

Konfigurieren der Remote-Support-Autorisierung in ISE 3.4

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[RADKit Service Setup](#)

[Konfigurieren einer Remote-Support-Autorisierung](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Remote Support-Autorisierung für Cisco Identity Services Engine (ISE) Version 3.4 konfigurieren, um den Zugriff durch Cisco Agents zuzulassen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse der Cisco ISE® verfügen.

Um den RADKit-Dienst einzurichten, muss der primäre ISE-Administrationsknoten entweder direkt oder über einen konfigurierten Proxy über HTTPS-Verbindungen mit prod.radkit-cloud.cisco.com verfügen. Darüber hinaus ist ein gültiges CCO-Konto erforderlich.

Verwendete Komponenten

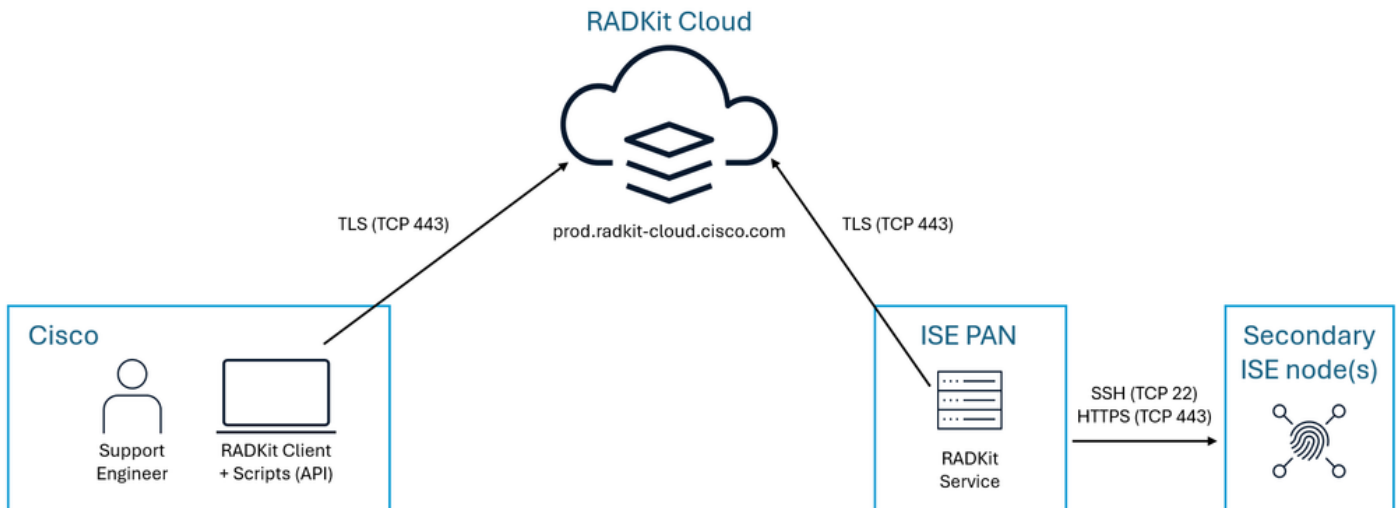
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ISE Version 3.4 Patch 2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Die Remote Support Authorization-Funktion ermöglicht Cisco Spezialisten Cisco RADkitden sicheren, überwachten Remote-Zugriff auf ausgewählte ISE-Knoten in Ihrer Umgebung, um die Fehlerbehebung zu vereinfachen.



