# Security Manager-Integration mit ACS

## Inhalt



## Einführung

In diesem Dokument wird beschrieben, wie der Cisco Security Manager in den Cisco Secure Access Control Server (ACS) integriert wird.

Cisco Secure ACS bietet Befehlsautorisierung für Benutzer, die Managementanwendungen wie Cisco Security Manager zum Konfigurieren verwalteter Netzwerkgeräte verwenden. Die Unterstützung für die Befehlsautorisierung wird von eindeutigen Befehls-Autorisierungsset-Typen bereitgestellt, die als Rollen in Cisco Security Manager bezeichnet werden und eine Reihe von Berechtigungen enthalten. Diese Berechtigungen, auch als Berechtigungen bezeichnet, bestimmen die Aktionen, die Benutzer mit bestimmten Rollen in Cisco Security Manager ausführen können.

Cisco Secure ACS verwendet TACACS+, um mit Verwaltungsanwendungen zu kommunizieren. Damit Cisco Security Manager mit Cisco Secure ACS kommunizieren kann, müssen Sie den CiscoWorks-Server in Cisco Secure ACS als AAA-Client konfigurieren, der TACACS+ verwendet. Darüber hinaus müssen Sie dem CiscoWorks-Server den Namen und das Kennwort des

Administrators angeben, den Sie für die Anmeldung beim Cisco Secure ACS verwenden. Wenn Sie diese Anforderungen erfüllen, wird die Gültigkeit der Kommunikation zwischen Cisco Security Manager und Cisco Secure ACS sichergestellt.

Wenn Cisco Security Manager anfänglich mit Cisco Secure ACS kommuniziert, wird Cisco ACS die Erstellung von Standardrollen angewiesen, die im Abschnitt "Komponenten des gemeinsam genutzten Profils" der HTML-Schnittstelle von Cisco Secure ACS angezeigt werden. Außerdem wird ein benutzerdefinierter Dienst für die Genehmigung durch TACACS+ vorgegeben. Dieser benutzerdefinierte Dienst wird auf der Seite TACACS+ (Cisco IOS®) im Abschnitt Schnittstellenkonfiguration der HTML-Schnittstelle angezeigt. Anschließend können Sie die in jeder Cisco Security Manager-Rolle enthaltenen Berechtigungen ändern und diese Rollen auf Benutzer und Benutzergruppen anwenden.

**Hinweis:** CSM kann nicht in ACS 5.2 integriert werden, da es nicht unterstützt wird.

# Voraussetzungen

## Anforderungen

Um Cisco Secure ACS zu verwenden, müssen Sie Folgendes sicherstellen:

- Sie definieren Rollen, die die Befehle enthalten, die zum Ausführen der erforderlichen Funktionen in Cisco Security Manager erforderlich sind.
- Die Netzwerkzugriffsbeschränkung (Network Access Restriction, NAR) umfasst die Gerätegruppe (oder die Geräte), die Sie verwalten möchten, wenn Sie ein NAR auf das Profil anwenden.
- Verwaltete Gerätenamen werden in Cisco Secure ACS und in Cisco Security Manager identisch geschrieben und kapitalisiert.

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

**Hinweis:** Wählen Sie vor der Installation in Ihrer Netzwerkumgebung die kompatiblen CSM- und ACS-Versionen aus. Beispielsweise hat Cisco ACS 3.3 nur mit CSM 3.0 getestet und bei späteren CSM-Versionen gestoppt. Es wird daher empfohlen, CSM 3.0 mit ACS 3.3 zu verwenden. Weitere Informationen zu verschiedenen Softwareversionen finden Sie in der Tabelle Compatabilty Matrix.

| Cisco Security Manager-Versionen | Getestete CS ACS-Versionen |
|---|---|
| 3.0.0 3.0.0 SP1 | Windows 3.3(3) und 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) und 4.1(3) |
| 3.1.1 3.0.2 SP1 | Solutions Engine v4.0(1) Windows |

| | |
|---|---|
| 3.0.2 SP2 | 4.1(2), 4.1(3) und 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) und 4.2(0) |
| 3,2/0 | Solutions Engine 4.1(4) Windows 4.1(4) und 4.2(0) |
| 3,2/1 | Solutions Engine 4.1(4) Windows 4.2(0) |

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

### Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

## Integration von Cisco Security Manager in Cisco Secure ACS

In diesem Abschnitt werden die Schritte beschrieben, die für die Integration von Cisco Security Manager in Cisco Secure ACS erforderlich sind. Einige Schritte enthalten mehrere Unterschritte. Diese Schritte und Umspannwerke müssen in der richtigen Reihenfolge ausgeführt werden. Dieser Abschnitt enthält auch Verweise auf spezifische Prozeduren, die zum Durchführen der einzelnen Schritte verwendet werden.

