Security Manager-integratie met ACS

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco Security Manager kunt integreren met Cisco Secure Access Control Server (ACS).

Cisco Secure ACS biedt opdrachtautorisatie voor gebruikers die beheertoepassingen gebruiken, zoals Cisco Security Manager, om beheerde netwerkapparaten te configureren. De ondersteuning voor opdrachtautorisatie wordt geboden door unieke types van de opdrachtautorisatie, rollen in Cisco Security Manager genoemd, die een set permissies bevatten. Deze rechten, ook genaamd privileges, bepalen de handelingen die gebruikers met bepaalde rollen kunnen uitvoeren binnen Cisco Security Manager.

Cisco Secure ACS gebruikt TACACS+ om te communiceren met beheertoepassingen. Voor Cisco Security Manager om met Cisco Secure ACS te communiceren, moet u de CiscoWorks server in Cisco Secure ACS als een AAA-client configureren die TACACS+ gebruikt. Daarnaast moet u de CiscoWorks-server de naam en het wachtwoord van de beheerder geven die u gebruikt om in Cisco Secure ACS te loggen. Wanneer u aan deze vereisten voldoet, garandeert het de

geldigheid van communicatie tussen Cisco Security Manager en Cisco Secure ACS.

Wanneer Cisco Security Manager oorspronkelijk communiceert met Cisco Secure ACS, dicteert dit aan Cisco ACS de creatie van standaardrollen, die verschijnen in het gedeelte Shared Profile Componenten van de Cisco Secure ACS HTML-interface. Het dicteert ook dat een aangepaste dienst door TACACS+ moet worden toegestaan. Deze aangepaste service verschijnt op de pagina TACACS+ (Cisco IOS®) in het gedeelte Interface Configuration van de HTML-interface. U kunt de rechten die in elke rol van Cisco Security Manager zijn opgenomen dan wijzigen en deze rollen op gebruikers en gebruikersgroepen toepassen.

Opmerking: Het is niet mogelijk CSM te integreren met ACS 5.2, omdat het niet wordt ondersteund.

Voorwaarden

Vereisten

Als u Cisco Secure ACS wilt gebruiken, zorg er dan voor dat:

- U definieert rollen die de opdrachten omvatten die vereist zijn om de benodigde functies in Cisco Security Manager uit te voeren.
- De Network Access Bepertion (NAR) omvat de apparaatgroep (of de apparaten) die u wilt beheren, als u een NAR op het profiel toepast.
- De beheerde apparaatnamen worden op identieke wijze gespeld en gekapitaliseerd in Cisco Secure ACS en in Cisco Security Manager.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

Opmerking: Zorg ervoor dat u de compatibele CSM- en ACS-versies kiest voordat u deze op uw netwerkomgeving installeert. Cisco heeft bijvoorbeeld ACS 3.3 getest met alleen CSM 3.0 en is gestopt voor latere CSM-versies. U wordt dus aangeraden om CSM 3.0 te gebruiken met ACS 3.3. Zie de tabel met compacte matrixprinter voor meer informatie over verschillende softwareversies.

Cisco Security Manager-versies	CS ACS-versies getest
3.0.0 3.0.0 SP1	Windows 3.3(3) en 4.0(1)
3.0.1 3.0.1 SP1 3.0.1 SP2	Oplossingen Engine 4.0(1) Windows 4.0(1)
3.1.0 3.0.2	Oplossingen Engine 4.0(1) Windows 4.1(1) en 4.1(3)
3.1.1 3.0.2 SP1 3.0.2 SP2	Oplossingen Engine v4.0(1) Windows 4.1(2), 4.1(3) en 4.1(4)
3.1.1 SP1	Oplossingen Engine 4.0(1) Windows 4.1(4)

3.1.1 SP2	Oplossingen Engine 4.0(1) Windows 4.1(4) en 4.2(0)
3.2.0	Oplossingen Engine 4.1(4) Windows 4.1(4) en 4.2(0)
3.2.1	Oplossingen Engine 4.1(4) Windows 4.2(0)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Cisco Security Manager integreren met Cisco Secure ACS

In deze sectie worden de stappen beschreven die vereist zijn om Cisco Security Manager te integreren met Cisco Secure ACS. Sommige stappen bevatten meerdere substappen. Deze stappen en substappen moeten in volgorde worden uitgevoerd. Deze paragraaf bevat ook verwijzingen naar specifieke procedures die worden gebruikt om elke stap uit te voeren.

