Integración de Security Manager con ACS

Contenido

Introducción

Este documento describe cómo integrar Cisco Security Manager con Cisco Secure Access Control Server (ACS).

Cisco Secure ACS proporciona autorización de comandos a los usuarios que utilizan aplicaciones de administración, como Cisco Security Manager, para configurar los dispositivos de red gestionados. La compatibilidad con la autorización de comandos se proporciona mediante tipos de conjuntos de autorización de comandos únicos, llamados roles en Cisco Security Manager, que contienen un conjunto de permisos. Estos permisos, también denominados privilegios, determinan las acciones que pueden realizar los usuarios con funciones específicas dentro de Cisco Security Manager.

Cisco Secure ACS utiliza TACACS+ para comunicarse con las aplicaciones de administración. Para que Cisco Security Manager se comunique con Cisco Secure ACS, debe configurar el servidor CiscoWorks en Cisco Secure ACS como un cliente AAA que utilice TACACS+. Además, debe proporcionar al servidor CiscoWorks el nombre de administrador y la contraseña que utiliza

para iniciar sesión en Cisco Secure ACS. Cuando cumple estos requisitos, garantiza la validez de las comunicaciones entre Cisco Security Manager y Cisco Secure ACS.

Cuando Cisco Security Manager se comunica inicialmente con Cisco Secure ACS, indica a Cisco ACS la creación de funciones predeterminadas, que aparecen en la sección Componentes de Perfil Compartidos de la interfaz HTML de Cisco Secure ACS. También dicta un servicio personalizado que debe ser autorizado por TACACS+. Este servicio personalizado aparece en la página TACACS+ (Cisco IOS®) de la sección Configuración de la interfaz de la interfaz HTML. A continuación, puede modificar los permisos incluidos en cada función de Cisco Security Manager y aplicar estas funciones a usuarios y grupos de usuarios.

Nota: No es posible integrar CSM con ACS 5.2 ya que no es compatible.

Prerequisites

Requirements

Para utilizar Cisco Secure ACS, asegúrese de que:

- Usted define roles que incluyen los comandos requeridos para realizar las funciones necesarias en Cisco Security Manager.
- La restricción de acceso a la red (NAR) incluye el grupo de dispositivos (o los dispositivos) que desea administrar, si aplica un NAR al perfil.
- Los nombres de los dispositivos administrados se escriben y capitalizan de forma idéntica en Cisco Secure ACS y en Cisco Security Manager.

Componentes Utilizados

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

- Cisco Security Manager versión 3.0
- Cisco Secure ACS versión 3.3

Nota: Asegúrese de elegir las versiones compatibles de CSM y ACS antes de instalar en su entorno de red. Por ejemplo, Cisco probó ACS 3.3 con sólo CSM 3.0 y se detuvo para versiones CSM posteriores. Por lo tanto, se recomienda utilizar CSM 3.0 con ACS 3.3. Consulte la tabla Matriz de compatibilidad para obtener más información sobre varias versiones de software.

Versiones de Cisco Security Manager	Versiones ACS de CS probadas
3.0.0 3.0.0 SP1	Windows 3.3(3) y 4.0(1)
3.0.1 3.0.1 SP1 3.0.1 SP2	Motor de soluciones 4.0(1) Windows 4.0(1)
3.1.0 3.0.2	Motor de soluciones 4.0(1) Windows 4.1(1) y 4.1(3)
3.1.1 3.0.2 SP1 3.0.2 SP2	Motor de soluciones v4.0(1) Windows 4.1(2), 4.1(3) y 4.1(4)
3.1.1 SP1	Motor de soluciones 4.0(1) Windows 4.1(4)

3.1.1 SP2	Motor de soluciones 4.0(1) Windows 4.1(4) y 4.2(0)
3.2.0	Motor de soluciones 4.1(4) Windows 4.1(4) y 4.2(0)
3.2.1	Motor de soluciones 4.1(4) Windows 4.2(0)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Integre Cisco Security Manager con Cisco Secure ACS

En esta sección se describen los pasos necesarios para integrar Cisco Security Manager con Cisco Secure ACS. Algunos pasos contienen varios subpasos. Estos pasos y subpasos deben realizarse en orden. Esta sección también contiene referencias a procedimientos específicos utilizados para realizar cada paso.