Gehen Sie wie folgt vor:

1. **Planen Sie Ihr Verwaltungsauthentifizierungs- und Autorisierungsmodell.**Bevor Sie Cisco Security Manager verwenden, müssen Sie Ihr Verwaltungsmodell festlegen. Dazu gehört auch die Definition der Verwaltungsrollen und -konten, die Sie verwenden möchten.**Tipp:** Wenn Sie die Rollen und Berechtigungen potenzieller Administratoren definieren, sollten Sie auch berücksichtigen, ob Workflow aktiviert werden soll oder nicht. Diese Auswahl beeinflusst, wie Sie den Zugriff einschränken können.
2. **Installieren Sie Cisco Secure ACS, Cisco Security Manager und CiscoWorks Common Services.**Installieren Sie Cisco Secure ACS Version 3.3 auf einem Windows 2000/2003-Server. Installieren Sie CiscoWorks Common Services und Cisco Security Manager auf einem anderen Windows 2000/Windows 2003-Server.Weitere Informationen finden Sie in diesen Dokumenten:Installationsanleitung für Cisco Security Manager 3.0Installationsanleitung für Cisco Secure ACS für Windows 3.3**Hinweis:** In der Kompatibilitätsmatrix finden Sie weitere Informationen, bevor Sie die Softwareversionen CSM und ACS auswählen.
3. **Durchführen von Integrationsverfahren in Cisco Secure ACS**Definieren Sie Cisco Security Manager-Benutzer als ACS-Benutzer, und weisen Sie sie entsprechend ihrer geplanten Rolle den Benutzergruppen zu, fügen Sie alle verwalteten Geräte (sowie den CiscoWorks/Security Manager-Server) als AAA-Clients hinzu, und erstellen Sie einen Benutzer für die

Administrationssteuerung. Weitere Informationen finden Sie unter Integrationsverfahren, die in Cisco Secure ACS durchgeführt werden.

4. **Durchführen von Integrationsverfahren in CiscoWorks Common Services.**Konfigurieren Sie einen lokalen Benutzer, der dem in Cisco Secure ACS definierten Administrator entspricht, definieren Sie diesen Benutzer für die Systemidentitätseinrichtung, und konfigurieren Sie ACS als AAA-Setup-Modus.Weitere Informationen finden Sie unter Integrationsverfahren in CiscoWorks.
5. **Weisen Sie Benutzergruppen in Cisco Secure ACS Rollen zu.**Weisen Sie jeder Benutzergruppe, die in Cisco Secure ACS konfiguriert ist, Rollen zu. Die Vorgehensweise hängt davon ab, ob Sie Netzwerkgerätegruppen (NDGs) konfiguriert haben.Weitere Informationen finden Sie unter Zuweisen von Rollen zu Benutzergruppen in Cisco Secure ACS.

# Integrationsverfahren in Cisco Secure ACS

In diesem Abschnitt werden die Schritte beschrieben, die Sie in Cisco Secure ACS ausführen müssen, um es in Cisco Security Manager zu integrieren:

1. Definieren von Benutzern und Benutzergruppen in Cisco Secure ACS
2. Hinzufügen verwalteter Geräte als AAA-Clients in Cisco Secure ACS
3. Erstellen eines Administrationssteuerungsbenutzers in Cisco Secure ACS

## Definieren von Benutzern und Benutzergruppen in Cisco Secure ACS

Alle Benutzer von Cisco Security Manager müssen in Cisco Secure ACS definiert sein und eine ihrer Funktion entsprechende Rolle zugewiesen werden. Die einfachste Methode hierfür besteht darin, die Benutzer je nach der in ACS verfügbaren Standardrolle in verschiedene Gruppen aufzuteilen. Weisen Sie beispielsweise alle Systemadministratoren einer Gruppe, alle Netzwerkbetreiber einer anderen Gruppe usw. zu. Weitere Informationen zu den Standardrollen in ACS finden Sie unter Cisco Secure ACS Default Roles.

Darüber hinaus müssen Sie einen zusätzlichen Benutzer erstellen, dem die Rolle des Systemadministrators mit vollständigen Berechtigungen zugewiesen wird. Die für diesen Benutzer erstellten Anmeldeinformationen werden später auf der Seite System Identity Setup (System-Identitätseinrichtung) in CiscoWorks verwendet. Weitere Informationen finden Sie unter Definieren des Systemidentitätsbenutzers.

Beachten Sie, dass Sie in dieser Phase nur Benutzer verschiedenen Gruppen zuweisen. Die tatsächliche Zuweisung der Rollen an diese Gruppen erfolgt später, nachdem CiscoWorks, Cisco Security Manager und alle anderen Anwendungen für Cisco Secure ACS registriert wurden.

**Tipp:** Bevor Sie fortfahren, installieren Sie CiscoWorks Common Services und Cisco Security Manager auf einem Windows 2000/2003-Server. Installieren Sie Cisco Secure ACS auf einem anderen Windows 2000/2003-Server.

