Integração do Security Manager com ACS

Contents

Introduction

Este documento descreve como integrar o Cisco Security Manager ao Cisco Secure Access Control Server (ACS).

O Cisco Secure ACS fornece autorização de comando para usuários que utilizam aplicativos de gerenciamento, como o Cisco Security Manager, para configurar dispositivos de rede gerenciados. O suporte para autorização de comandos é fornecido por tipos de conjunto de autorizações de comandos exclusivos, chamados de funções no Cisco Security Manager, que contêm um conjunto de permissões. Essas permissões, também chamadas de privilégios, determinam as ações que os usuários com funções específicas podem executar no Cisco Security Manager.

O Cisco Secure ACS usa TACACS+ para se comunicar com aplicativos de gerenciamento. Para que o Cisco Security Manager se comunique com o Cisco Secure ACS, você deve configurar o servidor CiscoWorks no Cisco Secure ACS como um cliente AAA que usa TACACS+. Além disso, você deve fornecer ao servidor CiscoWorks o nome de administrador e a senha que você usa

para fazer login no Cisco Secure ACS. Quando você atende a esses requisitos, ele garante a validade das comunicações entre o Cisco Security Manager e o Cisco Secure ACS.

Quando o Cisco Security Manager se comunica inicialmente com o Cisco Secure ACS, ele dita ao Cisco ACS a criação de funções padrão, que aparecem na seção Componentes de perfil compartilhado da interface HTML do Cisco Secure ACS. Também determina que um serviço personalizado seja autorizado pelo TACACS+. Esse serviço personalizado aparece na página TACACS+ (Cisco IOS®) na seção Interface Configuration da interface HTML. Você pode modificar as permissões incluídas em cada função do Cisco Security Manager e aplicar essas funções a usuários e grupos de usuários.

Observação: não é possível integrar o CSM ao ACS 5.2, pois ele não é suportado.

Prerequisites

Requirements

Para usar o Cisco Secure ACS, certifique-se de que:

- Você define funções que incluem os comandos necessários para executar as funções necessárias no Cisco Security Manager.
- A NAR (Network Access Restriction, Restrição de Acesso à Rede) inclui o grupo de dispositivos (ou os dispositivos) que você deseja administrar, se você aplicar um NAR ao perfil.
- Os nomes de dispositivos gerenciados são escritos e capitalizados de forma idêntica no Cisco Secure ACS e no Cisco Security Manager.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

Observação: certifique-se de escolher as versões compatíveis do CSM e do ACS antes de instalar em seu ambiente de rede. Por exemplo, a Cisco testou o ACS 3.3 com apenas o CSM 3.0 e parou para versões posteriores do CSM. Portanto, é recomendável usar o CSM 3.0 com ACS 3.3. Consulte a tabela Matriz de compatibilidade para obter mais informações sobre várias versões de software.

Versões do Cisco Security Manager	Versões do CS ACS testadas
3.0.0 3.0.0 SP1	Windows 3.3(3) e 4.0(1)
3.0.1 3.0.1 SP1 3.0.1 SP2	Solutions Engine 4.0(1) Windows 4.0(1)
3.1.0 3.0.2	Solutions Engine 4.0(1) Windows 4.1(1) e 4.1(3)
3.1.1 3.0.2 SP1 3.0.2 SP2	Solutions Engine v4.0(1) Windows 4.1(2), 4.1(3) e 4.1(4)

3.1.1 SP1	Solutions Engine 4.0(1) Windows 4.1(4)
3.1.1 SP2	Solutions Engine 4.0(1) Windows 4.1(4) e 4.2(0)
3.2.0	Solutions Engine 4.1(4) Windows 4.1(4) e 4.2(0)
3.2.1	Solutions Engine 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.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Integre o Cisco Security Manager com o Cisco Secure ACS

Esta seção descreve as etapas necessárias para integrar o Cisco Security Manager ao Cisco Secure ACS. Algumas etapas contêm vários subpassos. Essas etapas e subetapas devem ser executadas em ordem. Esta seção também contém referências a procedimentos específicos usados para executar cada etapa.

