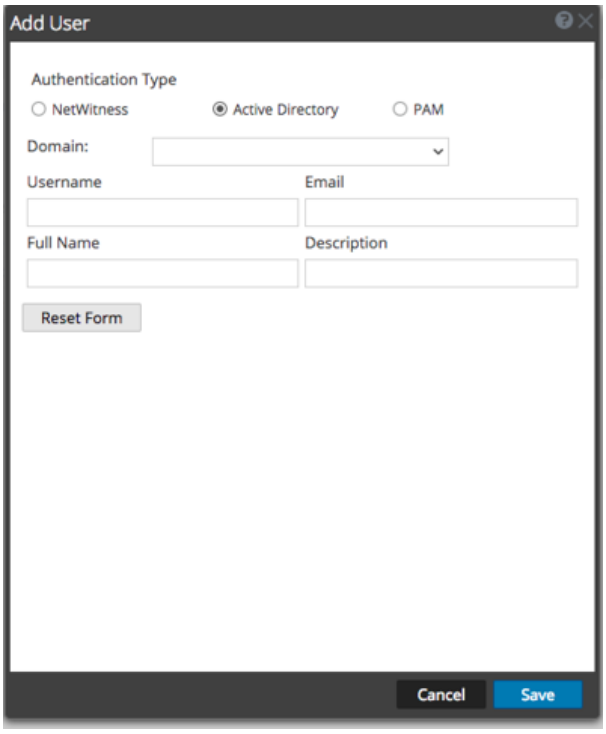


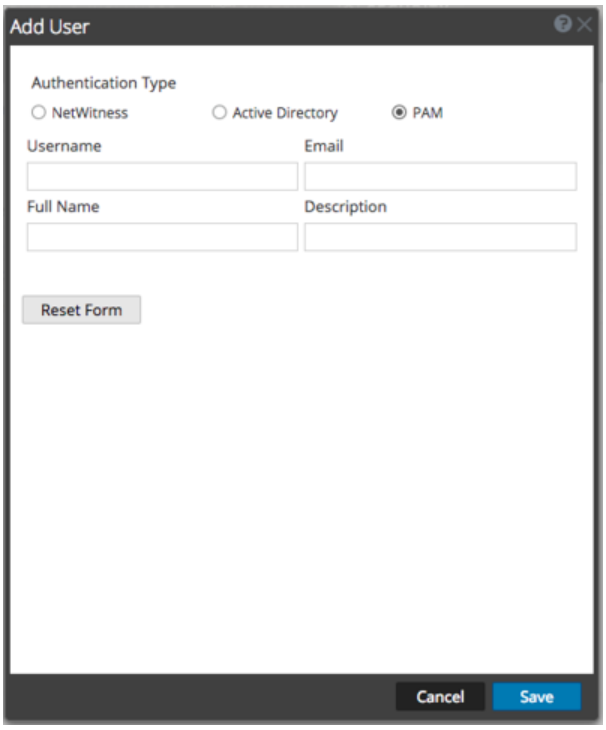
Agregar un usuario para autenticación externa

Requisito previo: La autenticación externa debe estar configurada. Consulte Paso 4. (Opcional) Configurar la autenticación externa.

Para agregar un usuario que se autentica externamente, fuera de NetWitness Suite:

1. En la pestaña **Usuarios**, haga clic en + en la barra de herramientas.
   Se muestra el cuadro de diálogo **Agregar usuario**.
2. Para **Tipo de autenticación**, seleccione **Active Directory** o **PAM**. El cuadro de diálogo se actualizará para mostrar los campos requeridos para el tipo de autenticación externa seleccionado.





3. Escriba la siguiente información:
   - **Dominio** (si selecciona autenticación de Active Directory solamente): Seleccione el dominio de Active Directory para el usuario en la lista desplegable de dominios disponibles.
   - **Nombre de usuario** para iniciar sesión en NetWitness Suite
   - Dirección de **Correo electrónico**
   - **Nombre completo** del nuevo usuario
   - (Opcional) **Descripción** de la cuenta de usuario
4. Haga clic en **Guardar**. La pestaña Usuarios muestra la nueva cuenta de usuario, que aún necesita una función y permisos.
5. Para mapear una función al usuario nuevo, consulte Paso 5. (Opcional) Mapear funciones de usuario a grupos externos.

Cambiar información o funciones del usuario

Para cambiar la información de cuenta o las funciones asignadas del usuario:

1. En la pestaña **Usuarios**, seleccione un usuario y haga clic en  en la barra de herramientas.Se muestra el cuadro de diálogo **Editar usuario**.

2. Para editar la información del usuario, cambie cualquiera de los campos siguientes:
   - **Correo electrónico**
   - **Nombre completo**
   - **Descripción**
3. Para dar vencimiento a la contraseña del usuario **interno** la próxima vez que inicia sesión, seleccione **Forzar cambio de contraseña en el próximo inicio de sesión**.
   Esto no afecta a las sesiones de usuario activas. El ícono  aparece en la fila del usuario para mostrar que su contraseña venció. Una vez que se produce el vencimiento de la contraseña, no es posible deshacerlo. Esta casilla de verificación se deselecciona la próxima vez que se edita la cuenta de usuario.
4. En la sección **Funciones**:
   - Para asignar otra función, haga clic en  , seleccione una función y haga clic en **Agregar**.
   - Para quitar una función asignada, seleccione la función y haga clic en .
5. Haga clic en **Guardar**.

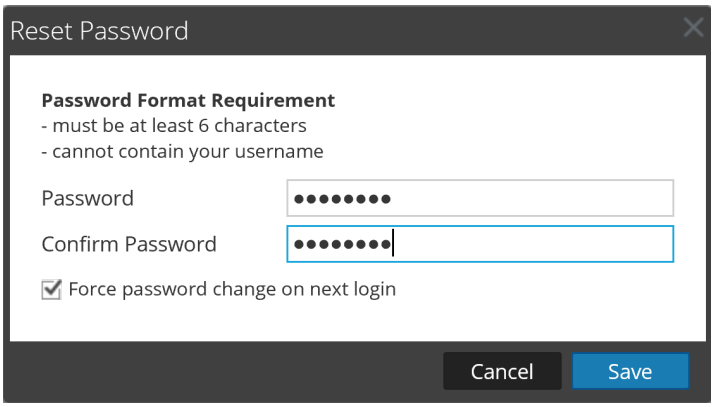
Eliminar un usuario

1. En la pestaña **Usuarios**, seleccione un usuario.
2. En la barra de herramientas, haga clic en .
3. Haga clic en **Guardar**.

Nota: Para eliminar completamente un usuario que se autentica externamente mediante Active Directory, también debe eliminar el usuario en el grupo de AD.

Restablecer la contraseña de un usuario

1. En la pestaña **Usuarios**, seleccione un usuario.
2. En la barra de herramientas, haga clic en **Restablecer contraseña**.



   En la sección **Requisito de formato de contraseña** se enumeran los requisitos específicos de la contraseña. Los administradores pueden ajustar estos requisitos para todos los usuarios internos en la política de contraseña. Consulte Paso 1. Configurar la complejidad de las contraseñas.

3. Elija si desea forzar un cambio de contraseña la próxima vez que el usuario inicie sesión en NetWitness Suite.
4. Haga clic en **Guardar**.

Habilitar, desbloquear y eliminar cuentas de usuarios

En este tema se proporcionan instrucciones para habilitar, desbloquear y eliminar cuentas de usuarios.

Todos los usuarios de NetWitness Suite deben contar con una cuenta de usuario local con nombre de usuario y contraseña o tener una cuenta de usuario externo. En NetWitness Suite, puede habilitar, deshabilitar y eliminar cuentas de usuario locales.

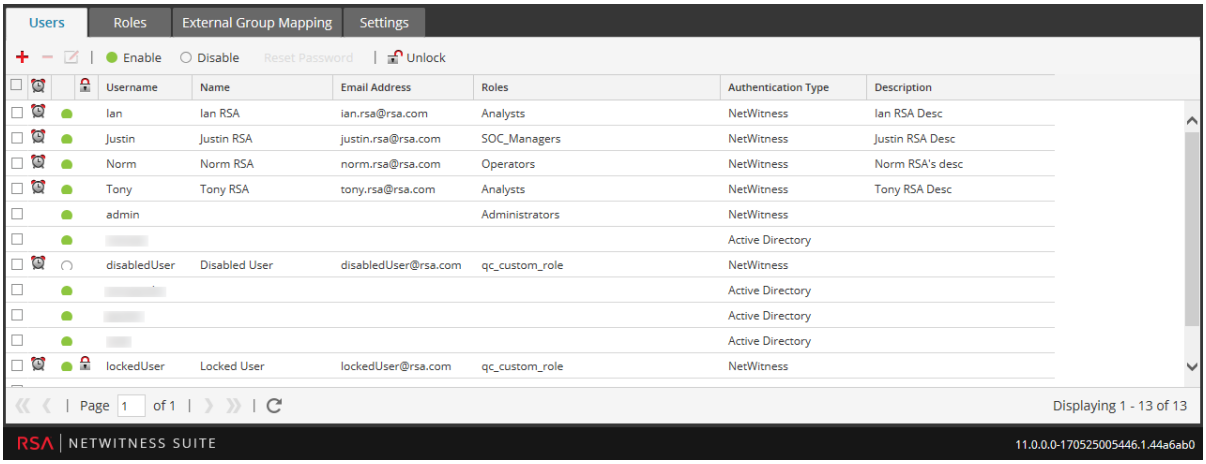
La primera vez que un usuario externo inicia sesión en NetWitness Suite, se crea automáticamente una nueva entrada de usuario con NetWitness Suite. NetWitness Suite administra solamente la información de identificación del usuario; por ejemplo, el nombre completo y el correo electrónico.

Puede desbloquear cuentas bloqueadas para usuarios locales y externos.

Habilitar cuentas de usuario deshabilitadas de NetWitness Suite

Para habilitar cuentas de usuario de NetWitness Suite que se hayan deshabilitado:

1. En NetWitness Suite, vaya a **ADMIN > Seguridad**.
   La vista Seguridad se muestra con la pestaña **Usuarios** abierta.