1. Melden Sie sich bei Cisco Secure ACS an.
2. Konfigurieren Sie einen Benutzer mit vollständigen Berechtigungen:Klicken Sie in der Navigationsleiste auf **User Setup** (Benutzereinrichtung).Geben Sie auf der Seite für die Benutzereinrichtung einen Namen für den neuen Benutzer ein, und klicken Sie dann auf

**Hinzufügen/Bearbeiten**.Wählen Sie in der Liste Password Authentication (Kennwortauthentifizierung) unter User Setup (Benutzereinrichtung) eine Authentifizierungsmethode aus.Geben Sie das Kennwort für den neuen Benutzer ein, und bestätigen Sie es.Wählen Sie **Gruppe 1** als Gruppe aus, der der Benutzer zugewiesen ist.Klicken Sie auf **Senden**, um das Benutzerkonto zu erstellen.

3. Wiederholen Sie Schritt 2 für jeden Cisco Security Manager-Benutzer. Cisco empfiehlt, die Benutzer je nach zugewiesener Rolle in Gruppen aufzuteilen:Gruppe 1 - SystemadministratorenGruppe 2 - SicherheitsadministratorenGruppe 3 - SicherheitsgenehmigerGruppe 4 - NetzwerkadministratorenGruppe 5 - GenehmigerGruppe 6 - NetzwerkbetreiberGruppe 7 - HelpdeskIn der Tabelle finden Sie weitere Informationen zu den Standardberechtigungen für die einzelnen Rollen. Weitere Informationen zum Anpassen von Benutzerrollen finden Sie unter Anpassen von Cisco Secure ACS-Rollen.**Hinweis:** In dieser Phase sind die Gruppen selbst Sammlungen von Benutzern ohne Rollendefinitionen. Nach Abschluss des Integrationsprozesses weisen Sie jeder Gruppe Rollen zu. Weitere Informationen finden Sie unter Zuweisen von Rollen zu Benutzergruppen in Cisco Secure ACS.
4. Erstellen Sie einen weiteren Benutzer, und weisen Sie diesen Benutzer der Gruppe der Systemadministratoren zu. Die für diesen Benutzer erstellten Anmeldeinformationen werden später auf der Seite System Identity Setup (System-Identitätseinrichtung) in CiscoWorks verwendet. Weitere Informationen finden Sie unter Definieren des Systemidentitätsbenutzers.
5. Fahren Sie mit dem Hinzufügen verwalteter Geräte als AAA-Clients in Cisco Secure ACS fort.

## Hinzufügen verwalteter Geräte als AAA-Clients in Cisco Secure ACS

Bevor Sie Geräte in Cisco Security Manager importieren können, müssen Sie jedes Gerät zuerst als AAA-Client in Ihrem Cisco Secure ACS konfigurieren. Darüber hinaus müssen Sie den CiscoWorks/Security Manager-Server als AAA-Client konfigurieren.

Wenn Cisco Security Manager Sicherheitskontexte verwaltet, die auf Firewall-Geräten konfiguriert sind. Dazu gehören Sicherheitskontexte, die auf FWSMs für Catalyst 6500/7600-Geräte konfiguriert wurden, muss jeder Kontext dem Cisco Secure ACS einzeln hinzugefügt werden.

Die Methode, die Sie zum Hinzufügen verwalteter Geräte verwenden, hängt davon ab, ob Sie die Verwaltung bestimmter Geräte durch Benutzer mit Netzwerkgerätegruppen (NDGs) einschränken möchten. Siehe einen der folgenden Abschnitte:

- Wenn Benutzer Zugriff auf alle Geräte haben sollen, fügen Sie die Geräte hinzu, wie unter Geräte als AAA-Clients ohne NDGs hinzufügen beschrieben.
- Wenn Benutzer nur Zugriff auf bestimmte NDGs haben möchten, fügen Sie die Geräte hinzu, wie unter Netzwerkgerätegruppen für die Verwendung im Security Manager konfigurieren beschrieben.

## Hinzufügen von Geräten als AAA-Clients ohne NDGs

In diesem Verfahren wird beschrieben, wie Geräte als AAA-Clients eines Cisco Secure ACS hinzugefügt werden. Ausführliche Informationen zu allen verfügbaren Optionen finden Sie im *Abschnitt AAA-Client-Konfiguration* der Netzwerkkonfiguration.

