

Configurazione dell'autorizzazione per il supporto remoto in ISE 3.4

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurazione servizio RADKit](#)

[Configurare un'autorizzazione per il supporto remoto](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare Remote Support Authorization sulla versione Cisco Identity Services Engine (ISE) 3.4 per consentire l'accesso dagli agenti Cisco.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza base di Cisco ISE®.

Per configurare il servizio RADKit, il nodo di amministrazione primario ISE deve avere connettività HTTPS a prod.radkit-cloud.cisco.com, direttamente o tramite un proxy configurato. È inoltre necessario un account CCO valido.

Componenti usati

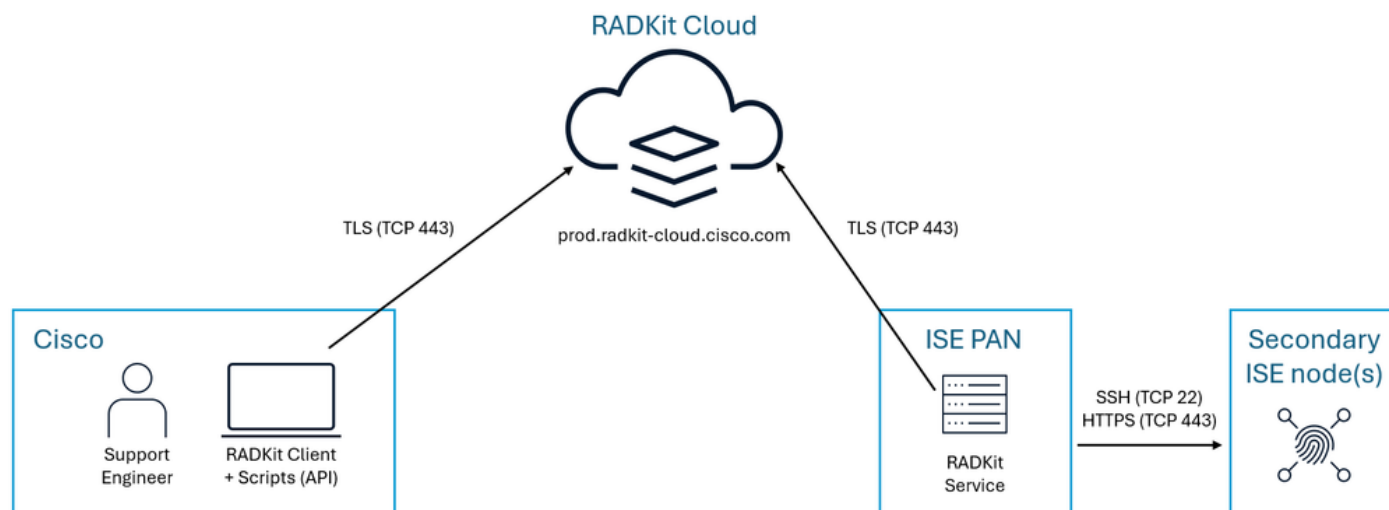
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE versione 3.4 patch 2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

La funzione di autorizzazione del supporto remoto sfrutta Cisco RADKit per fornire agli specialisti Cisco un accesso remoto sicuro e verificato a determinati nodi ISE dell'ambiente in uso, al fine di semplificare la risoluzione dei problemi.



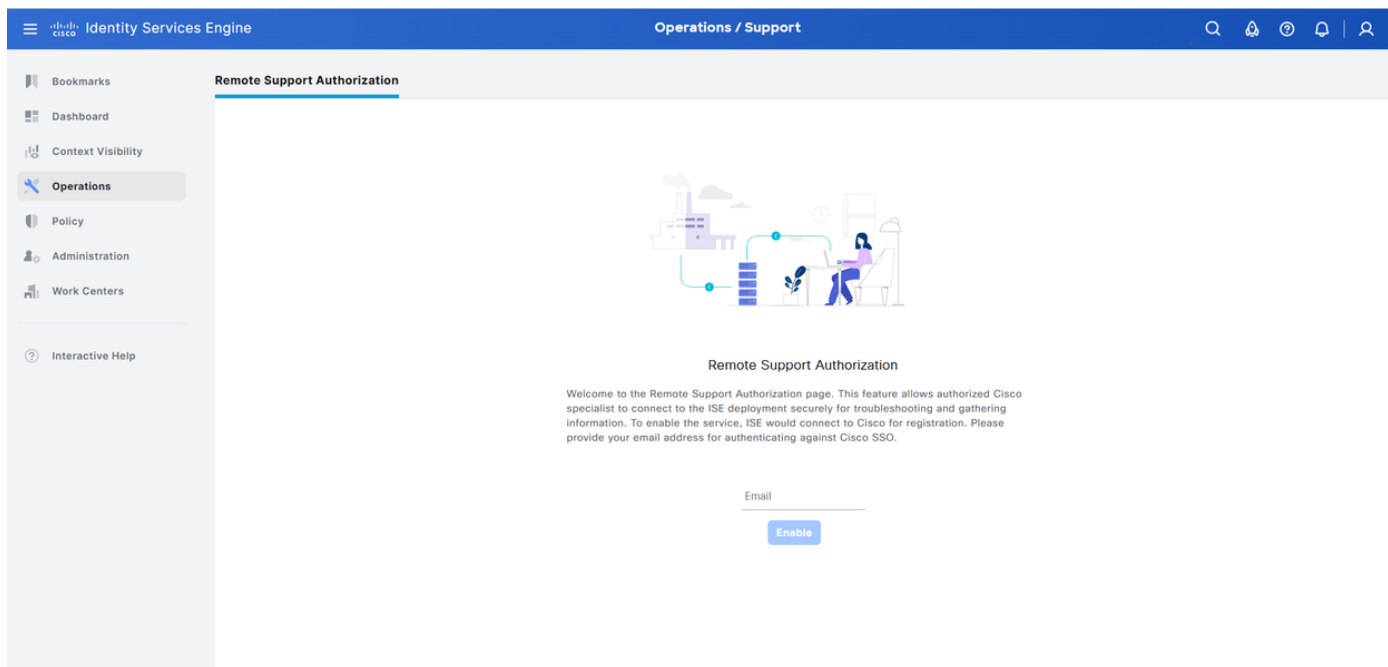
Panoramica dell'architettura di RADKit ISE