Complete estos pasos:

1. **Planifique su modelo de autorización y autenticación administrativa.**Debe decidir sobre su modelo administrativo antes de utilizar Cisco Security Manager. Esto incluye la definición de las funciones administrativas y las cuentas que planea utilizar.**Sugerencia:** Cuando defina las funciones y los permisos de los administradores potenciales, considere también si desea activar o no el flujo de trabajo. Esta selección afecta a la forma de restringir el acceso.
2. **Instale Cisco Secure ACS, Cisco Security Manager y CiscoWorks Common Services.**Instale Cisco Secure ACS versión 3.3 en un servidor Windows 2000/2003. Instale CiscoWorks Common Services y Cisco Security Manager en un servidor diferente de Windows 2000/Windows 2003.Si desea más información, consulte estos documentos:Guía de instalación de Cisco Security Manager 3.0Guía de instalación de Cisco Secure ACS para Windows 3.3**Nota:** Consulte la tabla Matriz de compatibilidad para obtener más información antes de elegir las versiones de software CSM y ACS.
3. **Realice procedimientos de integración en Cisco Secure ACS.**Defina los usuarios de Cisco Security Manager como usuarios ACS y asígnelos a grupos de usuarios en función de su función planificada, agregue todos sus dispositivos administrados (así como el servidor de CiscoWorks/Security Manager) como clientes AAA y cree un usuario de control de administración. Consulte Procedimientos de Integración Realizados en Cisco Secure ACS para obtener más información.
4. **Realice procedimientos de integración en CiscoWorks Common Services.**Configure un usuario local que coincida con el administrador definido en Cisco Secure ACS, defina ese mismo usuario para la configuración de la identidad del sistema y configure ACS como el modo de configuración AAA.Consulte Procedimientos de Integración Realizados en CiscoWorks para obtener más información.

5. **Asignar funciones a grupos de usuarios en Cisco Secure ACS.**Asigne funciones a cada grupo de usuarios configurado en Cisco Secure ACS. El procedimiento que utilice depende de si ha configurado grupos de dispositivos de red (NDG).Consulte Asignación de Funciones a Grupos de Usuarios en Cisco Secure ACS para obtener más información.

Procedimientos de integración realizados en Cisco Secure ACS

Esta sección describe los pasos que debe completar en Cisco Secure ACS para integrarlo con Cisco Security Manager:

1. Definir usuarios y grupos de usuarios en Cisco Secure ACS
2. Agregar dispositivos administrados como clientes AAA en Cisco Secure ACS
3. Crear un usuario de control de administración en Cisco Secure ACS

Definir usuarios y grupos de usuarios en Cisco Secure ACS

Todos los usuarios de Cisco Security Manager deben estar definidos en Cisco Secure ACS y se les debe asignar una función adecuada a su función de trabajo. La forma más sencilla de hacerlo es dividir a los usuarios en diferentes grupos según cada función predeterminada disponible en ACS. Por ejemplo, asigne todos los administradores del sistema a un grupo, todos los operadores de red a otro grupo, etc. Consulte Funciones Predeterminadas de Cisco Secure ACS para obtener más información sobre las funciones predeterminadas en ACS.

Además, debe crear un usuario adicional al que se asigne la función de administrador del sistema con permisos completos. Las credenciales establecidas para este usuario se utilizan posteriormente en la página Configuración de identidad del sistema de CiscoWorks. Consulte Definición del Usuario de Identidad del Sistema para obtener más información.