Voer de volgende stappen uit:

1. **Plan uw administratieve authenticatie en autorisatie model.**U moet een besluit nemen over uw beheermodel voordat u Cisco Security Manager gebruikt. Dit omvat de definitie van de administratieve taken en rekeningen die u van plan bent te gebruiken.**Tip:** Als u de rollen en permissie van potentiële beheerders definieert, moet u ook overwegen of u Werkstroom al dan niet moet inschakelen. Deze selectie beïnvloedt hoe u de toegang kunt beperken.
2. **Installeer Cisco Secure ACS, Cisco Security Manager en CiscoWorks gemeenschappelijke services.**Installeer Cisco Secure ACS versie 3.3 op een Windows 2000/2003-server. Installeer CiscoWorks Common Services en Cisco Security Manager op een andere Windows 2000/Windows 2003-server.Raadpleeg deze documenten voor meer informatie:Installatiegids voor Cisco Security Manager 3.0Installatiegids voor Cisco Secure ACS voor Windows 3.3**Opmerking:** Zie de tabel Compatable Matrix voor meer informatie voordat u de CSM- en ACS-softwareversies kiest.
3. **Voer integratieprocedures uit in Cisco Secure ACS.**Defineer Cisco Security Manager-gebruikers als ACS-gebruikers en wijs ze toe aan gebruikersgroepen op basis van hun geplande rol, voeg al uw beheerde apparaten (evenals de CiscoWorks/Security Manager server) toe als AAA-clients en creëer een beheergebruiker. Zie Integratieprocedures uitgevoerd in Cisco Secure ACS voor meer informatie.
4. **Voer integratieprocedures uit in CiscoWorks Gemeenschappelijke services.**Configureer een lokale gebruiker die de beheerder aanpast die in Cisco Secure ACS is gedefinieerd, definieer die zelfde gebruiker voor de instelling van de systeemidentiteit en stel ACS als de AAA-setup-modus in.Zie Integratieprocedures uitgevoerd in CiscoWorks voor meer informatie.
5. **Toewijzen rollen aan gebruikersgroepen in Cisco Secure ACS.**Toewijzen rollen aan elke gebruikersgroep die in Cisco Secure ACS wordt ingesteld. De procedure die u gebruikt, is

afhankelijk van de vraag of u groepen netwerkapparaten (NDGs) hebt ingesteld.Zie Rollen toewijzen aan gebruikersgroepen in Cisco beveiligde ACS voor meer informatie.

Integratieprocedures die worden uitgevoerd in Cisco beveiligde ACS

In deze sectie worden de stappen beschreven die u in Cisco Secure ACS moet voltooien om het met Cisco Security Manager te integreren:

1. Gebruikers en gebruikersgroepen definiëren in Cisco beveiligde ACS
2. Voeg beheerde apparaten toe als AAA-clients in Cisco Secure ACS
3. Een beheergebruiker in Cisco beveiligde ACS maken

Gebruikers en gebruikersgroepen definiëren in Cisco beveiligde ACS

Alle gebruikers van Cisco Security Manager moeten in Cisco Secure ACS worden gedefinieerd en een rol toegewezen die geschikt is voor hun taakfunctie. De makkelijkste manier om dit te doen is de gebruikers in verschillende groepen te verdelen gebaseerd op elke standaard rol beschikbaar in ACS. Verdeel bijvoorbeeld alle systeembeheerders aan één groep, alle netwerkexploitanten aan een andere groep, enzovoort. Raadpleeg Cisco Secure ACS Default Roles voor meer informatie over de standaardrollen in ACS.

Daarnaast moet u een extra gebruiker maken die de systeembeheerderrol met volledige rechten krijgt toegewezen. De aanmeldingsgegevens die voor deze gebruiker zijn gemaakt, worden later gebruikt op de pagina System Identity Setup in CiscoWorks. Zie De gebruiker van de systeemidentiteit definiëren voor meer informatie.