Conclua estes passos:

1. **Planeje a autenticação administrativa e o modelo de autorização.**Você deve decidir sobre seu modelo administrativo antes de usar o Cisco Security Manager. Isso inclui a definição das funções e contas administrativas que você planeja usar.**Dica:** ao definir as funções e permissões de administradores em potencial, considere também se deseja ou não ativar o fluxo de trabalho. Essa seleção afeta a maneira como você pode restringir o acesso.
2. **Instale o Cisco Secure ACS, o Cisco Security Manager e o CiscoWorks Common Services.**Instale o Cisco Secure ACS versão 3.3 em um servidor Windows 2000/2003. Instale o CiscoWorks Common Services e o Cisco Security Manager em um servidor diferente do Windows 2000/Windows 2003.Consulte estes documentos para obter outras informações:Guia de instalação do Cisco Security Manager 3.0Guia de instalação do Cisco Secure ACS para Windows 3.3**Observação:** consulte a tabela Matriz de compatibilidade para obter mais informações antes de escolher as versões do software CSM e ACS.
3. **Execute os procedimentos de integração no Cisco Secure ACS.**Defina usuários do Cisco Security Manager como usuários do ACS e atribua-os a grupos de usuários com base na função planejada, adicione todos os dispositivos gerenciados (bem como o servidor CiscoWorks/Security Manager) como clientes AAA e crie um usuário de controle de administração. Consulte Procedimentos de integração executados no Cisco Secure ACS para obter mais informações.
4. **Execute os procedimentos de integração no CiscoWorks Common Services.**Configure um usuário local que corresponda ao administrador definido no Cisco Secure ACS, defina esse mesmo usuário para a configuração de identidade do sistema e configure o ACS como o

modo de configuração AAA.Consulte Procedimentos de Integração Executados no CiscoWorks para obter mais informações.

5. **Atribuir funções a grupos de usuários no Cisco Secure ACS.**Atribua funções a cada grupo de usuários configurado no Cisco Secure ACS. O procedimento usado depende de você ter configurado os NDGs (Network Device Groups, grupos de dispositivos de rede).Consulte Atribuir funções a grupos de usuários no Cisco Secure ACS para obter mais informações.

Procedimentos de integração executados no Cisco Secure ACS

Esta seção descreve as etapas que você deve concluir no Cisco Secure ACS para integrá-lo ao Cisco Security Manager:

1. Definir usuários e grupos de usuários no Cisco Secure ACS
2. Adicionar dispositivos gerenciados como clientes AAA no Cisco Secure ACS
3. Crie um usuário de controle administrativo no Cisco Secure ACS

Definir usuários e grupos de usuários no Cisco Secure ACS

Todos os usuários do Cisco Security Manager devem ser definidos no Cisco Secure ACS e ter uma função apropriada para sua função de trabalho. A maneira mais fácil de fazer isso é dividir os usuários em diferentes grupos com base em cada função padrão disponível no ACS. Por exemplo, atribua todos os administradores do sistema a um grupo, todos os operadores de rede a outro grupo e assim por diante. Consulte Cisco Secure ACS Default Roles para obter mais informações sobre as funções padrão no ACS.

Além disso, você deve criar um usuário adicional ao qual seja atribuída a função de administrador do sistema com permissões completas. As credenciais estabelecidas para esse usuário são posteriormente usadas na página Configuração de identidade do sistema no CiscoWorks. Consulte Definir o Usuário de Identidade do Sistema para obter mais informações.

Observe que, nesse estágio, você apenas atribui usuários a diferentes grupos. A atribuição real de funções a esses grupos é realizada posteriormente, depois que o CiscoWorks, o Cisco Security Manager e quaisquer outros aplicativos são registrados no Cisco Secure ACS.

Dica: antes de continuar, instale o CiscoWorks Common Services e o Cisco Security Manager em um servidor Windows 2000/2003. Instale o Cisco Secure ACS em um servidor Windows 2000/2003 diferente.