Tenga en cuenta que en esta etapa simplemente se asignan usuarios a diferentes grupos. La asignación real de roles a estos grupos se realiza más tarde, después de que CiscoWorks, Cisco Security Manager y cualquier otra aplicación se registren en Cisco Secure ACS.

Sugerencia: Antes de continuar, instale CiscoWorks Common Services y Cisco Security Manager en un servidor de Windows 2000/2003. Instale Cisco Secure ACS en otro servidor de Windows 2000/2003.

1. Inicie sesión en Cisco Secure ACS.
2. Configure un usuario con permisos completos:Haga clic en **User Setup** en la barra de navegación.En la página User Setup (Configuración de usuario), introduzca un nombre para el nuevo usuario y, a continuación, haga clic en **Add/Edit (Agregar/editar)**.Seleccione un método de autenticación en la lista Autenticación de contraseña en Configuración de usuario.Introduzca y confirme la contraseña del nuevo usuario.Seleccione **Grupo 1** como el grupo al que se asigna el usuario.Haga clic en **Enviar** para crear la cuenta de usuario.
3. Repita el paso 2 para cada usuario de Cisco Security Manager. Cisco recomienda dividir los usuarios en grupos según la función que cada usuario tenga asignada:Grupo 1: Administradores del sistemaGrupo 2: Administradores de seguridadGrupo 3: aprobadores de seguridadGrupo 4: administradores de redGrupo 5: aprobadoresGrupo 6: operadores de redGrupo 7: soporte técnicoVea la tabla para obtener más información sobre los permisos predeterminados asociados a cada función. Consulte Personalización de las Funciones ACS

de Cisco Secure para obtener más información sobre la personalización de las funciones de usuario.**Nota:** En esta etapa, los propios grupos son colecciones de usuarios sin ninguna definición de rol. Después de completar el proceso de integración, se asignan funciones a cada grupo. Consulte Asignación de Funciones a Grupos de Usuarios en Cisco Secure ACS para obtener más información.
4. Cree un usuario adicional y asigne este usuario al grupo de administradores del sistema. Las credenciales establecidas para este usuario se utilizan posteriormente en la página Configuración de identidad del sistema de CiscoWorks. Consulte Definición del Usuario de Identidad del Sistema para obtener más información.
5. Continúe con Agregar dispositivos administrados como clientes AAA en Cisco Secure ACS.

Agregar dispositivos administrados como clientes AAA en Cisco Secure ACS

Antes de poder comenzar a importar dispositivos a Cisco Security Manager, primero debe configurar cada dispositivo como cliente AAA en Cisco Secure ACS. Además, debe configurar el servidor de CiscoWorks/Security Manager como un cliente AAA.

Si Cisco Security Manager administra contextos de seguridad configurados en dispositivos de firewall, que incluyen contextos de seguridad configurados en FWSM para dispositivos Catalyst 6500/7600, cada contexto se debe agregar individualmente a Cisco Secure ACS.

El método que se utiliza para agregar dispositivos administrados depende de si se desea restringir el acceso de los usuarios a un conjunto concreto de dispositivos con grupos de dispositivos de red (NDG). Vea una de estas secciones:

- Si desea que los usuarios tengan acceso a todos los dispositivos, agregue los dispositivos como se describe en Agregar dispositivos como clientes AAA sin NDG.
- Si desea que los usuarios tengan acceso sólo a ciertos NDG, agregue los dispositivos tal y como se describe en Configurar grupos de dispositivos de red para su uso en el Administrador de seguridad.

Agregar dispositivos como clientes AAA sin NDG

Este procedimiento describe cómo agregar dispositivos como clientes AAA de un Cisco Secure ACS. Refiérase a la sección *Configuración del Cliente AAA de* Configuración de Red para obtener información completa sobre todas las opciones disponibles.

Nota: Recuerde agregar el servidor de CiscoWorks/Security Manager como cliente AAA.

