Cisco DNA Center Remote Support Authorization-Funktion konfigurieren

Inhalt

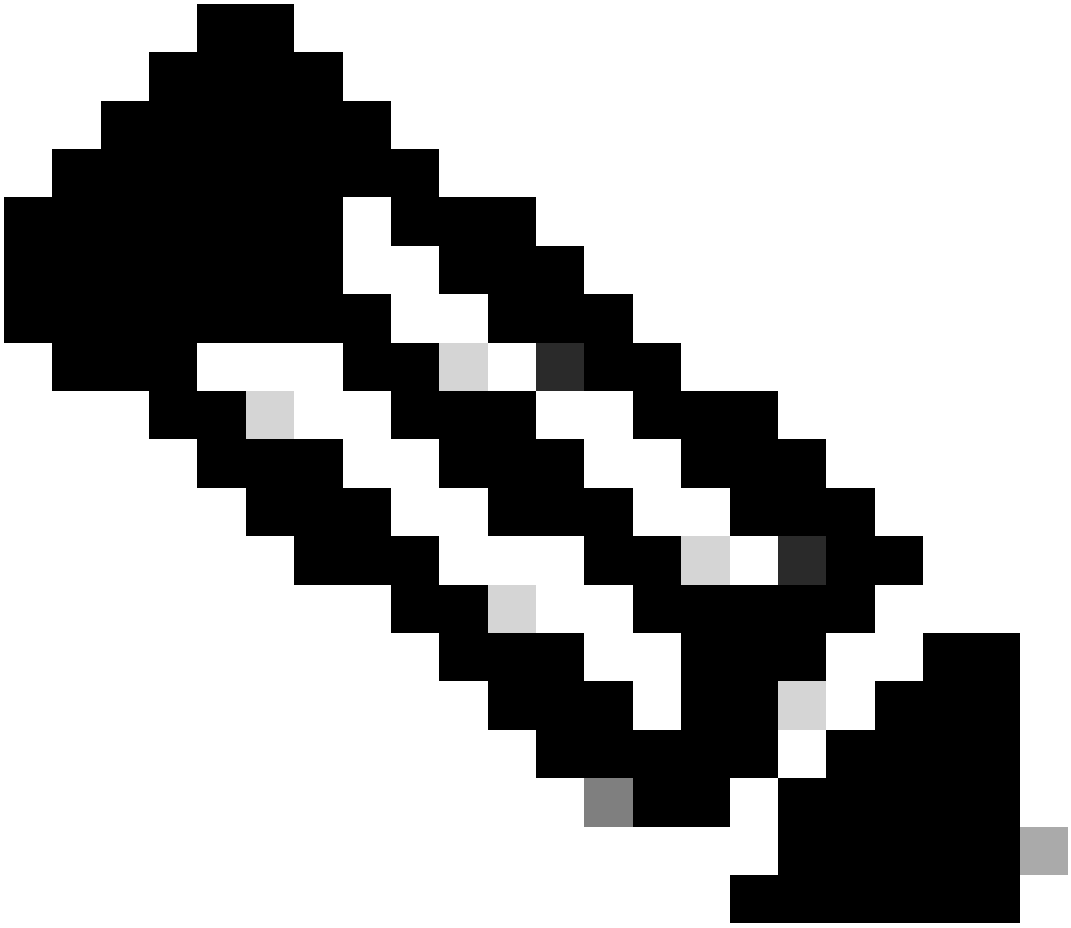
Einleitung

In diesem Dokument wird die Einrichtung der Remote Support-Autorisierungsfunktion in Cisco DNA Center beschrieben.

Voraussetzungen

Um die neue Remote Support Authorization-Funktion in Cisco DNA Center vollständig nutzen zu können, müssen bestimmte Kriterien erfüllt sein:

- Cisco DNA Center muss Version 2.3.5.x oder höher sein.
- Das Support Services-Paket muss im Cisco DNA Center installiert werden.
- Remote-Autorisierungsunterstützung durch die Firewall oder den Proxy zulassen: wss://prod.radkit-cloud.cisco.com:443 .



Hinweis: Die Remote Support-Autorisierung wurde in Cisco DNA Center 2.3.3.x eingeführt, bietet aber nur einen eingeschränkten Funktionsumfang. Nur der Zugriff auf Netzwerkgeräte ist zulässig, der Zugriff über die Cisco DNA Center CLI ist in dieser früheren Version nicht möglich.

Beschreibung

Cisco RADKit (radkit.cisco.com) bietet sichere interaktive Verbindungen zu entfernten Terminals und Web-Benutzeroberflächen. Die Cisco RADKit-Funktionen sind in Cisco DNA Center integriert und werden als Remote Support Authorization bezeichnet. Wenn Benutzer die Remote Support Authorization-Funktion nutzen, können Benutzer das Cisco TAC remote in ihre Cisco DNA Center-Umgebung integrieren, um Informationen zu erfassen oder Probleme zu beheben. Dadurch wird die Zeit reduziert, die Benutzer für Videoanrufe benötigen, wenn das TAC eingetretene Probleme untersucht.

Einschränkungen

Die aktuelle Version der Remote Support-Autorisierung weist im Vergleich zur RADKit-Standalone-Version folgende Einschränkungen auf:

- Wenn der Support-Techniker die Befehle "maglev", "sudo" oder "rca" in Ihrem Cisco DNA Center ausführt, werden Sie aufgefordert, Ihre Anmeldeinformationen anzugeben. Die Remote Support-Autorisierung automatisiert die Verarbeitung dieser Anmeldeinformationen nicht. Daher müssen Sie diese Anmeldeinformationen möglicherweise an den Support-Techniker weitergeben.

- Über den Remore Support Authorization Service ist es nicht möglich, eine Verbindung zur grafischen Benutzeroberfläche (GUI) des Cisco DNA Centers oder zu einer beliebigen GUI der Netzwerkgeräte herzustellen.

- Es ist nicht möglich, einen Remote-Zugriff auf Geräte bereitzustellen, die nicht im Cisco DNA Center-Inventar enthalten sind, aber möglicherweise für die Fehlerbehebung erforderlich sind (z. B. die ISE).

- Es ist nicht möglich, einen Remote-Zugriff auf Wireless Access Points bereitzustellen, selbst wenn diese im Inventar des Cisco DNA Center enthalten sind.

- Der Remote-Zugriff ist auf jeweils 24 Stunden beschränkt. Um einen längeren Zugriff zu ermöglichen, muss alle 24 Stunden eine neue Autorisierung erstellt werden.

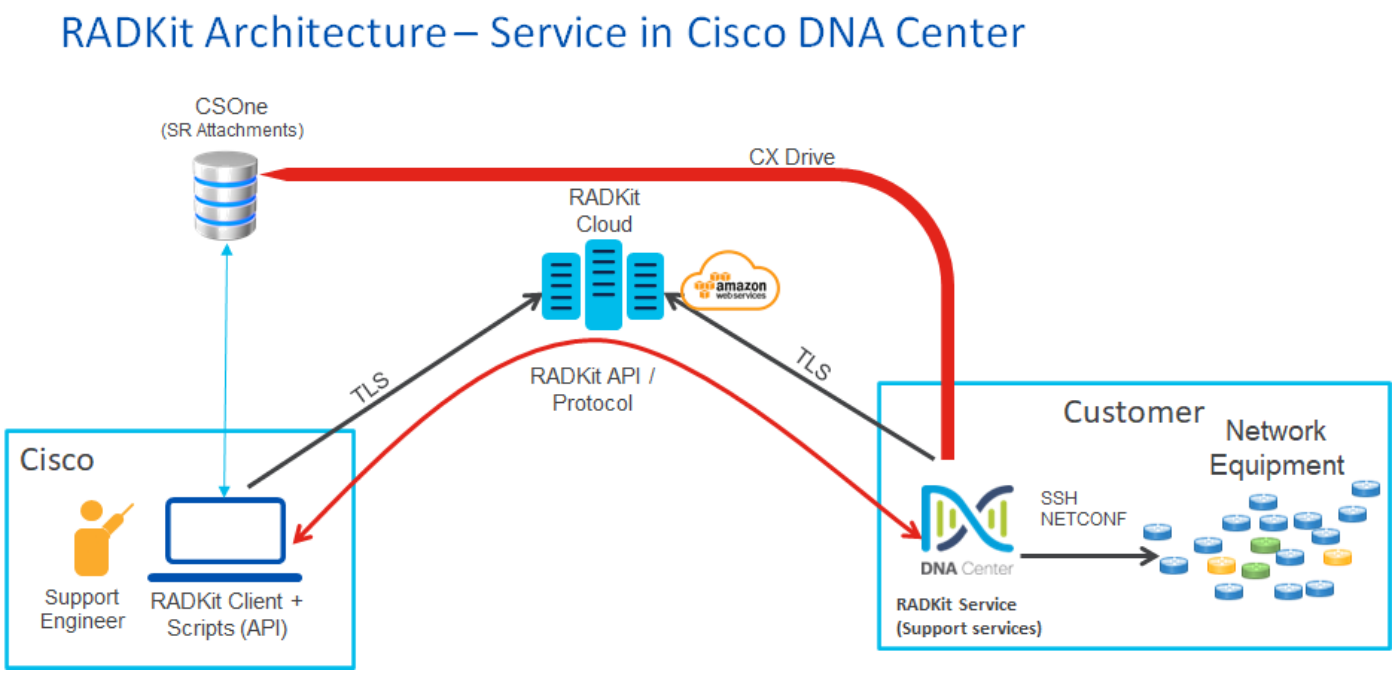
- Durch die Erstellung einer Autorisierung ermöglichen Sie den Zugriff auf alle Geräte im Bestand des Cisco DNA Center. Es ist nicht möglich, den Zugriff auf bestimmte Netzwerkgeräte einzuschränken.

Um diese Einschränkungen zu überwinden, können Sie stattdessen die Installation des eigenständigen RADKit-Service in Betracht ziehen. Installationsprogramme sind für Windows, Mac und Linux verfügbar. Weitere Informationen finden Sie unter https://radkit.cisco.com

-

Netzwerkkonnektivität

Cisco DNA Center wird über AWS mit dem Cisco RADKit-Connector verbunden. Der Cisco RADKit-Connector ist in die Remote Support Authorization-Funktion integriert. TAC stellt über AWS eine Verbindung zum Cisco RADKit-Connector her und verwendet einen Cisco RADKit-Client. Nachdem eine Support-ID von der Cisco DNA Center-Umgebung generiert wurde, stellt der Cisco RADKit-Client mithilfe der Support-ID eine Verbindung mit dem Cisco DNA Center her.