1. Faça login no Cisco Secure ACS.
2. Configurar um usuário com permissões completas:Clique em **User Setup** na barra de navegação.Na página User Setup, digite um nome para o novo usuário e clique em **Add/Edit**.Selecione um método de autenticação na lista Autenticação de senha em Configuração do usuário.Digite e confirme a senha para o novo usuário.Selecione **Grupo 1** como o grupo ao qual o usuário está atribuído.Clique em **Submit** para criar a conta de usuário.
3. Repita a etapa 2 para cada usuário do Cisco Security Manager. A Cisco recomenda que você divida os usuários em grupos com base na função atribuída a cada usuário:Grupo 1 — Administradores de sistemaGrupo 2 — Administradores de segurançaGrupo 3 — Aprovadores de segurançaGrupo 4 — Administradores de redeGrupo 5—AprovadoresGrupo

6 — Operadores de redeGrupo 7 — Help deskConsulte a Tabela para obter mais informações sobre as permissões padrão associadas a cada função. Consulte Personalização das funções do Cisco Secure ACS para obter mais informações sobre como personalizar funções de usuário.**Nota:** Neste estágio, os próprios grupos são coleções de usuários sem nenhuma definição de função. Você atribui funções a cada grupo após concluir o processo de integração. Consulte Atribuir funções a grupos de usuários no Cisco Secure ACS para obter mais informações.
4. Crie um usuário adicional e atribua esse usuário ao grupo de administradores do sistema. As credenciais estabelecidas para esse usuário são posteriormente usadas na página Configuração de identidade do sistema no CiscoWorks. Consulte Definir o Usuário de Identidade do Sistema para obter mais informações.
5. Continue com Adicionar dispositivos gerenciados como clientes AAA no Cisco Secure ACS.

Adicionar dispositivos gerenciados como clientes AAA no Cisco Secure ACS

Antes de começar a importar dispositivos para o Cisco Security Manager, você deve primeiro configurar cada dispositivo como um cliente AAA no Cisco Secure ACS. Além disso, você deve configurar o servidor CiscoWorks/Security Manager como um cliente AAA.

Se o Cisco Security Manager gerencia contextos de segurança configurados em dispositivos de firewall, o que inclui contextos de segurança configurados em FWSMs para dispositivos Catalyst 6500/7600, cada contexto deve ser adicionado individualmente ao Cisco Secure ACS.

O método usado para adicionar dispositivos gerenciados depende de se você deseja restringir os usuários a gerenciar um conjunto específico de dispositivos com grupos de dispositivos de rede (NDGs). Veja uma destas seções:

- Se desejar que os usuários tenham acesso a todos os dispositivos, adicione os dispositivos conforme descrito em Adicionar dispositivos como clientes AAA sem NDGs.
- Se quiser que os usuários tenham acesso apenas a determinados NDGs, adicione os dispositivos conforme descrito em Configurar grupos de dispositivos de rede para uso no Gerenciador de segurança.

Adicionar dispositivos como clientes AAA sem NDGs

Este procedimento descreve como adicionar dispositivos como clientes AAA de um Cisco Secure ACS. Consulte a seção *AAA Client Configuration* da Network Configuration para obter informações completas sobre todas as opções disponíveis.

Observação: lembre-se de adicionar o servidor CiscoWorks/Security Manager como um cliente AAA.

1. Clique em **Network Configuration** na barra de navegação Cisco Secure ACS.
2. Clique em **Add Entry** abaixo da tabela AAA Clients.
3. Digite o nome de host do cliente AAA (até 32 caracteres) na página Adicionar cliente AAA. O nome de host do cliente AAA deve corresponder ao nome de exibição que você planeja usar para o dispositivo no Cisco Security Manager.Por exemplo, se você pretende adicionar um nome de domínio ao nome do dispositivo no Cisco Security Manager, o nome de host do cliente AAA no ACS deve ser **<nome_do_dispositivo>.<nome_do_domínio>**.Ao nomear o

servidor CiscoWorks, é recomendável usar o nome de host totalmente qualificado. Certifique-se de soletrar o nome do host corretamente. O nome do host não diferencia maiúsculas e minúsculas.Ao nomear um contexto de segurança, anexe o nome do contexto (_**<context_name>**) ao nome do dispositivo. Para FWSMs, esta é a convenção de nomenclatura:Blade FWSM—**<chassis_name>_FW_<slot_number>**Contexto de segurança—**<chassis_name>_FW_<slot_number>_<context_name>**
4. Insira o endereço IP do dispositivo de rede no campo AAA Client IP Address (Endereço IP do cliente AAA).
5. Digite o segredo compartilhado no campo Chave.
6. Selecione **TACACS+ (Cisco IOS)** na lista Authenticate Using (Autenticar usando).
7. Clique em **Enviar** para salvar suas alterações. O dispositivo adicionado aparece na tabela Clientes AAA.
8. Repita as etapas de 1 a 7 para adicionar dispositivos adicionais.
9. Depois de adicionar todos os dispositivos, clique em **Enviar + Reiniciar**.
10. Continue com Criar um usuário de controle de administração no Cisco Secure ACS.