1. Haga clic en **Configuración de red** en la barra de navegación de Cisco Secure ACS.
2. Haga clic en **Agregar entrada** debajo de la tabla Clientes AAA.
3. Introduzca el nombre de host del cliente AAA (hasta 32 caracteres) en la página Add AAA Client (Agregar cliente AAA). El nombre de host del cliente AAA debe coincidir con el nombre de visualización que planea utilizar para el dispositivo en Cisco Security Manager.Por ejemplo, si desea agregar un nombre de dominio al nombre del dispositivo en Cisco Security Manager, el nombre de host del cliente AAA en ACS debe ser **<nombre_dispositivo>.<nombre_dominio>** .Cuando nombre el servidor de CiscoWorks, se recomienda utilizar el nombre de host completo. Asegúrese de escribir correctamente el nombre de host. El nombre de host no distingue entre mayúsculas y minúsculas.Cuando

nombre un contexto de seguridad, añada el nombre de contexto (_**<context_name>**) al nombre del dispositivo. Para los FWSM, esta es la convención de nomenclatura:Blade FWSM—**<nombre_chasis>_FW_<número_ranura>**Contexto de seguridad: **<nombre_chasis>_FW_<número_ranura>_<nombre_contexto>**

4. Introduzca la dirección IP del dispositivo de red en el campo AAA Client IP Address (Dirección IP del cliente AAA).
5. Introduzca el secreto compartido en el campo Key (Clave).
6. Seleccione **TACACS+ (Cisco IOS)** en la lista Autenticar mediante.
7. Haga clic en **Enviar** para guardar los cambios. El dispositivo agregado aparece en la tabla Clientes AAA.
8. Repita los pasos 1 a 7 para agregar dispositivos adicionales.
9. Después de agregar todos los dispositivos, haga clic en **Enviar + Reiniciar**.
10. Continúe con Creación de un Usuario de Control de Administración en Cisco Secure ACS.

Configuración de Grupos de Dispositivos de Red para su Uso en el Administrador de Seguridad

Cisco Secure ACS permite configurar grupos de dispositivos de red (NDG) que contienen dispositivos específicos que se deben gestionar. Por ejemplo, puede crear NDG para cada región geográfica o NDG que coincidan con su estructura organizativa. Cuando se utiliza con Cisco Security Manager, los NDG le permiten proporcionar a los usuarios diferentes niveles de permisos en función de los dispositivos que deben administrar. Por ejemplo, con los NDG puede asignar permisos de administrador del sistema User A a los dispositivos ubicados en Europa y permisos de Help Desk a los dispositivos ubicados en Asia. A continuación, puede asignar los permisos opuestos al usuario B.

Los NDG no se asignan directamente a los usuarios. En su lugar, los NDG se asignan a las funciones que define para cada grupo de usuarios. Cada NDG se puede asignar a una única función, pero cada función puede incluir varios NDG. Estas definiciones se guardan como parte de la configuración del grupo de usuarios seleccionado.

Estos temas describen los pasos básicos necesarios para configurar los NDG:

- Activar la función NDG
- Crear NDG
- Asociar NDG y roles a grupos de usuarios

Activar la función NDG

Debe activar la función NDG antes de poder crear NDG y rellenarlos con dispositivos.

1. Haga clic en **Interface Configuration** en la barra de navegación de Cisco Secure ACS.
2. Haga clic en **Advanced Options**.
3. Desplácese hacia abajo y, a continuación, marque la casilla de verificación **Grupos de dispositivos de red**.
4. Haga clic en Submit (Enviar).
5. Continúe con Crear NDG.

Crear NDG

Este procedimiento describe cómo crear NDG y rellenarlos con dispositivos. Cada dispositivo puede pertenecer a un solo NDG.

Nota: Cisco recomienda crear un NDG especial que contenga el servidor de CiscoWorks/Security Manager.