Merk op dat u in deze fase alleen gebruikers aan verschillende groepen toewijzen. De eigenlijke toewijzing van rollen aan deze groepen wordt uitgevoerd later, nadat CiscoWorks, Cisco Security Manager en andere toepassingen worden geregistreerd op Cisco Secure ACS.

Tip: Voordat u verdergaat, installeert u CiscoWorks Gemeenschappelijke Services en Cisco Security Manager op één Windows 2000/2003-server. Installeer Cisco Secure ACS op een andere Windows 2000/2003-server.

1. Meld u aan bij Cisco Secure ACS.
2. Configureer een gebruiker met volledige rechten:Klik op **Gebruikersinstelling** in de navigatiebalk.Voer in de pagina Gebruikersinstelling een naam voor de nieuwe gebruiker in en klik vervolgens op **Toevoegen/Bewerken**.Selecteer een verificatiemethode in de lijst Wachtwoordverificatie onder Gebruikersinstelling.Voer het wachtwoord in en bevestig voor de nieuwe gebruiker.Selecteer **Groep 1** als de groep waaraan de gebruiker is toegewezen.Klik op **Inzenden** om de gebruikersaccount te maken.
3. Herhaal stap 2 voor elke Cisco Security Manager-gebruiker. Cisco raadt u aan om de gebruikers in groepen te verdelen op basis van de rol die elke gebruiker krijgt toegewezen:Groep 1—SysteembeheerdersGroep 2—BeveiligingsbeheerdersGroep 3—BeveiligingsbenaderingenGroep 4—NetwerkbeheerdersGroep 5—BenaversGroep 6—NetwerkoperatorenGroep 7—Help-bureauZie de Tabel voor meer informatie over de standaardinstellingen verbonden met elke rol. Raadpleeg Cisco Secure ACS-rollen aanpassen voor meer informatie over het aanpassen van gebruikersrollen.**Toelichting:** In dit

stadium zijn de groepen zelf collecties van gebruikers zonder roldefinities. U kent rollen toe aan elke groep nadat u het integratieproces hebt voltooid. Zie Rollen toewijzen aan gebruikersgroepen in Cisco beveiligde ACS voor meer informatie.
4. Maak een extra gebruiker en wijs deze gebruiker aan de groep systeembeheerders toe. De aanmeldingsgegevens die voor deze gebruiker zijn gemaakt, worden later gebruikt op de pagina System Identity Setup in CiscoWorks. Zie De gebruiker van de systeemidentiteit definiëren voor meer informatie.
5. Ga verder met Add Managed Devices als AAA-clients in Cisco Secure ACS.

Voeg beheerde apparaten toe als AAA-clients in Cisco Secure ACS

Voordat u apparaten in Cisco Security Manager kunt importeren, moet u elk apparaat eerst configureren als een AAA-client in uw Cisco Secure ACS. Daarnaast moet u de CiscoWorks/Security Manager server als een AAA-client configureren.

Als Cisco Security Manager beveiligingscontexten beheert die zijn geconfigureerd op firewallapparaten, wat security contexten omvat die op FWSM's zijn ingesteld voor Catalyst 6500/7600 apparaten, moet elke context afzonderlijk aan Cisco Secure ACS worden toegevoegd.

De methode u gebruikt om beheerde apparaten toe te voegen hangt af van de vraag of u gebruikers wilt beperken om een bepaalde reeks apparaten met netwerkapparaatgroepen (NDGs) te beheren. Zie één van deze rubrieken:

- Als u wilt dat gebruikers toegang tot alle apparaten hebben, voegt u de apparaten toe zoals beschreven in Add Devices als AAA-clients zonder NDGs.
- Als u wilt dat gebruikers alleen toegang hebben tot bepaalde NDGs, voegt u de apparaten toe zoals beschreven in Configureren Apparaatgroepen voor gebruik in Security Manager.

Apparaten toevoegen als AAA-clients zonder NDGs

Deze procedure beschrijft hoe u apparaten als AAA-klanten van een Cisco Secure ACS kunt toevoegen. Raadpleeg het *gedeelte AAA-clientconfiguratie van* netwerkconfiguratie voor volledige informatie over alle beschikbare opties.

Opmerking: Vergeet niet de server CiscoWorks/Security Manager als een AAA-client toe te voegen.