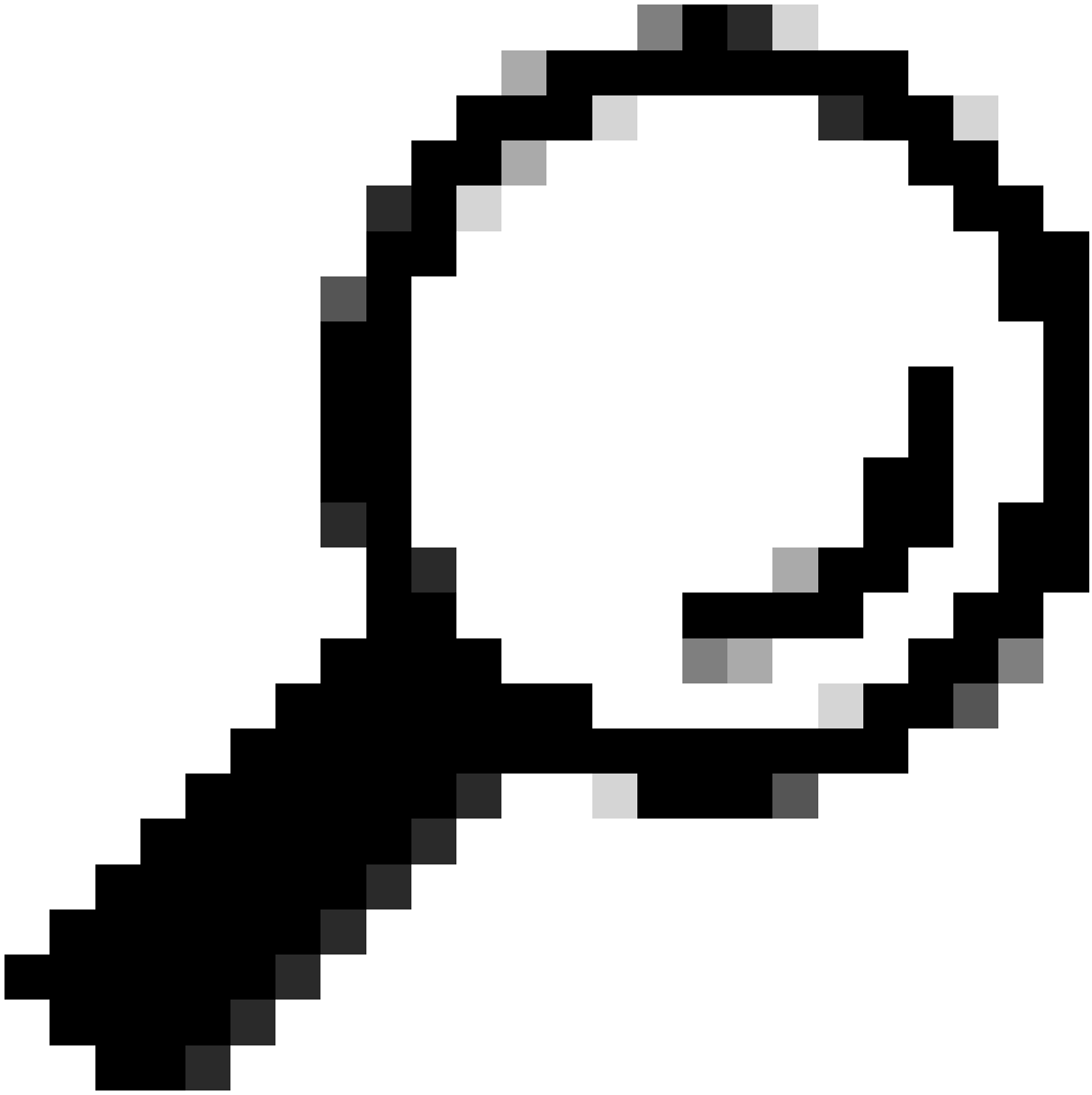


Remote Support-Autorisierung einrichten

Damit die Remote Support-Autorisierung aktiviert wird, damit das TAC eine Remote-Teilnahme ermöglicht, müssen folgende Schritte durchgeführt werden:
1. Stellen Sie sicher, dass die Firewall die erforderliche URL durchlässt.
2. Installieren Sie das Support Services-Paket.
3. Konfigurieren Sie die SSH-Anmeldeinformationen für den Remote Support Authorization-Workflow.
4. Neue Autorisierung erstellen.

Schritt 1

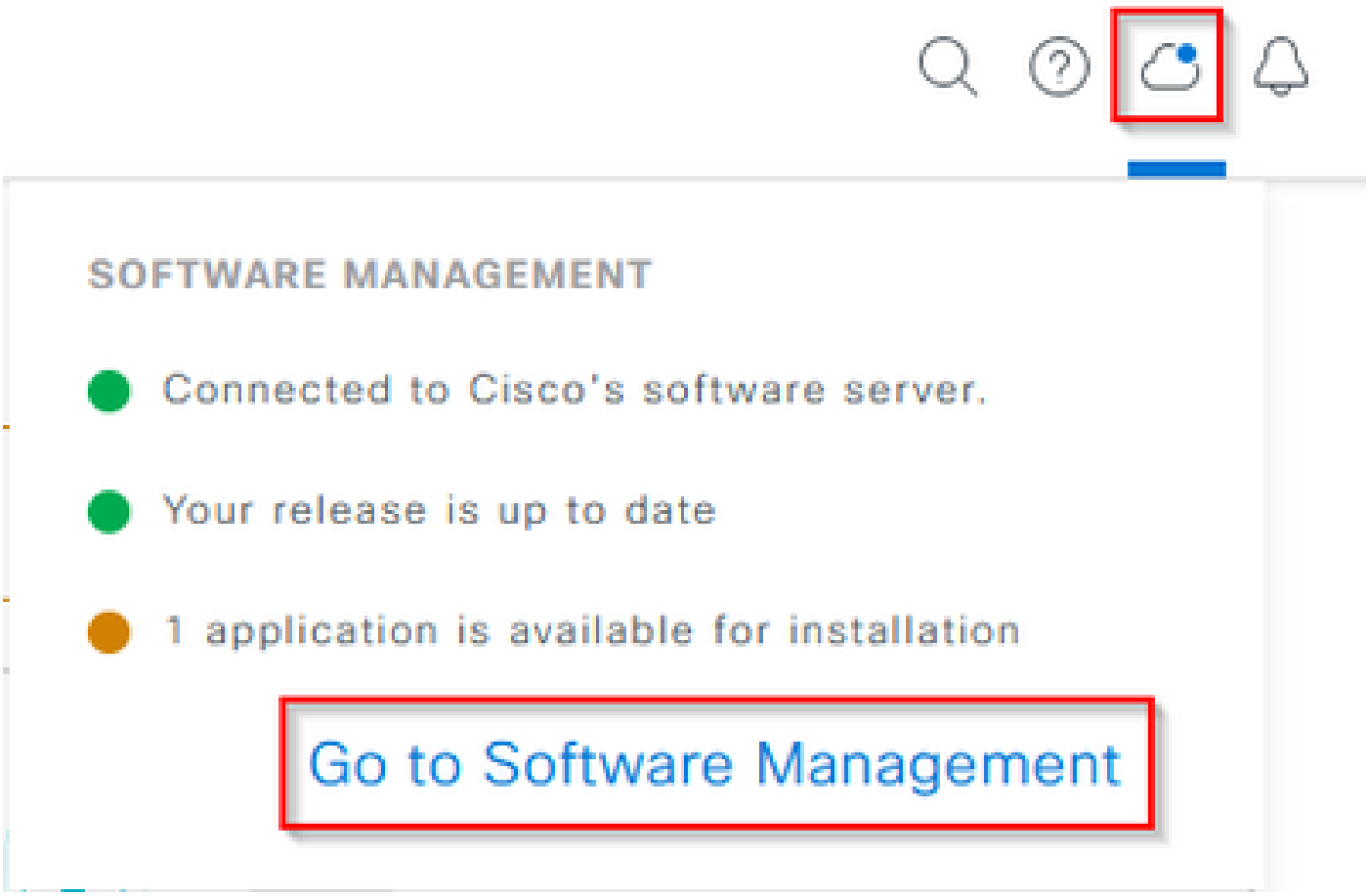
Damit die Remote Support-Autorisierung funktioniert, muss der Cisco DNA Center-Connector mit dem AWS-Connector kommunizieren können. Um diese Kommunikation sicherzustellen, muss diese URL über die Firewall zugelassen werden, sofern eine konfiguriert ist:
wss://prod.radkit-cloud.cisco.com:443



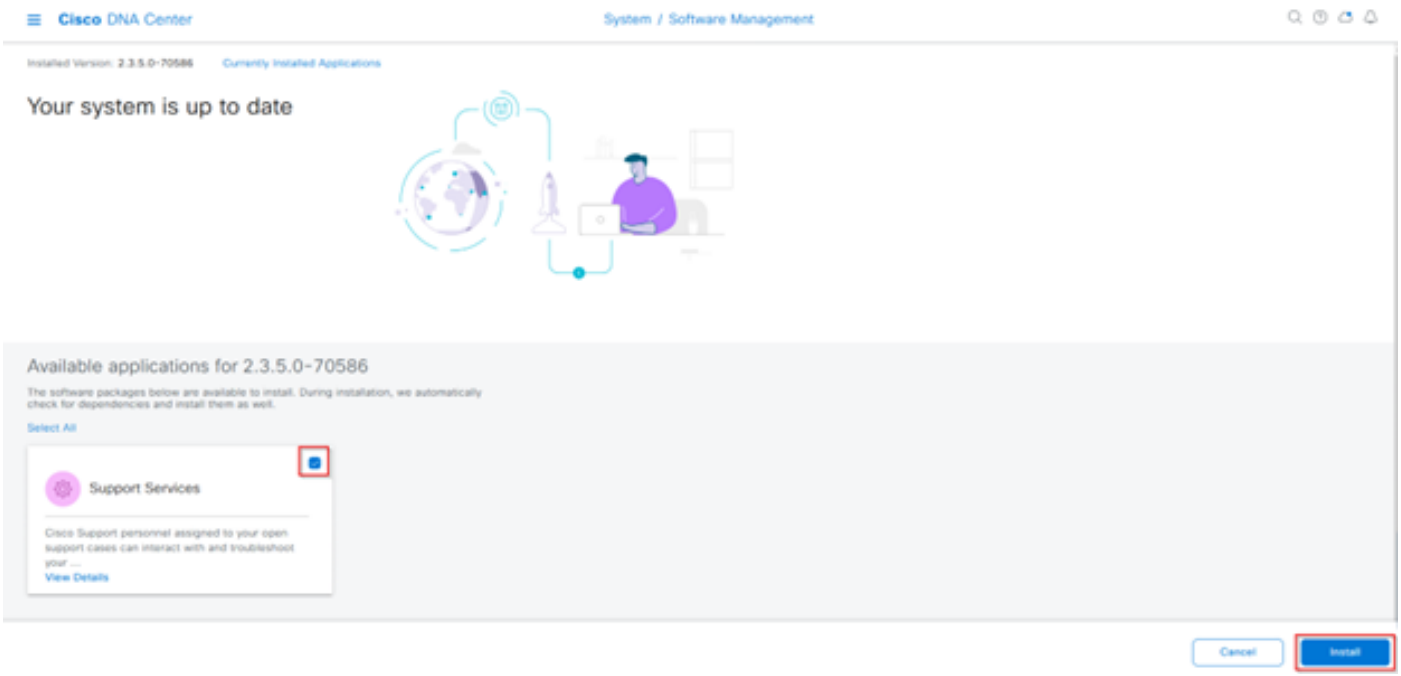
Tipp: Weitere Informationen zu spezifischen Ports und URLs, die zugelassen/geöffnet werden müssen, damit die Funktionen von Cisco DNA Center funktionieren, finden Sie im Abschnitt Planung der Bereitstellung des Installationshandbuchs.