1. Haga clic en **Configuración de red** en la barra de navegación.Todos los dispositivos se colocan inicialmente en No asignado, que contiene todos los dispositivos que no se colocaron en un NDG. Tenga en cuenta que No asignado no es un NDG.
2. Crear NDG:Haga clic en **Agregar entrada**.Introduzca un nombre para el NDG en la página Nuevo grupo de dispositivos de red. La longitud máxima es de 24 caracteres. Se permiten espacios.**Opcional cuando con la versión 4.0 o posterior:** Introduzca una clave que deben utilizar todos los dispositivos del NDG. Si define una clave para el NDG, reemplaza cualquier clave definida para los dispositivos individuales en el NDG.Haga clic en **Enviar** para guardar el NDG.Repita los pasos a a d para crear más NDG.
3. Rellene los NDG con dispositivos:Haga clic en el nombre del NDG en el área Grupos de dispositivos de red.Haga clic en **Agregar entrada** en el área Clientes AAA.Defina los detalles del dispositivo que desea agregar al NDG y, a continuación, haga clic en **Enviar**. Consulte Agregar dispositivos como clientes AAA sin NDG para obtener más información.Repita los pasos b y c para agregar el resto de los dispositivos a los NDG. El único dispositivo que puede dejar en la categoría No asignado es el servidor AAA predeterminado.Después de configurar el último dispositivo, haga clic en **Enviar + Reiniciar**.
4. Continúe con Creación de un Usuario de Control de Administración en Cisco Secure ACS.

Crear un usuario de control de administración en Cisco Secure ACS

Utilice la página Administration Control en Cisco Secure ACS para definir la cuenta de administrador que se utiliza al definir el modo de configuración AAA en CiscoWorks Common Services. Consulte Configuración del Modo de Configuración AAA en CiscoWorks para obtener más información.

1. Haga clic en **Control de administración** en la barra de navegación de Cisco Secure ACS.
2. Haga clic en **Agregar administrador**.
3. En la página Agregar administrador, introduzca un nombre y una contraseña para el administrador.
4. Haga clic en **Conceder todo** en el área Privilegios del administrador para proporcionar permisos administrativos completos a este administrador.
5. Haga clic en **Enviar** para crear el administrador.

Nota: Consulte Administradores y Política Administrativa para obtener más información sobre las opciones disponibles al configurar un administrador.

Procedimientos de integración realizados en CiscoWorks

Esta sección describe los pasos que se deben completar en CiscoWorks Common Services para integrarlo con Cisco Security Manager:

- Crear un usuario local en CiscoWorks
- Definir el usuario de identidad del sistema

- Configure el modo de configuración AAA en CiscoWorks

Complete estos pasos después de completar los procedimientos de integración realizados en Cisco Secure ACS. Common Services realiza el registro real de cualquier aplicación instalada, como Cisco Security Manager, Auto-Update Server e IPS Manager en Cisco Secure ACS.

Crear un usuario local en CiscoWorks

Utilice la página Local User Setup (Configuración de usuario local) en CiscoWorks Common Services para crear una cuenta de usuario local que duplique al administrador que creó previamente en Cisco Secure ACS. Esta cuenta de usuario local se utiliza posteriormente para la configuración de la identidad del sistema. Consulte para obtener más información.

Nota: Antes de continuar, cree un administrador en Cisco Secure ACS. Consulte Definición de Usuarios y Grupos de Usuarios en Cisco Secure ACS para obtener instrucciones.

1. Inicie sesión en CiscoWorks con la cuenta de usuario **admin** predeterminada.
2. Elija **Server > Security** de Common Services y luego elija **Local User Setup** de la TOC.
3. Haga clic en Add (Agregar).
4. Introduzca el mismo nombre y contraseña que introdujo al crear el administrador en Cisco Secure ACS. Consulte el paso 4 en Definición de Usuarios y Grupos de Usuarios en Cisco Secure ACS.
5. Active todas las casillas de verificación en Roles excepto Datos de exportación.
6. Haga clic en **Aceptar** para crear el usuario.