1. Klik op **Network Configuration** op de Cisco Secure ACS-navigatiebalk.
2. Klik op **Ingang toevoegen** onder de tabel AAA-clients.
3. Voer de AAA-clienthostname (maximaal 32 tekens) in op de pagina Add AAA-client. De hostname van de AAA-client moet overeenkomen met de weergavenaam die u voor het apparaat in Cisco Security Manager wilt gebruiken.Als u bijvoorbeeld van plan bent een domeinnaam aan de apparaatnaam in Cisco Security Manager toe te voegen, moet de AAA-client-hostname in ACS **<device_name>.<domein_name>**.Wanneer u de server van CiscoWorks noemt, wordt het aanbevolen om de volledig-gekwalificeerde hostname te gebruiken. Vergeet niet de hostname correct te spellen. De hostname is niet hoofdlettergevoelig.Wanneer u een beveiligingscontext noemt, voegt u de contextnaam (**_<context_name>**) toe aan de apparaatnaam. Voor FWSM's is dit de naamgevingsconventie:Bladzijde voor

FWSM—**<chassis_name>_FW_<sleuf_nummer>**Beveiligingscontext—**<chassis_naam>_FW_<sleuf_nummer>_<context_naam>**

4. Voer het IP-adres van het netwerkapparaat in het veld AAA-clientadres.
5. Voer het gedeelde geheim in het veld Key in.
6. Selecteer **TACACS+ (Cisco IOS)** uit de lijst Verificeren met behulp van.
7. Klik op **Inzenden** om de wijzigingen op te slaan. Het toegevoegde apparaat verschijnt in de AAA Clients tabel.
8. Herhaal stap 1 tot en met 7 om extra apparaten toe te voegen.
9. Nadat u alle apparaten hebt toegevoegd, klikt u op **Inzenden + opnieuw starten**.
10. Ga verder met Create a Administration User in Cisco Secure ACS.

Netwerkapparaatgroepen configureren in Security Manager

Cisco Secure ACS stelt u in staat om netwerkapparaatgroepen (NDGs) te configureren die specifieke apparaten bevatten om te worden beheerd. U kunt bijvoorbeeld NDGs maken voor elke geografische regio of NDGs die overeenkomen met uw organisatiestructuur. Wanneer gebruikt met Cisco Security Manager, stellen NDGs u in staat om gebruikers van verschillende niveaus van toegang te voorzien, gebaseerd op de apparaten die ze moeten beheren. Met NDGs kunt u bijvoorbeeld de rechten van de gebruiker aan de systeembeheerder toewijzen aan de apparaten in Europa en de rechten van de helpdesk aan de apparaten in Azië toewijzen. U kunt dan de tegenovergestelde rechten aan Gebruiker B toewijzen.

NDGs worden niet rechtstreeks aan gebruikers toegewezen. In plaats daarvan worden NDGs toegewezen aan de rollen die u voor elke gebruikersgroep definieert. Elke NDG kan slechts aan één rol worden toegewezen, maar elke rol kan meerdere NDG's omvatten. Deze definities worden opgeslagen als deel van de configuratie voor de geselecteerde gebruikersgroep.

Deze onderwerpen schetsen de basisstappen die vereist zijn om NDGs te configureren:

- De NDG-functie activeren
- NDGs maken
- NDGs en rollen koppelen aan gebruikersgroepen

De NDG-functie activeren

U moet de NDG-functie activeren voordat u NDGs kunt maken en deze met apparaten kunt bevolken.

1. Klik op **Interface Configuration** op de Cisco Secure ACS-navigatiebalk.
2. Klik op **Geavanceerde opties**.
3. Scrolt neer, en controleer vervolgens het vakje **Network Devices Groepen**.
4. Klik op **Inzenden**.
5. Ga door met NDGs maken.

NDGs maken

In deze procedure wordt beschreven hoe u NDGs kunt maken en hoe u deze met apparaten kunt bevolken. Elk apparaat kan tot slechts één NDG behoren.

Opmerking: Cisco raadt u aan een speciale NDG te maken die de CiscoWorks/Security Manager server bevat.