2. En la cuadrícula **Usuarios**, seleccione una o más cuentas.
3. Haga clic en Enable.
   Un cuadro de diálogo solicita confirmación.
4. Si desea habilitar las cuentas, haga clic en **Sí**.
   Las cuentas se habilitan y el usuario puede iniciar sesión en NetWitness Suite.

Deshabilitar cuentas de usuario de NetWitness Suite

Puede bloquear el acceso de usuarios desactivándolos. La deshabilitación del usuario no elimina sus preferencias. Esta acción bloquea el acceso de los usuarios sin eliminar sus preferencias, de forma que al volver a habilitarlos, estas permanezcan intactas. Puede reactivar usuarios para restaurar el acceso de usuarios. La desactivación de usuarios se aplica solo a usuarios locales y no a usuarios externos.

Para deshabilitar cuentas de usuario de NetWitness Suite:

1. En la cuadrícula **Usuarios**, seleccione una o más cuentas.
2. Haga clic en Disable.

   Un cuadro de diálogo solicita confirmación.
3. Si desea deshabilitar las cuentas, haga clic en **Sí**.

   Las cuentas se deshabilitan y el usuario ya no puede iniciar sesión en NetWitness Suite.

Desbloquear cuentas de usuario bloqueadas de NetWitness Suite

El usuario se bloquea durante un periodo de tiempo después de un número consecutivo de intentos de inicio de sesión fallidos. Para desbloquear cuentas de usuario de NetWitness Suite que estén bloqueadas debido a una cantidad excesiva de intentos de inicio de sesión fallidos:

1. En la cuadrícula **Usuarios**, seleccione una o más cuentas.
2. Haga clic en Unlock.

   Un cuadro de diálogo solicita confirmación.
3. Si desea desbloquear las cuentas, haga clic en **Sí**.

   Las cuentas se desbloquean y el usuario puede iniciar sesión en NetWitness Suite.

Eliminar cuentas de usuario de NetWitness Suite

Si no está utilizando autenticación externa, un usuario puede iniciar sesión en NetWitness Suite mediante una cuenta local. Estas cuentas locales se administran directamente mediante NetWitness Suite. Para revocar el acceso a un usuario local, deshabilite la cuenta o elimínela completamente del sistema.

Nota: Esto elimina todas las preferencias de usuario para la cuenta de NetWitness Suite. Si no es la intención, deshabilite el usuario en lugar de eliminar el usuario.

Para eliminar cuentas de usuario de NetWitness Suite:

1. Vaya a **ADMIN > Seguridad**.

   La vista Seguridad se muestra con la pestaña **Usuarios** abierta.
2. En la lista Usuarios, seleccione una o más cuentas.

3. Haga clic en .
   Un cuadro de diálogo de advertencia solicita confirmación.
4. Si desea eliminar las cuentas, haga clic en **Sí**.
   Las cuentas se eliminan de NetWitness Suite y los usuarios ya no pueden iniciar sesión en NetWitness Suite.

Paso 5. (Opcional) Mapear funciones de usuario a grupos externos

En este tema se describe el método para asignar funciones de usuario de NetWitness Suite a grupos externos.

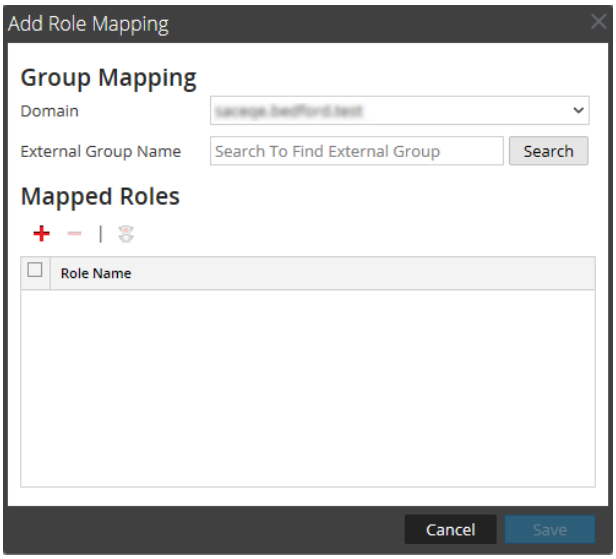
En NetWitness Suite, los grupos externos obtienen los permisos para varios módulos y vistas a partir de las funciones de usuario de NetWitness Suite, las cuales tienen permisos asignados. Para proporcionar acceso a un grupo externo, asígnele funciones de usuario. Para modificar el acceso de un grupo externo, edite las funciones asignadas a él. Agregue y elimine funciones hasta que el grupo externo tenga el acceso necesario. Los cambios se hacen efectivos inmediatamente.

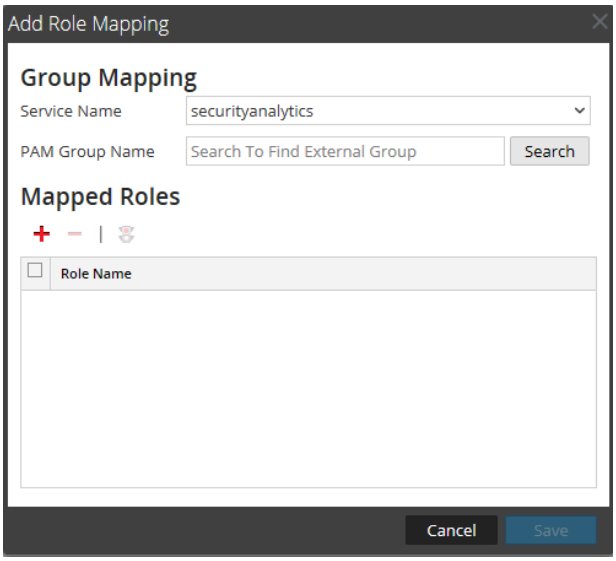
Requisitos previos

En la pestaña Ajustes de configuración, debe configurar un método para que la autenticación de usuarios externos haga visibles los grupos externos para NetWitness Suite.

Agregar asignación de funciones para un grupo externo

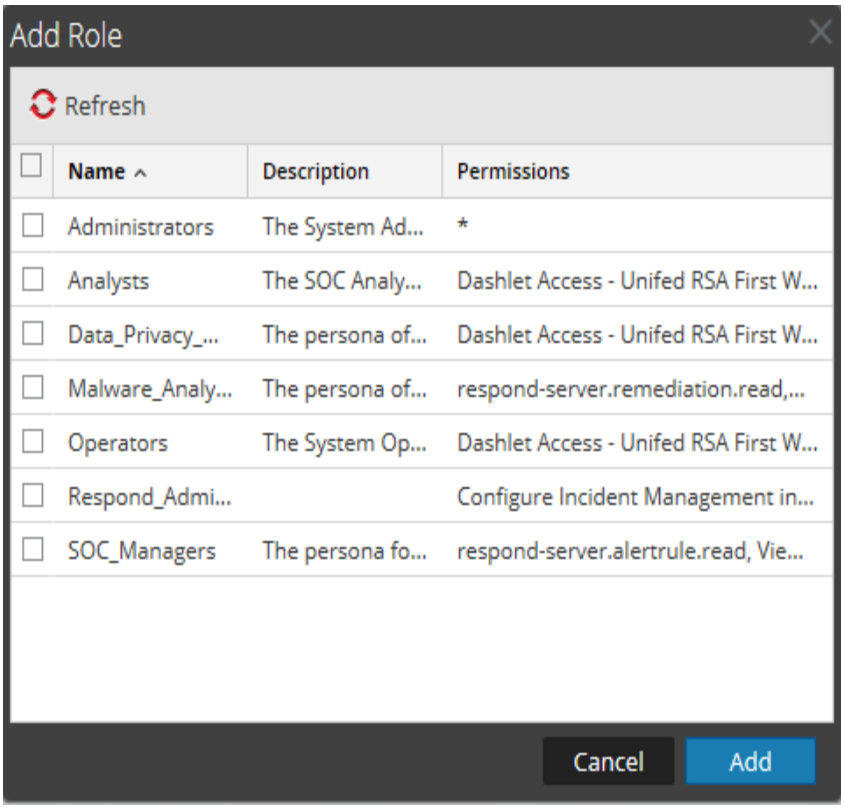
1. En NetWitness Suite, vaya a **ADMIN > Seguridad**.
   La vista Seguridad se muestra con la pestaña **Usuarios** abierta.
2. Haga clic en la pestaña **Mapeo de grupo externo**.
3. En la barra de herramientas, haga clic en +.
   Se muestra el cuadro de diálogo **Agregar asignación de funciones** correspondiente al método de autenticación externo que seleccionó.





4. Haga clic en **Buscar**, busque un nombre de grupo externo en el cuadro de diálogo Buscar grupos externos y luego seleccione un nombre de grupo externo.

5. Para agregar funciones al mapeo de grupo, haga clic en + en la sección **Funciones mapeadas**.
   Se muestra el cuadro de diálogo **Agregar función**.



6. Haga clic en la casilla de verificación de la barra de título para seleccionar todas las funciones o seleccionar funciones individualmente.
7. Para agregar las funciones a la sección **Funciones mapeadas** en el cuadro de diálogo Agregar asignación de funciones, haga clic en **Agregar**.
   El cuadro de diálogo se cierra y las funciones seleccionadas aparecen en la sección Funciones mapeadas.
8. Si desea eliminar funciones de la sección **Funciones mapeadas**, selecciónelas y haga clic en −.
9. Cuando el cuadro de diálogo **Agregar asignación de funciones** refleje la asignación de funciones que desea definir para el grupo, haga clic en **Guardar**.
   El cuadro de diálogo Agregar asignación de funciones se cierra, y la nueva asignación de funciones aparece en la lista de la pestaña Mapeo de grupo externo.