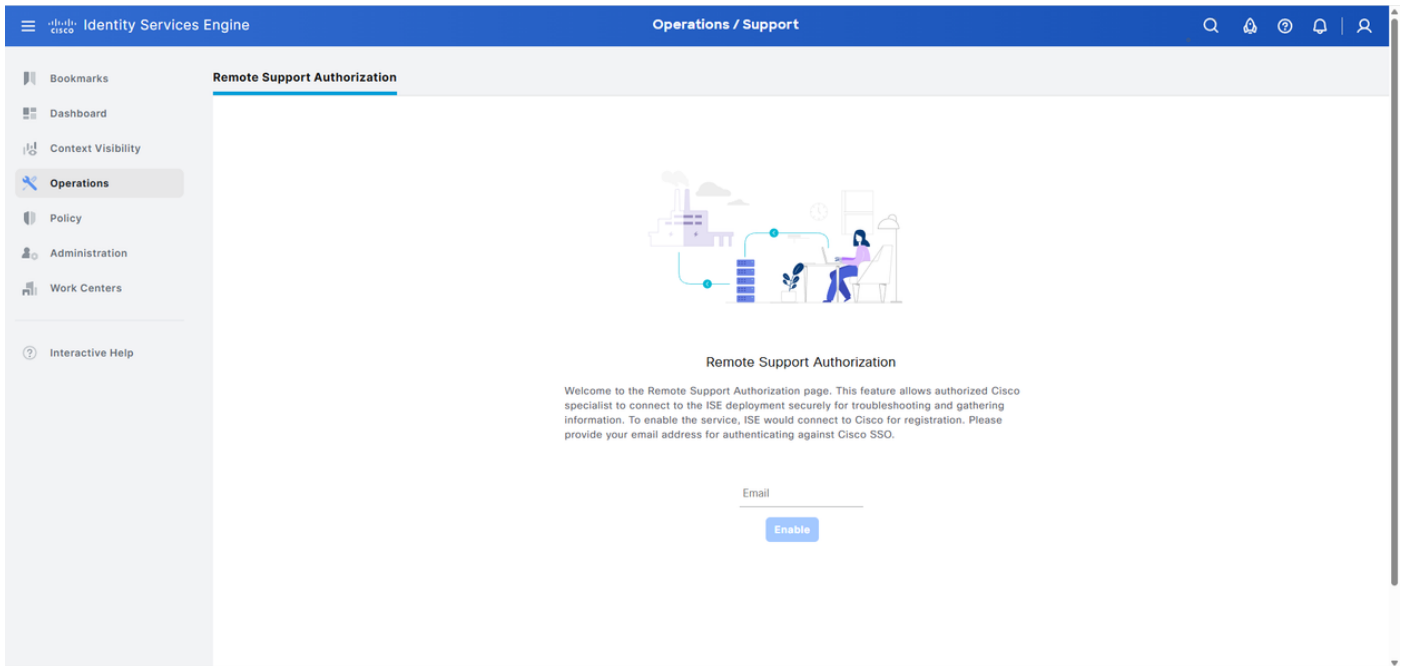
RADKit ISE-Architekturübersicht

RADKit wurde von CSDL genehmigt. CSDL ist ein Prozess von Cisco, der Software auf Sicherheitsrisiken, Datenschutz und Einhaltung von Lizenzbestimmungen durch Drittanbieter überprüft. RADKit wurde einer strengen Sicherheitsüberprüfung unterzogen: Codequalität und -abhängigkeiten werden während des gesamten Entwicklungsprozesses analysiert; unsere Dienstleistungen werden ständig überwacht. Alle ruhenden oder übertragenen Daten sind durch branchenübliche Algorithmen (AES, RSA, SHA-2, ECDH...) und Protokolle (2-Wege-authentifiziertes TLS1.3, SSH) mit branchenweit empfohlenen Parametern geschützt.

RADKit ermöglicht nur die Datenübertragung, jedoch wird von RADKit nichts in der RADKit Cloud gesammelt oder gespeichert. Es ist nur eine effiziente Methode für Sie, Daten zu sammeln, und eine sicherere Möglichkeit, Daten mit Ihrem Support-Techniker auszutauschen, als E-Mails zu senden oder manuell an einen Serviceticket zu senden. Die einzige Ausnahme zu dieser Regel ist der Prüfpfad, den wir für Ihre Sicherheit erstellen, der Ihnen gehört und Ihr System niemals verlässt.

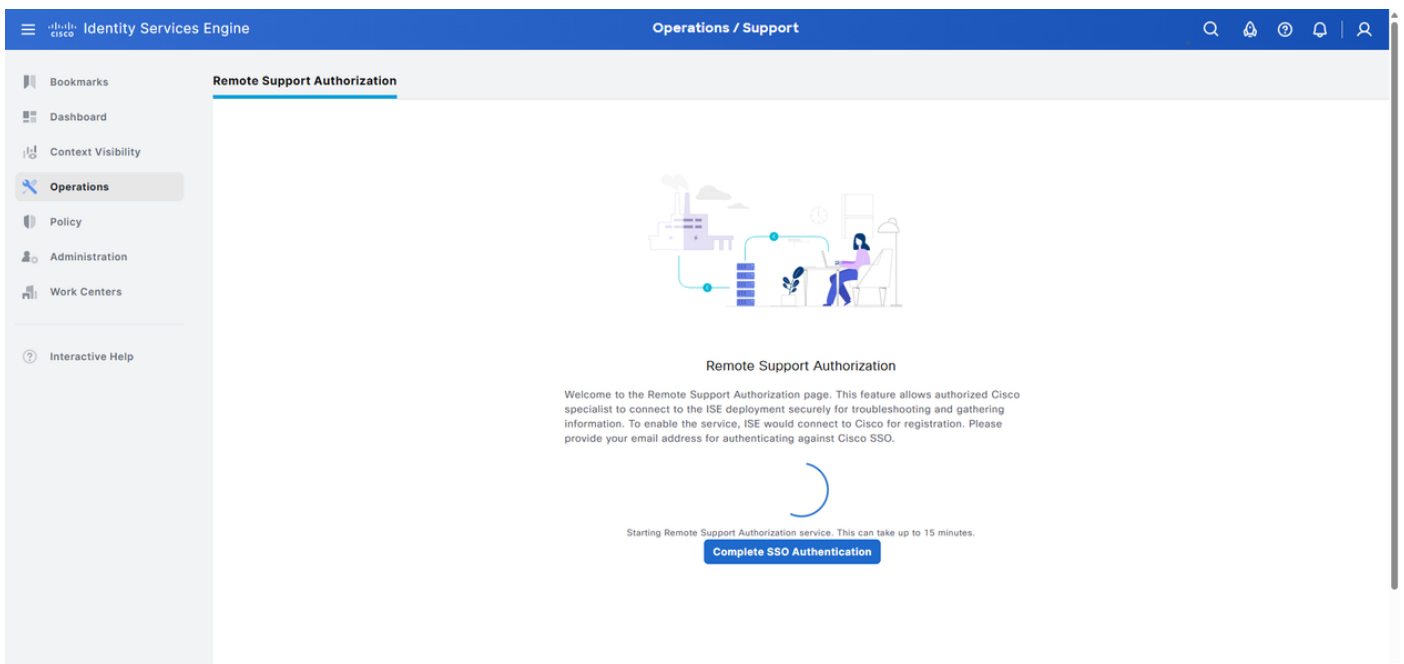
RADKit Service Setup

Navigieren Sie zu **. Operations > Support > Remote Support Authorization** Geben Sie Ihre mit Cisco SSO verknüpfte E-Mail-Adresse für die Authentifizierung ein.