1. Klik op **Network Configuration** op de navigatiebalk.Alle apparaten worden aanvankelijk geplaatst onder Not Assigned, dat alle apparaten bevat die niet in een NDG geplaatst waren. Houd in gedachten dat Not Assigned geen NDG is.
2. NDGs maken:Klik op **Toevoegen**.Voer een naam voor de NDG in op de pagina Nieuw netwerkapparaat. De maximale lengte is 24 tekens. Ruimten zijn toegestaan.**Optioneel wanneer met versie 4.0 of hoger:** Voer een sleutel in die door alle apparaten in de NDG's moet worden gebruikt. Als je een sleutel voor de NDG definieert, gaat deze met de overbelaste toetsen die zijn gedefinieerd voor de afzonderlijke apparaten in de NDG.Klik op **Inzenden** om de NDG op te slaan.Herhaal stappen a tot en met d om meer NDGs te maken.
3. Populeer de NDGs met apparaten:Klik de naam van de NDG in het gebied Netwerkapparaatgroepen aan.Klik op **Ingang toevoegen** in het gebied AAA-clients.Defineert de gegevens van het apparaat dat aan de NDG moet worden toegevoegd, en klik vervolgens op **Inzenden**. Zie Apparaten toevoegen als AAA-clients zonder NDGs voor meer informatie.Herhaal stap b en c om de rest van de apparaten aan NDGs toe te voegen. Het enige apparaat dat u in de categorie Niet toegewezen kunt verlaten is de standaard AAA server.Nadat u het laatste apparaat hebt configureren klikt u op **Inzenden + opnieuw starten**.
4. Ga verder met Create a Administration User in Cisco Secure ACS.

Een beheergebruiker in Cisco beveiligde ACS maken

Gebruik de pagina Beheer in Cisco Secure ACS om de beheerderaccount te definiëren die wordt gebruikt bij het definiëren van de AAA-setup-modus in CiscoWorks Gemeenschappelijke services. Zie De AAA Setup-modus configureren in CiscoWorks voor meer informatie.

1. Klik op **Beheer** op de Cisco Secure ACS-navigatiebalk.
2. Klik op **beheerder toevoegen**.
3. Voer in de pagina Administrator een naam en wachtwoord voor de beheerder in.
4. Klik op **allen** in het gebied Administrator Privileges om deze beheerder volledige beheerrechten te geven.
5. Klik op **Inzenden** om de beheerder te maken.

Opmerking: Raadpleeg Administrateurs en administratief beleid voor meer informatie over de beschikbare opties wanneer u een beheerder configureren.

Integratieprocedures die in CiscoWorks worden uitgevoerd

In deze sectie worden de stappen beschreven om in CiscoWorks Common Services te voltooien om het met Cisco Security Manager te integreren:

- Een lokale gebruiker in CiscoWorks maken
- De systeemidentiteitsgebruiker definiëren
- De AAA-setup-modus in CiscoWorks configureren

Voltooi deze stappen nadat u de integratieprocedures hebt voltooid die in Cisco Secure ACS zijn uitgevoerd. De gemeenschappelijke services voeren de eigenlijke registratie van geïnstalleerde toepassingen uit, zoals Cisco Security Manager, Auto-Update Server en IPS Manager in Cisco Secure ACS.

Een lokale gebruiker in CiscoWorks maken

Gebruik de pagina Local User Setup in CiscoWorks Common Services om een lokale gebruikersaccount te maken die de beheerder dupliceert die u eerder in Cisco Secure ACS hebt gemaakt. Deze lokale gebruikersaccount wordt later gebruikt voor de instellingen van de systeemidentiteit. Zie voor meer informatie.

Opmerking: Voordat u verdergaat, maakt u een beheerder in Cisco Secure ACS. Zie Gebruikers en gebruikersgroepen definiëren in Cisco beveiligde ACS voor instructies.

1. Meld u aan bij CiscoWorks met de standaard beheergebruikersaccount.
2. Kies **Server > Beveiliging** van Gemeenschappelijke diensten en kies vervolgens **Plaatselijke gebruikersinstelling** van de TOC.
3. Klik op **Add** (Toevoegen).
4. Voer dezelfde naam en het wachtwoord in dat u hebt ingevoerd toen u de beheerder in Cisco Secure ACS hebt gemaakt. Zie stap 4 in Definitie gebruikers en gebruikersgroepen in Cisco Secure ACS.
5. Controleer alle vinkjes onder Rollen behalve Exportwedgegevens.
6. Klik op **OK** om de gebruiker te maken.