Editar asignación de funciones para un grupo

1. En la barra de acciones **Mapeo de grupo externo**, haga clic en **Editar**.
   El cuadro de diálogo **Editar asignación de funciones** aparece con el nombre de grupo en el campo **Nombre de grupo externo**.
2. Para agregar funciones al mapeo, haga clic en + en la sección **Funciones mapeadas**.
   Se muestra el cuadro de diálogo Agregar función.
3. Haga clic en la casilla de verificación de la barra de título para seleccionar todas las funciones o seleccionar funciones individualmente.
4. Para agregar las funciones a la sección **Funciones mapeadas** en el cuadro de diálogo **Agregar asignación de funciones**, haga clic en **Agregar**.
   El cuadro de diálogo se cierra y las funciones seleccionadas aparecen en la sección Funciones mapeadas.
5. Si desea eliminar funciones de la sección **Funciones mapeadas**, selecciónelas y haga clic en −.
6. Cuando el cuadro de diálogo **Editar asignación de funciones** refleje la asignación de funciones que desea definir para el grupo, haga clic en **Guardar**.
   El cuadro de diálogo se cierra y la asignación de funciones editada aparece en la pestaña Mapeo de grupo externo.

Tema relacionado

- Buscar grupos externos

Buscar grupos externos

En este tema se proporcionan instrucciones para buscar grupos externos que tienen asignadas funciones de usuario de NetWitness Suite.

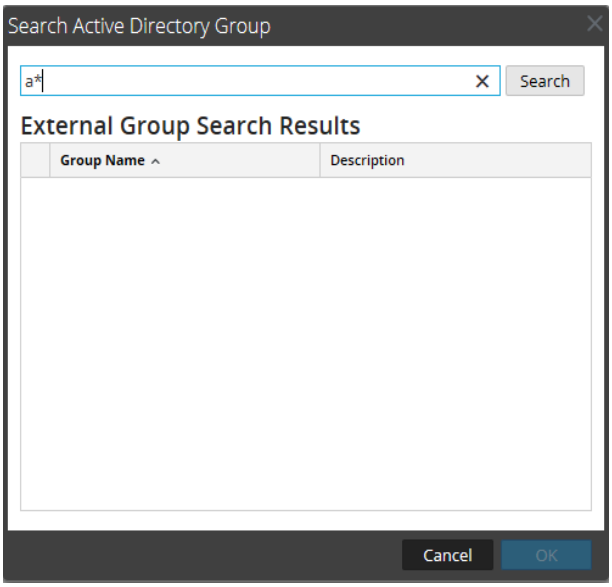
Requisitos previos

Se debe activar un método para la autenticación de usuarios externos.

Procedimiento

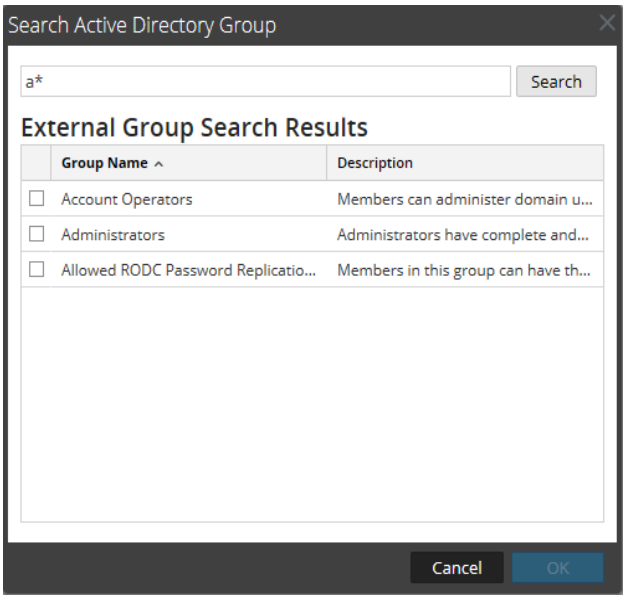
Para buscar un grupo externo:

1. En NetWitness Suite, vaya a **ADMIN > Seguridad**.
   La vista Seguridad se muestra con la pestaña **Usuarios** abierta.
2. Haga clic en la pestaña **Mapeo de grupo externo**.
3. En la barra de herramientas, haga clic en + o .
   Se muestra el cuadro de diálogo **Agregar asignación de funciones** correspondiente al método de autenticación externo que seleccionó.
4. La sección **Mapeo de grupos** depende del método de autenticación externa seleccionado.
   - En el caso de **Active Directory**, seleccione un **Dominio**. A continuación, haga clic en **Buscar** junto a **Nombre de grupo externo**.
   - En el caso de **PAM**, haga clic en **Buscar** junto a **Nombre del grupo PAM**.
     Se muestra el cuadro de diálogo **Buscar grupos externos**.
5. En **Nombre común**, escriba un nombre de grupo o parte de un nombre de grupo con el carácter comodín (*).



6. Haga clic en **Buscar**.

   Los resultados se muestran en la sección **Resultados de búsqueda de grupos externos**.



7. Seleccione el grupo al cual desea asignar funciones y haga clic en **Aceptar**.

Referencias

Este tema es un conjunto de referencias sobre la seguridad del sistema y administración de usuarios en NetWitness Suite.

Temas

Vista Seguridad de Admin

En este tema se describe cada elemento de la interfaz del usuario de Admin > vista Seguridad y de todos los cuadros de diálogo y las pestañas relacionados. Los componentes de la interfaz aparecen en orden alfabético.

En Admin > vista Seguridad se proporciona la funcionalidad necesaria para administrar cuentas de usuario, administrar funciones de usuario, mapear grupos externos a funciones de NetWitness Suite y modificar otros parámetros del sistema relacionados con la seguridad. Estos se aplican al sistema NetWitness Suite y se utilizan junto con los ajustes de seguridad de cada servicio.

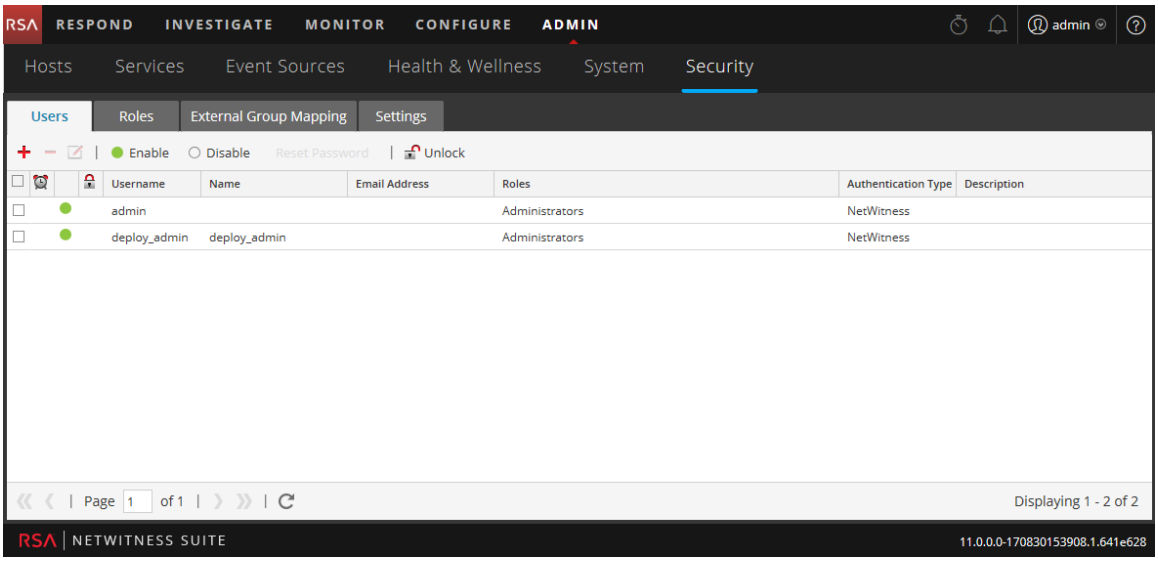
¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Administrar usuarios	Paso 4. Configurar un usuario
Administrador	Administrar funciones	Paso 1. Revisar las funciones preconfiguradas de NetWitness Paso 2. (Opcional) Agregar una función y asignar permisos
Administrador	(Opcional) Configurar mapeos de grupos externos	Paso 5. (Opcional) Mapear funciones de usuario a grupos externos
Administrador	Configurar ajustes	Paso 3. Configurar ajustes de seguridad en el nivel del sistema

Temas relacionados

- Pestaña Usuarios
- Pestaña Funciones
- Pestaña Mapeo de grupo externo
- Pestaña Ajustes de configuración

Para mostrar la vista Seguridad de Admin, vaya a **ADMIN > Seguridad**.



En Admin > vista Seguridad, hay cuatro pestañas:

- La pestaña **Usuarios** proporciona una manera de administrar las cuentas de usuario.
- La pestaña **Funciones** proporciona una manera de definir las funciones de seguridad y asignar funciones a las cuentas de usuario.
- La pestaña **Mapeo de grupo externo** proporciona una manera de administrar los parámetros de acceso a los grupos LDAP.
- En la pestaña **Ajustes de configuración** se proporciona una manera de configurar la complejidad y el vencimiento de las contraseñas de los usuarios internos de NetWitness Suite y de configurar el comportamiento del sistema ante inicios de sesión fallidos e inactividad. También se proporciona una manera de configurar la autenticación externa.

Pestaña Usuarios

En este tema se presentan las características y las funciones para configurar una cuenta de usuario en Admin > vista Seguridad > pestaña Usuarios.

Cada usuario de NetWitness Suite debe tener una cuenta de usuario. La pestaña Usuarios permite crear, editar, eliminar, habilitar/inhabilitar y desbloquear una cuenta de usuario.