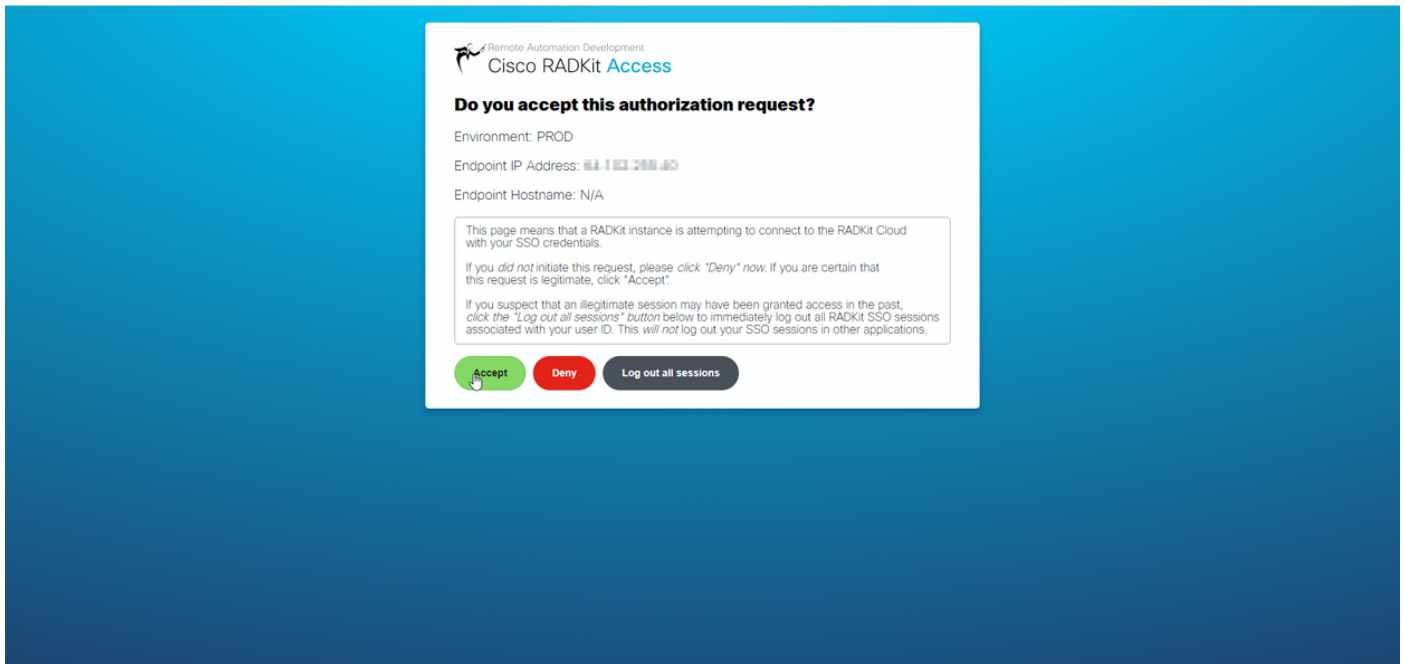
Anfängliche Seite für die Remote Support-Autorisierung, auf der eine E-Mail-Eingabe erforderlich ist

Wenn der Remote Support Authorization-Service gestartet wurde, klicken Sie auf **Complete sso Authentication**.



Nach Eingabe von E-Mail erscheint die Schaltfläche "SSO-Authentifizierung abschließen".

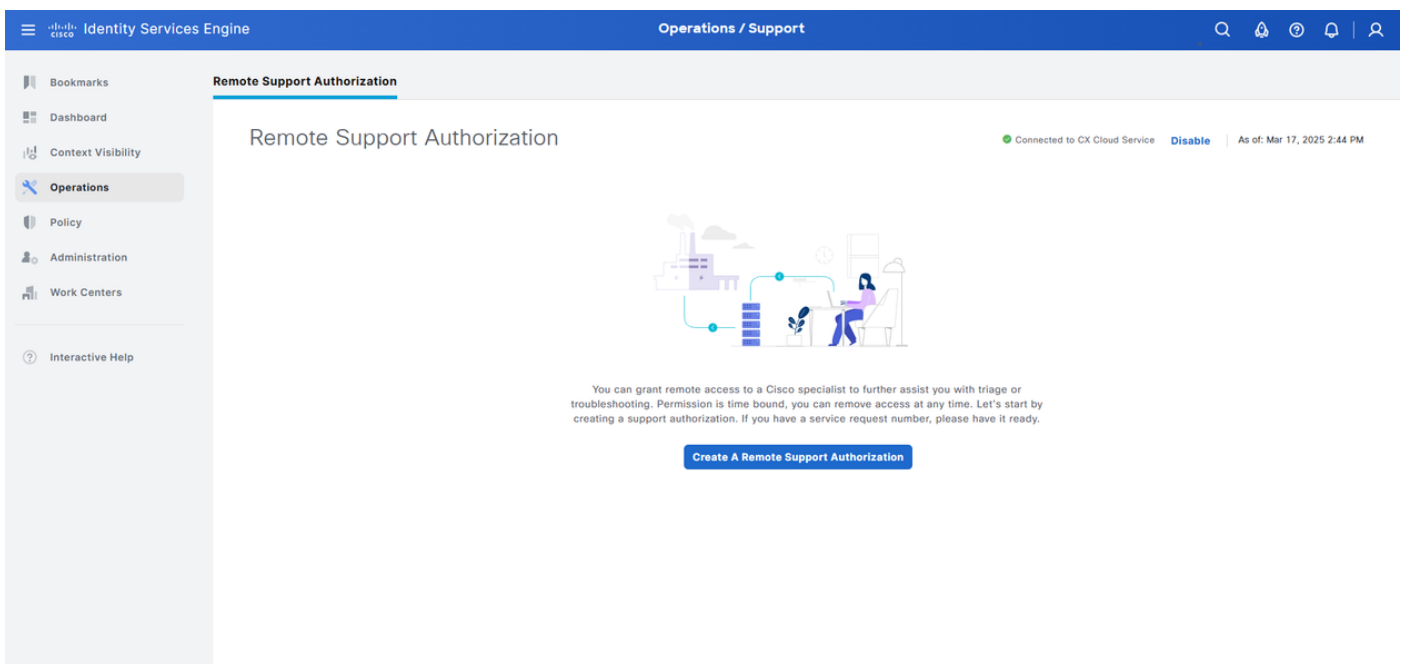
Klicken Sie **Accept** auf das neu geöffnete Fenster, um die Autorisierung für Cisco RADkit Cloud abzuschließen.