De systeemidentiteitsgebruiker definiëren

Gebruik de pagina System Identity Setup in CiscoWorks Common Services om een vertrouwensgebruiker te maken die bekend staat als de gebruiker System Identity, die communicatie mogelijk maakt tussen servers die deel uitmaken van hetzelfde domein en toepassingsprocessen die op dezelfde server geplaatst zijn. Toepassingen gebruiken de gebruiker van de Systeemidentiteit om processen op lokale of externe CiscoWorks-servers te authentiseren. Dit is vooral handig wanneer de toepassingen moeten synchroniseren voordat een gebruiker heeft inlogd.

Bovendien wordt de gebruiker System Identity vaak gebruikt om een subtaak uit te voeren wanneer de primaire taak al is geautoriseerd voor de ingelogde gebruiker. Om een apparaat in Cisco Security Manager te kunnen bewerken, is bijvoorbeeld de communicatie tussen toepassingen vereist tussen Cisco Security Manager en de CTRF. Nadat de gebruiker is geautoriseerd om de bewerkingstaak uit te voeren, wordt de gebruiker van de systeemidentiteit gebruikt om een beroep te doen op de DCR.

De gebruiker die u hier instelt, moet identiek zijn aan de gebruiker met administratieve (volledige) toegangsrechten die u in ACS hebt ingesteld. Als u dit niet doet, kan dit resulteren in een onvermogen om alle apparaten en beleid te bekijken die in Cisco Security Manager zijn geconfigureerd.

Opmerking: Voordat u verdergaat, kunt u een lokale gebruiker met dezelfde naam en wachtwoord maken als deze beheerder in CiscoWorks Common Services. Zie Een lokale gebruiker in CiscoWorks maken voor instructies.

1. Kies **Server > Security** en kies vervolgens **Multiserver Trust Management > System Identity Setup** van het TOC.
2. Voer de naam in van de beheerder die u voor Cisco Secure ACS hebt gemaakt. Zie stap 4 in Definitie gebruikers en gebruikersgroepen in Cisco Secure ACS.
3. Voer het wachtwoord voor deze gebruiker in en controleer dit.

4. Klik op **Apply** (Toepassen).

De AAA-setup-modus in CiscoWorks configureren

Gebruik de pagina AAA Setup Mode in CiscoWorks Common Services om uw Cisco Secure ACS als de AAA-server te definiëren, die de gewenste poort en gedeelde geheime sleutel bevat. Daarnaast kunt u maximaal twee reserveservers definiëren.

Deze stappen voeren de eigenlijke registratie van CiscoWorks, Cisco Security Manager, IPS Manager (en optioneel, Auto-Update Server) in Cisco Secure ACS uit.