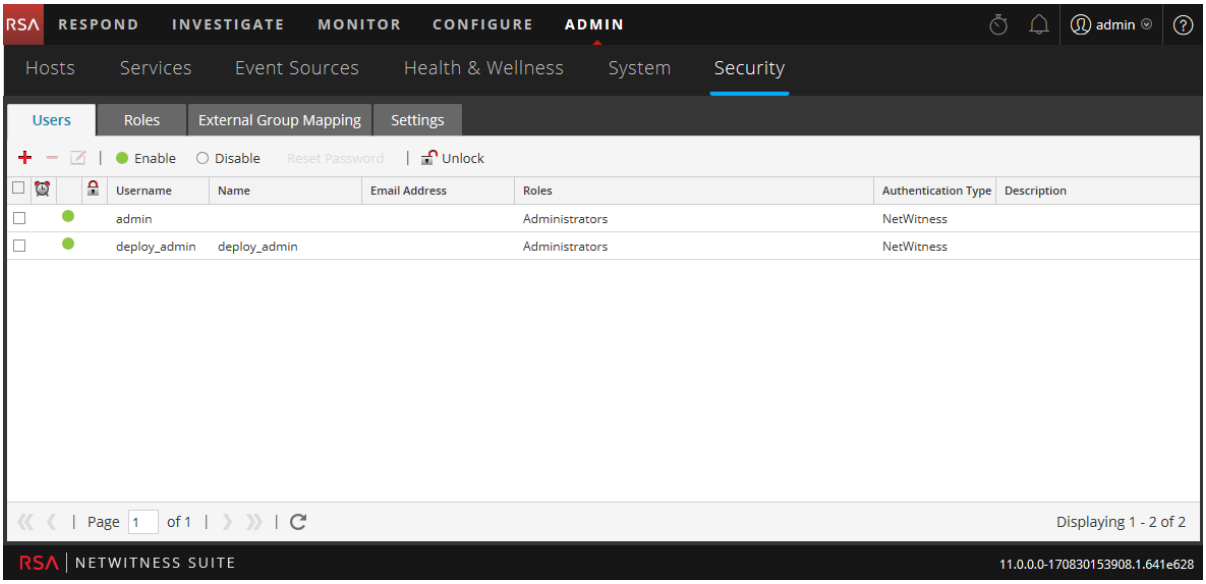
¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Configurar un usuario nuevo	Paso 4. Configurar un usuario Agregar un usuario y asignar una función
Administrador	Administrar cuentas de usuario	Habilitar, desbloquear y eliminar cuentas de usuarios

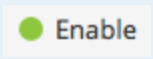
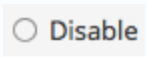
Temas relacionados

- Cuadro de diálogo Agregar/Editar usuario

Para acceder a esta vista, vaya a **ADMIN > Seguridad**. La vista Seguridad se abre de manera predeterminada en la pestaña **Usuarios**.



La pestaña Usuarios consta de la lista Usuario y tiene una barra de herramientas en la parte superior. Estas son las funcionalidades de la barra de tareas.

Función	Descripción
+	Abre el cuadro de diálogo Agregar usuario.
−	Elimina el usuario seleccionado.
	Abre el cuadro de diálogo Editar usuario para el usuario seleccionado.
	Activa y desactiva una cuenta de usuario sin modificar las preferencias de usuario.
	Bloquea el acceso de los usuarios sin eliminar las preferencias de usuario, de forma que al volver a habilitar a los usuarios, las preferencias no tengan modificaciones.
Restablecer contraseña	Abre el cuadro de diálogo Restablecer contraseña, el cual permite cambiar la contraseña del usuario seleccionado. Este cuadro de diálogo enumera los requisitos de formato de las contraseñas necesarios para cambiar la contraseña y permite obligar al usuario a cambiar su contraseña en el próximo inicio de sesión.
 Desbloquear	Desbloquea una cuenta de usuario que se bloqueó debido a que se produjeron demasiados intentos fallidos de inicio de sesión.

La lista **Usuarios** tiene las siguientes columnas.

Columna	Descripción
	Si aparece este ícono en una fila de usuario, indica que la contraseña de usuario venció.
Nombre de usuario	Nombre de usuario para iniciar sesión en NetWitness Suite.
Nombre	Nombre de usuario al cual pertenece la cuenta.
Dirección de correo electrónico	Dirección de correo electrónico del usuario.

Columna	Descripción
Funciones	Función asignada al usuario.
Externo	Método de autenticación, que puede ser externo mediante Active Directory o PAM, o interno mediante NetWitness Suite.
Descripción	Descripción de la cuenta de usuario.

Cuadro de diálogo Agregar/Editar usuario

En este tema se presentan los cuadros de diálogo Agregar usuario y Editar usuario, a los cuales se accede desde Admin > vista Seguridad > pestaña Usuarios.

Todos los usuarios deben tener una cuenta de usuario local con nombre de usuario y contraseña o una cuenta de usuario externa que está mapeada a NetWitness Suite.

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Agregar un usuario y asignar una función	Paso 2. (Opcional) Agregar una función y asignar permisos
Administrador	Cambiar la información del usuario	Paso 2. (Opcional) Agregar una función y asignar permisos
Administrador	Restablecer la contraseña de un usuario	Paso 2. (Opcional) Agregar una función y asignar permisos
Administrador	Agregar un usuario para autenticación externa	Paso 2. (Opcional) Agregar una función y asignar permisos

Temas relacionados

- Administrar usuarios con funciones y permisos
- Habilitar, desbloquear y eliminar cuentas de usuarios

Preferencias de usuario

Para mostrar el cuadro de diálogo **Agregar usuario** o **Editar usuario**:

1. En NetWitness Suite, vaya a **ADMIN > Seguridad**.
   La vista Seguridad se muestra con la pestaña **Usuarios** abierta.
2. Realice una de las siguientes acciones:
   - En la barra de acciones, haga clic en  .
     Se muestra el cuadro de diálogo **Agregar usuario**.

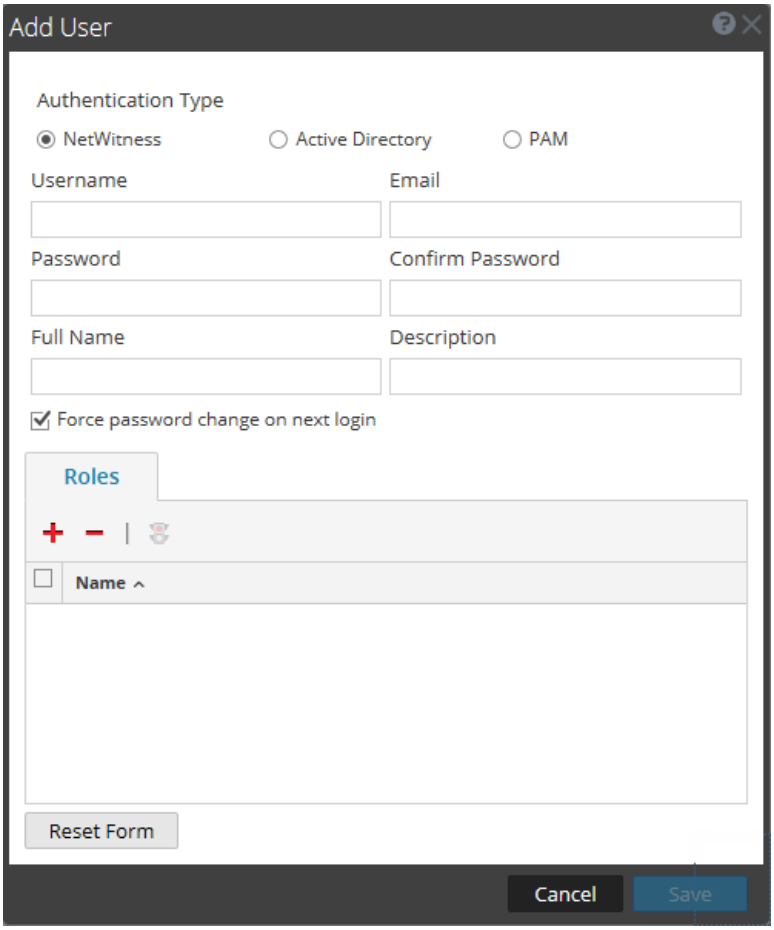
- Seleccione un usuario y, en la barra de acciones, haga clic en .

  Se muestra el cuadro de diálogo **Editar usuario**.

Los cuadros de diálogo Agregar usuario y Editar usuario son iguales, salvo que el cuadro de diálogo Agregar usuario contiene los campos adicionales **Contraseña** y **Confirmar contraseña**. Puede agregar una contraseña para un usuario nuevo en el cuadro de diálogo Agregar usuario. Los usuarios pueden cambiar sus propias contraseñas en las preferencias de usuario. Puede restablecer una contraseña para un usuario directamente desde la pestaña Usuarios.

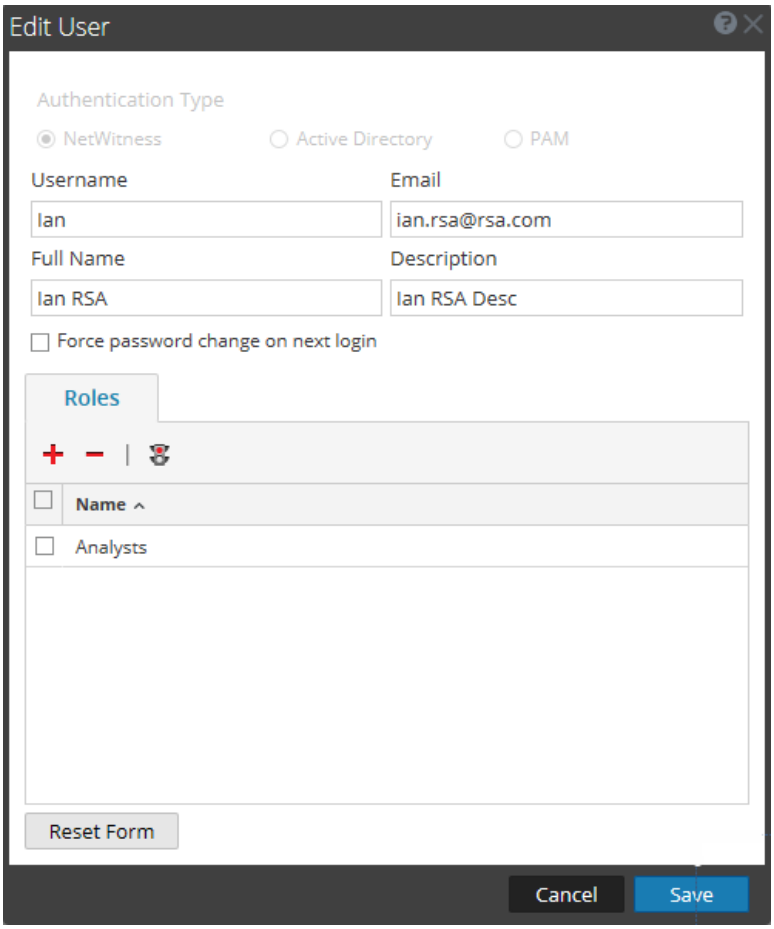
Cuadro de diálogo Agregar usuario

Este es el cuadro de diálogo Agregar usuario para un usuario interno.