SSO-Authentifizierungsseite, auf der die Autorisierung abgeschlossen wurde

Konfigurieren einer Remote-Support-Autorisierung

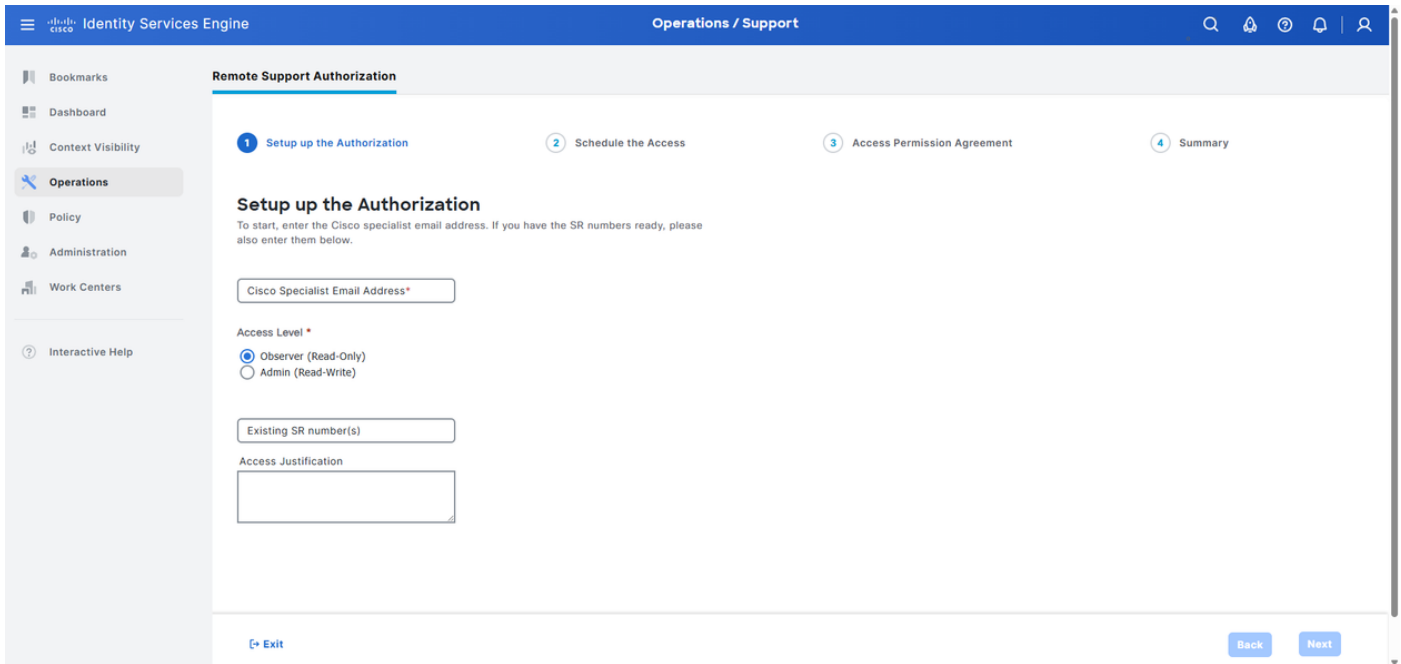
Klicken Sie hier **Create A Remote Support Authorization**, um eine Remotezugriffssitzung zu konfigurieren.



Nach der Authentifizierung wird die Option Create Remote Support Authorization (Remote-Support-Autorisierung erstellen) angezeigt

Geben Sie die E-Mail-Adresse des Cisco Specialist ein, auf den Sie Zugriff gewähren möchten. Wählen Sie diese Option aus, **Observer (Read-Only)** um dem Cisco Spezialisten schreibgeschützten Zugriff **Admin (Read-Write)** zu gewähren, oder um dem Cisco Spezialisten vollen Lese- und Schreibzugriff zu gewähren. Wenn sich dieser Zugriff auf eine vorhandene TAC-Serviceanfrage bezieht, können Sie die SR-Nummer sowie eine andere Begründung für den Remote-Zugriff eingeben. Klicken Sie **Next** nach Eingabe der erforderlichen Informationen auf.

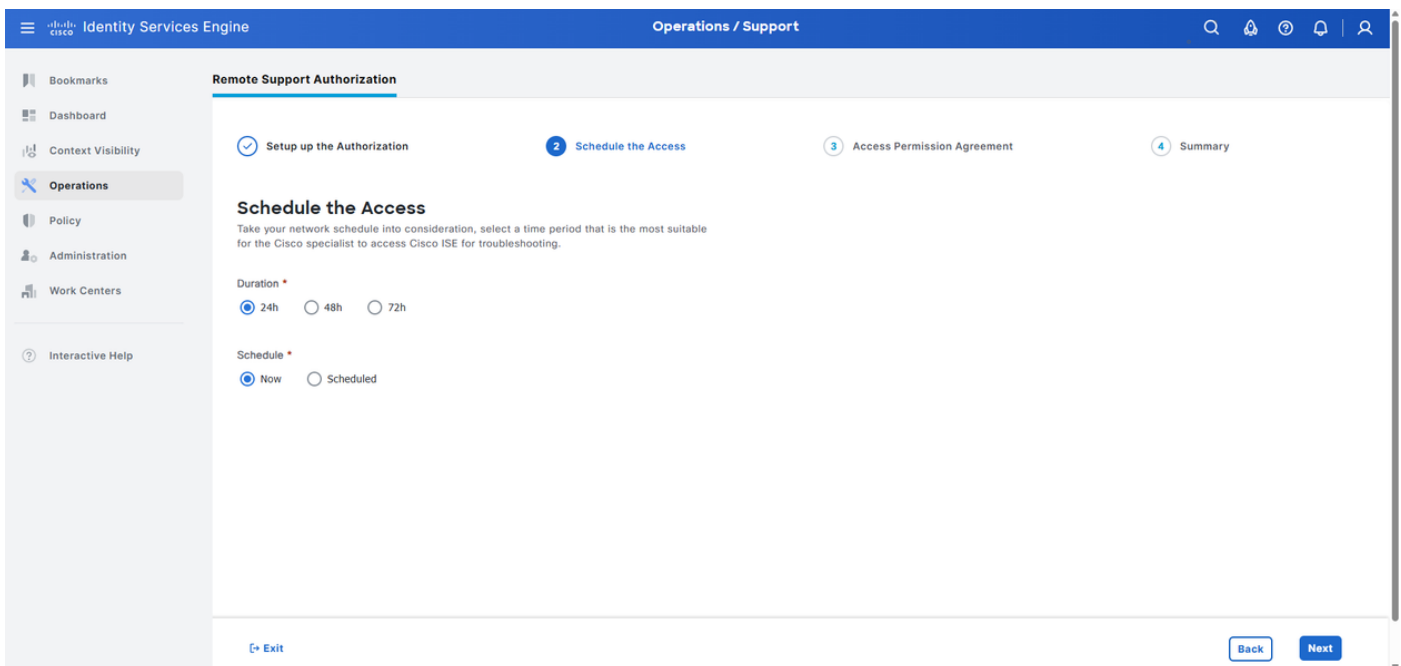
 Anmerkung: Durch Bereitstellen der SR-Nummern kann das TAC die gesammelten Protokolle automatisch und ohne Eingriff hochladen. Dies hilft auch bei der Dokumentation der Remote-Verbindung und der Befehle im SR.