**Hinweis:** Denken Sie daran, den CiscoWorks/Security Manager-Server als AAA-Client hinzuzufügen.

1. Klicken Sie in der Navigationsleiste von Cisco Secure ACS auf **Network Configuration** (Netzwerkkonfiguration).
2. Klicken Sie unter der Tabelle AAA-Clients auf **Eintrag hinzufügen**.
3. Geben Sie auf der Seite AAA-Client hinzufügen den AAA-Client-Hostnamen (bis zu 32 Zeichen) ein. Der Hostname des AAA-Clients muss mit dem Anzeigenamen übereinstimmen, den Sie für das Gerät in Cisco Security Manager verwenden möchten.Wenn Sie beispielsweise in Cisco Security Manager einen Domänennamen an den Gerätenamen anhängen möchten, muss der AAA-Client-Hostname in ACS **<device_name>.<domain_name>** lauten.Wenn Sie den CiscoWorks-Server benennen, wird empfohlen, den vollqualifizierten Hostnamen zu verwenden. Achten Sie darauf, den Hostnamen korrekt zu buchstabieren. Beim Hostnamen wird die Groß-/Kleinschreibung nicht beachtet.Wenn Sie einen Sicherheitskontext benennen, fügen Sie den Kontextnamen (**_<context_name>**) dem Gerätenamen hinzu. Für FWSMs ist dies die Namenskonvention:FWSM-Blade - **<Chassis_Name>_FW_<Steckplatznummer>**Sicherheitskontext - **<Chassis_Name>_FW_<Steckplatznummer>_<Context_Name>**
4. Geben Sie die IP-Adresse des Netzwerkgeräts im Feld "AAA Client IP Address" ein.
5. Geben Sie den gemeinsamen geheimen Schlüssel in das Feld Schlüssel ein.
6. Wählen Sie **TACACS+ (Cisco IOS)** aus der Liste "Authenticate Using" (Über Authentifizierung authentifizieren) aus.
7. Klicken Sie auf **Senden**, um Ihre Änderungen zu speichern. Das hinzugefügte Gerät wird in der Tabelle AAA-Clients angezeigt.
8. Wiederholen Sie die Schritte 1 bis 7, um weitere Geräte hinzuzufügen.
9. Nachdem Sie alle Geräte hinzugefügt haben, klicken Sie auf **Senden + Neu starten**.
10. Fahren Sie mit Erstellen eines Administrationssteuerungsbenutzers in Cisco Secure ACS fort.

## Konfigurieren der Netzwerkgerätegruppen für die Verwendung im Sicherheitsmanager

Mit Cisco Secure ACS können Sie Netzwerkgerätegruppen (NDGs) konfigurieren, die bestimmte zu verwaltende Geräte enthalten. Sie können beispielsweise NDGs für jede geografische Region oder NDGs erstellen, die Ihrer Organisationsstruktur entsprechen. In Verbindung mit Cisco Security Manager können Sie mithilfe der NDGs Benutzern je nach zu verwaltenden Geräten verschiedene Berechtigungsebenen bereitstellen. Mit NDGs können Sie beispielsweise den in Europa befindlichen Geräten Benutzer-A-Systemadministratorberechtigungen und den Geräten in Asien Helpdesk-Berechtigungen zuweisen. Sie können dann Benutzer B die gegenteiligen Berechtigungen zuweisen.

NDGs werden nicht direkt den Benutzern zugewiesen. Vielmehr werden NDGs den Rollen zugewiesen, die Sie für jede Benutzergruppe definieren. Jedes NDG kann nur einer Rolle zugewiesen werden, aber jede Rolle kann mehrere NDGs umfassen. Diese Definitionen werden als Teil der Konfiguration für die ausgewählte Benutzergruppe gespeichert.

In diesen Themen werden die grundlegenden Schritte beschrieben, die zur Konfiguration der NDGs erforderlich sind:

- Aktivieren der NDG-Funktion
- NDGs erstellen
- Zuordnen von NDGs und Rollen zu Benutzergruppen

## Aktivieren der NDG-Funktion

Sie müssen die NDG-Funktion aktivieren, bevor Sie NDGs erstellen und mit Geräten füllen können.

1. Klicken Sie in der Navigationsleiste von Cisco Secure ACS auf **Schnittstellenkonfiguration**.
2. Klicken Sie auf **Erweiterte Optionen**.
3. Blättern Sie nach unten, und aktivieren Sie das Kontrollkästchen **Netzwerkgerätegruppen**.
4. Klicken Sie auf **Senden**.
5. Fahren Sie mit der Erstellung von NDGs fort.

## NDGs erstellen

In diesem Verfahren wird beschrieben, wie Sie NDGs erstellen und mit Geräten füllen. Jedes Gerät kann nur einem NDG angehören.