RADKit è approvato da CSDL. CSDL è un processo Cisco che analizza i rischi per la sicurezza, la riservatezza dei dati e la conformità delle licenze di terze parti. RADKit è stato sottoposto a una rigorosa revisione della sicurezza: la qualità del codice e le dipendenze sono analizzate durante tutto il processo di sviluppo; i nostri servizi sono costantemente monitorati. Tutti i dati inattivi o in transito sono protetti da algoritmi standard (AES, RSA, SHA-2, ECDH...) e protocolli (TLS1.3 autenticato a 2 vie, SSH) con parametri consigliati dal settore.

RADKit facilita solo il trasferimento dei dati, ma non viene raccolto né archiviato da RADKit in RADKit Cloud. Si tratta solo di un modo efficiente per raccogliere dati e di un modo più sicuro per scambiare i dati con il tecnico di assistenza rispetto all'invio di e-mail o al caricamento manuale in una SR. L'unica eccezione a questa regola è l'audit trail generato per la sicurezza dell'utente, di proprietà dell'utente e che non lascia mai il sistema.

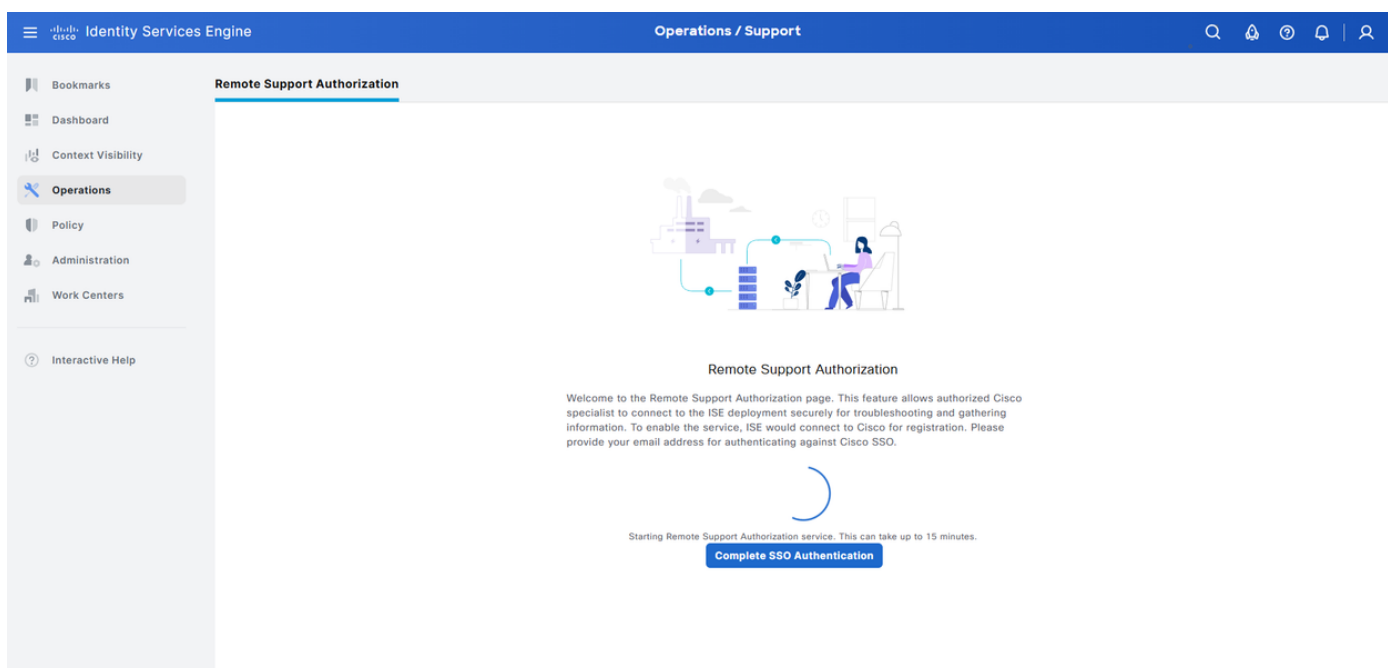
Configurazione servizio RADKit

Passare a **Operations > Support > Remote Support Authorization**. Immettere l'indirizzo e-mail associato a Cisco SSO per l'autenticazione.