Definir el usuario de identidad del sistema

Utilice la página Configuración de identidad del sistema de CiscoWorks Common Services para crear un usuario de confianza, conocido como usuario de identidad del sistema, que permita la comunicación entre servidores que forman parte del mismo dominio y procesos de aplicación que se encuentran en el mismo servidor. Las aplicaciones utilizan el usuario de identidad del sistema para autenticar procesos en servidores CiscoWorks locales o remotos. Esto es especialmente útil cuando las aplicaciones deben sincronizarse antes de que cualquier usuario haya iniciado sesión.

Además, el usuario de identidad del sistema se utiliza a menudo para realizar una subtarea cuando la tarea principal ya está autorizada para el usuario que ha iniciado sesión. Por ejemplo, para editar un dispositivo en Cisco Security Manager, se requiere comunicación entre aplicaciones entre Cisco Security Manager y Common Services DCR. Después de que el usuario esté autorizado para realizar la tarea de edición, se utiliza la identidad del sistema para invocar el DCR.

El usuario de identidad del sistema que configure aquí debe ser idéntico al usuario con permisos administrativos (completos) configurados en ACS. Si no lo hace, no podrá ver todos los dispositivos y políticas configurados en Cisco Security Manager.

Nota: Antes de continuar, cree un usuario local con el mismo nombre y contraseña que este administrador en CiscoWorks Common Services. Consulte Creación de un Usuario Local en CiscoWorks para obtener instrucciones.

1. Elija **Server > Security** y, a continuación, elija **Multi-Server Trust Management > System Identity Setup** de la TOC.

2. Introduzca el nombre del administrador que creó para Cisco Secure ACS. Consulte el paso 4 en Definición de Usuarios y Grupos de Usuarios en Cisco Secure ACS.
3. Introduzca y verifique la contraseña para este usuario.
4. Haga clic en Apply (Aplicar).

Configure el modo de configuración AAA en CiscoWorks

Utilice la página AAA Setup Mode en CiscoWorks Common Services para definir su Cisco Secure ACS como el servidor AAA, que incluye el puerto requerido y la clave secreta compartida. Además, puede definir hasta dos servidores de copia de seguridad.

Estos pasos realizan el registro real de CiscoWorks, Cisco Security Manager, IPS Manager (y opcionalmente, Auto-Update Server) en Cisco Secure ACS.

1. Elija **Server > Security** y luego elija **AAA Mode Setup** de la TOC.
2. Marque la casilla de verificación **TACACS+** bajo Módulos de inicio de sesión disponibles.
3. Seleccione **ACS** como tipo AAA.
4. Introduzca las direcciones IP de hasta tres servidores Cisco Secure ACS en el área Detalles del servidor. Los servidores secundarios y terciarios actúan como respaldo en caso de que falle el servidor primario.**Nota:** Si todos los servidores TACACS+ configurados no responden, debe iniciar sesión con la cuenta local de CiscoWorks de administración y, a continuación, cambiar el modo AAA nuevamente a Non-ACS/CiscoWorks Local. Después de que los servidores TACACS+ se restablezcan al servicio, debe cambiar el modo AAA nuevamente a ACS.
5. En el área Inicio de sesión, introduzca el nombre del administrador que definió en la página Control de administración de Cisco Secure ACS. Consulte Creación de un Usuario de Control de Administración en Cisco Secure ACS para obtener más información.
6. Introduzca y verifique la contraseña de este administrador.
7. Ingrese y verifique la clave secreta compartida que ingresó al agregar el servidor del Administrador de seguridad como cliente AAA de Cisco Secure ACS. Vea el paso 5 en Agregar dispositivos como clientes AAA sin NDG.
8. Marque la casilla de verificación **Registrar todas las aplicaciones instaladas con ACS** para registrar Cisco Security Manager y cualquier otra aplicación instalada con Cisco Secure ACS.
9. Haga clic en **Apply para guardar sus configuraciones.** Una barra de progreso muestra el progreso del registro. Aparece un mensaje cuando se completa el registro.
10. Si integra Cisco Security Manager con cualquier versión de ACS, reinicie el servicio Cisco Security Manager Daemon Manager. Consulte Reiniciar el Daemon Manager para obtener instrucciones.**Nota:** Después de CSM 3.0.0, Cisco ya no realiza pruebas con ACS 3.3(x) porque está muy parcheado y su fin de vida (EOL) ha sido anunciado. Por lo tanto, debe utilizar la versión ACS adecuada para la versión 3.0.1 y posterior de CSM. Consulte la tabla Matriz de compatibilidad para obtener más información.
11. Vuelva a iniciar sesión en Cisco Secure ACS para asignar funciones a cada grupo de usuarios. Consulte Asignación de Funciones a Grupos de Usuarios en Cisco Secure ACS para obtener instrucciones.**Nota:** La configuración AAA configurada aquí no se conserva si desinstala CiscoWorks Common Services o Cisco Security Manager. Además, no se puede realizar una copia de seguridad de esta configuración ni restaurarla después de la reinstalación. Por lo tanto, si actualiza a una nueva versión de cualquiera de las