**Hinweis:** Cisco empfiehlt, ein spezielles NDG zu erstellen, das den CiscoWorks/Security Manager-Server enthält.

1. Klicken Sie in der Navigationsleiste auf **Netzwerkkonfiguration**.Alle Geräte werden anfänglich nicht zugewiesen, d. h. alle Geräte, die nicht einem NDG zugeordnet wurden. Beachten Sie, dass Not Assigned kein NDG ist.
2. NDGs erstellen:Klicken Sie auf **Eintrag hinzufügen**.Geben Sie auf der Seite "New Network Device Group" (Neue Netzwerkgerätegruppe) einen Namen für das NDG ein. Die maximale Länge beträgt 24 Zeichen. Leerzeichen sind zulässig.**Optional bei Version 4.0 oder höher:** Geben Sie einen Schlüssel für alle Geräte im NDG ein. Wenn Sie einen Schlüssel für das NDG definieren, überschreibt er alle Schlüssel, die für die einzelnen Geräte im NDG definiert sind.Klicken Sie auf **Senden**, um das NDG zu speichern.Wiederholen Sie die Schritte a bis d, um weitere NDGs zu erstellen.
3. Füllen Sie die NDGs mit Geräten aus:Klicken Sie im Bereich Netzwerkgerätegruppen auf den Namen des NDG.Klicken Sie im Bereich AAA-Clients auf **Eintrag hinzufügen**.Definieren Sie die Details des Geräts, das dem NDG hinzugefügt werden soll, und klicken Sie dann auf **Senden**. Weitere Informationen finden Sie unter Hinzufügen von Geräten als AAA-Clients ohne NDGs.Wiederholen Sie die Schritte b und c, um die restlichen Geräte den NDGs hinzuzufügen. Das einzige Gerät, das Sie in der Kategorie Nicht zugewiesen lassen können, ist der standardmäßige AAA-Server.Nachdem Sie das letzte Gerät konfiguriert haben, klicken Sie auf **Senden + Neu starten**.
4. Fahren Sie mit Erstellen eines Administrationssteuerungsbenutzers in Cisco Secure ACS fort.

## Erstellen eines Administrationssteuerungsbenutzers in Cisco Secure ACS

Auf der Seite "Administration Control" (Administration-Steuerung) in Cisco Secure ACS können Sie das Administratorkonto definieren, das bei der Definition des AAA-Einrichtungsmodus in

CiscoWorks Common Services verwendet wird. Weitere Informationen finden Sie unter Konfigurieren des AAA-Setup-Modus in CiscoWorks.

1. Klicken Sie in der Navigationsleiste von Cisco Secure ACS auf **Administration Control**.
2. Klicken Sie auf **Administrator hinzufügen**.
3. Geben Sie auf der Seite "Administrator hinzufügen" einen Namen und ein Kennwort für den Administrator ein.
4. Klicken Sie im Bereich "Administratorberechtigungen" auf **Alle** gewähren, um diesem Administrator vollständige Administratorberechtigungen zur Verfügung zu stellen.
5. Klicken Sie auf **Senden**, um den Administrator zu erstellen.

**Hinweis:** Unter Administratoren und Verwaltungsrichtlinien finden Sie weitere Informationen zu den Optionen, die beim Konfigurieren eines Administrators verfügbar sind.

# In CiscoWorks ausgeführte Integrationsverfahren

In diesem Abschnitt werden die Schritte beschrieben, die zur Integration in Cisco Security Manager in CiscoWorks Common Services ausgeführt werden müssen:

- Erstellen eines lokalen Benutzers in CiscoWorks
- Definieren des Systemidentitätsbenutzers
- Konfigurieren des AAA-Setup-Modus in CiscoWorks

Führen Sie diese Schritte aus, nachdem Sie die in Cisco Secure ACS ausgeführten Integrationsverfahren abgeschlossen haben. Common Services führt die eigentliche Registrierung aller installierten Anwendungen wie Cisco Security Manager, Auto Update Server und IPS Manager in Cisco Secure ACS durch.

## Erstellen eines lokalen Benutzers in CiscoWorks

Auf der Seite für die lokale Benutzereinrichtung in CiscoWorks Common Services können Sie ein lokales Benutzerkonto erstellen, das den zuvor in Cisco Secure ACS erstellten Administrator dupliziert. Dieses lokale Benutzerkonto wird später für die Systemidentität verwendet. Weitere Informationen finden Sie unter .

**Hinweis:** Bevor Sie fortfahren, erstellen Sie einen Administrator in Cisco Secure ACS. Anweisungen finden Sie unter Definieren von Benutzern und Benutzergruppen in Cisco Secure ACS.

1. Melden Sie sich mit dem Standard-**Admin-**Benutzerkonto bei CiscoWorks an.
2. Wählen Sie **Server > Sicherheit** aus den allgemeinen Diensten aus, und wählen Sie dann **Lokales Benutzer-Setup** aus der Inhaltsverzeichnis aus.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie denselben Namen und dasselbe Kennwort ein, den Sie bei der Erstellung des Administrators in Cisco Secure ACS eingegeben haben. Siehe Schritt 4 Definieren von Benutzern und Benutzergruppen in Cisco Secure ACS.
5. Aktivieren Sie alle Kontrollkästchen unter "Rollen außer Daten exportieren".
6. Klicken Sie auf **OK**, um den Benutzer zu erstellen.