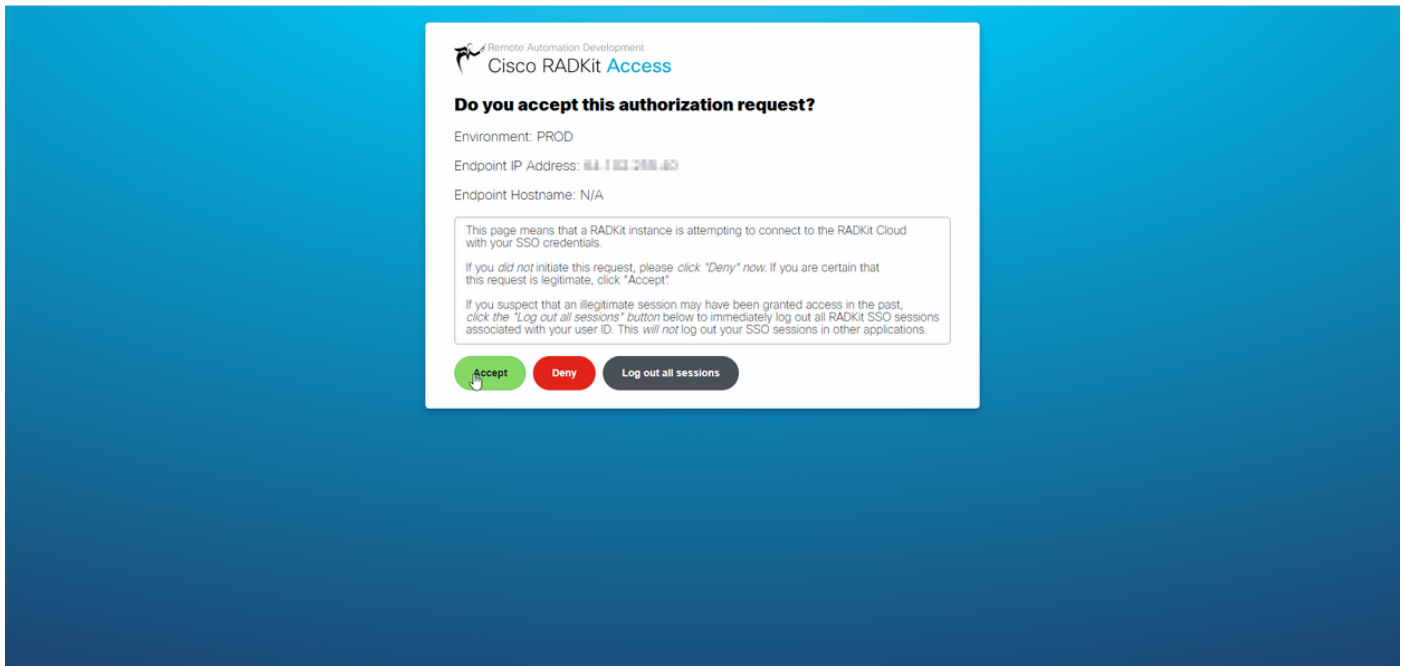
Pagina iniziale di autorizzazione del supporto remoto in cui è richiesta la voce di posta elettronica

Dopo l'avvio del servizio Autorizzazione supporto remoto, fare clic su **Complete SSO Authentication**.



Dopo l'immissione dell'e-mail, viene visualizzato il pulsante Complete SSO Authentication (Completa autenticazione SSO)