Cuadro de diálogo Editar usuario

Este es el cuadro de diálogo Editar usuario para un usuario interno.



Los cuadros de diálogo Agregar usuario y Editar usuario muestran:

- Tipo de autenticación
- Información del usuario
- Funciones a las cuales pertenece el usuario

Información del usuario

En la siguiente tabla se proporcionan descripciones de la información del usuario.

Campo	Descripción
Tipo de autenticación	El tipo de autenticación para el usuario. La selección predeterminada es NetWitness y designa a un usuario interno. Las opciones para los usuarios externos son Active Directory y PAM. Este campo se deshabilita cuando se edita un usuario.

Campo	Descripción
Nombre de usuario	Nombre de usuario de la cuenta de usuario de NetWitness Suite.
Nombre completo	Nombre del usuario.
Contraseña	(Solo el cuadro de diálogo Agregar usuario) Contraseña para iniciar sesión en NetWitness Suite.
Confirmar contraseña	(Solo el cuadro de diálogo Agregar usuario) Confirmación de la contraseña para agregar la contraseña del usuario.
Correo electrónico	Dirección de correo electrónico del usuario.
Descripción	(Opcional) Descripción del usuario.
Forzar cambio de contraseña en el próximo inicio de sesión	Da vencimiento a la contraseña del usuario la próxima vez que inicia sesión en NetWitness Suite. Este campo se aplica solo a los usuarios internos. Esto no afecta a las sesiones de usuario activas. El ícono ⏰ aparece en la fila del usuario para mostrar que su contraseña venció. Una vez que se produce el vencimiento de la contraseña, no es posible deshacerlo. Esta casilla de verificación se deselecciona la próxima vez que se edita la cuenta de usuario.
Restablecer formulario	Elimina los cambios que están en curso.

Pestaña Funciones

En la siguiente tabla se proporcionan descripciones de las opciones de la pestaña Funciones. La pestaña Funciones muestra las funciones que están asignadas al usuario.

Opción	Descripción
+	Abre el cuadro de diálogo Agregar función que indica las funciones que podría asignar al usuario.
−	Elimina la función seleccionada para que no se asigne al usuario.
	Muestra los permisos de la función seleccionada.
Nombre	Indica cada función asignada al usuario.

Pestaña Funciones

En este tema se presentan las funciones de Admin > vista Seguridad > pestaña Funciones.

Se asignan funciones a todos los usuarios deNetWitness Suite. Los usuarios reciben los permisos que permiten las funciones. En la pestaña Funciones puede crear, duplicar, editar y eliminar una función. También puede ver una lista de todas las funciones y sus permisos respectivos.

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Ver funciones preconfiguradas	Paso 1. Revisar las funciones preconfiguradas de NetWitness
Administrador	Cree una función nueva	Paso 2. (Opcional) Agregar una función y asignar permisos

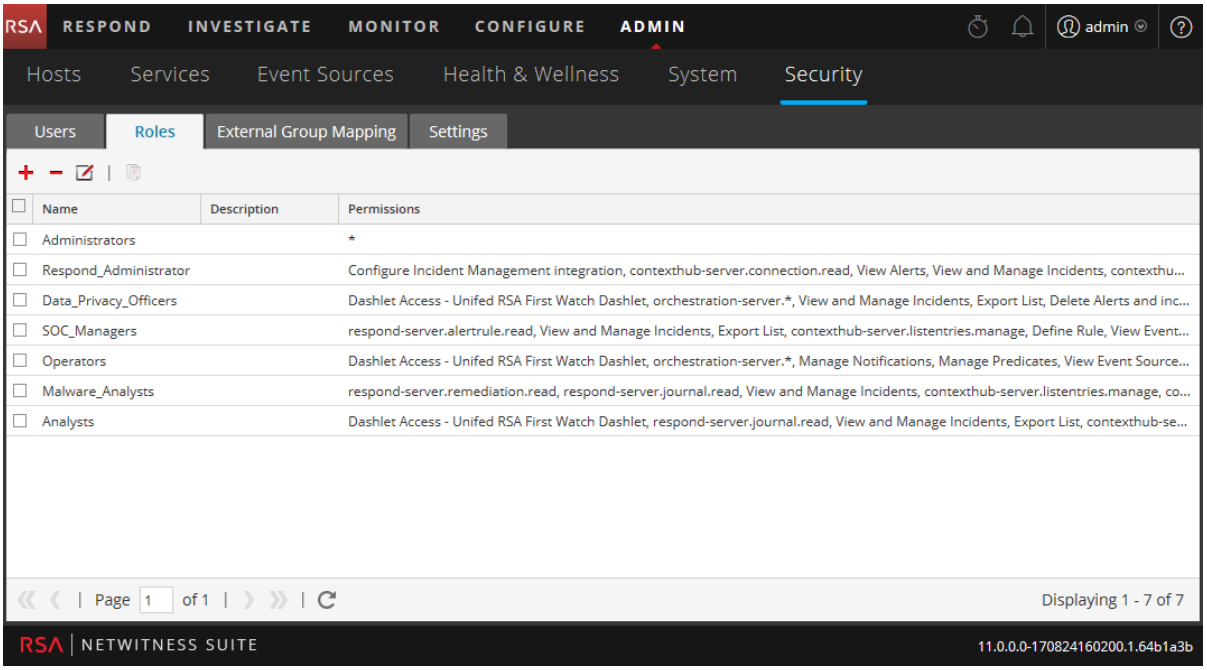
Temas relacionados

- Cuadro de diálogo Agregar/Editar función

Para acceder a esta vista:

1. Vaya a **ADMIN > Seguridad**.
   La vista Seguridad se abre de forma predeterminada en la pestaña **Usuarios**.

2. Haga clic en la pestaña **Funciones**.



La pestaña Funciones consta de la lista Funciones con una barra de herramientas en la parte superior.

En la siguiente tabla se describen las funciones de la barra de herramientas.

Función	Descripción
+	Muestra el cuadro de diálogo Agregar función.
✎	Muestra el cuadro de diálogo Editar función.
−	Muestra un mensaje de advertencia y pide confirmación cuando desea eliminar una función.
⧉	Duplica una función para guardarla con otro nombre.

En la siguiente tabla se describen las características de la lista Funciones.

Columna	Descripción
Nombre	Muestra el nombre de una función que puede otorgarse a un usuario.
Descripción	Muestra una descripción de la función.

Columna	Descripción
Permisos	Muestra los permisos asignados a la función.

Cuadro de diálogo Agregar/Editar función

En este tema se presentan los cuadros de diálogo Agregar función y Editar función, a los cuales se accede desde Admin > vista Seguridad > pestaña Funciones.

En los cuadros de diálogo Agregar función y Editar función, puede agregar o editar una función y los permisos que se le asignan. También puede especificar atributos de manejo de consultas para los miembros de la función con el fin de controlar la información que pueden recuperar. La estructura de estos cuadros de diálogo es igual. La única diferencia es que se agrega una función nueva o que se modifica una función existente.

Cuando cambia los permisos de una función y después que la función se guarda, el cambio se aplica de inmediato a los usuarios a quienes se asigna esa función específica.

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Ver funciones preconfiguradas	Paso 1. Revisar las funciones preconfiguradas de NetWitness
Administrador	Cree una función nueva	Paso 2. (Opcional) Agregar una función y asignar permisos
Administrador	Editar una función	Paso 2. (Opcional) Agregar una función y asignar permisos
Administrador	Eliminar una función	Paso 2. (Opcional) Agregar una función y asignar permisos

Para acceder a esta vista:

1. En NetWitness Suite, vaya a **ADMIN > Seguridad**.
   La vista Seguridad se abre de forma predeterminada en la pestaña **Usuarios**.
2. Haga clic en la pestaña **Funciones**.

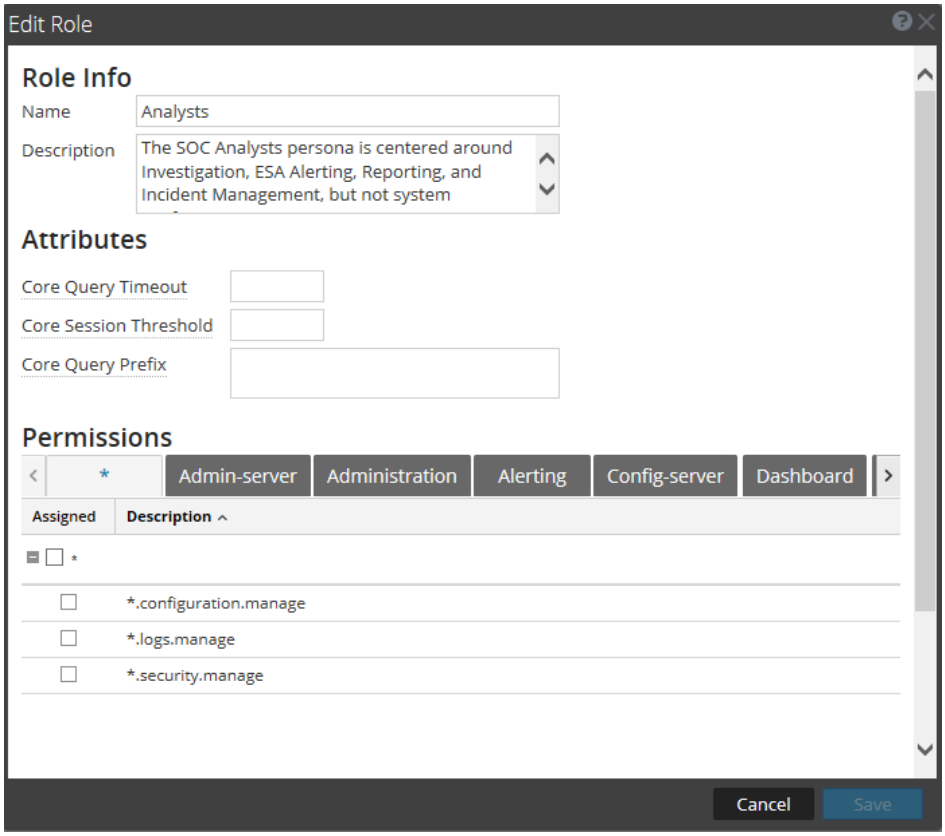
3. Realice una de las siguientes acciones:

   - En la barra de acciones, haga clic en  .