1. Kies **Server > Beveiliging** en kies vervolgens **AAA mode Setup** vanuit het hoofdscherm.
2. Controleer het vakje **TACACS+** onder Beschikbare inlogmodules.
3. Selecteer **ACS** als het AAA-type.
4. Voer de IP-adressen in van maximaal drie Cisco Secure ACS-servers in het gebied Server Details. De secundaire en tertiaire servers fungeren als back-ups voor het geval de primaire server faalt.**Opmerking:** Als alle geconfigureerde TACACS+-servers niet reageren, moet u inloggen met de lokale account van de beheerder CiscoWorks, dan moet u de AAA-modus terugzetten naar de lokale instellingen van niet-ACS/CiscoWorks. Nadat de TACACS+-servers zijn hersteld, moet u de AAA-modus terugzetten naar ACS.
5. In het Login gebied, voer de naam van de beheerder in die u op de pagina van de Controle van het Beheer van Cisco Secure ACS definieerde. Zie Een gebruiker van de Controle van het Beheer in Cisco Bevestigd ACS voor meer informatie creëren.
6. Voer het wachtwoord in en controleer dit voor deze beheerder.
7. Voer de gedeelde geheime sleutel in en controleer die u hebt ingevoerd toen u de Security Manager server als een AAA client voor Cisco Secure ACS toevoegde. Zie stap 5 in Add Devices als AAA-clients zonder NDGs.
8. Controleer het **dialoogvenster Alle geïnstalleerde toepassingen met de ACS-**optie om Cisco Security Manager en alle andere geïnstalleerde toepassingen te registreren met Cisco Secure ACS.
9. Klik op **Toepassen** om uw instellingen op te slaan. In een voortgangsbalk wordt de voortgang van de registratie weergegeven. Er verschijnt een bericht wanneer de registratie is voltooid.
10. Als u Cisco Security Manager met een ACS-versie integreren, moet u de Cisco Security Manager-service opnieuw opstarten. Zie De Daemon Manager opnieuw starten voor meer informatie.**Opmerking:** Na CSM 3.0.0 heeft Cisco niet langer tests met ACS 3.3(x) uitgevoerd omdat deze sterk gepatcheerd is en de end-of-life (End-of-life) ervan aangekondigd is. Daarom moet u de juiste ACS-versie voor CSM versie 3.0.1 en hoger gebruiken. Zie de Matrixtabel met compactheid voor meer informatie.
11. Log terug in Cisco Secure ACS om rollen toe te wijzen aan elke gebruikersgroep. Zie Rollen toewijzen aan gebruikersgroepen in Cisco beveiligde ACS voor instructies.**N.B.:** De AAA-instellingen die hier zijn ingesteld, blijven niet behouden als u CiscoWorks Common Services of Cisco Security Manager verwijdert. Bovendien kan er na het opnieuw installeren geen back-up en herstel van de configuratie worden gemaakt. Als u daarom een upgrade naar een nieuwe versie van een van beide toepassingen uitvoert, moet u de AAA setup-modus opnieuw configureren en Cisco Security Manager opnieuw registreren met ACS. Dit proces is niet vereist voor geleidelijke updates. Als u extra toepassingen, zoals AUS, bovenop CiscoWorks installeert, moet u de nieuwe toepassingen en Cisco Security Manager registreren.

Start Daemon Manager opnieuw

Deze procedure beschrijft hoe u de Daemon Manager van de Cisco Security Manager server opnieuw kunt starten. U dient dit te doen om de ingestelde AAA-instellingen te kunnen uitvoeren. U kunt dan terugloggen naar CiscoWorks met de referenties die in Cisco Secure ACS zijn gedefinieerd.

1. Log in op de machine waarop de Cisco Security Manager server is geïnstalleerd.
2. Kies **Start > Programma's > Administratieve hulpmiddelen > Services** om het venster Services te openen.
3. Selecteer in de lijst met services in het rechter deelvenster de optie **Cisco Security Manager-beheerder**.
4. Klik in de werkbalk op de knop **Herstart-service**.
5. Doorgaan met Rollen toewijzen aan gebruikersgroepen in Cisco beveiligde ACS.

Rollen toewijzen aan gebruikersgroepen in Cisco beveiligde ACS

Nadat u CiscoWorks, Cisco Security Manager en andere geïnstalleerde toepassingen voor Cisco Secure ACS registreert, kunt u rollen toewijzen aan elk van de gebruikersgroepen die u eerder in Cisco Secure ACS hebt ingesteld. Deze rollen bepalen de acties die de gebruikers in elke groep mogen uitvoeren in Cisco Security Manager.

De procedure die u gebruikt om rollen toe te wijzen aan gebruikersgroepen hangt af van de vraag of NDGs worden gebruikt:

- Rollen toewijzen aan gebruikersgroepen zonder NDGs
- NDGs en rollen koppelen aan gebruikersgroepen

Rollen toewijzen aan gebruikersgroepen zonder NDGs

Deze procedure beschrijft hoe de standaardrollen aan gebruikersgroepen moeten worden toegewezen wanneer NDGs niet worden gedefinieerd. Raadpleeg Cisco Secure ACS Default Roles voor meer informatie.

Opmerking: Voordat u verdergaat:

- Maak een gebruikersgroep voor elke standaardrol. Zie Gebruikers en gebruikersgroepen definiëren in Cisco beveiligde ACS voor instructies.
- Voltooi de procedures die zijn beschreven in integratieprocedures die zijn uitgevoerd in Cisco Secure ACS en integratieprocedures die worden uitgevoerd in CiscoWorks.