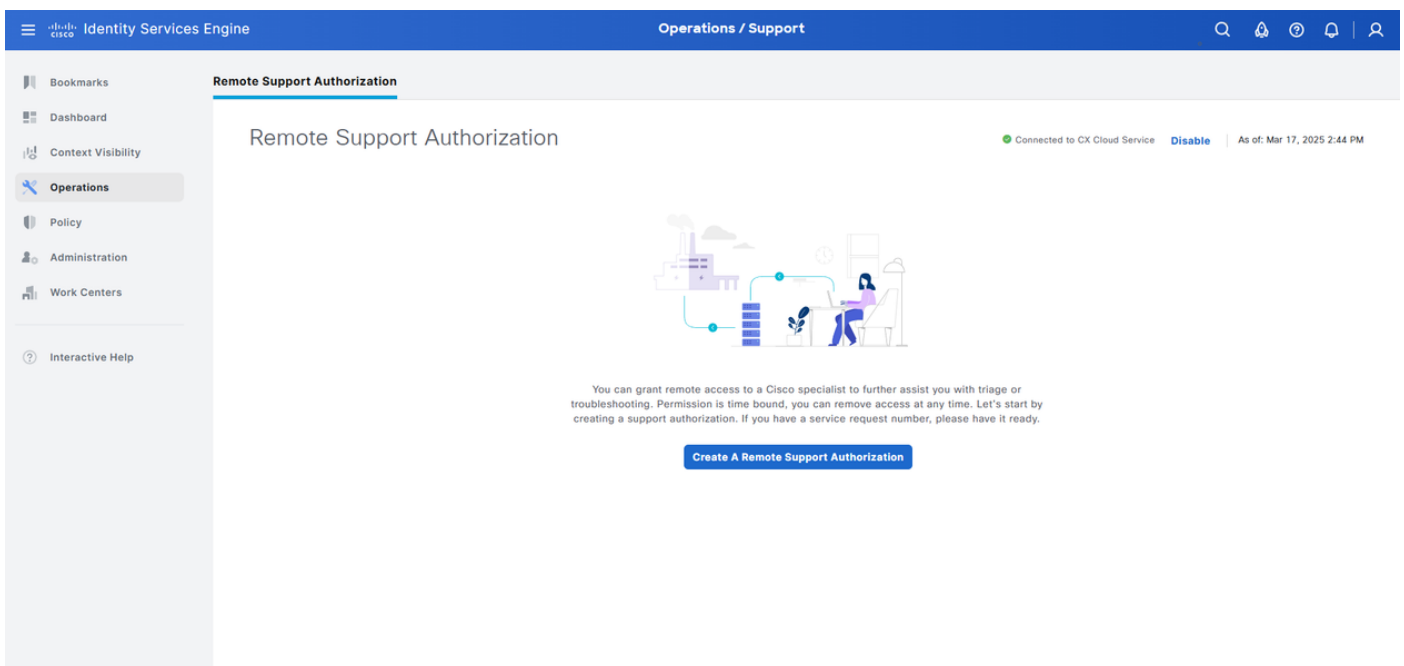
Fare clic **Accept** sulla finestra appena aperta per completare l'autorizzazione per il Cisco RADkit Cloud.



Pagina di autenticazione SSO in cui è stata completata l'autorizzazione

Configurare un'autorizzazione per il supporto remoto

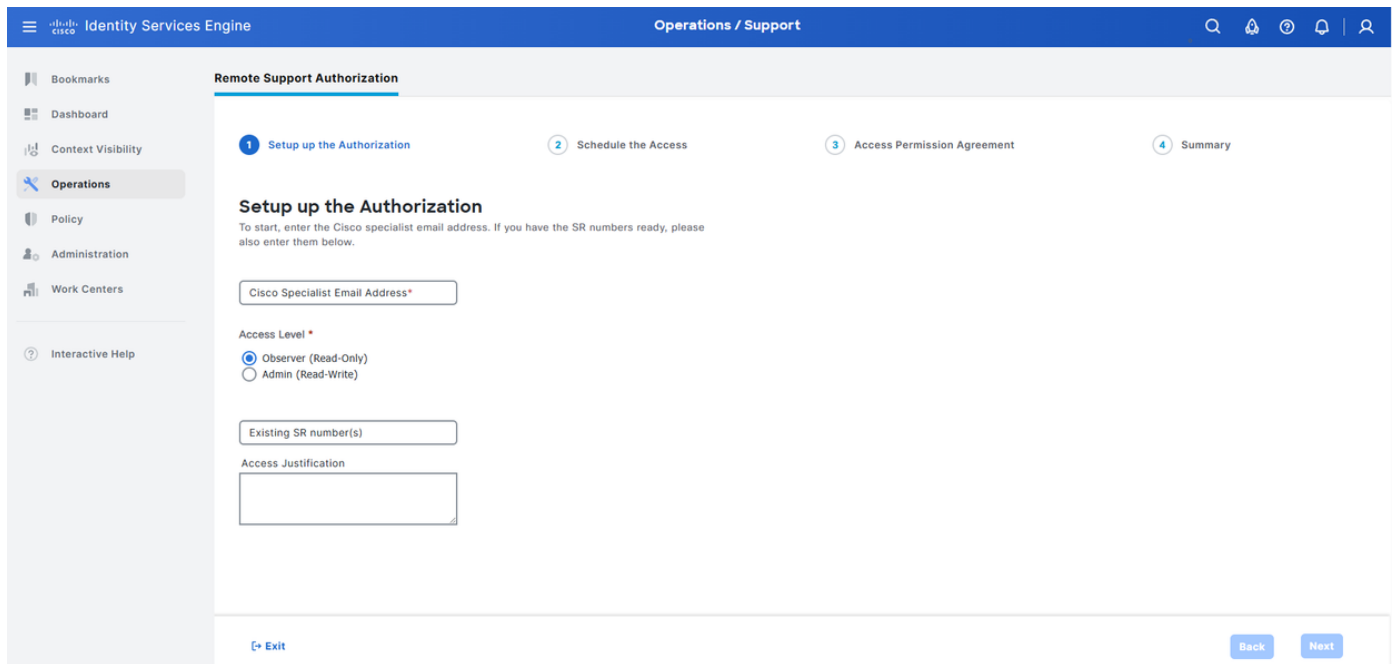
Fare clic **Create A Remote Support Authorization** su per configurare una sessione di accesso remoto.