## Definieren des Systemidentitätsbenutzers

Verwenden Sie die Seite System Identity Setup (System-Identitätseinrichtung) in CiscoWorks Common Services, um einen vertrauenswürdigen Benutzer, den Systemidentitätsbenutzer, zu erstellen, der die Kommunikation zwischen Servern ermöglicht, die Teil derselben Domäne sind, und Anwendungsprozessen, die sich auf demselben Server befinden. Anwendungen verwenden den System Identity-Benutzer, um Prozesse auf lokalen oder Remote-CiscoWorks-Servern zu authentifizieren. Dies ist besonders dann nützlich, wenn die Anwendungen synchronisiert werden müssen, bevor sich Benutzer angemeldet haben.

Darüber hinaus wird der Systemidentitätsbenutzer häufig zum Ausführen einer Unteraufgabe verwendet, wenn die primäre Aufgabe bereits für den angemeldeten Benutzer autorisiert ist. Um ein Gerät in Cisco Security Manager zu bearbeiten, ist beispielsweise eine anwendungsübergreifende Kommunikation zwischen Cisco Security Manager und dem Common Services DCR erforderlich. Nachdem der Benutzer zum Ausführen der Bearbeitungsaufgabe autorisiert wurde, wird der System Identity-Benutzer zum Aufrufen des DCR verwendet.

Der hier konfigurierte Systemidentitätsbenutzer muss mit dem Benutzer identisch sein, der über (vollständige) Administratorberechtigungen verfügt, die Sie in ACS konfiguriert haben. Andernfalls können nicht alle Geräte und Richtlinien angezeigt werden, die in Cisco Security Manager konfiguriert wurden.

**Hinweis:** Erstellen Sie vor dem Fortfahren einen lokalen Benutzer mit demselben Namen und Kennwort wie dieser Administrator in CiscoWorks Common Services. Anweisungen finden Sie unter Lokalen Benutzer in CiscoWorks erstellen.

1. Wählen Sie **Server > Security aus**, und wählen Sie dann **Multi-Server Trust Management > System Identity Setup** aus.
2. Geben Sie den Namen des Administrators ein, den Sie für Cisco Secure ACS erstellt haben. Siehe Schritt 4 Definieren von Benutzern und Benutzergruppen in Cisco Secure ACS.
3. Geben Sie das Kennwort für diesen Benutzer ein, und überprüfen Sie es.
4. Klicken Sie auf **Übernehmen**.

## Konfigurieren des AAA-Setup-Modus in CiscoWorks

Auf der Seite für den AAA-Setup-Modus in CiscoWorks Common Services können Sie Ihren Cisco Secure ACS als AAA-Server definieren, der den erforderlichen Port und den gemeinsamen geheimen Schlüssel enthält. Darüber hinaus können Sie bis zu zwei Backup-Server definieren.

Bei diesen Schritten wird die eigentliche Registrierung von CiscoWorks, Cisco Security Manager, IPS Manager (und optional Auto Update Server) in Cisco Secure ACS durchgeführt.

1. Wählen Sie **Server > Security aus**, und wählen Sie dann **AAA Mode Setup** aus dem TOC aus.
2. Aktivieren Sie das Kontrollkästchen **TACACS+** unter Available Login Modules (Verfügbare Anmeldemodule).
3. Wählen Sie **ACS** als AAA-Typ aus.
4. Geben Sie die IP-Adressen von bis zu drei Cisco Secure ACS-Servern im Bereich Serverdetails ein. Der sekundäre und der tertiäre Server fungieren als Backups, falls der primäre Server ausfällt.**Hinweis:** Wenn alle konfigurierten TACACS+-Server nicht reagieren, müssen Sie sich mit dem lokalen Admin-Konto von CiscoWorks anmelden und den AAA-Modus wieder auf "Non-ACS/CiscoWorks Local" ändern. Nachdem die TACACS+-Server wieder in Betrieb genommen wurden, müssen Sie den AAA-Modus wieder in ACS ändern.