Configurar grupos de dispositivos de rede para uso no Gerenciador de segurança

O Cisco Secure ACS permite que você configure grupos de dispositivos de rede (NDGs) que contêm dispositivos específicos a serem gerenciados. Por exemplo, você pode criar NDGs para cada região geográfica ou NDGs que correspondem à sua estrutura organizacional. Quando usados com o Cisco Security Manager, os NDGs permitem que você forneça aos usuários níveis diferentes de permissões, com base nos dispositivos que eles precisam gerenciar. Por exemplo, com os NDGs, você pode atribuir permissões de administrador de sistema do Usuário A aos dispositivos localizados na Europa e permissões do Help Desk aos dispositivos localizados na Ásia. Você pode, então, atribuir as permissões opostas ao Usuário B.

Os NDGs não são atribuídos diretamente aos usuários. Em vez disso, os NDGs são atribuídos às funções que você define para cada grupo de usuários. Cada NDG pode ser atribuído a uma única função apenas, mas cada função pode incluir vários NDGs. Essas definições são salvas como parte da configuração do grupo de usuários selecionado.

Estes tópicos descrevem as etapas básicas necessárias para configurar NDGs:

- Ative o recurso NDG
- Criar NDGs
- Associar NDGs e funções a grupos de usuários

Ative o recurso NDG

Você deve ativar o recurso NDG antes de criar NDGs e preenchê-los com dispositivos.

1. Clique em **Interface Configuration** na barra de navegação do Cisco Secure ACS.
2. Clique em **Opções Avançadas**.
3. Role para baixo e marque a caixa de seleção **Network Device Groups (Grupos de dispositivos de rede)**.
4. Clique em Submit.
5. Continue com Criar NDGs.

Criar NDGs

Este procedimento descreve como criar NDGs e preenchê-las com dispositivos. Cada dispositivo pode pertencer a apenas um NDG.

Observação: a Cisco recomenda que você crie um NDG especial que contenha o servidor CiscoWorks/Security Manager.

1. Clique em **Network Configuration** na barra de navegação.Todos os dispositivos são inicialmente colocados em Não atribuído, que contém todos os dispositivos que não foram colocados em um NDG. Lembre-se de que Não atribuído não é um NDG.
2. Criar NDGs:Clique em **Adicionar entrada**.Digite um nome para o NDG na página Novo grupo de dispositivos de rede. O comprimento máximo é de 24 caracteres. Os espaços são permitidos.**Opcional quando com a versão 4.0 ou posterior:** Insira uma chave a ser usada por todos os dispositivos no NDG. Se você definir uma chave para o NDG, ela substituirá qualquer chave definida para os dispositivos individuais no NDG.Clique em **Submit** para salvar o NDG.Repita as etapas de a a d para criar mais NDGs.
3. Preencha os NDGs com dispositivos:Clique no nome do NDG na área Network Device Groups (Grupos de dispositivos de rede).Clique em **Add Entry** na área AAA Clients.Defina os detalhes do dispositivo a ser adicionado ao NDG e clique em **Enviar**. Consulte Adicionar dispositivos como clientes AAA sem NDGs para obter mais informações.Repita as etapas b e c para adicionar o restante dos dispositivos aos NDGs. O único dispositivo que você pode deixar na categoria Não atribuído é o servidor AAA padrão.Depois de configurar o último dispositivo, clique em **Enviar + Reiniciar**.
4. Continue com Criar um usuário de controle de administração no Cisco Secure ACS.

Crie um usuário de controle administrativo no Cisco Secure ACS

Use a página de controle de administração no Cisco Secure ACS para definir a conta de administrador que é usada ao definir o modo de configuração AAA no CiscoWorks Common Services. Consulte Configurar o modo de configuração de AAA no CiscoWorks para obter mais informações.