Dopo l'autenticazione, viene visualizzata l'opzione Crea autorizzazione supporto remoto

Immettere l'indirizzo e-mail dello specialista Cisco a cui si desidera fornire l'accesso. Selezionare questa opzione **Observer (Read-Only)** per fornire un accesso in sola lettura allo specialista Cisco o **Admin (Read-Write)** per fornire un accesso completo in lettura/scrittura allo specialista Cisco. Se l'accesso è associato a una richiesta di servizio TAC esistente, è possibile immettere il numero SR e qualsiasi altra giustificazione per l'accesso remoto. Fare clic **Next** dopo aver immesso le informazioni richieste.

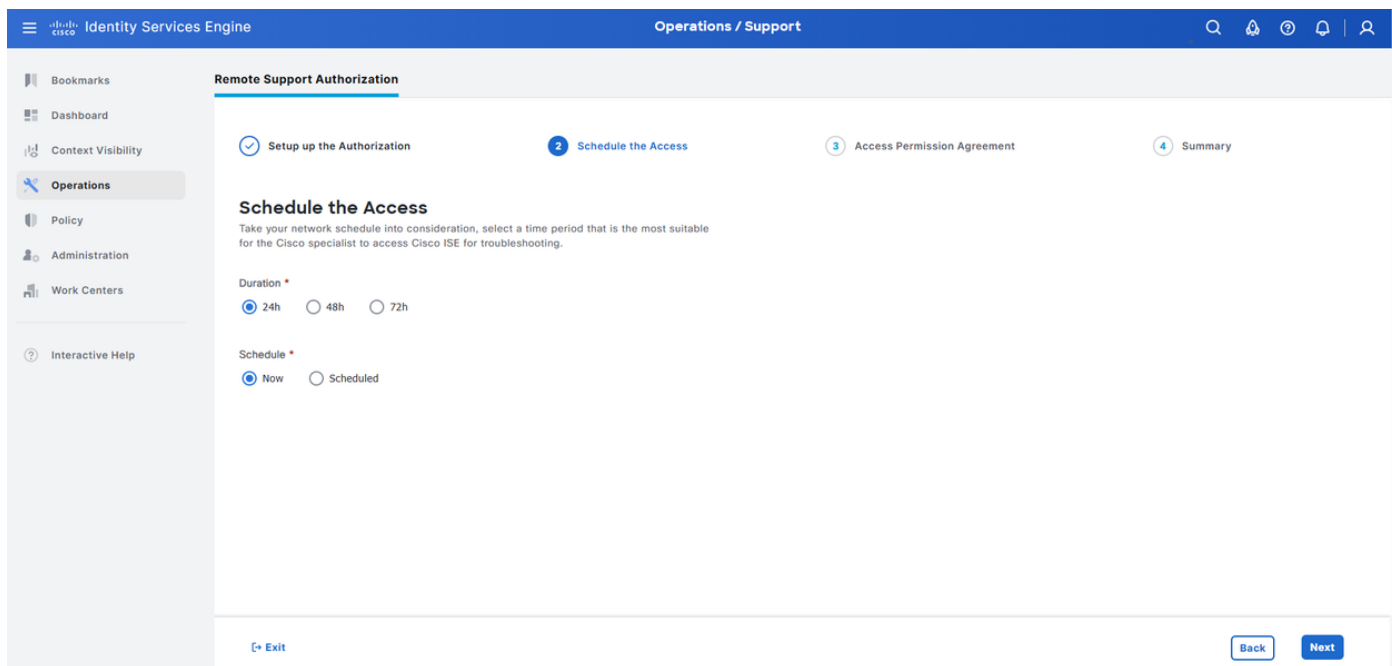
 Nota: Fornendo i numeri SR, TAC è in grado di caricare automaticamente i log raccolti senza alcun intervento. Inoltre, consente di documentare la connessione remota e i comandi nella SR.



The screenshot shows the 'Remote Support Authorization' section of the Cisco Identity Services Engine (ISE) interface. The page is titled 'Setup up the Authorization' and is the first step in a four-step process: 1. Setup up the Authorization, 2. Schedule the Access, 3. Access Permission Agreement, and 4. Summary. The instructions state: 'To start, enter the Cisco specialist email address. If you have the SR numbers ready, please also enter them below.' The form includes a text input 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 for 'Existing SR number(s)', and a text area for 'Access Justification'. Navigation buttons 'Exit', 'Back', and 'Next' are visible at the bottom.

Prima pagina di creazione autorizzazione

Pianificare la durata e i tempi dell'autorizzazione remota. Per pianificare l'accesso immediatamente, selezionare **Now**. Per pianificare l'accesso per una data o un'ora successiva, selezionare **Scheduled** e impostare le informazioni richieste in **Start Date** e fare **Start Time**. Clic su **Next** dopo aver immesso le informazioni richieste.