aplicaciones, debe reconfigurar el modo de configuración AAA y volver a registrar Cisco Security Manager con ACS. Este proceso no es necesario para las actualizaciones incrementales. Si instala aplicaciones adicionales, como AUS, sobre CiscoWorks, debe volver a registrar las nuevas aplicaciones y Cisco Security Manager.

Reiniciar el administrador Daemon

Este procedimiento describe cómo reiniciar el Daemon Manager del servidor de Cisco Security Manager. Debe hacer esto para que la configuración AAA que configuró tenga efecto. A continuación, puede volver a iniciar sesión en CiscoWorks con las credenciales definidas en Cisco Secure ACS.

1. Inicie sesión en la máquina en la que está instalado el servidor de Cisco Security Manager.
2. Elija **Inicio > Programas > Herramientas administrativas > Servicios** para abrir la ventana Servicios.
3. En la lista de servicios mostrados en el panel derecho, seleccione **Administrador del demonio de Cisco Security Manager**.
4. Haga clic en el botón **Reiniciar servicio** en la barra de herramientas.
5. Continúe con Asignación de Funciones a los Grupos de Usuarios en Cisco Secure ACS.

Asignación de Funciones a Grupos de Usuarios en Cisco Secure ACS

Después de registrar CiscoWorks, Cisco Security Manager y otras aplicaciones instaladas en Cisco Secure ACS, puede asignar funciones a cada uno de los grupos de usuarios que configuró previamente en Cisco Secure ACS. Estas funciones determinan las acciones que los usuarios de cada grupo pueden realizar en Cisco Security Manager.

El procedimiento que se utiliza para asignar funciones a grupos de usuarios depende de si se utilizan NDG:

- Asignar funciones a grupos de usuarios sin NDG
- Asociar NDG y roles a grupos de usuarios

Asignar funciones a grupos de usuarios sin NDG

Este procedimiento describe cómo asignar las funciones predeterminadas a los grupos de usuarios cuando no se definen las NDG. Refiérase a Funciones Predeterminadas de Cisco Secure ACS para obtener más información.

Nota: Antes de continuar:

- Cree un grupo de usuarios para cada función predeterminada. Consulte Definición de Usuarios y Grupos de Usuarios en Cisco Secure ACS para obtener instrucciones.
- Complete los procedimientos descritos en Procedimientos de Integración Realizados en Cisco Secure ACS y Procedimientos de Integración Realizados en CiscoWorks.

Complete estos pasos:

1. Inicie sesión en Cisco Secure ACS.
2. Haga clic en **Group Setup** en la barra de navegación.
3. En la lista, seleccione el grupo de usuarios para los administradores del sistema. Consulte el paso 2 de Definir Usuarios y Grupos de Usuarios en Cisco Secure ACS y luego haga clic en **Editar Configuración**.