Schritt 2

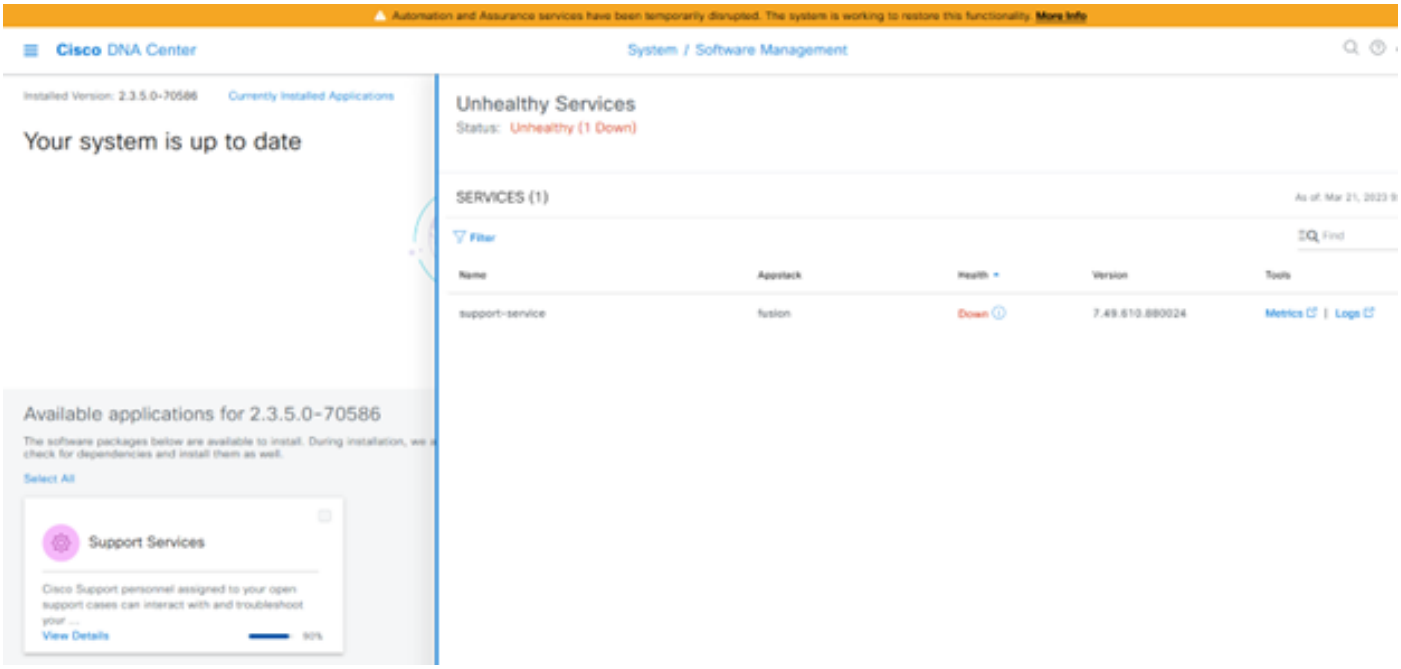
Nach Abschluss einer Neuinstallation oder eines Upgrades von Cisco DNA Center auf Version 2.3.5.x oder höher muss das Support Services-Paket manuell installiert werden. Dies ist ein optionales Paket und wird nicht standardmäßig installiert. Navigieren Sie zur Benutzeroberfläche von Cisco DNA Center. Wählen Sie auf der Startseite der Benutzeroberfläche von Cisco DNA Center das Cloud-Symbol oben rechts im Bildschirm aus, und wählen Sie Gehe zu Softwareverwaltung.



Auf der Seite für die Softwareverwaltung werden die aktuell installierte Version, alle verfügbaren Versionen für das Upgrade und alle verfügbaren optionalen Pakete angezeigt. Das Support Services-Paket ist ein optionales Paket und wird nach einer abgeschlossenen Neuinstallation oder einem Upgrade, bei dem das Paket zuvor nicht bereitgestellt wurde, nicht automatisch installiert. Klicken Sie in der Liste der verfügbaren Pakete auf das Feld für das Support Services-Paket, und klicken Sie dann unten rechts auf dem Bildschirm auf die Schaltfläche Installieren.



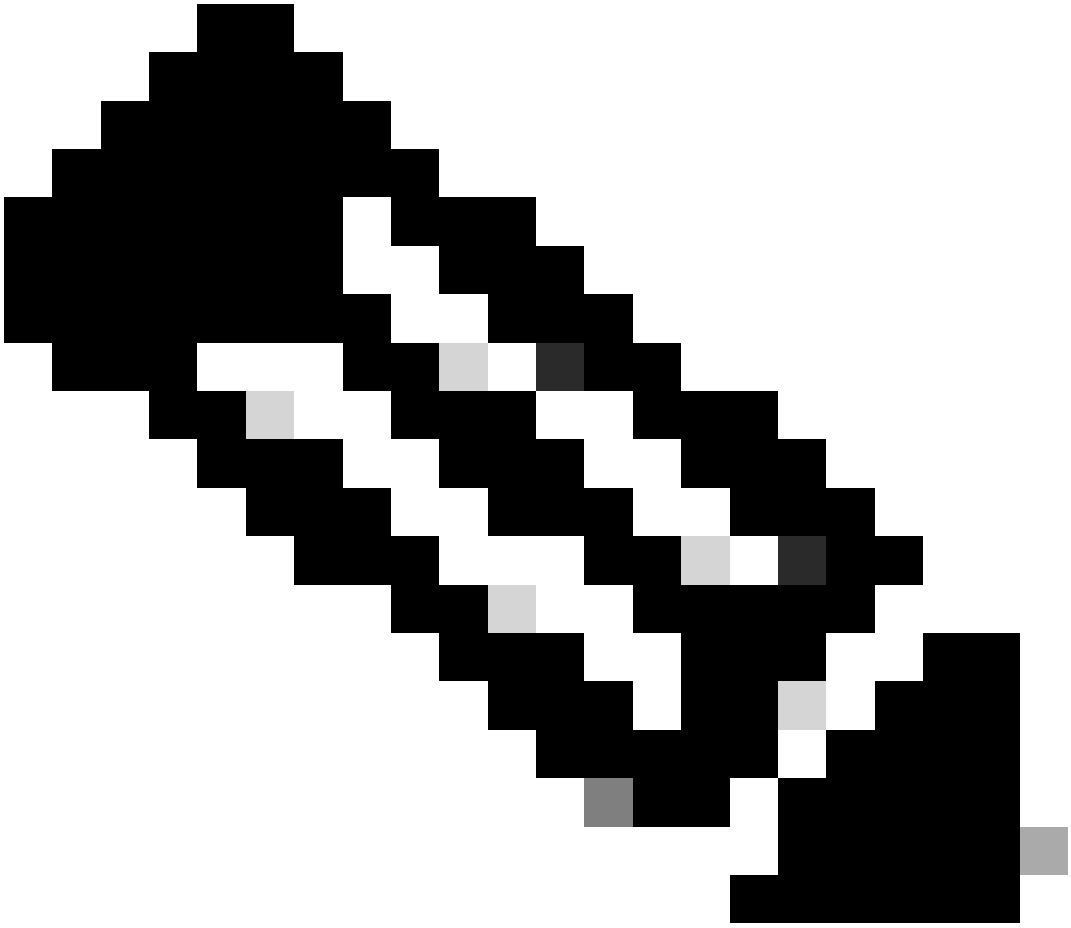
Es wird ein Popup-Fenster für eine Abhängigkeitsprüfung der ausgewählten Pakete angezeigt. Wenn die Überprüfung abgeschlossen ist, wählen Sie Weiter.
Das/die ausgewählte(n) Paket(e) beginnt dann mit der Installation. Die Dauer dieses Prozesses hängt von der Anzahl der Pakete ab, die sich derzeit im Bereitstellungsprozess befinden. Während der Bereitstellung des Pakets wird oben im Bildschirm ein orangefarbenes Banner mit der Meldung angezeigt, dass die Automatisierungs- und Versicherungsservices vorübergehend unterbrochen wurden. Dies geschieht aufgrund des neuen Support-Service-POD, der erstellt wird und gerade gestartet wird.