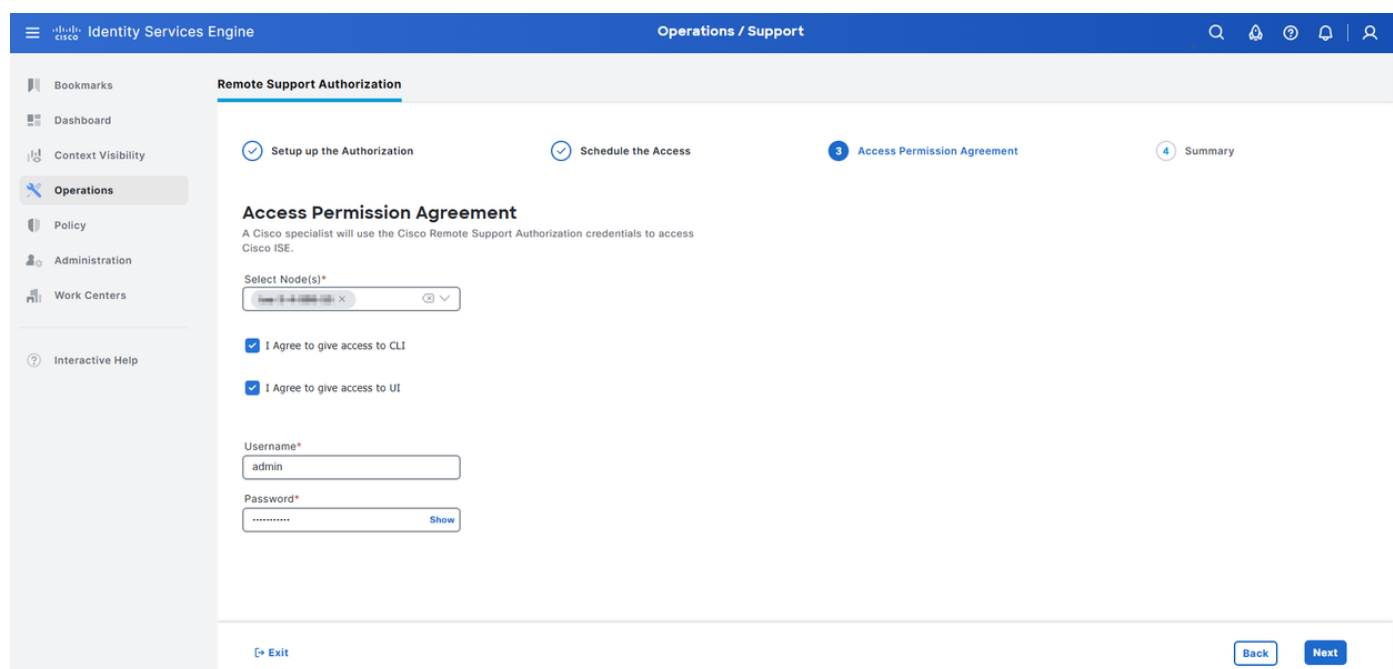
The screenshot shows the 'Schedule the Access' page in the Cisco Identity Services Engine (ISE) interface. The page is titled 'Schedule the Access' and is the second step in a four-step process: 1. Setup up the Authorization, 2. Schedule the Access, 3. Access Permission Agreement, and 4. Summary. The instructions state: 'Take your network schedule into consideration, select a time period that is the most suitable for the Cisco specialist to access Cisco ISE for troubleshooting.' The form includes a radio button selection for 'Duration' (24h is selected, 48h and 72h are unselected) and a radio button selection for 'Schedule' (Now is selected, Scheduled is unselected). Navigation buttons 'Exit', 'Back', and 'Next' are visible at the bottom.

Seconda pagina di creazione autorizzazione

Selezionare ciascun nodo ISE a cui si desidera dare accesso. Per abilitare l'accesso remoto CLI ai

nodì, selezionare **I Agree to give access to CLI**. Per abilitare l'accesso remoto UI ai nodi, selezionare **I Agree to give access to UI**. Fare clic su **Next** dopo aver immesso le informazioni richieste.

 **Nota:** Per consentire l'accesso all'interfaccia utente, è necessario configurare un nome utente e una password di amministratore dell'interfaccia utente. Questo account viene usato per creare un nuovo utente amministratore che lo specialista Cisco usa per accedere con il livello di accesso specificato, quindi l'account immesso deve avere le autorizzazioni necessarie per creare un nuovo account amministratore. Le credenziali devono essere per un utente amministratore interno a meno che Active Directory non sia configurato come origine dell'identità dell'interfaccia utente, nel qual caso è possibile utilizzare anche le credenziali di amministratore di Active Directory.



Identity Services Engine Operations / Support

Remote Support Authorization

1 Setup up the Authorization 2 Schedule the Access 3 Access Permission Agreement 4 Summary

Access Permission Agreement

A Cisco specialist will use the Cisco Remote Support Authorization credentials to access Cisco ISE.