1. Clique em **Administration Control** na barra de navegação do Cisco Secure ACS.
2. Clique em **Adicionar administrador**.
3. Na página Adicionar administrador, digite um nome e uma senha para o administrador.
4. Clique em **Conceder tudo** na área Privilégios de Administrador para fornecer permissões administrativas completas a este administrador.
5. Clique em **Submit** para criar o administrador.

Observação: consulte Administradores e Política administrativa para obter mais informações sobre as opções disponíveis ao configurar um administrador.

Procedimentos de integração executados no CiscoWorks

Esta seção descreve as etapas a serem concluídas no CiscoWorks Common Services para integrá-lo ao Cisco Security Manager:

- Crie um usuário local no CiscoWorks

- Definir o Usuário de Identidade do Sistema
- Configurar o modo de configuração AAA no CiscoWorks

Conclua estes passos depois de concluir os procedimentos de integração executados no Cisco Secure ACS. O Common Services executa o registro real de qualquer aplicativo instalado, como o Cisco Security Manager, o Auto Update Server e o IPS Manager no Cisco Secure ACS.

Crie um usuário local no CiscoWorks

Use a página Configuração de usuário local no CiscoWorks Common Services para criar uma conta de usuário local que duplique o administrador criado anteriormente no Cisco Secure ACS. Esta conta de usuário local é mais tarde usada para a configuração de identidade do sistema. Consulte para obter mais informações.

Observação: antes de continuar, crie um administrador no Cisco Secure ACS. Consulte Definir usuários e grupos de usuários no Cisco Secure ACS para obter instruções.

1. Efetue login no CiscoWorks com a conta de usuário **admin** padrão.
2. Escolha **Server > Security** em Common Services e, em seguida, escolha **Local User Setup** no TOC.
3. Clique em Add.
4. Digite o mesmo nome e senha que você digitou ao criar o administrador no Cisco Secure ACS. Consulte a etapa 4 em Definir usuários e grupos de usuários no Cisco Secure ACS.
5. Marque todas as caixas de seleção em Funções, exceto Exportar dados.
6. Clique em **OK** para criar o usuário.

Definir o Usuário de Identidade do Sistema

Use a página Configuração de identidade do sistema no CiscoWorks Common Services para criar um usuário confiável, conhecido como usuário de identidade do sistema, que permite a comunicação entre servidores que fazem parte do mesmo domínio e processos de aplicativos localizados no mesmo servidor. Os aplicativos usam o usuário Identidade do sistema para autenticar processos em servidores CiscoWorks locais ou remotos. Isso é especialmente útil quando os aplicativos devem ser sincronizados antes que qualquer usuário faça logon.

Além disso, o usuário de Identidade do Sistema é frequentemente usado para executar uma subtarefa quando a tarefa principal já está autorizada para o usuário conectado. Por exemplo, para editar um dispositivo no Cisco Security Manager, a comunicação entre aplicativos é necessária entre o Cisco Security Manager e o Common Services DCR. Depois que o usuário é autorizado a executar a tarefa de edição, o usuário de Identidade do sistema é usado para chamar o DCR.

O usuário de identidade do sistema que você configura aqui deve ser idêntico ao usuário com permissões administrativas (completas) que você configurou no ACS. Se isso não for feito, poderá ocorrer a incapacidade de visualizar todos os dispositivos e políticas configurados no Cisco Security Manager.

Observação: antes de continuar, crie um usuário local com o mesmo nome e senha desse administrador no CiscoWorks Common Services. Consulte Criar um usuário local no CiscoWorks para obter instruções.

1. Escolha **Server > Security** e escolha **Multi-Server Trust Management > System Identity**

Setup no TOC.
2. Digite o nome do administrador que você criou para o Cisco Secure ACS. Consulte a etapa 4 em Definir usuários e grupos de usuários no Cisco Secure ACS.
3. Digite e verifique a senha para este usuário.
4. Clique em Apply.

Configurar o modo de configuração AAA no CiscoWorks

Use a página AAA Setup Mode no CiscoWorks Common Services para definir o Cisco Secure ACS como o servidor AAA, que inclui a porta necessária e a chave secreta compartilhada. Além disso, você pode definir até dois servidores de backup.

Essas etapas executam o registro real do CiscoWorks, Cisco Security Manager, IPS Manager (e, opcionalmente, Auto Update Server) no Cisco Secure ACS.