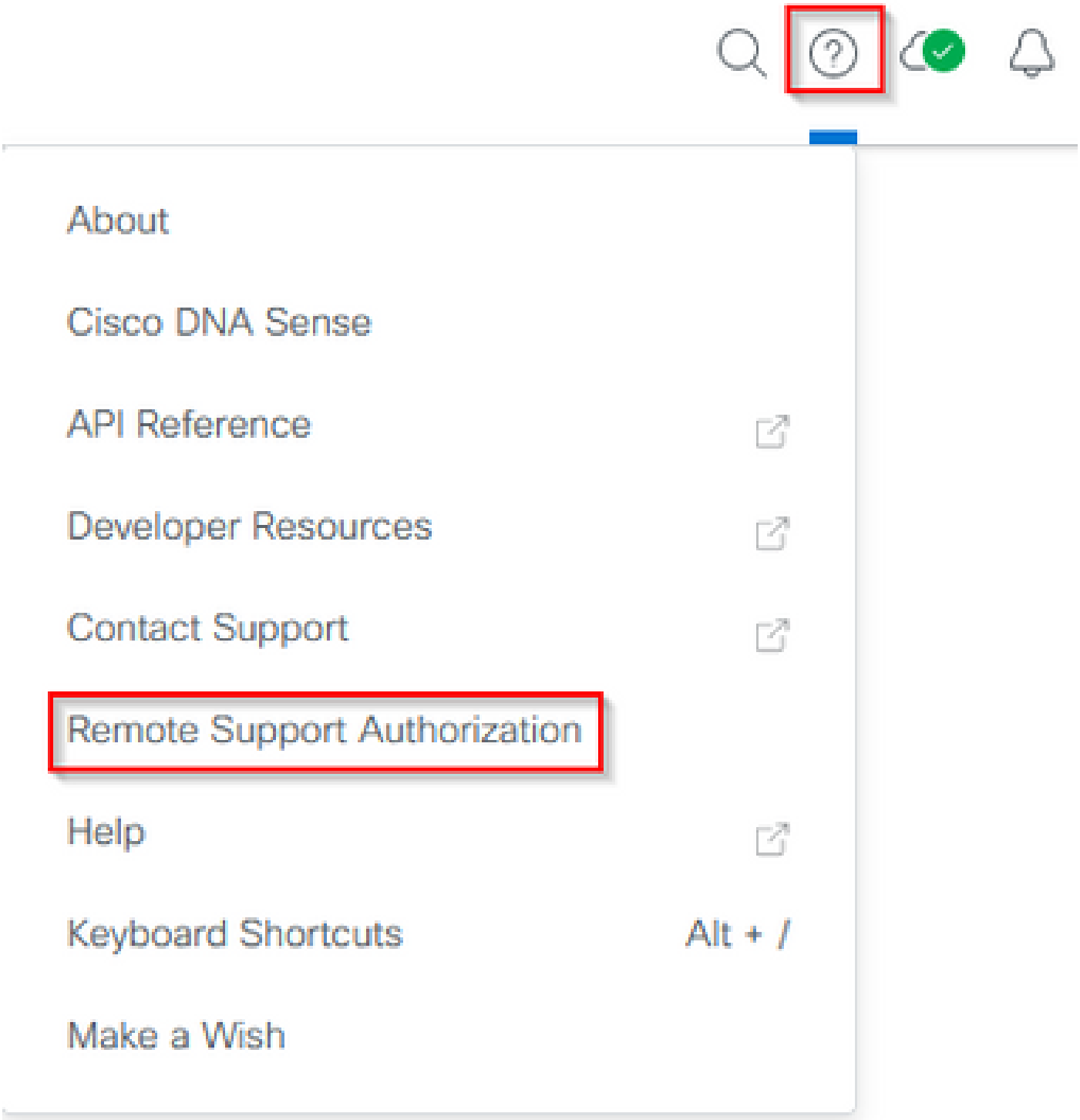
Nach etwa 10 bis 20 Minuten ist der neue POD vollständig betriebsbereit, und die Installation des Support Services-Pakets ist abgeschlossen. Aktualisieren Sie nach der Installation des Pakets den Browser, und fahren Sie mit Schritt 3 fort.

Schritt 3

Für den vollständigen Zugriff auf die Remote Support-Autorisierungsfunktion müssen die SSH-Anmeldeinformationen in den Einstellungen für die Remote Support-Autorisierung konfiguriert werden. Ohne diese Anmeldeinformationen kann das TAC die Cisco RADKit-Lösung nicht für die Remote-Fehlerbehebung verwenden. Um die SSH-Anmeldeinformationen zu konfigurieren, navigieren Sie zum Fragezeichen oben rechts in der Benutzeroberfläche von Cisco DNA Center. Wählen Sie in der Liste Remote Support Authorization (Remote-Support-Autorisierung) aus.



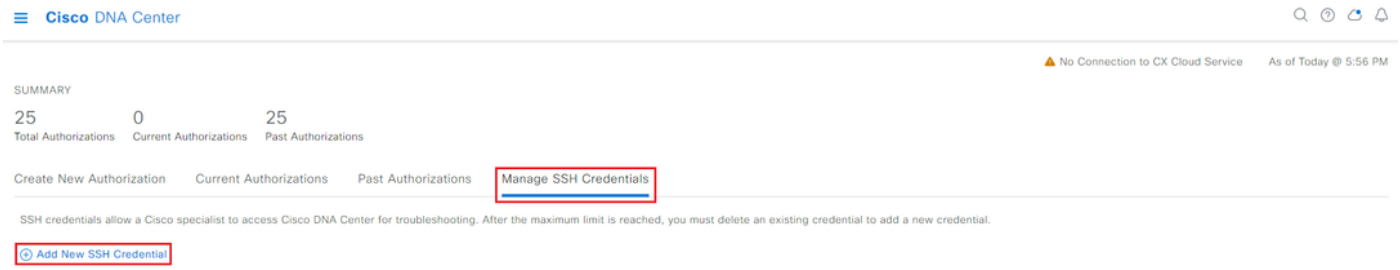
Hinweis: Bitte beachten Sie, dass die Remote Support-Autorisierung nur angezeigt wird, nachdem das Support Services-Paket installiert und der Browser aktualisiert wurde. Weitere Informationen hierzu finden Sie in Schritt 2.



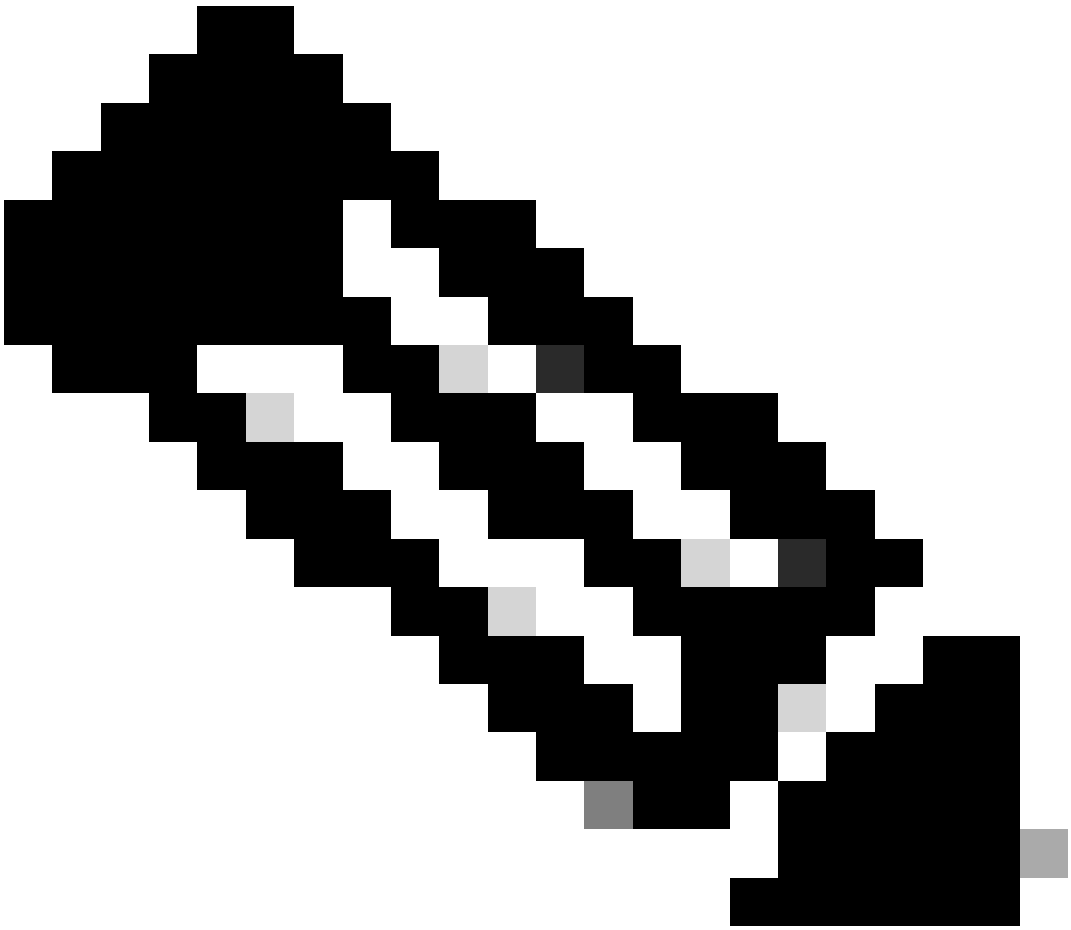
Sie werden zur Seite Remote Support Authorization (Remote-Support-Autorisierung) weitergeleitet. Es werden vier Registerkarten aufgelistet:

- Neue Autorisierung erstellen
- Derzeitige Genehmigungen
- Frühere Genehmigungen
- SSH-Anmeldeinformationen verwalten

Navigieren Sie zur Registerkarte SSH-Anmeldeinformationen verwalten. Wählen Sie Neue SSH-Anmeldeinformationen hinzufügen aus.



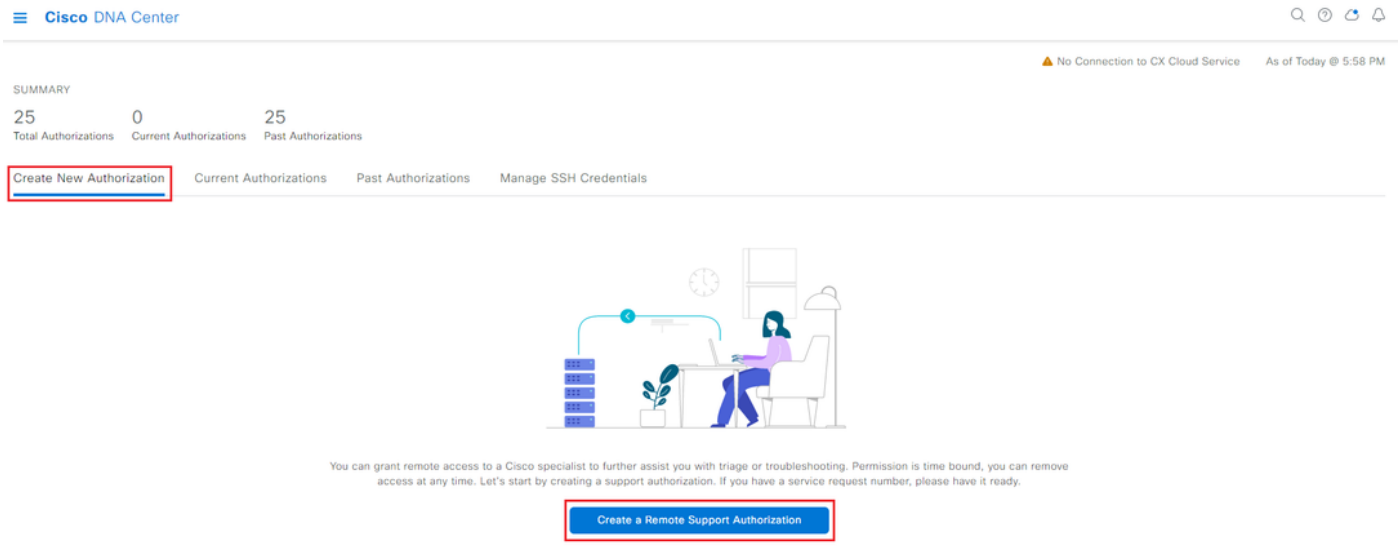
Es wird ein neues Fenster geöffnet. Geben Sie das aktuelle SSH-Kennwort für die Cisco DNA Center-Appliance und eine Beschreibung ein. Das Passwort muss mit dem übereinstimmen, was derzeit für SSH in der Cisco DNA Center-Appliance verwendet wird. Wählen Sie Hinzufügen aus. Ein Eintrag wird nun unter VORHANDENEN SSH-ANMELDEINFORMATIONEN angezeigt.