Asociar NDG y roles a grupos de usuarios

Cuando asocia NDG a funciones para su uso en Cisco Security Manager, debe crear definiciones en dos lugares de la página Configuración de grupo:

- área CiscoWorks
- área de Cisco Security Manager

Las definiciones de cada área deben coincidir tanto como sea posible. Cuando asocia funciones personalizadas o funciones ACS que no existen en CiscoWorks Common Services, intente definir el equivalente más cercano posible en función de los permisos asignados a esa función.

Debe crear asociaciones para cada grupo de usuarios que se utilizará con Cisco Security Manager. Por ejemplo, si tiene un grupo de usuarios que contiene personal de soporte para la región occidental, puede seleccionar ese grupo de usuarios y, a continuación, asociar el NDG que contiene los dispositivos de esa región a la función de soporte técnico.

Nota: Antes de continuar, active la función NDG y cree NDG. Consulte Configuración de Grupos de Dispositivos de Red para su Uso en el Administrador de Seguridad para obtener más información.

1. Haga clic en **Group Setup** en la barra de navegación.
2. Seleccione un grupo de usuarios de la lista Grupo y, a continuación, haga clic en **Editar configuración**.
3. Asignar NDG y funciones para su uso en CiscoWorks:En la página Group Setup (Configuración de grupo), desplácese hacia abajo hasta el área CiscoWorks bajo TACACS+ Settings (Parámetros de TACACS+).Seleccione **Asignar un CiscoWorks por grupo de dispositivos de red**.Seleccione un NDG de la lista Grupo de dispositivos.Seleccione la función a la que se asociará este NDG de la segunda lista.Haga clic en **Agregar asociación**. La asociación aparece en el cuadro Grupo de dispositivos.Repita los pasos c a e para crear asociaciones adicionales.**Nota:** Para quitar una asociación, selecciónela del grupo de dispositivos y, a continuación, haga clic en Quitar asociación.
4. Desplácese hacia abajo hasta el área de Cisco Security Manager y cree asociaciones que coincidan lo más posible con las asociaciones definidas en el paso 3.**Nota:** Cuando selecciona las funciones de aprobador de seguridad o administrador de seguridad en Cisco Secure ACS, se recomienda seleccionar Administrador de red como el rol equivalente más cercano de CiscoWorks.
5. Haga clic en **Enviar** para guardar los parámetros.
6. Repita los pasos 2 a 5 para definir los NDG para el resto de los grupos de usuarios.
7. Después de asociar los NDG y las funciones a cada grupo de usuarios, haga clic en **Enviar + Reiniciar**.

Troubleshoot

1. Antes de poder comenzar a importar dispositivos a Cisco Security Manager, primero debe configurar cada dispositivo como cliente AAA en Cisco Secure ACS. Además, debe configurar el servidor de CiscoWorks/Security Manager como un cliente AAA.
2. Si recibe un registro de intentos fallidos, el autor falló con un error en Cisco Secure ACS.
   ```
   "service=Athena cmd=OGS authorize-deviceGroup*(Not Assigned) authorize-deviceGroup*Test
   Devices authorize-deviceGroup*HQ Routers authorize-deviceGroup*HQ Switches
   authorize-deviceGroup*HQ Security Devices authorize-deviceGroup*Agent Routers authoriz"
   ```
   Para resolver este problema, asegúrese de que el nombre del dispositivo en ACS necesita ser un nombre de dominio completamente calificado.

Información Relacionada

- Página de soporte de Cisco Security Access Control Server para Windows
- Página de soporte de Cisco Security Manager
- Cisco Secure Access Control Server para Windows
- Guía de Configuración de Cisco Secure ACS 4.1
- Guía de solución de problemas en línea de Cisco Secure ACS, 4.1
- Avisos de campos de productos de seguridad (incluido CiscoSecure ACS para Windows)
- Soporte Técnico y Documentación - Cisco Systems