The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar is blue with the Cisco logo and 'Identity Services Engine' on the left, and 'Operations / Support' on the right. A search bar and notification icons are on the far right. The left sidebar contains a menu with 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations' (highlighted), 'Policy', 'Administration', 'Work Centers', and 'Interactive Help'. The main content area is titled 'Remote Support Authorization' and shows a progress bar with four steps: 1. Setup up the Authorization (active), 2. Schedule the Access, 3. Access Permission Agreement, and 4. Summary. Below the progress bar, the section 'Setup up the Authorization' is displayed. It includes a text input field for 'Cisco Specialist Email Address*', a radio button selection for 'Access Level' (Observer (Read-Only) is selected, Admin (Read-Write) is unselected), a text input field for 'Existing SR number(s)', and a text area for 'Access Justification'. At the bottom, there is a 'Back' button and a 'Next' button.

Erste Seite der Autorisierung

Planen Sie Dauer und Zeitplan für die Remote-Autorisierung. Um den Zugriff sofort zu planen, wählen Sie **Now**. Um den Zugriff für ein späteres Datum oder eine spätere Uhrzeit zu planen, wählen Sie die gewünschte Information aus, **scheduled** und legen Sie sie in fest. Klicken Sie dann nach der Eingabe der gewünschten Informationen auf **Start Date** und **Start Time**. dann **Next** auf.



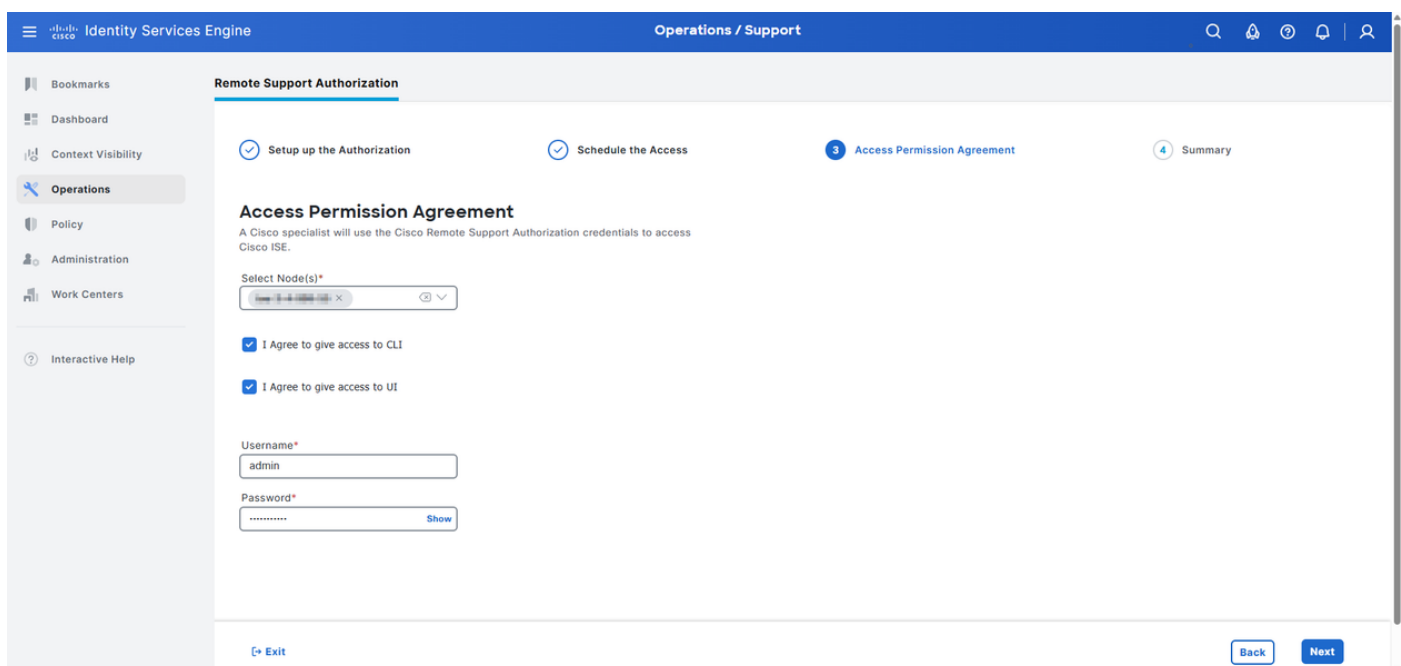
The screenshot shows the Cisco Identity Services Engine (ISE) interface, specifically the 'Schedule the Access' step. The top navigation bar and left sidebar are the same as in the previous screenshot. The main content area is titled 'Remote Support Authorization' and shows the progress bar with step 2, 'Schedule the Access', highlighted. Below the progress bar, the section 'Schedule the Access' is displayed. It includes a text input field for 'Duration' with radio button options for 24h (selected), 48h, and 72h. Below that, there is a radio button selection for 'Schedule' (Now is selected, Scheduled is unselected). At the bottom, there is a 'Back' button and a 'Next' button.