Voer de volgende stappen uit:

1. Meld u aan bij Cisco Secure ACS.
2. Klik op **Groepsinstelling** in de navigatiebalk.
3. Selecteer de gebruikersgroep voor systeembeheerders in de lijst. Zie stap 2 van Definieer Gebruikers en gebruikersgroepen in Cisco Secure ACS en klik vervolgens op **Instellingen bewerken**.

NDGs en rollen koppelen aan gebruikersgroepen

Wanneer u NDGs met rollen voor gebruik in Cisco Security Manager associeert, moet u definities in twee plaatsen op de pagina van de Instellen van de Groep creëren:

- CiscoWorks-gebied
- Cisco Security Manager-gebied

De definities op elk gebied moeten zo nauw mogelijk aansluiten. Wanneer u aangepaste rollen of ACS rollen associeert die niet in de Gemeenschappelijke Diensten van CiscoWorks bestaan, probeer zo nauw mogelijk te definiëren op basis van de permissies die aan die rol zijn toegewezen.

U moet associaties voor elke gebruikersgroep maken die met Cisco Security Manager gebruikt moeten worden. Als u bijvoorbeeld een gebruikersgroep hebt die ondersteuningspersoneel voor de westerse regio bevat, kunt u die gebruikersgroep selecteren en vervolgens de NDG associëren dat de apparaten in die regio bevat met de rol van de Help-woestijn.

N.B.: Activeer de NDG-functie voordat u verdergaat en maak NDGs. Zie Netwerkapparaatgroepen configureren voor gebruik in Security Manager voor meer informatie.

1. Klik op **Groepsinstelling** in de navigatiebalk.
2. Selecteer een gebruikersgroep uit de lijst Groep en klik vervolgens op **Instellingen bewerken**.
3. Kaart NDGs en rollen voor gebruik in CiscoWorks:Op de pagina Groepsinstallatie scrollen naar het CiscoWorks-gebied onder TACACS+ instellingen.Selecteer **Een CiscoWorks op een basis voor netwerkapparaten toewijzen**.Selecteer een NDG in de lijst Apparaatgroep.Selecteer de rol waaraan deze NDG moet worden gekoppeld in de tweede lijst.Klik op **Associatie toevoegen**. De associatie verschijnt in het vak Apparaatgroep.Herhaal stappen c door e om extra associaties te creëren.**Opmerking:** als u een associatie wilt verwijderen, selecteert u deze uit de Apparaatgroep en vervolgens klikt u op Associatie verwijderen.
4. Rol naar het gebied van de Manager van de Veiligheid van Cisco en creëer verenigingen die zo nauw mogelijk overeenkomen met de verenigingen die in stap 3 worden bepaald.**Opmerking:** Wanneer u de beveiligingsbenadering of de beveiligingsbeheerderrollen in Cisco Secure ACS selecteert, wordt aanbevolen om de netwerkbeheerder te selecteren als de dichtstbijzijnde equivalente CiscoWorks-rol.
5. Klik op **Inzenden** om de instellingen op te slaan.
6. Herhaal stap 2 tot en met 5 om NDGs voor de rest van de gebruikersgroepen te definiëren.
7. Nadat u NDGs en rollen met elke gebruikersgroep associeert, klik op **Inzenden + Herstart**.

Problemen oplossen

1. Voordat u apparaten in Cisco Security Manager kunt importeren, moet u elk apparaat eerst configureren als een AAA-client in uw Cisco Secure ACS. Daarnaast moet u de CiscoWorks/Security Manager server als een AAA-client configureren.
2. Als u een mislukt poging logbestand ontvangt, is de auteur mislukt met fout in 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"
   ```
   Om deze kwestie op te lossen, zorg ervoor dat de naam van het apparaat in ACS een volledig gekwalificeerde domeinnaam moet zijn.

Gerelateerde informatie

- Cisco Security Access Control Server voor Windows-ondersteuningspagina
- Ondersteuning voor Cisco Security Manager
- Cisco Secure Access Control Server voor Windows
- Configuratiehandleiding voor Cisco Secure ACS 4.1
- Cisco Secure ACS online probleemoplossing, gids 4.1
- Security meldingen uit het veld (inclusief Cisco Secure ACS voor Windows)
- Technische ondersteuning en documentatie – Cisco Systems