Select Node(s)*

☒ I Agree to give access to CLI

☒ I Agree to give access to UI

Username*

admin

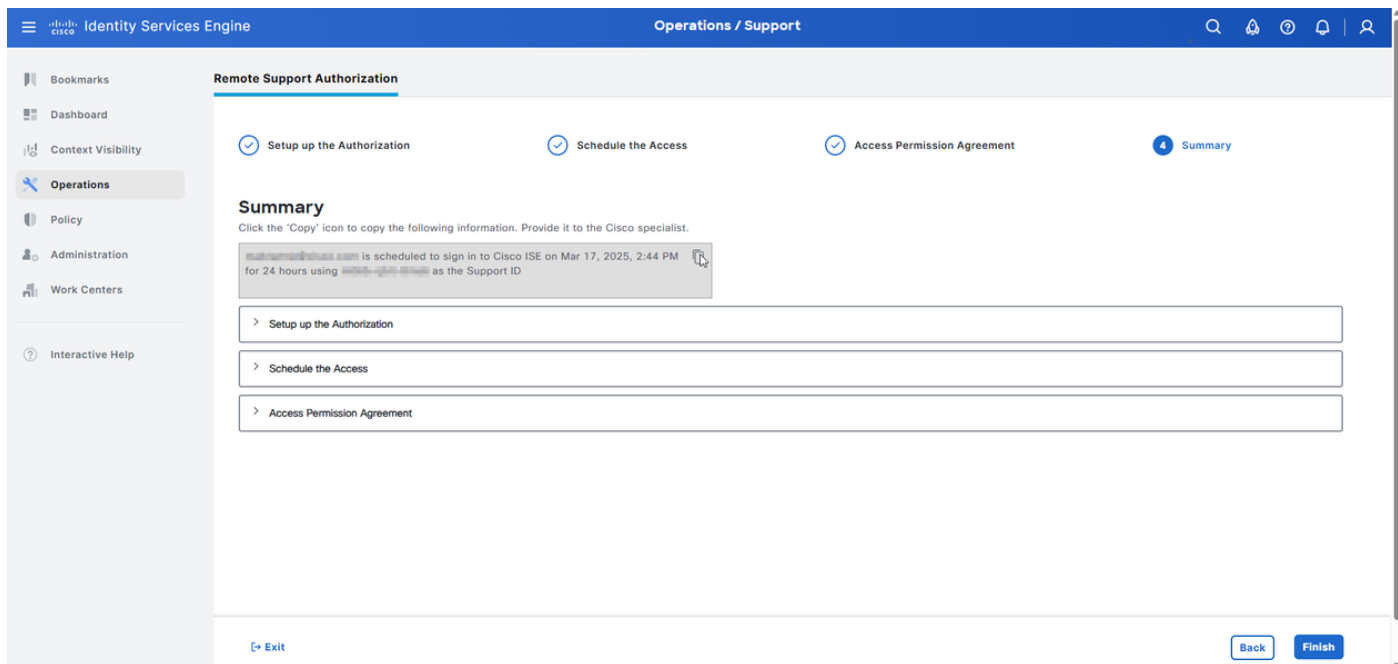
Password*

..... [Show](#)

[Exit](#) [Back](#) [Next](#)

Terza pagina di creazione autorizzazione

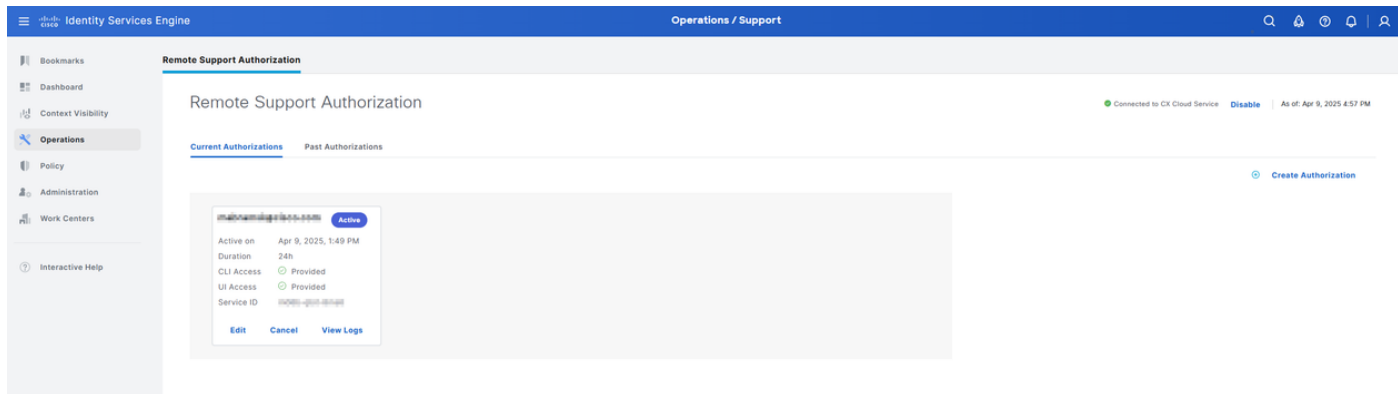
Fare clic sull'icona di copia per copiare le informazioni di autorizzazione del supporto remoto e fornirle allo specialista Cisco. Fare clic **Finish** per finalizzare l'autorizzazione di accesso remoto.