     Se muestra el cuadro de diálogo **Agregar función**.

   - Seleccione una función y, en la barra de acciones, haga clic en  .

     Se muestra el cuadro de diálogo **Editar función**.



Los cuadros de diálogo Agregar función y Editar función incluyen tres secciones: **Información de función**, **Atributos** y **Permisos**.

Información de función

Esta es la información de la sección **Información de función**.

Función	Descripción
Nombre	El nombre de la función de usuario.
Descripción	Una descripción opcional de la función del usuario.

Atributos

Esta es la información de la sección **Atributos**. Un valor mostrado en cursiva indica un valor predeterminado; por ejemplo, *5*. Un valor que no se muestra en cursiva indica un cambio respecto del valor predeterminado; por ejemplo, `1200`. Paso 3. Verificar atributos de consultas y sesiones por función se proporciona más información.

Función	Descripción
Tiempo de espera agotado de consulta de Core	(Opcional) Especifica la cantidad máxima de minutos que un usuario puede ejecutar una consulta. El valor predeterminado es 5 minutos. Este tiempo de espera solo se aplica a las consultas que se ejecutan desde Investigation. Si se configura este valor, debe ser cero (0) o mayor. Un valor de cero especifica que no hay un tiempo de espera. Cuando se migra a NetWitness Suite 10.5 y superior, si no hay ningún valor configurado en las funciones, 5 minutos se configura de manera predeterminada. **Nota:** NetWitness Suite 10.5 y los servicios principales superiores usan este campo.
Umbral de sesión de Core	Controla la forma en que el servicio escanea valores de metadatos para determinar los conteos de las sesiones. Este valor debe ser cero (0) o mayor. Si este valor es mayor de cero, una optimización de consulta extrapolará los conteos de sesiones totales que superen el umbral. Cuando el valor de metadatos que devuelve la consulta alcance el umbral, el sistema: • Detendrá su determinación del conteo de sesiones • Mostrará el umbral y el porcentaje de tiempo de consulta utilizado para alcanzar el umbral El valor predeterminado es `100000`. El límite que especifica aquí reemplaza el valor **Máximo de exportación de sesiones** definido en la configuración de la vista INVESTIGATE.

Función	Descripción
Prefijo de consulta de Core	(Opcional) Filtra los resultados de la consulta para restringir lo que ven los miembros de la función. De forma predeterminada, este valor está en blanco. Por ejemplo, se antepone el prefijo de consulta `'service' = 80` a cualquier consulta que ejecute el usuario y este solo puede acceder a metadatos de sesiones HTTP.

Permisos

Esta es la información de la sección **Permisos**. En Permisos de función se describen los permisos.

Función	Descripción
Pestañas de módulos	Hay ocho pestañas, una para cada módulo: Administration, Alerting, Incidents, Investigation, Live, Malware, Reports y Dashboard. Cada pestaña indica los permisos de un módulo.
Columna Descripción	Lista de todos los permisos del módulo.
Columna Asignado	Casilla de verificación que indica si asignó permiso de módulo a la función.
Guardar	Guarda la función con los permisos seleccionados que se le asignaron.
Cancelar	Cancela el trabajo y cierra el cuadro de diálogo.

Pestaña Mapeo de grupo externo

Si configuró la autenticación externa de usuarios, puede mapear funciones de usuario deNetWitness Suite a un grupo externo. La pestaña Mapeo de grupo externo proporciona información sobre cada grupo externo al cual mapeó funciones.

¿Qué desea hacer?

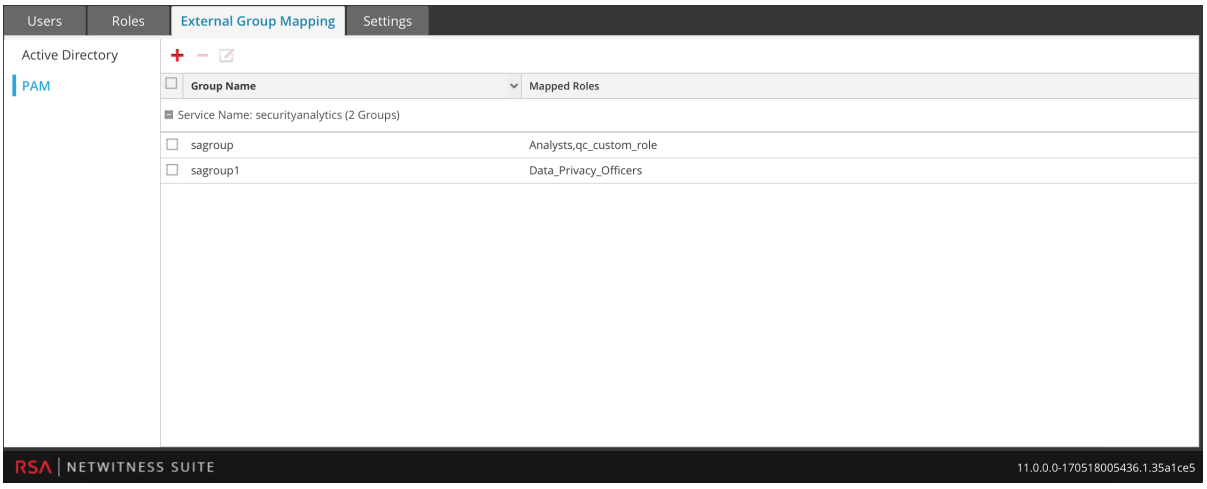
Función	Deseo…	Mostrarme cómo
Administrador	Mapear una función a un grupo externo	Paso 5. (Opcional) Mapear funciones de usuario a grupos externos
Administrador	Buscar un grupo externo	Buscar grupos externos

Temas relacionados

- Cuadro de diálogo Agregar asignación de funciones
- Cuadro de diálogo Buscar grupos externos

Para acceder a esta vista:

1. En NetWitness Suite, vaya a **ADMIN > Seguridad**.
   La vista Seguridad se muestra con la pestaña **Usuarios** abierta.
2. Haga clic en la pestaña **Mapeo de grupo externo**.



La pestaña Mapeo de grupo externo consta de una barra de herramientas y una lista.

La lista tiene las siguientes funciones.

Función	Descripción
Tipo de grupo	En la columna de la izquierda, haga clic en **Active Directory** o **PAM** para mostrar los grupos correspondientes al tipo seleccionado.
Cuadro de selección	En una fila, alterna la selección de un nombre de grupo. En la barra de título, alterna la selección de todos los nombres de grupo.
Nombre del grupo	Muestra el nombre del grupo externo que tiene acceso a NetWitness Suite.
Funciones mapeadas	Muestra las funciones de NetWitness Suite mapeadas al grupo externo.

La **barra de herramientas** tiene las siguientes funciones.

Función	Descripción
	Muestra el cuadro de diálogo Agregar asignación de funciones, en el cual puede seleccionar un grupo externo y mapearlo a una función deNetWitness Suite.
	Muestra un mensaje de advertencia y solicita confirmación para quitar todas las funciones de NetWitness Suite mapeadas al grupo externo.
	Muestra el cuadro de diálogo Editar asignación de funciones, en el cual puede agregar funciones de NetWitness Suite al grupo externo o quitarlas.

Cuadro de diálogo Agregar asignación de funciones

En este tema se presentan las funciones de Admin > Seguridad > pestaña Mapeo de grupo externo > cuadro de diálogo Agregar asignación de funciones.

En NetWitness Suite, cada función de usuario tiene su propio conjunto de permisos. Puede mapear una o más funciones deNetWitness Suite a un grupo externo, lo cual otorga al grupo el mismo conjunto de permisos que tiene cada función.

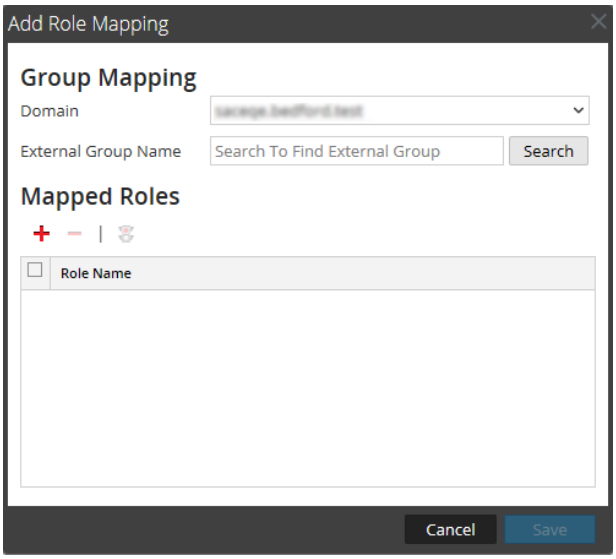
¿Qué desea hacer?

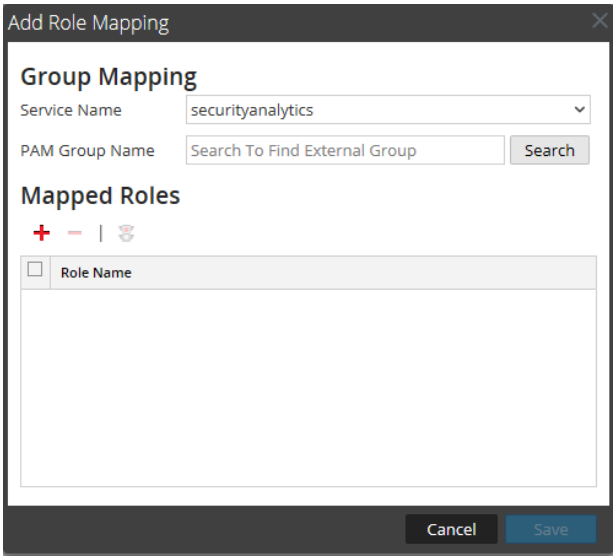
Función	Deseo…	Mostrarme cómo
Administrador	Mapear una función a un grupo externo	Paso 5. (Opcional) Mapear funciones de usuario a grupos externos
Administrador	Buscar un grupo externo	Buscar grupos externos

Para acceder a este cuadro de diálogo:

1. En NetWitness Suite, vaya a **ADMIN > Seguridad**.
2. Haga clic en la pestaña **Mapeo de grupo externo**.
3. En la barra de herramientas, haga clic en +.