Hinweis: Beachten Sie, dass bei Bereitstellungen mit einem Knoten nur eine Anmeldeinformation erstellt werden kann. Für Bereitstellungen mit drei Knoten können bis zu drei Anmeldedaten erstellt werden. Wenn das SSH-Kennwort jedoch für alle drei Knoten identisch ist, muss nur eine Anmeldeinformation erstellt werden.

Schritt 4

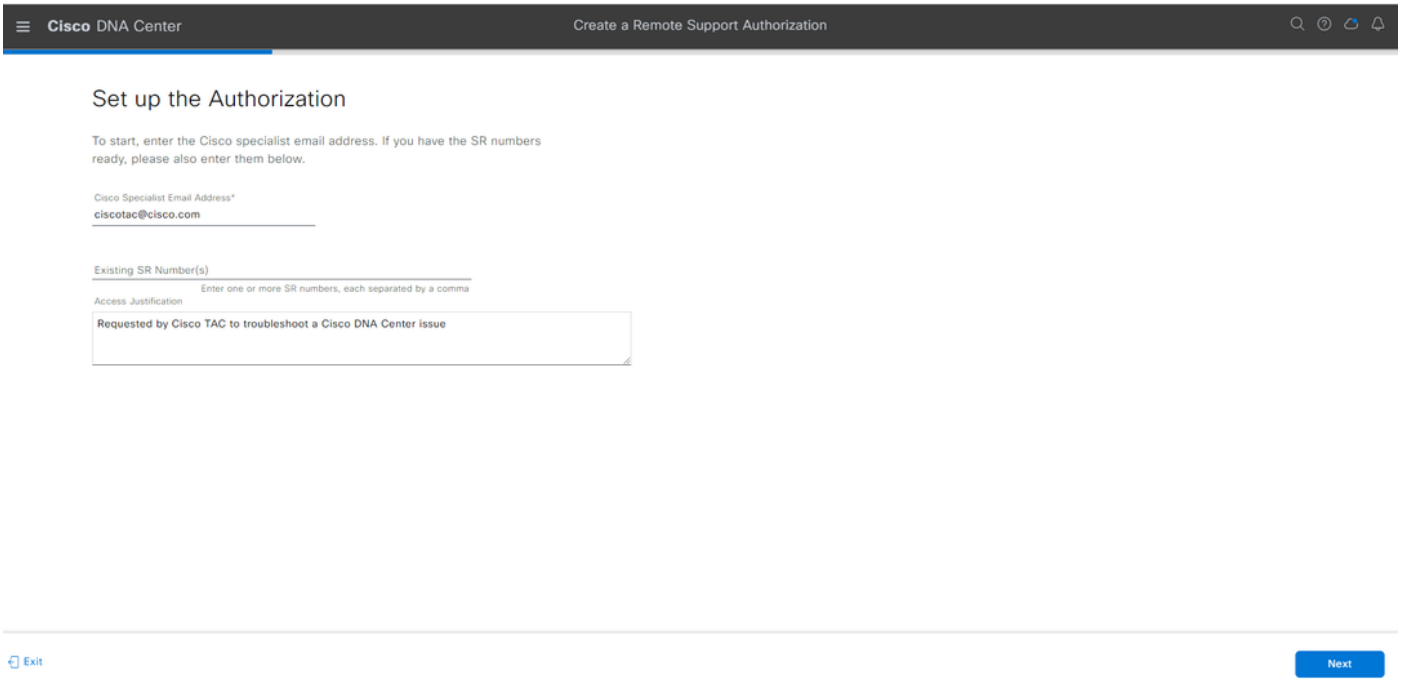
Navigieren Sie auf der Seite "Remote Support Authorization" (Remote-Support-Autorisierung) zur Registerkarte "Create New Authorization" (Neue Autorisierung erstellen). Wählen Sie Create a Remote Support Authorization (Remote-Support-Autorisierung erstellen).



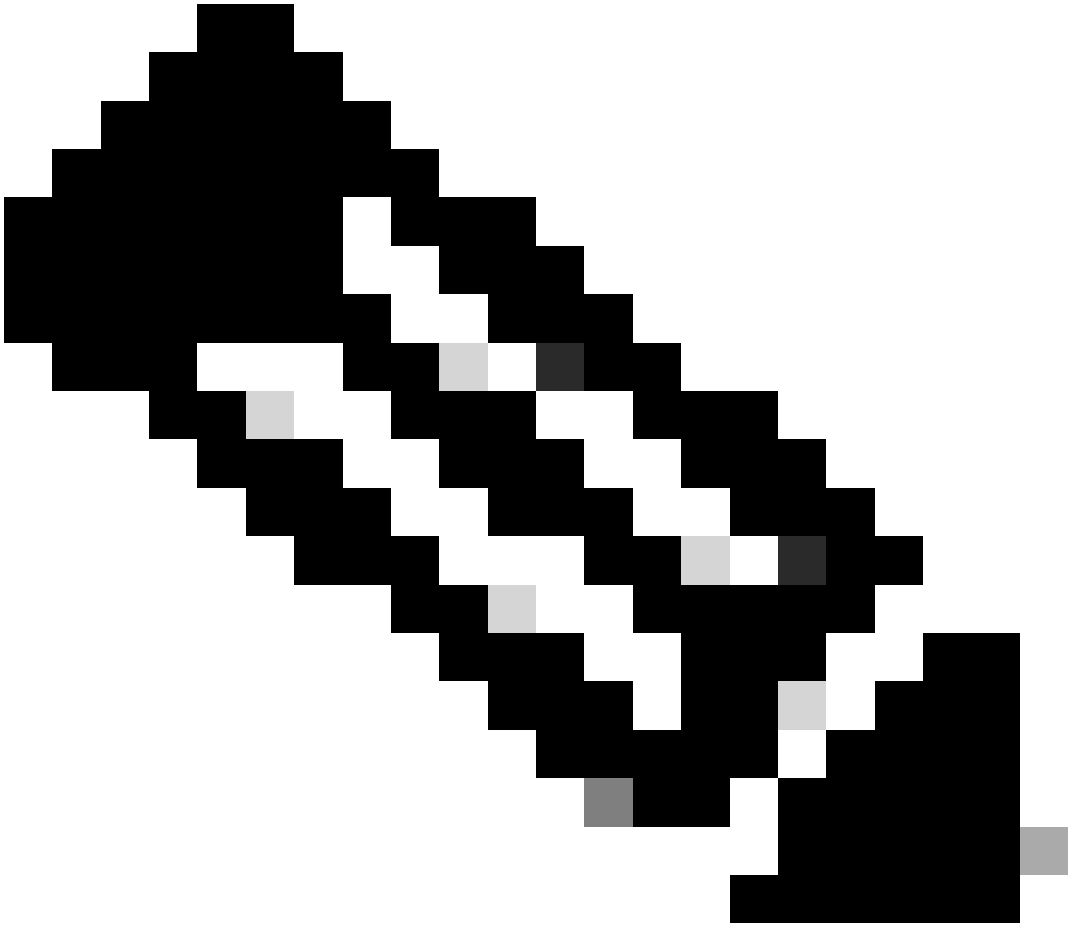
Sie werden zu einer Workflowseite weitergeleitet, um mit der Einrichtung der Autorisierung zu beginnen. Sie müssen die E-Mail-Adresse des TAC-Technikers eingeben. Beispiel: "ciscotac@cisco.com".
Diese beiden Felder sind optional:

- Bestehende(r) Serviceticket(s)
- Begründung des Zugangs

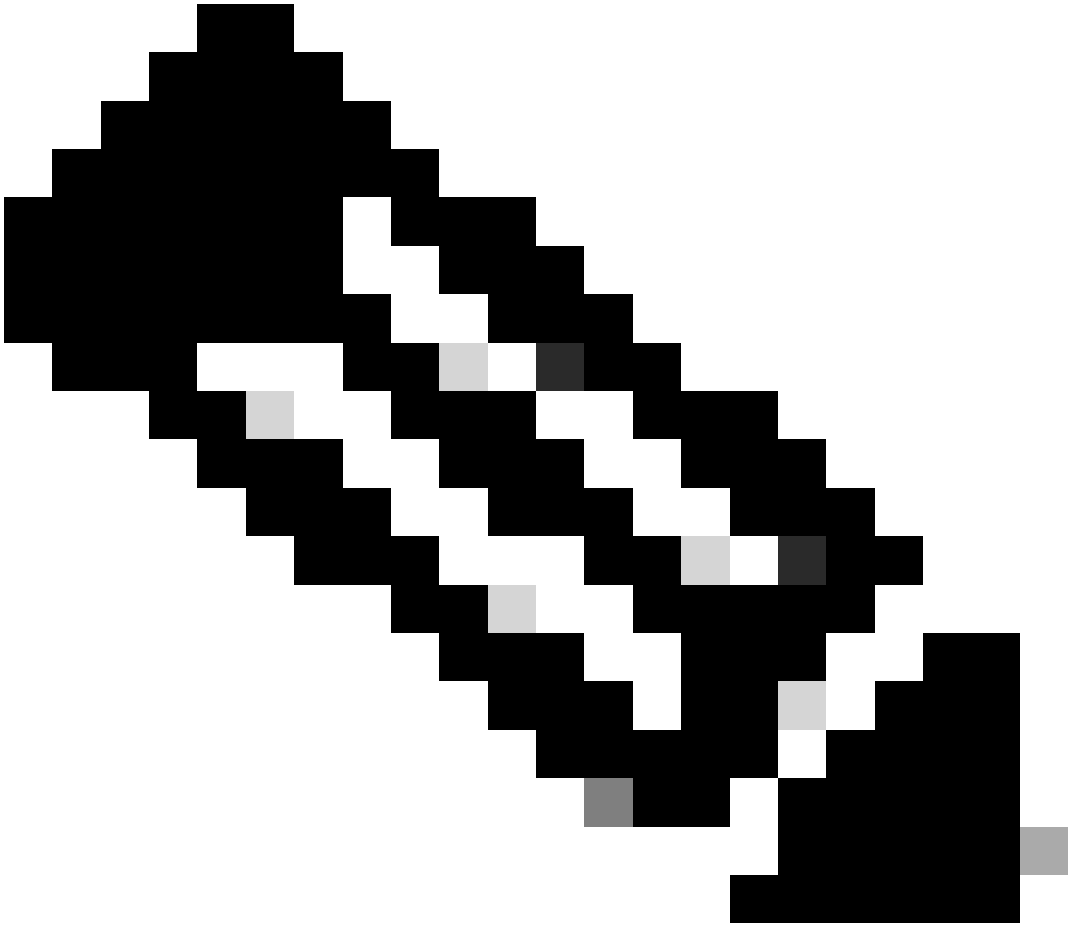
Wenn Sie ein offenes TAC-Serviceticket haben, geben Sie diese Serviceticket-Nummer in das Feld Bestehende(r) Serviceticket-Nummer(n) ein.
Wenn Sie Dokumentation für die Remote Support-Autorisierung hinzufügen möchten, geben Sie dies in das Feld "Access Justification" (Begründung für den Zugriff) ein, z. B. "Required by the TAC to help ubleshoot an issue problem seen" (Vom TAC erforderlich, um bei der Behebung eines festgestellten Problems zu helfen). Klicken Sie auf Next (Weiter).



Sie werden zum Schritt Schedule the Access (Zugriff planen) weitergeleitet. Wählen Sie hier entweder Jetzt oder Später aus. Sie können sofort mit der Autorisierung beginnen oder die Autorisierung im Voraus planen.

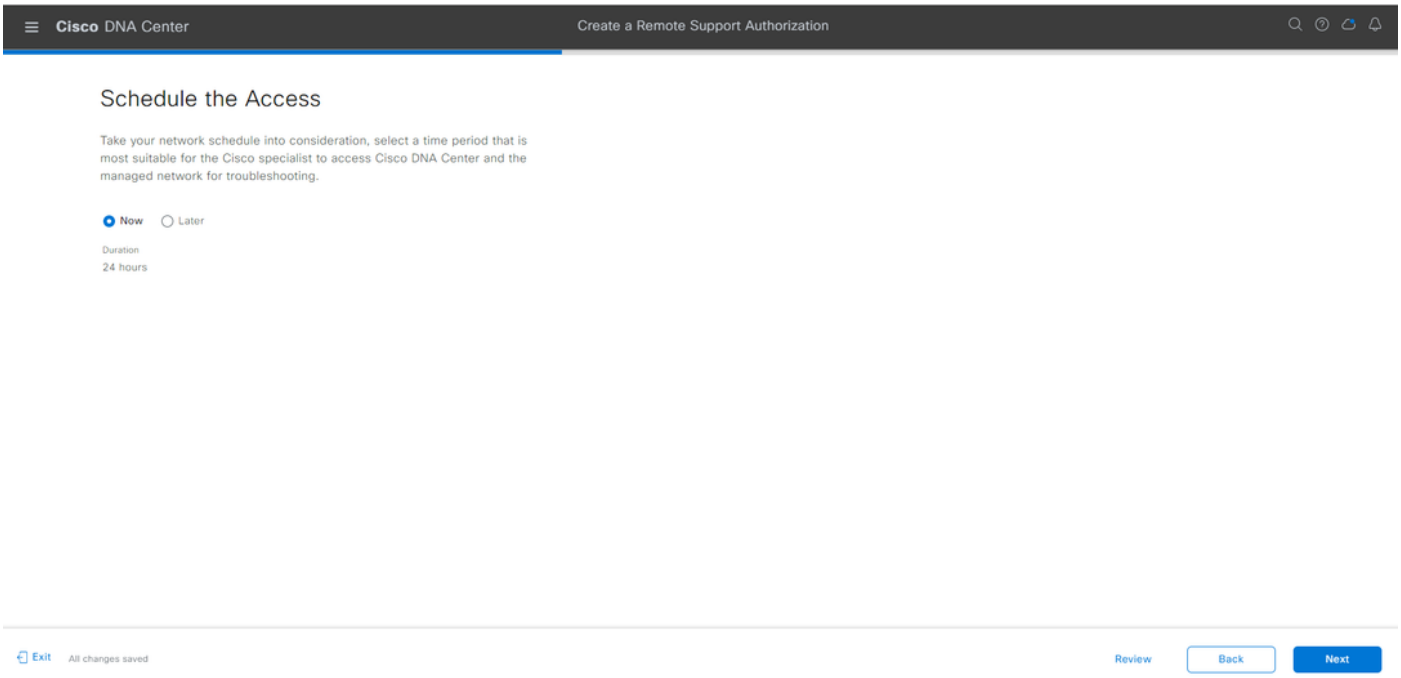


Hinweis: Beachten Sie, dass die Autorisierung nur im erweiterten Modus für bis zu 30 Tage ab dem aktuellen Datum geplant werden kann, an dem die Autorisierungsanfrage erstellt wird.



Hinweis: Bitte beachten Sie, dass die Autorisierungsanfrage 24 Stunden dauert. Die Autorisierung kann zwar vorzeitig storniert werden, die Dauer kann jedoch nicht von 24 Stunden geändert werden.

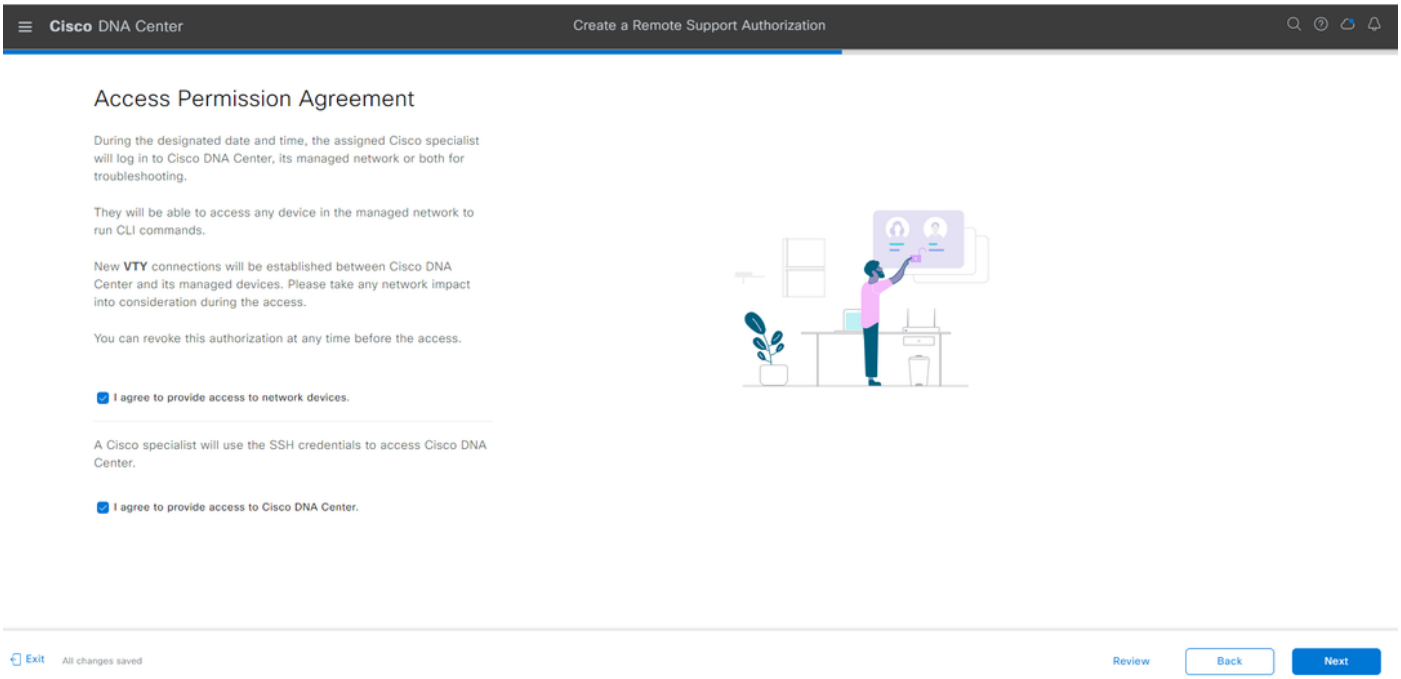
Wählen Sie Jetzt aus, und klicken Sie dann auf Weiter.