1. Escolha **Server > Security** e, em seguida, escolha **AAA Mode Setup** no TOC.
2. Marque a caixa de seleção **TACACS+** em Available Login Modules (Módulos de login disponíveis).
3. Selecione **ACS** como o tipo AAA.
4. Insira os endereços IP de até três servidores Cisco Secure ACS na área Detalhes do servidor. Os servidores secundários e terciários atuam como backups caso o servidor primário falhe.**Observação:** se todos os servidores TACACS+ configurados não responderem, você deve fazer login com a conta local do CiscoWorks e, em seguida, alterar o modo AAA de volta para Non-ACS/CiscoWorks Local. Depois que os servidores TACACS+ forem restaurados para serviço, você deverá alterar o modo AAA de volta para ACS.
5. Na área Logon, digite o nome do administrador que você definiu na página Controle de administração do Cisco Secure ACS. Consulte Criar um usuário de controle administrativo no Cisco Secure ACS para obter mais informações.
6. Digite e verifique a senha para este administrador.
7. Digite e verifique a chave secreta compartilhada que você inseriu quando adicionou o servidor do Security Manager como um cliente AAA do Cisco Secure ACS. Veja a etapa 5 em Adicionar dispositivos como clientes AAA sem NDGs.
8. Marque a caixa de seleção **Registrar todos os aplicativos instalados com o ACS** para registrar o Cisco Security Manager e quaisquer outros aplicativos instalados com o Cisco Secure ACS.
9. Clique em **Aplicar para salvar as configurações.** Uma barra de progresso exibe o progresso do registro. Uma mensagem é exibida quando o registro é concluído.
10. Se você integrar o Cisco Security Manager a qualquer versão do ACS, reinicie o serviço Cisco Security Manager Daemon Manager. Consulte Reiniciar o Daemon Manager para obter instruções.**Observação:** depois do CSM 3.0.0, a Cisco não testa mais o ACS 3.3(x) porque ele tem patches muito altos e seu EOL (End-Of-Life [fim da vida útil]) foi anunciado. Portanto, você precisa usar a versão ACS apropriada para o CSM versão 3.0.1 e posterior. Consulte a tabela Matriz de compatibilidade para obter mais informações.
11. Faça login novamente no Cisco Secure ACS para atribuir funções a cada grupo de usuários. Consulte Atribuir funções a grupos de usuários no Cisco Secure ACS para obter instruções.**Observação:** a configuração de AAA configurada aqui não é retida se você desinstalar o CiscoWorks Common Services ou o Cisco Security Manager. Além disso, não é possível fazer backup e restaurar esta configuração após a reinstalação. Portanto, se

você atualizar para uma nova versão de um dos aplicativos, reconfigure o modo de configuração AAA e registre novamente o Cisco Security Manager com ACS. Este processo não é necessário para atualizações incrementais. Se você instalar aplicativos adicionais, como o AUS, além do CiscoWorks, deverá registrar novamente os novos aplicativos e o Cisco Security Manager.

Reinicie o Daemon Manager

Este procedimento descreve como reiniciar o Daemon Manager do servidor do Cisco Security Manager. Você deve fazer isso para que as configurações de AAA definidas entrem em vigor. Em seguida, você pode fazer logon novamente no CiscoWorks com as credenciais definidas no Cisco Secure ACS.

1. Efetue login na máquina na qual o servidor do Cisco Security Manager está instalado.
2. Escolha **Iniciar > Programas > Ferramentas Administrativas > Serviços** para abrir a janela Serviços.
3. Na lista de serviços exibida no painel direito, selecione **Cisco Security Manager Daemon Manager**.
4. Clique no botão **Reiniciar serviço** na barra de ferramentas.
5. Continue com Atribuir funções a grupos de usuários no Cisco Secure ACS.

Atribuir funções a grupos de usuários no Cisco Secure ACS

Depois de registrar o CiscoWorks, o Cisco Security Manager e outros aplicativos instalados no Cisco Secure ACS, você pode atribuir funções a cada um dos grupos de usuários configurados anteriormente no Cisco Secure ACS. Essas funções determinam as ações que os usuários em cada grupo têm permissão para executar no Cisco Security Manager.