   Se muestra el cuadro de diálogo **Agregar asignación de funciones** correspondiente al método de autenticación externo que configuró.





Los cuadros de diálogo Agregar asignación de funciones y Editar asignación de funciones son casi idénticos. La única diferencia es que en el cuadro de diálogo Editar asignación de funciones no puede realizar búsquedas.

Mapeo de grupos

La sección **Mapeo de grupos** tiene las siguientes funciones.

Función	Descripción
Dominio	Se muestra si configuró Active Directory para la autenticación externa de usuarios. Es el nombre de dominio del grupo AD externo al cual se mapean las funciones.

Función	Descripción
Nombre de grupo externo	Se muestra si configuró Active Directory para la autenticación externa de usuarios. Es el grupo externo al cual se mapean las funciones.
Nombre del grupo PAM	Se muestra si configuró PAM para la autenticación externa de usuarios. Es el nombre del grupo externo al cual se mapean las funciones.
Buscar	Muestra un cuadro de diálogo de búsqueda en el cual puede buscar grupos externos. La búsqueda no está disponible en el cuadro de diálogo Editar asignación de funciones.

Funciones mapeadas

La sección **Funciones mapeadas** tiene las siguientes funciones.

Función	Descripción
+	Abre el cuadro de diálogo Agregar función, en el cual se muestran las funciones de usuario de NetWitness Suite configuradas que se agregarán.
−	Elimina las funciones seleccionadas de la cuadrícula Funciones mapeadas.
Nombre	Muestra el nombre de la función del usuario de NetWitness Suite.
Permisos	Muestra los permisos asociados con la función de usuario de NetWitness Suite.
Cancelar	Cancela el mapeo de un grupo nuevo o el mapeo de un grupo modificado y cierra el cuadro de diálogo.
Guardar	Guarda el mapeo de un grupo nuevo o el mapeo de un grupo modificado y cierra el cuadro de diálogo.

Cuadro de diálogo Buscar grupos externos

En este tema se describen las funciones de Admin > vista Seguridad > cuadro de diálogo Buscar grupos externos.

Si configuró la autenticación externa de usuarios, puede mapear funciones de usuario de NetWitness Suite a grupos externos. Busque grupos externos para seleccionar los grupos a los cuales desea mapear funciones de NetWitness Suite.

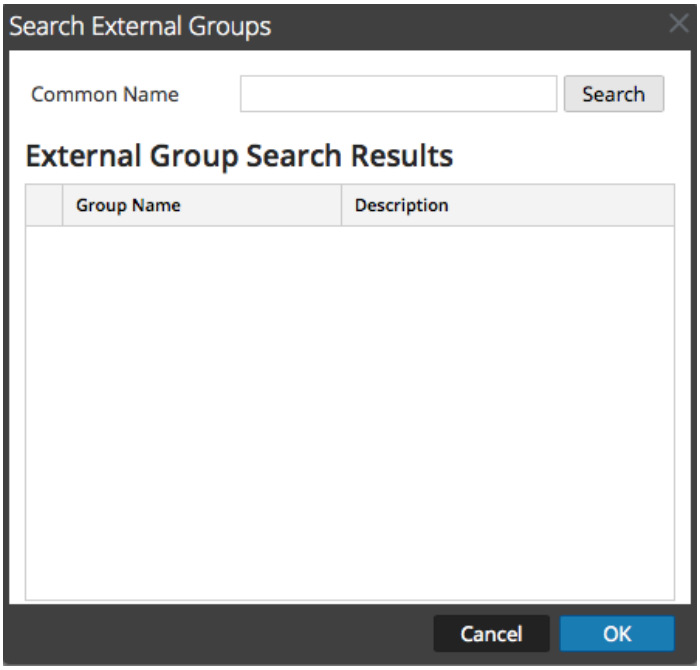
¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Mapear una función a un grupo externo	Paso 5. (Opcional) Mapear funciones de usuario a grupos externos
Administrador	Ver mapeos de grupos externos	Pestaña Mapeo de grupo externo
Administrador	Buscar grupos externos	Buscar grupos externos

Para acceder a este cuadro de diálogo:

1. Vaya a **ADMIN > Seguridad**.
   La vista Seguridad se muestra con la pestaña **Usuarios** abierta.
2. Haga clic en la pestaña **Mapeo de grupo externo**.
3. En la barra de herramientas, haga clic en +.
   Se muestra el cuadro de diálogo Agregar asignación de funciones correspondiente al método de autenticación externo que configuró.
4. En la sección Mapeo de grupos, seleccione un **dominio**.

5. En la sección Mapeo de grupos, haga clic en **Buscar**.
   Se muestra el cuadro de diálogo **Buscar grupos externos**.



En la siguiente tabla se describen las funciones del cuadro de diálogo Buscar grupos externos.

Función	Descripción
Nombre común	Nombre de grupo para el cual está realizando la búsqueda. Puede ser el nombre exacto o puede contener el carácter comodín (*) para que coincida con cualquier carácter.
Nombre del grupo	Grupo externo al cual puede mapear funciones.
Descripción	Texto opcional sobre el grupo.
Aceptar	Muestra el cuadro de diálogo Agregar asignación de funciones con el grupo externo que seleccionó.
Cancelar	Cierra el cuadro de diálogo.

Pestaña Ajustes de configuración

En este tema se presenta una explicación de Admin > vista Seguridad > pestaña Ajustes de configuración. La pestaña Ajustes de configuración permite establecer la complejidad de las contraseñas para los usuarios internos de NetWitness Suite y los parámetros de seguridad de todo el sistema.

Para obtener información sobre la configuración de la seguridad de NetWitness Suite, consulte Configurar la seguridad del sistema.

Los requisitos de complejidad de las contraseñas se aplican solo a los usuarios internos y no se imponen a los usuarios externos. Los usuarios externos dependen de sus propios métodos y sistemas para imponer la complejidad de las contraseñas.

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Administrador	Configurar la complejidad de las contraseñas	Paso 1. Configurar la complejidad de las contraseñas
Administrador	Configurar ajustes de seguridad en el nivel del sistema	Paso 3. Configurar ajustes de seguridad en el nivel del sistema
Administrador	(Opcional) Configurar la autenticación externa	Paso 4. (Opcional) Configurar la autenticación externa

Temas relacionados

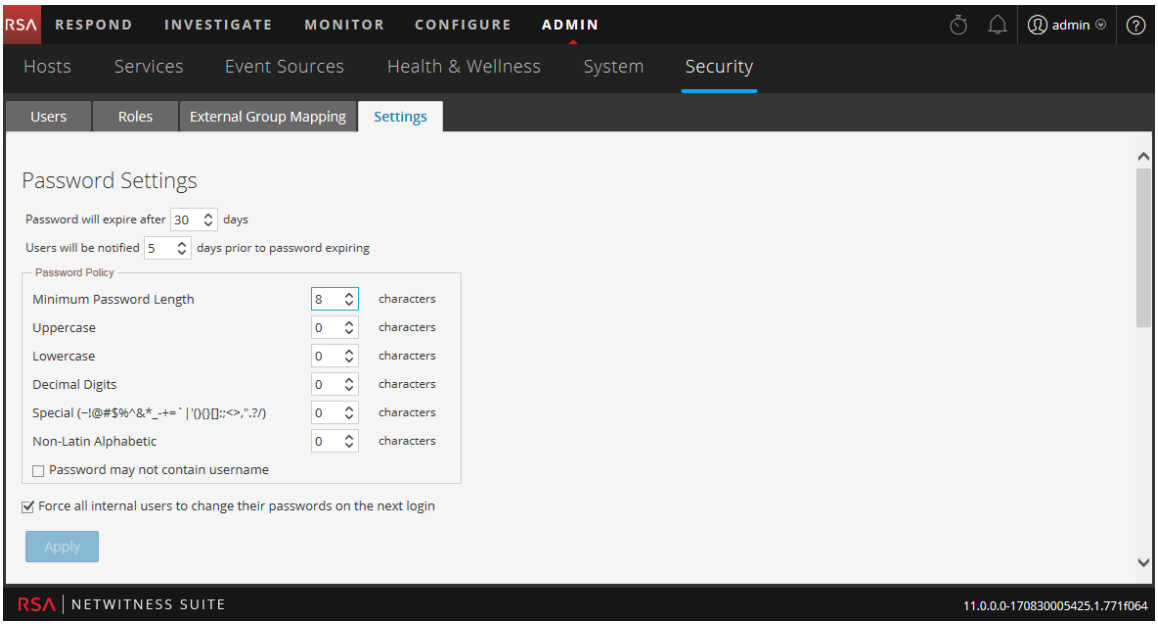
- Configurar la seguridad del sistema

Pestaña Ajustes de configuración de la vista Seguridad de Admin

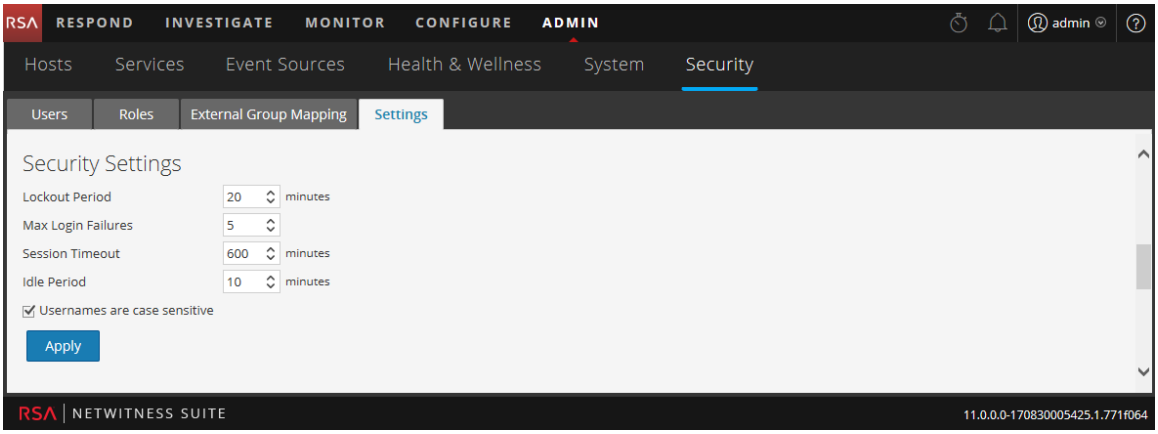
Para acceder a la pestaña Ajustes de configuración:

1. Vaya a **ADMIN > Seguridad**.
   La vista Seguridad se muestra con la pestaña **Usuarios** abierta.
2. Haga clic en la pestaña **Ajustes de configuración**.