Zweite Seite der Autorisierung

Wählen Sie jeden ISE-Knoten aus, auf den Sie Zugriff gewähren möchten. Wählen Sie zum

Aktivieren des Remote-CLI-Zugriffs auf die Knoten die Option **I Agree to give access to CLI**. Zum Aktivieren des Remote-UI-Zugriffs auf die Knoten aus. Klicken Sie **I Agree to give access to UI**nach der Eingabe der erforderlichen Informationen auf **Next**.

 Anmerkung: Um den Zugriff auf die Benutzeroberfläche zu ermöglichen, müssen Sie einen Benutzernamen/ein Kennwort für den UI-Administrator konfigurieren. Mit diesem Konto wird ein neuer Admin-Benutzer erstellt, über den sich der Cisco Experte mit der angegebenen Zugriffsebene anmeldet. Das eingegebene Konto muss daher über die erforderlichen Berechtigungen zum Erstellen eines neuen Admin-Kontos verfügen. Die Anmeldeinformationen müssen für einen internen Administrator-Benutzer angegeben werden, es sei denn, Active Directory ist als UI-Identitätsquelle konfiguriert. In diesem Fall können auch AD-Administratoranmeldeinformationen verwendet werden.



The screenshot displays the 'Remote Support Authorization' interface in the Cisco Identity Services Engine (ISE). The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Operations / Support'. A left sidebar lists various navigation options like Bookmarks, Dashboard, Context Visibility, Operations (highlighted), Policy, Administration, Work Centers, and Interactive Help. The main content area shows a four-step process: 1. Setup up the Authorization, 2. Schedule the Access, 3. Access Permission Agreement (active), and 4. Summary. The 'Access Permission Agreement' section contains a 'Select Node(s)*' dropdown, two checked checkboxes for 'I Agree to give access to CLI' and 'I Agree to give access to UI', and input fields for 'Username*' (admin) and 'Password*' (masked). At the bottom, there are 'Exit', 'Back', and 'Next' buttons.

Dritte Seite der Autorisierungserstellung

Klicken Sie auf das Symbol "Kopieren", um die Informationen zur Remote-Support-Autorisierung zu kopieren und dem Cisco-Spezialisten zur Verfügung zu stellen. Klicken Sie auf, um die Autorisierung für den Remote-Zugriff abzuschließen **Finish**.

Identity Services Engine Operations / Support

Remote Support Authorization

Setup up the Authorization Schedule the Access Access Permission Agreement **4 Summary**

Summary
Click the 'Copy' icon to copy the following information. Provide it to the Cisco specialist.

xxxxxxxxxxxx is scheduled to sign in to Cisco ISE on Mar 17, 2025, 2:44 PM for 24 hours using xxxxxxxx as the Support ID

> Setup up the Authorization

> Schedule the Access

> Access Permission Agreement

Exit Back Finish

Seite "Übersicht über die Autorisierung"

Überprüfung

Auf der **Current Authorizations** Registerkarte können Sie alle derzeit aktiven Remote-Support-Autorisierungen überprüfen. Auf der **Past Authorizations** Registerkarte können Sie alle vorherigen Autorisierungen für den Remote-Support anzeigen.

Identity Services Engine Operations / Support

Remote Support Authorization

Connected to CX Cloud Service Disable As of: Apr 9, 2025 4:57 PM

Current Authorizations Past Authorizations

Create Authorization

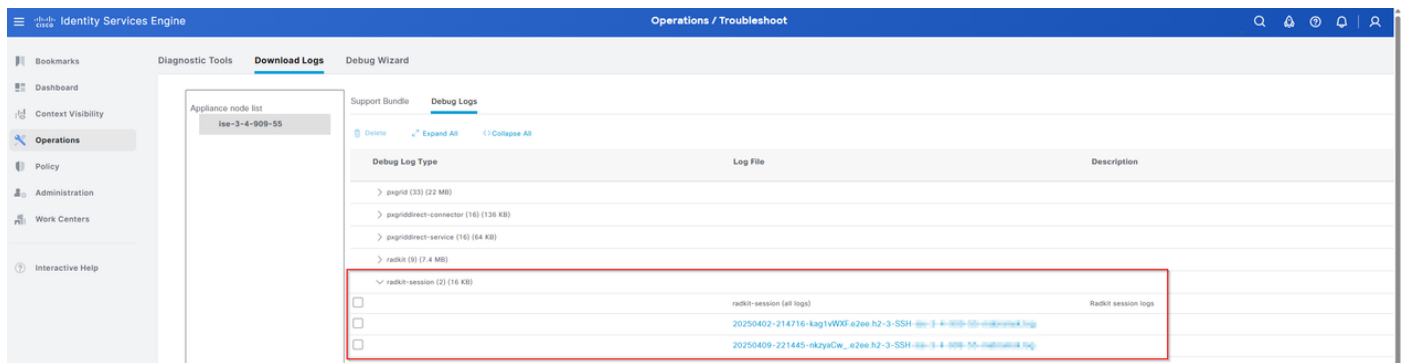
Active on	Duration	CLI Access	UI Access	Service ID
Apr 9, 2025, 1:49 PM	24h	Provided	Provided	xxxxxxxxxx

Edit Cancel View Logs

Aktive Autorisierungen überprüfen

Rufen Sie zum Anzeigen von CLI-Sitzungsüberwachungsprotokollen für einen Knoten **Operations > Support > Troubleshoot > Download Logs** den Knoten auf, für den die Protokolle heruntergeladen werden sollen, und wählen Sie anschließend **Debug Logs**. Alle CLI-Sitzungen finden Sie im **radkit-session-**Ordner. Klicken Sie auf den Dateinamen, um die Überwachungsprotokolle herunterzuladen.