O procedimento usado para atribuir funções a grupos de usuários depende se os NDGs são usados:

- Atribuir funções a grupos de usuários sem NDGs
- Associar NDGs e funções a grupos de usuários

Atribuir funções a grupos de usuários sem NDGs

Este procedimento descreve como atribuir as funções padrão a grupos de usuários quando os NDGs não estão definidos. Consulte Cisco Secure ACS Default Roles para obter mais informações.

Nota: Antes de continuar:

- Crie um grupo de usuários para cada função padrão. Consulte Definir usuários e grupos de usuários no Cisco Secure ACS para obter instruções.
- Conclua os procedimentos descritos em Procedimentos de Integração Executados no Cisco Secure ACS e Procedimentos de Integração Executados no CiscoWorks.

Conclua estes passos:

1. Faça login no Cisco Secure ACS.

2. Clique em **Group Setup** na barra de navegação.
3. Selecione o grupo de usuários dos administradores do sistema na lista. Consulte a etapa 2 de Definir usuários e grupos de usuários no Cisco Secure ACS e clique em **Editar configurações**.

Associar NDGs e funções a grupos de usuários

Ao associar NDGs a funções para uso no Cisco Security Manager, você deve criar definições em dois locais na página Configuração do grupo:

- área CiscoWorks
- área do Cisco Security Manager

As definições em cada área devem corresponder o mais possível. Quando você associa funções personalizadas ou funções ACS que não existem no CiscoWorks Common Services, tente definir o equivalente o mais próximo possível com base nas permissões atribuídas a essa função.

Você deve criar associações para cada grupo de usuários a ser usado com o Cisco Security Manager. Por exemplo, se você tiver um grupo de usuários que contenha pessoal de suporte para a região Ocidental, poderá selecionar esse grupo de usuários e, em seguida, associar o NDG que contém os dispositivos nessa região à função Help Desk.

Observação: antes de continuar, ative o recurso NDG e crie NDGs. Consulte Configurar grupos de dispositivos de rede para uso no Gerenciador de segurança para obter mais informações.

1. Clique em **Group Setup** na barra de navegação.
2. Selecione um grupo de usuários na lista Grupo e clique em **Editar configurações**.
3. Mapear NDGs e funções para uso no CiscoWorks:Na página Configuração do grupo, role para baixo até a área CiscoWorks em TACACS+ Settings.Selecione **Atribuir um CiscoWorks em uma base por grupo de dispositivos de rede**.Selecione um NDG na lista Grupo de dispositivos.Selecione a função à qual esse NDG será associado na segunda lista.Clique em **Adicionar associação**. A associação é exibida na caixa Device Group (Grupo de dispositivos).Repita as etapas de c a e para criar associações adicionais.**Observação:** para remover uma associação, selecione-a no Grupo de dispositivos e clique em Remover associação.
4. Role para baixo até a área do Cisco Security Manager e crie associações que correspondam o mais próximo possível das associações definidas na etapa 3.**Observação:** ao selecionar as funções de Administrador de segurança ou Aprovador de segurança no Cisco Secure ACS, é recomendável selecionar Administrador de rede como a função equivalente mais próxima do CiscoWorks.
5. Clique em **Submit** para salvar suas configurações.
6. Repita as etapas de 2 a 5 para definir NDGs para o restante dos grupos de usuários.
7. Depois de associar NDGs e funções a cada grupo de usuários, clique em **Enviar + Reiniciar**.

Troubleshoot

1. Antes de começar a importar dispositivos para o Cisco Security Manager, você deve primeiro configurar cada dispositivo como um cliente AAA no Cisco Secure ACS. Além disso, você deve configurar o servidor CiscoWorks/Security Manager como um cliente AAA.

2. Se você receber um registro de tentativas com falha, o autor falhou com um erro no 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 esse problema, verifique se o nome do dispositivo no ACS precisa ser um nome de domínio totalmente qualificado.

Informações Relacionadas

- Página de suporte do Cisco Security Access Control Server para Windows
- Página de suporte do Cisco Security Manager
- Cisco Secure Access Control Server for Windows
- Guia de configuração do Cisco Secure ACS 4.1
- Guia de solução de problemas do Cisco Secure ACS Online, 4.1
- Avisos de campo de produto de segurança (incluindo CiscoSecure ACS for Windows)
- Suporte Técnico e Documentação - Cisco Systems