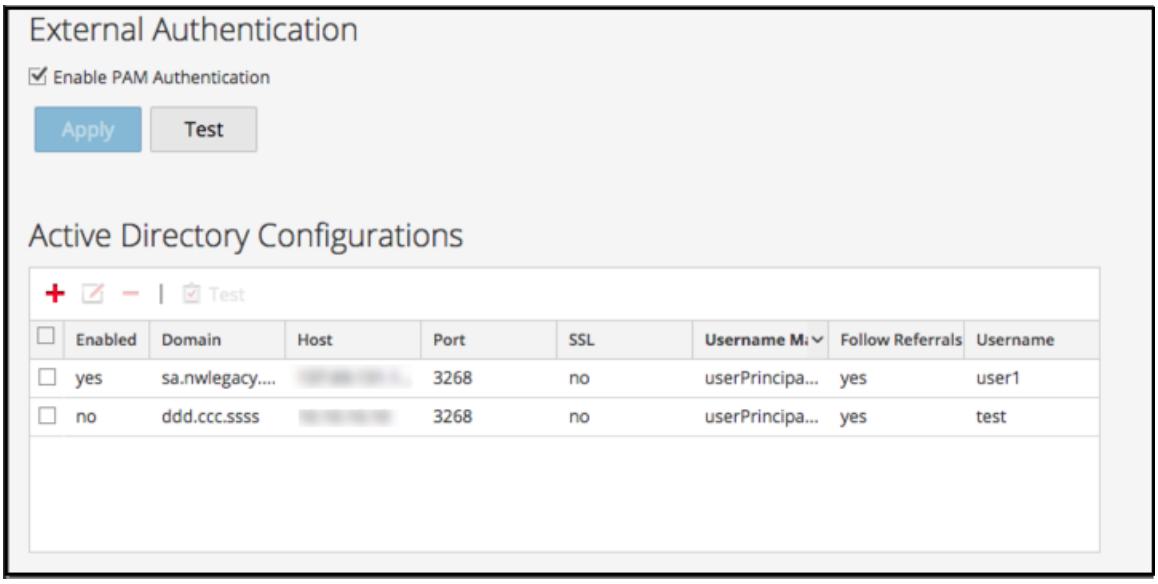
En la siguiente figura se muestra la sección Configuración de contraseña de la pestaña Ajustes de configuración.



En la siguiente figura se muestra la sección Configuración de seguridad de la pestaña Ajustes de configuración.



En la siguiente figura se muestran las secciones Autenticación de PAM y Configuraciones de Active Directory de la pestaña Ajustes de configuración.



Configuración de contraseña

La sección Política de contraseña permite establecer requisitos de complejidad de las contraseñas para los usuarios internos de NetWitness Suite cuando configuran sus contraseñas.

Opción	Descripción
La contraseña vencerá después de <n> días	La cantidad predeterminada de días antes de que venza una contraseña para todos los usuarios internos de NetWitness Suite. Un valor de cero (0) deshabilita el vencimiento de la contraseña. Para instalaciones nuevas, el valor predeterminado es 30. Para las actualizaciones, el valor anterior migra automáticamente a la instalación actualizada.
Se notificará a los usuarios <n> días antes del vencimiento de la contraseña.	La cantidad de días antes de la fecha de vencimiento de la contraseña que se informará a un usuario que su contraseña está a punto de vencer. Los usuarios reciben un único correo electrónico en la fecha especificada antes de que sus contraseñas venzan. También ven un cuadro de diálogo Mensaje de vencimiento de contraseña cuando inician sesión en NetWitness Suite. El valor mínimo es 1 día.

Opción	Descripción
Longitud mínima de la contraseña	Especifica un requisito de longitud mínima de la contraseña para las contraseñas de los usuarios de NetWitness Suite. Una longitud mínima de la contraseña impide que los usuarios usen contraseñas cortas que se pueden adivinar con facilidad.
Mayúscula	Especifica una cantidad mínima de caracteres en mayúscula para la contraseña. Esto incluye caracteres del idioma europeo de la A a la Z, con signos diacríticos, caracteres griegos y caracteres cirílicos. Por ejemplo: • Mayúscula cirílica: Д Ц • Mayúscula griega: Π Λ
Minúscula	Especifica una cantidad mínima de caracteres en minúscula para la contraseña. Esto incluye caracteres del idioma europeo de la a a la z, ese-zeta, con signos diacríticos, caracteres griegos y caracteres cirílicos. Por ejemplo: • Minúscula cirílica: д ц • Minúscula griega: π λ
Números	Especifica una cantidad mínima de caracteres decimales (del cero al nueve) para la contraseña.
Especial (~!@#$%^&*_-+=`|'(){}[]:;<>,".?/)	Especifica una cantidad mínima de caracteres especiales para la contraseña: `~!@#$%^&*_-+=`|'(){}[]:;<>,".?/`
Alfabético no latino	Especifica una cantidad mínima de caracteres alfabéticos Unicode que no correspondan a mayúscula ni minúscula. Esto incluye caracteres Unicode de idiomas asiáticos. Por ejemplo: • Kanji (japonés): 頁 (hoja) 枒 (árbol)

Opción	Descripción
La contraseña no puede contener el nombre de usuario	Especifica que una contraseña no puede contener el nombre del usuario sin distinción de mayúsculas y minúsculas.
Obligar a todos los usuarios internos a cambiar sus contraseñas en el próximo inicio de sesión	Exige a todos los usuarios internos que cambien sus contraseñas la próxima vez que inicien sesión en NetWitness Suite en lugar de hacerlo cuando crean o cambian sus contraseñas. Tenga en cuenta que esta configuración se selecciona de forma predeterminada.
Aplicar	Los ajustes de seguridad de las contraseñas se aplican cuando los usuarios de NetWitness Suite crean o cambian sus contraseñas. Si la opción **Obligar a todos los usuarios internos a cambiar sus contraseñas en el próximo inicio de sesión** está seleccionada, todos los usuarios internos deben cambiar su contraseña la próxima vez que inician sesión en NetWitness Suite.

Configuración de seguridad

La sección Configuración de seguridad permite establecer ajustes de seguridad globales para los usuarios de NetWitness Suite.

Opción	Descripción
Periodo de bloqueo	La cantidad de minutos para bloquear a un usuario de NetWitness Suite después de que se haya excedido la cantidad configurada de inicios de sesión fallidos. El valor predeterminado es 20 minutos.

Opción	Descripción
Número máximo de errores al iniciar sesión	La cantidad máxima de intentos de inicio de sesión fallidos antes de que un usuario se bloquee. El valor predeterminado es 5
Tiempo de espera de sesión agotado	La duración máxima de una sesión de usuario antes de que se agote el tiempo de espera en minutos. El valor predeterminado es 600. Si el valor es 0, no hay tiempo máximo para una sesión. Si el valor es un número entero positivo, el tiempo de espera de la sesión se agota cuando ha transcurrido el tiempo de espera configurado. El usuario debe volver a iniciar sesión.
Periodo de inactividad	La cantidad de minutos de inactividad antes de que se agote el tiempo de espera de una sesión. El valor predeterminado es 10. Si el valor es 0, no se agotará el tiempo de espera de la sesión.
Los nombres de usuario distinguen mayúsculas de minúsculas	Seleccione esta opción si desea que el campo Nombre de usuario en la pantalla de inicio de sesión de NetWitness Suite distinga mayúsculas de minúsculas. Por ejemplo, si los nombres de usuario distinguen mayúsculas de minúsculas, podría usar admin para iniciar sesión en NetWitness Suite, pero no podría usar Admin.
Aplicar	Los cambios se implementan de inmediato.

Autenticación de PAM

La sección Autenticación de PAM permite configurar NetWitness Suite de modo que use Active Directory o PAM para autenticar y probar nombres de inicio de sesión del usuario externos.

Opción	Descripción
Habilitar autenticación PAM	Permite a NetWitness Suite usar módulos de autenticación con capacidad para conectarse (PAM) para autenticar los inicios de sesión de usuarios externos.
Aplicar	Hace que los ajustes de configuración de PAM entre en vigor en el próximo inicio de sesión.
Probar	Solicita un nombre de usuario y una contraseña, y después prueba el método de autenticación de PAM habilitado actualmente.

Configuraciones de Active Directory

La sección Configuraciones de Active Directory permite configurar NetWitness Suite de modo que use Active Directory para autenticar nombres de inicio de sesión del usuario externos.

Opción	Descripción
Habilitado	Habilita la autenticación de Active Directory para los usuarios de NetWitness Suite.
Dominio	El nombre del dominio donde se encuentra el servicio Active Directory.
Host	El nombre de host o la dirección IP donde se encuentra el servicio Active Directory
Puerto	El puerto en el host que se utiliza para la autenticación del servicio Active Directory.
SSL	Indica si el servicio Active Directory usa SSL.
Mapeo de nombres de usuario	Indica el campo de búsqueda de Active Directory que se usará para el mapeo de nombres de usuario. Puede especificar userPrincipalName (UPN) o sAMAccountName.
Seguir referencias	Indica siNetWitness Suite seguirá las referencias de LDAP que hace Active Directory.

Opción	Descripción
Nombre de usuario	Si el nombre de usuario se proporciona aquí, se vincula al servicio Active Directory mientras se buscan grupos de Active Directory. Esta credencial no se usa con ningún otro propósito.