Anmerkung: Die CLI-Sitzungsüberwachung muss pro Knoten durchgeführt werden. Jeder Knoten verfügt über einen eigenen Radkit-Sitzungsordner mit spezifischen Überwachungsprotokollen für den Knoten.



CLI-Audit-Protokolle

Um UI-Prüfprotokolle anzuzeigen, können Sie die Prüfberichte in der ISE-Benutzeroberfläche verwenden. Navigieren Sie zu **Operations > Reports > Audit > Administrator Logins** , um alle Administratoranmeldungen in der Benutzeroberfläche oder der CLI anzuzeigen. Navigieren Sie zu **Operations > Reports > Audit > Change Configuration Audit** , um alle Änderungen anzuzeigen, die von Administratoren in der Benutzeroberfläche vorgenommen wurden.

 **Anmerkung:** Cisco Spezialisten, die sich auf der Benutzeroberfläche anmelden, verwenden den Benutzernamen <user>-CustomerSupport, wobei <user> der in der Autorisierung für den Remote-Support angegebene Benutzername ist. Cisco Spezialisten, die sich bei der CLI anmelden, verwenden den Benutzernamen customersuppadmin, wenn sie über Administratorzugriff (Read-Write) verfügen, oder customersuppreadonly, wenn sie über Beobachterzugriff (Read-Only) verfügen.

Fehlerbehebung

Um die Protokolle des Containers anzuzeigen, der während der ersten Einrichtung beginnt, bei der die E-Mail in die Benutzeroberfläche eingegeben wird, müssen wir die Datei ADE.log anzeigen. Geben Sie über die CLI den Befehl `show logging system ade/ADE.log tail` ein:

```
2025-05-20T14:21:07.670874-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Co
2025-05-20T14:21:07.818398-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] do
2025-05-20T14:21:07.821281-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] St
2025-05-20T14:21:07.824667-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] in
2025-05-20T14:21:07.828862-05:00 ise-3-4-909-55 ADEOSShell[594468]: ADEAUDIT 2061, type=USER, name=RADK
2025-05-20T14:21:07.829439-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] in
2025-05-20T14:21:07.877488-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] in
2025-05-20T14:21:08.057775-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Im
2025-05-20T14:21:08.060665-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Do
2025-05-20T14:21:08.063583-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Do
2025-05-20T14:21:08.066214-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Se
```

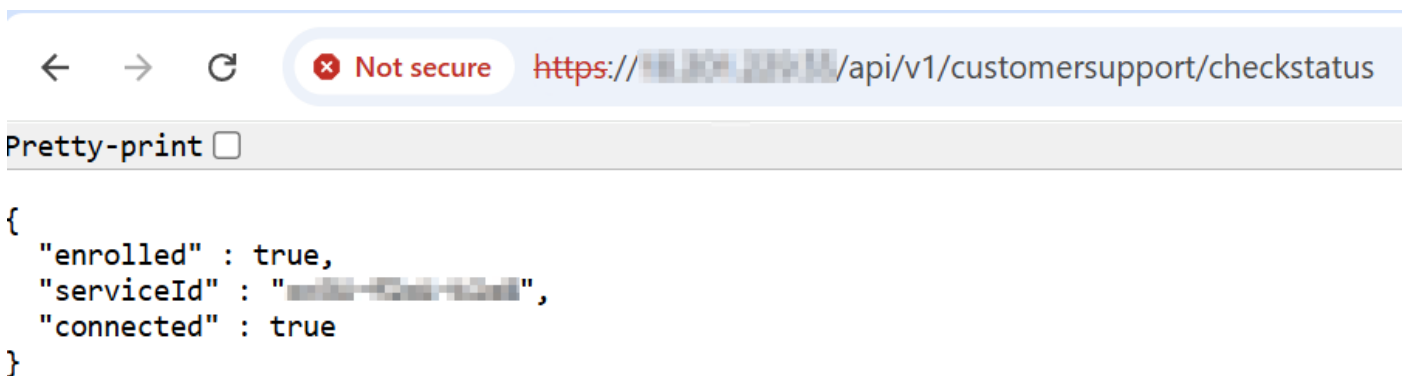
Die ISE überwacht den Container, um zu überprüfen, ob er ausgeführt wird und ob die RADKit-Anwendung bereit ist, bevor der Remote-Autorisierungsdienst als gestartet markiert wird.

```

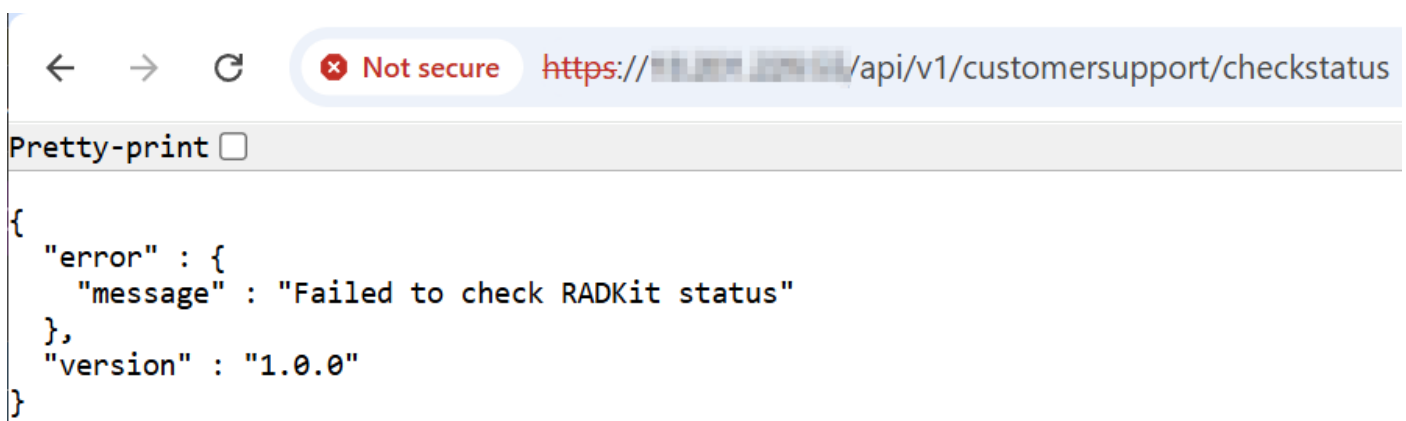
2025-05-20T14:21:24.477946-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Co
2025-05-20T14:21:24.800804-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] In
2025-05-20T14:21:24.804531-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] IS
2025-05-20T14:21:27.859691-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Co
2025-05-20T14:21:28.024853-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] In
2025-05-20T14:21:28.028121-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] IS
2025-05-20T14:21:31.079596-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Co
2025-05-20T14:21:31.232927-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] In
2025-05-20T14:21:31.236149-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] IS
2025-05-20T14:21:34.287758-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Co
2025-05-20T14:21:34.426699-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] In
2025-05-20T14:21:34.429983-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] IS
2025-05-20T14:21:37.486192-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Co
2025-05-20T14:21:37.621712-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Re