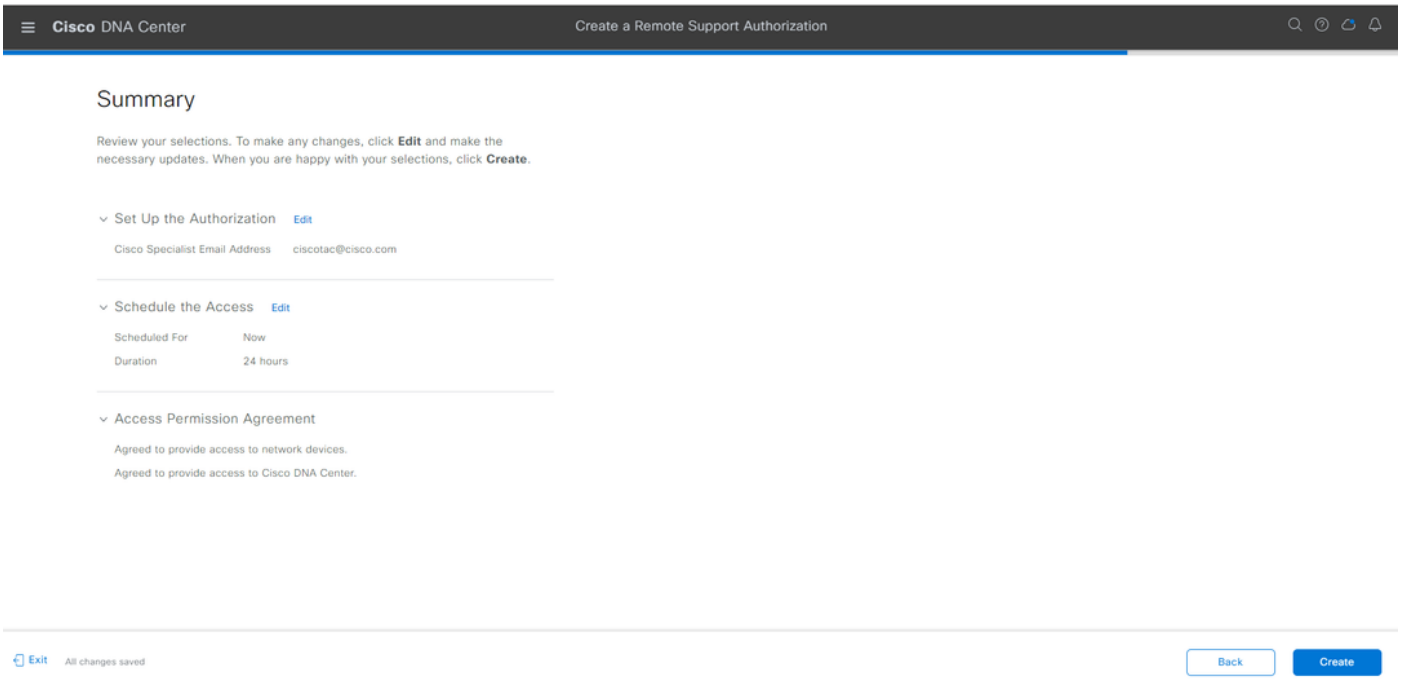
Sie werden zur Seite "Zugriffsberechtigungsvereinbarung" weitergeleitet. Diese Seite hat zwei Optionen:

- Neue VTY-Verbindungen zwischen dem Cisco DNA Center und den im Bestand verwalteten Geräten
- Zugriff auf die CLI der Cisco DNA Center Appliance(s)

Um eine SSH-Verbindung mit den vom Cisco DNA Center verwalteten Netzwerkgeräten herzustellen, muss die erste Option ausgewählt werden. Wenn diese Option nicht ausgewählt ist, können TAC-Techniker die Geräte mit Cisco RADKit nicht per SSH verbinden. Um eine SSH-Verbindung mit der/den Cisco DNA Center-Appliance(s) herzustellen, muss die zweite Option ausgewählt werden. Wenn diese Option nicht ausgewählt ist, können TAC-Techniker nicht auf das Cisco DNA Center mit Cisco RADKit zugreifen. Um die Remote Support Authorization-Funktion optimal zu nutzen, sollten Sie beide Optionen auswählen. Wenn Sie die gewünschten Optionen ausgewählt haben, klicken Sie auf Weiter.

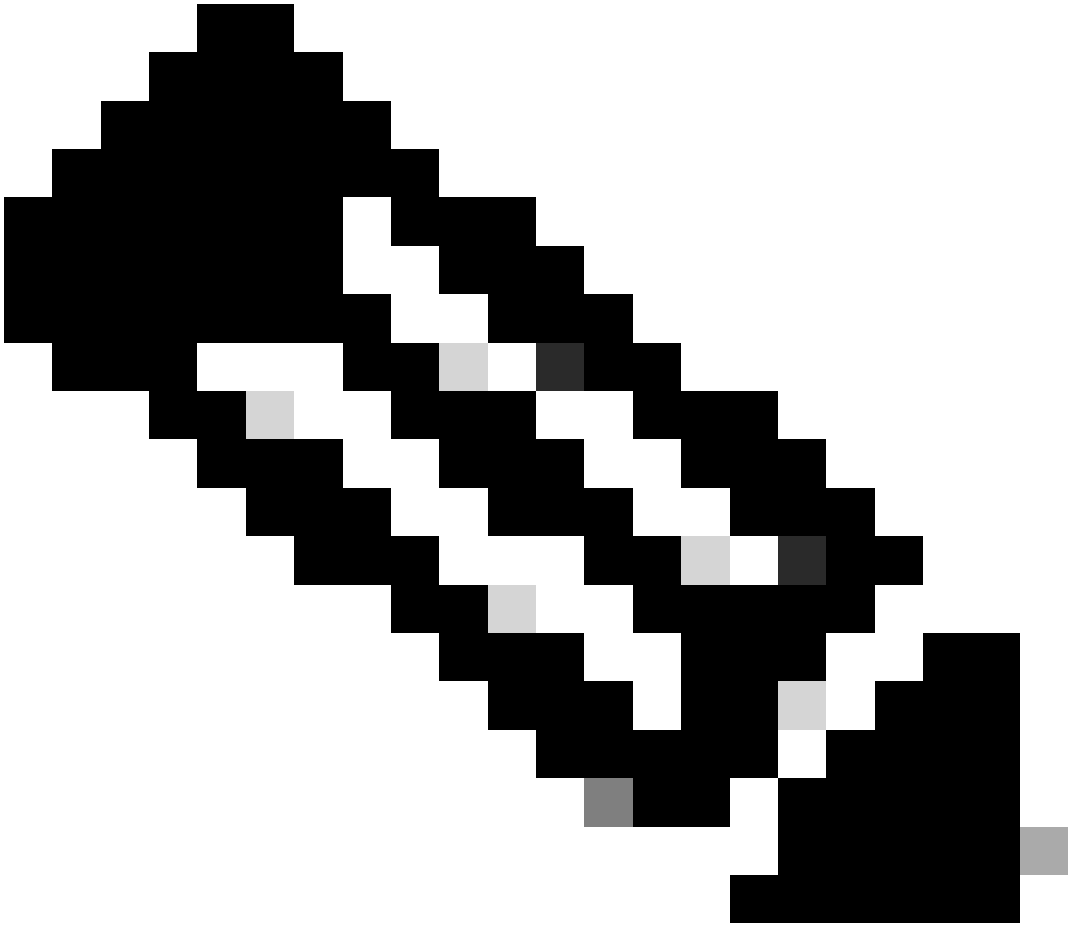


Sie werden auf die Seite "Übersicht" umgeleitet, auf der alle Informationen aufgeführt sind, die mit dem Workflow zum Erstellen einer Remote-Support-Autorisierung konfiguriert wurden. Hier können Sie bestätigen, dass die Einstellungen korrekt sind. Wenn die Einstellungen korrekt sind, klicken Sie auf Erstellen.

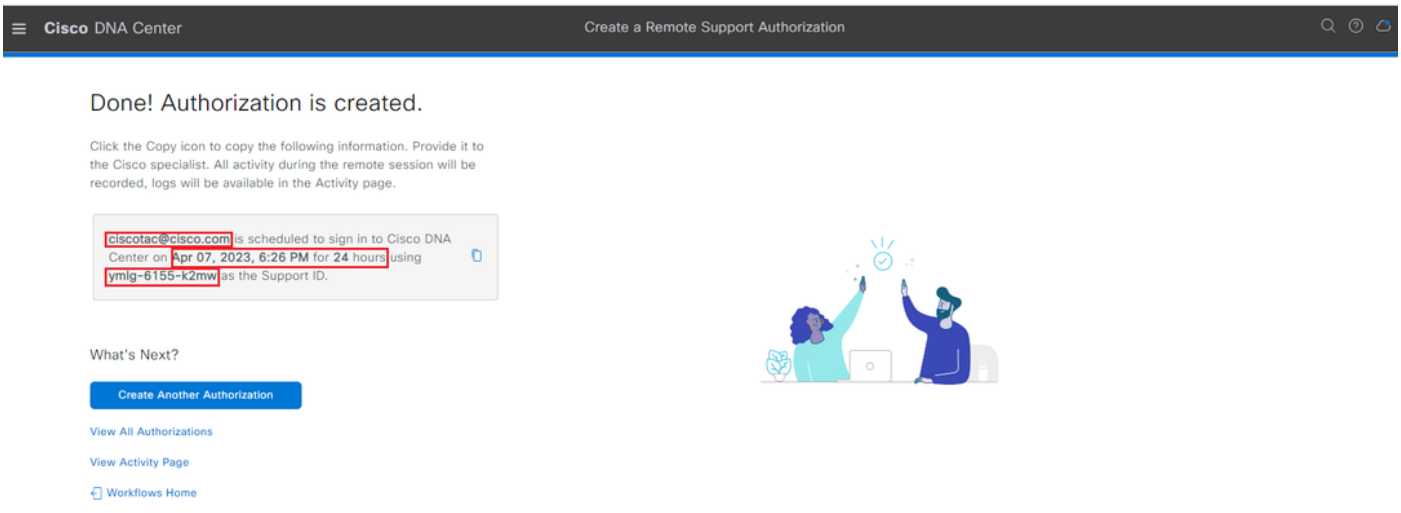


Klicken Sie auf Erstellen, um mit dem letzten Schritt fortzufahren. Sie werden auf eine Seite weitergeleitet, auf der angegeben ist, dass die Autorisierung erstellt wurde. Zu den wichtigsten Elementen auf dieser Seite gehören:

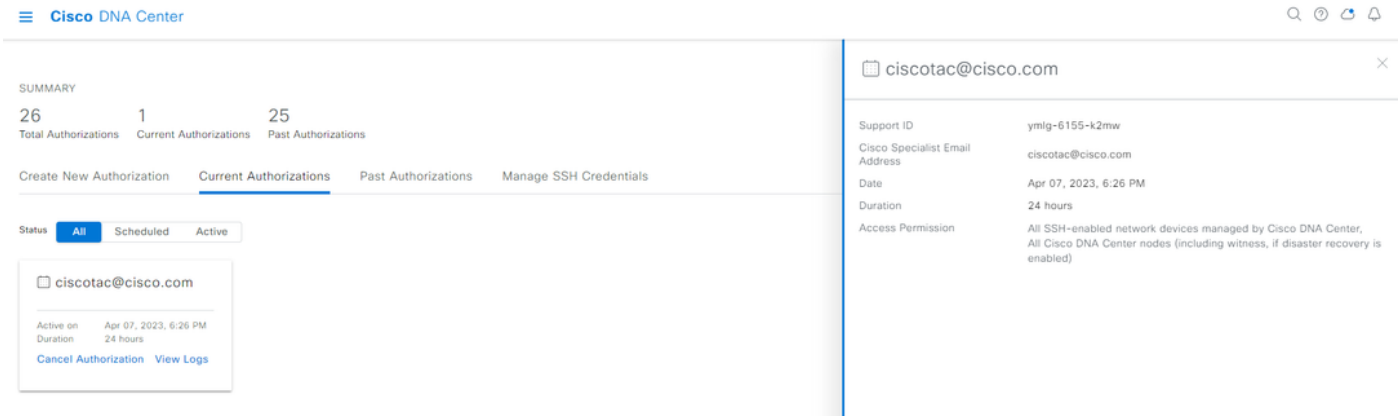
- E-Mail-Adresse des TAC-Technikers
- Geplante Startzeit und Dauer der Autorisierung
- Support-ID