5. Geben Sie im Bereich Login (Anmeldung) den Namen des Administrators ein, den Sie auf der Seite Administration Control (Verwaltungskontrolle) von Cisco Secure ACS definiert haben. Weitere Informationen finden Sie unter Erstellen eines Administrationssteuerungsbenutzers in Cisco Secure ACS.
6. Geben Sie das Kennwort für diesen Administrator ein, und überprüfen Sie es.
7. Geben Sie den gemeinsamen geheimen Schlüssel ein, den Sie eingegeben haben, als Sie den Security Manager-Server als AAA-Client von Cisco Secure ACS hinzugefügt haben, und überprüfen Sie diesen. Siehe Schritt 5 unter Hinzufügen von Geräten als AAA-Clients ohne NDGs.
8. Aktivieren Sie das Kontrollkästchen **Alle installierten Anwendungen mit ACS registrieren**, um Cisco Security Manager und alle anderen installierten Anwendungen mit Cisco Secure ACS zu registrieren.
9. Klicken Sie auf **Übernehmen**, um Ihre Einstellungen zu speichern. Eine Statusanzeige zeigt den Fortschritt der Registrierung an. Nach Abschluss der Registrierung wird eine Meldung angezeigt.
10. Wenn Sie Cisco Security Manager in eine beliebige ACS-Version integrieren, starten Sie den Cisco Security Manager Daemon Manager-Dienst neu. Anweisungen hierzu finden Sie unter Starten Sie den Daemon Manager neu.**Hinweis:** Nach CSM 3.0.0 führt Cisco keine Tests mehr mit ACS 3.3(x) durch, da ein hohes Patch installiert wurde und das Ende der Lebensdauer (End-of-Life, EOL) angekündigt wurde. Daher müssen Sie die entsprechende ACS-Version für die CSM-Version 3.0.1 und höher verwenden. Weitere Informationen finden Sie in der Tabelle Kompatibilitätsmatrix.
11. Melden Sie sich wieder bei Cisco Secure ACS an, um den einzelnen Benutzergruppen Rollen zuzuweisen. Anweisungen finden Sie unter Zuweisen von Rollen zu Benutzergruppen in Cisco Secure ACS.**Hinweis:** Die hier konfigurierte AAA-Konfiguration wird bei der Deinstallation von CiscoWorks Common Services oder Cisco Security Manager nicht beibehalten. Darüber hinaus kann diese Konfiguration nach der Neuinstallation nicht gesichert und wiederhergestellt werden. Daher müssen Sie beim Upgrade auf eine neue Version einer der Anwendungen den AAA-Setup-Modus neu konfigurieren und Cisco Security Manager mit ACS erneut registrieren. Dieser Prozess ist für inkrementelle Updates nicht erforderlich. Wenn Sie zusätzliche Anwendungen wie AUS auf CiscoWorks installieren, müssen Sie die neuen Anwendungen und Cisco Security Manager erneut registrieren.

## Starten Sie den Daemon Manager neu

Dieses Verfahren beschreibt, wie der Daemon Manager des Cisco Security Manager-Servers neu gestartet wird. Sie müssen dies tun, damit die von Ihnen konfigurierten AAA-Einstellungen wirksam werden. Anschließend können Sie sich mit den in Cisco Secure ACS definierten Anmeldeinformationen wieder bei CiscoWorks anmelden.

1. Melden Sie sich bei dem Computer an, auf dem der Cisco Security Manager-Server installiert ist.
2. Wählen Sie **Start > Programme > Verwaltung > Dienste**, um das Fenster Dienste zu öffnen.
3. Wählen Sie aus der Liste der im rechten Teilfenster angezeigten Dienste den **Cisco Security Manager Daemon Manager aus**.
4. Klicken Sie in der Symbolleiste auf **Service neu starten**.
5. Fahren Sie mit Zuweisen von Rollen zu Benutzergruppen in Cisco Secure ACS fort.

# Zuweisen von Rollen zu Benutzergruppen in Cisco Secure ACS

Nachdem Sie CiscoWorks, Cisco Security Manager und andere installierte Anwendungen für Cisco Secure ACS registriert haben, können Sie den zuvor in Cisco Secure ACS konfigurierten Benutzergruppen Rollen zuweisen. Diese Rollen bestimmen, welche Aktionen die Benutzer in den einzelnen Gruppen in Cisco Security Manager ausführen dürfen.

Das Verfahren, mit dem Sie Benutzergruppen Rollen zuweisen, hängt davon ab, ob NDGs verwendet werden:

- Zuweisen von Rollen zu Benutzergruppen ohne NDGs
- Zuordnen von NDGs und Rollen zu Benutzergruppen

## Zuweisen von Rollen zu Benutzergruppen ohne NDGs

Dieses Verfahren beschreibt, wie die Standardrollen Benutzergruppen zugewiesen werden, wenn keine NDGs definiert sind. Weitere Informationen finden Sie unter Cisco Secure ACS Default Roles (Standardrollen für Cisco Secure ACS).

**Hinweis:** Bevor Sie fortfahren:

- Erstellen Sie für jede Standardrolle eine Benutzergruppe. Anweisungen finden Sie unter Definieren von Benutzern und Benutzergruppen in Cisco Secure ACS.
- Führen Sie die in den in Cisco Secure ACS und in CiscoWorks durchgeführten Integrationsverfahren beschriebenen Verfahren durch.

Gehen Sie wie folgt vor:

1. Melden Sie sich bei Cisco Secure ACS an.
2. Klicken Sie in der Navigationsleiste auf **Group Setup** (Gruppeneinrichtung).
3. Wählen Sie die Benutzergruppe für Systemadministratoren aus der Liste aus. Siehe Schritt 2 von Definieren von Benutzern und Benutzergruppen in Cisco Secure ACS, und klicken Sie dann auf **Einstellungen bearbeiten**.