```

Sie können den Status des RADKit-Service auch mithilfe des API-Aufrufs
<https://<ISE PPAN>/api/v1/customersupport/checkstatus> überprüfen.



Ausgabe bei Ausführung des RadKit-Diensts



Ausgabe bei nicht ausgeführtem RadKit-Dienst

Um die RADKit-Dienstprotokolle nach dem Start des Remote Support Authorization Service anzuzeigen, geben Sie den Befehl `show logging application radkit/service/service.log` ein. Wenn der Dienst zum ersten Mal gestartet wird, erfolgt eine grundlegende Einrichtung mit der RADKit-Anwendung.

2025-05-20T19:21:31.730Z INFO | internal | MainThread

```
[ ] RADKit Service [version='1.6.12']
2025-05-20T19:21:31.731Z INFO | internal | MainThread
```

```
[ ] STDIN is not a terminal; assuming --headless
2025-05-20T19:21:31.732Z INFO | internal | MainThread
```

```
[ ] This RADKit release does not expire
2025-05-20T19:21:34.101Z INFO | internal | MainThread radkit_service.database.service_db [DB] Creating
2025-05-20T19:21:34.102Z INFO | internal | MainThread radkit_service.database.service_db [DB] Storing
2025-05-20T19:21:34.104Z INFO | internal | MainThread radkit_service.database.service_db [DB] Opening
2025-05-20T19:21:34.105Z INFO | internal | MainThread radkit_service.backup [SYSTEM] Ensuring backup d
```

Der RADKit-Dienst, der für Verbindungen zur Verfügung steht, wird erstellt.

```
2025-05-20T19:22:25.284Z INFO | radkit_control/superadmin/184f89f8 | MainThread radkit_service.service
2025-05-20T19:22:25.655Z INFO | radkit_control/superadmin/184f89f8 | MainThread Service(0x7F92596171D0)
2025-05-20T19:22:25.664Z INFO | radkit_control/superadmin/184f89f8 | MainThread SingleWebSocketForward
2025-05-20T19:22:25.679Z INFO | radkit_control/superadmin/c5f2549f | MainThread radkit_service.webserv
```

Wenn Sie in der grafischen Benutzeroberfläche eine Autorisierung für den Remote-Support hinzufügen, wird der Cisco Specialist als Remote-Benutzer erstellt.

```
2025-05-20T19:24:10.599Z INFO | radkit_control/superadmin/5d496186 | MainThread DBOperationsAPI(0x7F925A1
2025-05-20T19:24:10.600Z INFO | radkit_control/superadmin/5d496186 | MainThread radkit_service.webserv
```

Wenn der Cisco Specialist eine Verbindung zum Service herstellt und auf einen ISE-Knoten zugreift, wird dies in diesen Protokollen angezeigt.

```
2025-05-20T19:26:02.766Z INFO | cloud-rpc/mabramsk@cisco.com/4Kkevny_ | MainThread RPCServer(0x7F925A1
2025-05-20T19:26:03.033Z INFO | cloud-rpc/mabramsk@cisco.com/4Kkevny_ | MainThread CapabilitiesRespond
```

```

2025-05-20T19:26:03.117Z INFO | cloud-rpc/mabramsk@cisco.com/4Kkevny_ | MainThread CapabilitiesRespond
2025-05-20T19:26:03.121Z INFO | cloud-rpc/mabramsk@cisco.com/4Kkevny_ | MainThread RPCServer(0x7F925A1
2025-05-20T19:26:04.863Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR | MainThread EncryptedRPCServerT
2025-05-20T19:26:04.864Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee | MainThread H2Multiplexing
2025-05-20T19:26:04.869Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-1 | MainThread RPCServer
2025-05-20T19:26:04.879Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-1 | MainThread Inventory
2025-05-20T19:26:04.882Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-1 | MainThread Inventory
2025-05-20T19:26:04.885Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-1 | MainThread RPCServer
2025-05-20T19:26:26.083Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-3 | MainThread RPCServer
2025-05-20T19:26:26.090Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-3 | MainThread TerminalP
2025-05-20T19:26:26.146Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-3 | MainThread SSHPTYStr
2025-05-20T19:26:26.198Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-3 | MainThread radkit_se
2025-05-20T19:26:43.932Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-3 | MainThread TerminalP
2025-05-20T19:26:43.935Z INFO | cloud-rpc/mabramsk@cisco.com/cjZPy-yR.e2ee.h2-3 | MainThread RPCServer

```

Sobald die Remote-Autorisierung abläuft oder entfernt wird, wird der Remote-Benutzer vom RADKit-Dienst gelöscht.

```

2025-05-20T19:26:55.195Z INFO | radkit_control/superadmin/8fd4246f | MainThread radkit_service.webserv
2025-05-20T19:26:55.196Z INFO | radkit_control/superadmin/8fd4246f | MainThread radkit_service.webserv

```

Zugehörige Informationen

- [Administratorleitfaden für die Cisco Identity Services Engine, Version 3.4](#)
- [Versionshinweise für Cisco Identity Services Engine, Version 3.4](#)

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.