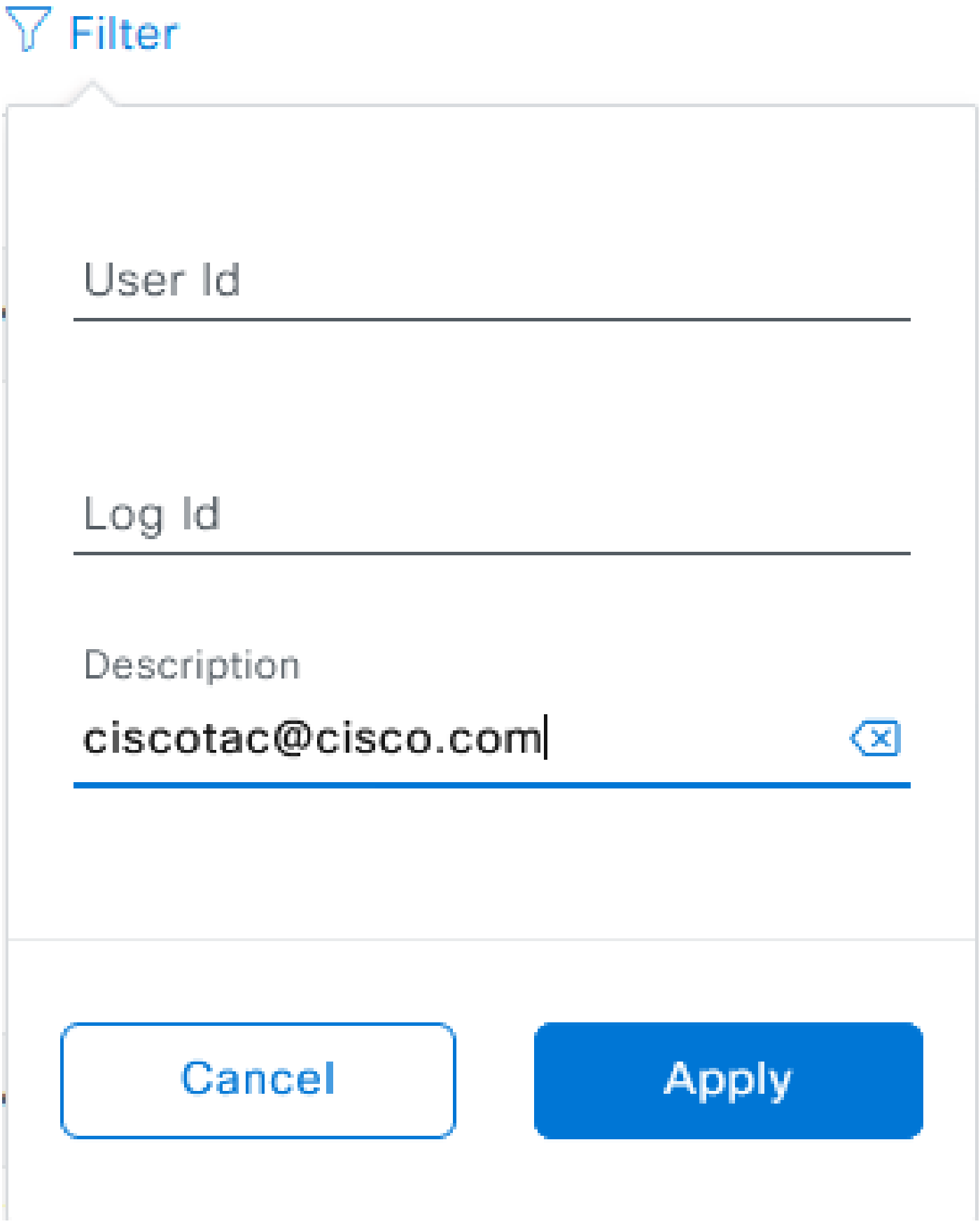
Hinweis: Beachten Sie, dass der TAC-Techniker die Support-ID benötigt, um sich mit dem Cisco RADKit-Client für diese Autorisierungsanfrage verbinden zu können. Kopieren Sie die bereitgestellten Informationen, und senden Sie sie an den TAC-Techniker.



Auf dieser Seite können Sie "Weitere Autorisierung erstellen", "Alle Autorisierungen anzeigen", "Aktivitätsseite anzeigen" oder "Workflow-Startseite" auswählen. Wenn keine weitere Autorisierung erstellt werden muss, können Sie Alle Autorisierungen anzeigen auswählen, um alle aktuellen und früheren Autorisierungen anzuzeigen. Die Seite "Aktivität anzeigen" leitet Sie zur Seite "Audit-Protokolle" um. Alle Autorisierungen anzeigen leitet Sie zur Seite "Aktuelle Autorisierungen" im Abschnitt "Remote Support-Autorisierung" um. Sie können alle, geplanten oder aktiven Autorisierungen anzeigen. Klicken Sie auf eine Autorisierung, um ein Seitenfenster zu öffnen, in dem die mit dem Workflow zum Erstellen einer Remote-Support-Autorisierung konfigurierten Einstellungen angezeigt werden.



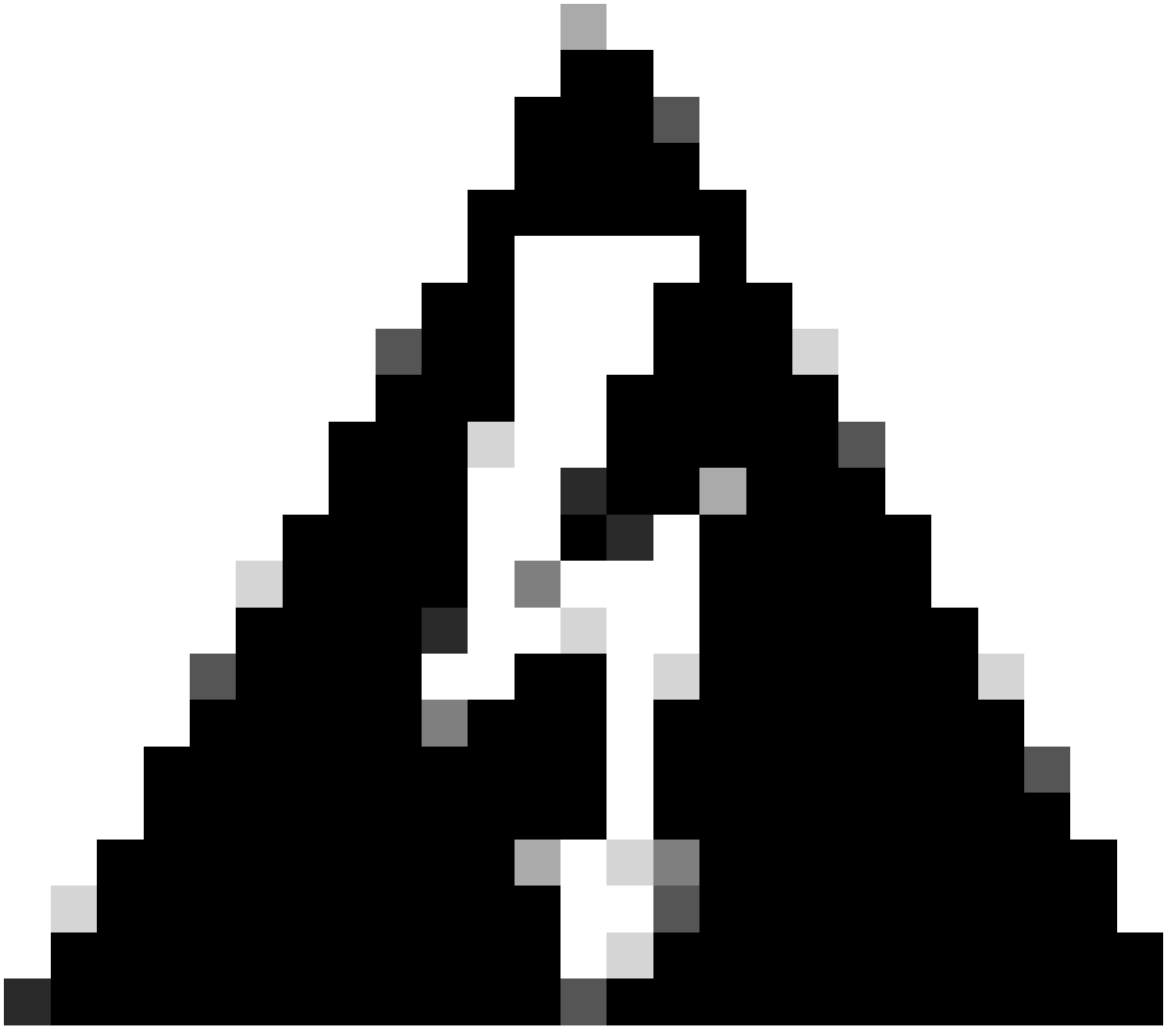
Sie können die Autorisierung abbrechen oder die Audit-Protokolle der Aktivitäten des TAC-Technikers in Ihrer Bereitstellung anzeigen. Sie können zur Registerkarte "Frühere Autorisierungen" wechseln, um historische Informationen zu früheren Autorisierungen abzurufen. Wählen Sie View Logs (Protokolle anzeigen) aus, um zur Seite Audit Logs (Überwachungsprotokolle) umgeleitet zu werden. Auf der Seite Audit Logs (Überwachungsprotokolle) können Sie Filter auswählen und dann nach Description (Beschreibung) mit der E-Mail-Adresse des TAC-Technikers filtern.



Wählen Sie Anwenden. Dadurch wird ein Filter basierend auf der E-Mail-Adresse des TAC-Technikers hinzugefügt, wie aus der Beschreibung der Audit-Protokolle ersichtlich wird, wenn

Cisco RADKit für die Remote-Bereitstellung verwendet wird.

Aus den Audit-Protokollen können Sie sehen, was genau der TAC-Techniker getan hat und wann er sich angemeldet hat.



Warnung: Die Remote Support-Autorisierungsfunktion von Cisco DNA Center Version 2.3.5.x wurde mit dem Cisco RADKit-Client 1.4.x getestet.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.