## Zuordnen von NDGs und Rollen zu Benutzergruppen

Wenn Sie NDGs Rollen zuordnen, die in Cisco Security Manager verwendet werden, müssen Sie Definitionen an zwei Stellen auf der Seite für die Gruppeneinrichtung erstellen:

- Bereich CiscoWorks
- Cisco Security Manager-Bereich

Die Definitionen in den einzelnen Bereichen müssen so genau wie möglich übereinstimmen. Wenn Sie benutzerdefinierte Rollen oder ACS-Rollen zuordnen, die in CiscoWorks Common Services nicht vorhanden sind, versuchen Sie, anhand der Berechtigungen, die dieser Rolle zugewiesen wurden, eine möglichst nahe liegende Entsprechung zu definieren.

Sie müssen Zuordnungen für jede Benutzergruppe erstellen, die mit Cisco Security Manager verwendet werden soll. Wenn Sie beispielsweise eine Benutzergruppe haben, die Support-Mitarbeiter für die westliche Region enthält, können Sie diese Benutzergruppe auswählen und dann das NDG, das die Geräte in dieser Region enthält, der Helpdesk-Rolle zuordnen.

**Hinweis:** Aktivieren Sie vor dem Fortfahren die NDG-Funktion, und erstellen Sie NDGs. Weitere Informationen finden Sie unter Netzwerkgerätegruppen für die Verwendung im Sicherheitsmanager konfigurieren.

1. Klicken Sie in der Navigationsleiste auf **Group Setup** (Gruppeneinrichtung).
2. Wählen Sie eine Benutzergruppe aus der Liste Gruppe aus, und klicken Sie dann auf **Einstellungen bearbeiten**.
3. Zuordnen von NDGs und Rollen zur Verwendung in CiscoWorks:Scrollen Sie auf der Seite "Group Setup" (Gruppeneinrichtung) unter "TACACS+ Settings" nach unten zum Bereich CiscoWorks.Wählen Sie **CiscoWorks pro Netzwerkgerätegruppe zuweisen aus**.Wählen Sie aus der Liste Gerätegruppen ein NDG aus.Wählen Sie aus der zweiten Liste die Rolle aus, der dieses NDG zugeordnet werden soll.Klicken Sie auf **Zuordnung hinzufügen**. Die Zuordnung wird im Feld Gerätegruppe angezeigt.Wiederholen Sie die Schritte c bis e, um weitere Zuordnungen zu erstellen.**Hinweis:** Um eine Zuordnung zu entfernen, wählen Sie sie aus der Gerätegruppe aus, und klicken Sie dann auf Zuordnung entfernen.
4. Blättern Sie nach unten zum Bereich Cisco Security Manager, und erstellen Sie Zuordnungen, die den in Schritt 3 definierten Zuordnungen möglichst genau entsprechen.**Hinweis:** Wenn Sie in Cisco Secure ACS die Rollen "Sicherheitsbeauftragter" oder "Sicherheitsadministrator" auswählen, wird empfohlen, "Netzwerkadministrator" als gleichwertige CiscoWorks-Rolle auszuwählen.
5. Klicken Sie auf **Senden**, um Ihre Einstellungen zu speichern.
6. Wiederholen Sie die Schritte 2 bis 5, um die NDGs für die restlichen Benutzergruppen zu definieren.
7. Wenn Sie den einzelnen Benutzergruppen NDGs und Rollen zugeordnet haben, klicken Sie auf **Senden + Neu starten**.

# Fehlerbehebung

1. Bevor Sie Geräte in Cisco Security Manager importieren können, müssen Sie jedes Gerät zuerst als AAA-Client in Ihrem Cisco Secure ACS konfigurieren. Darüber hinaus müssen Sie den CiscoWorks/Security Manager-Server als AAA-Client konfigurieren.
2. Wenn Sie ein Protokoll mit fehlgeschlagenen Versuchen erhalten, ist der Autor in Cisco Secure ACS fehlerhaft.
   ```
   "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"
   ```
   Um dieses Problem zu beheben, stellen Sie sicher, dass der Name des Geräts im ACS ein vollqualifizierter Domänenname sein muss.

# Zugehörige Informationen

- Cisco Security Access Control Server für Windows Support-Seite
- Support-Seite für Cisco Security Manager
- Cisco Secure Access Control Server für Windows
- Konfigurationsleitfaden für Cisco Secure ACS 4.1
- Cisco Secure ACS Online Troubleshooting Guide 4.1
- Problemhinweise zu Sicherheitsprodukten (einschließlich CiscoSecure ACS für Windows)
- Technischer Support und Dokumentation - Cisco Systems