Pagina Riepilogo della creazione dell'autorizzazione

Verifica

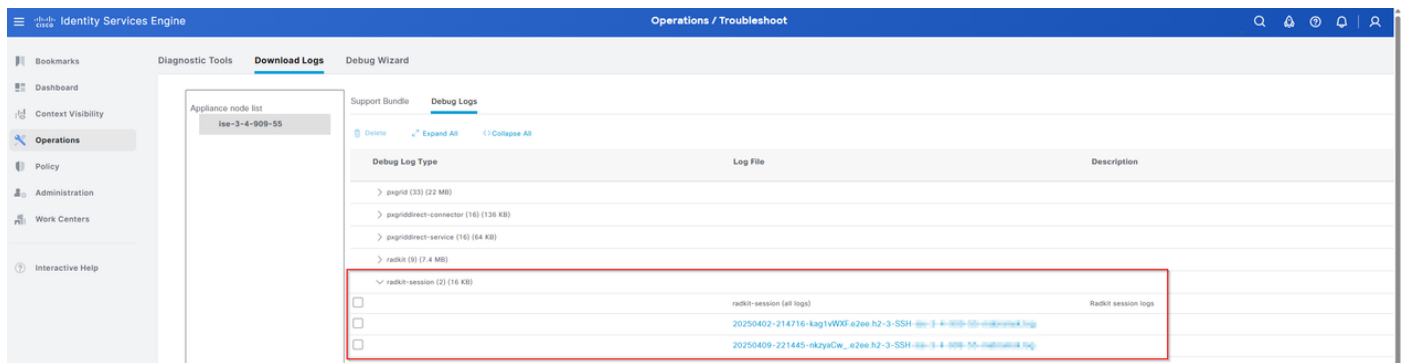
È possibile verificare tutte le autorizzazioni di supporto remoto attualmente attive nella **Current Authorizations** scheda. Nella **Past Authorizations** scheda è possibile visualizzare tutte le autorizzazioni di supporto remoto precedenti.



Verifica autorizzazioni attive

Per visualizzare i log di controllo delle sessioni CLI per un nodo, passare a **Operations > Support > Troubleshoot > Download Logs**, selezionare il nodo per il quale si desidera scaricare i log, quindi selezionare **Debug Logs**. Tutte le sessioni CLI sono disponibili nella cartella radkit-session. Fare clic sul nome del file per scaricare i log di controllo.

 **Nota:** Il monitoraggio delle sessioni CLI deve essere eseguito per nodo. Ogni nodo dispone di una propria cartella di sessioni radkit con registri di controllo specifici per il nodo.



Log di controllo CLI

Per visualizzare i log di controllo dell'interfaccia utente, è possibile utilizzare i report di controllo nell'interfaccia utente ISE. Passare alla sezione **Operations > Reports > Audit > Administrator Logins** per visualizzare gli accessi dell'amministratore all'interfaccia utente o alla CLI. Passare alla sezione **Operations > Reports > Audit > Change Configuration Audit** per visualizzare le modifiche apportate dagli amministratori nell'interfaccia utente.

 **Nota:** Gli specialisti Cisco che accedono all'interfaccia utente utilizzano il nome utente `<user>-CustomerSupport` dove `<user>` è il nome utente specificato nell'autorizzazione del supporto remoto. Gli specialisti Cisco che accedono alla CLI utilizzano il nome utente `customersupadmin` se dispongono dell'accesso Admin (lettura/scrittura) o `customersupreadonly` se dispongono dell'accesso Observer (sola lettura).

Risoluzione dei problemi

Per visualizzare i log sul contenitore a partire dal processo di configurazione iniziale in cui l'e-mail viene immessa nell'interfaccia utente, è necessario visualizzare il file `ADE.log`. Dalla CLI, immettere il comando `show logging system ade/ADE.log tail:`

```
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
```

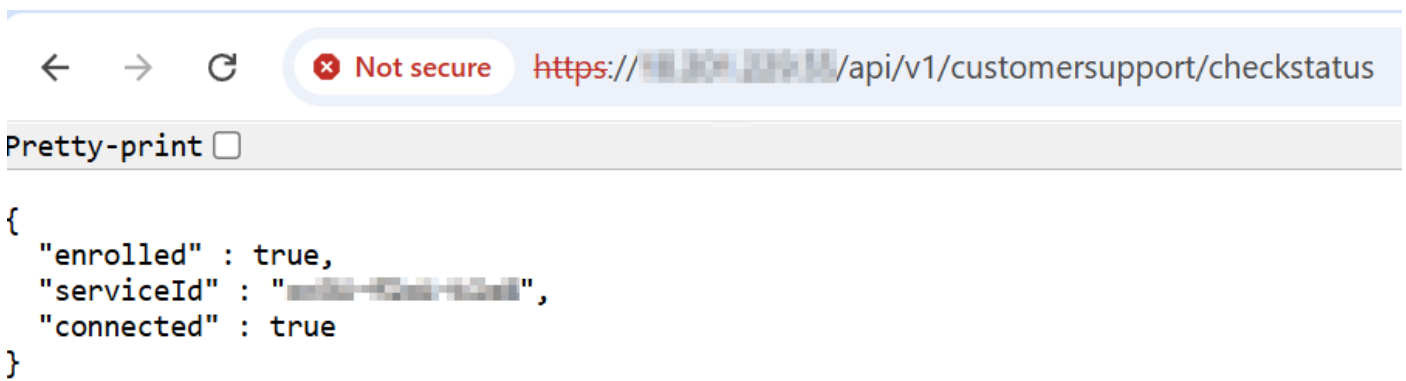
ISE esegue il monitoraggio del contenitore per verificare se è in esecuzione e se l'applicazione RADKit è pronta prima di contrassegnare il Servizio di autorizzazione remota come avviato.

```
2025-05-20T14:21:24.477946-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] Co
```

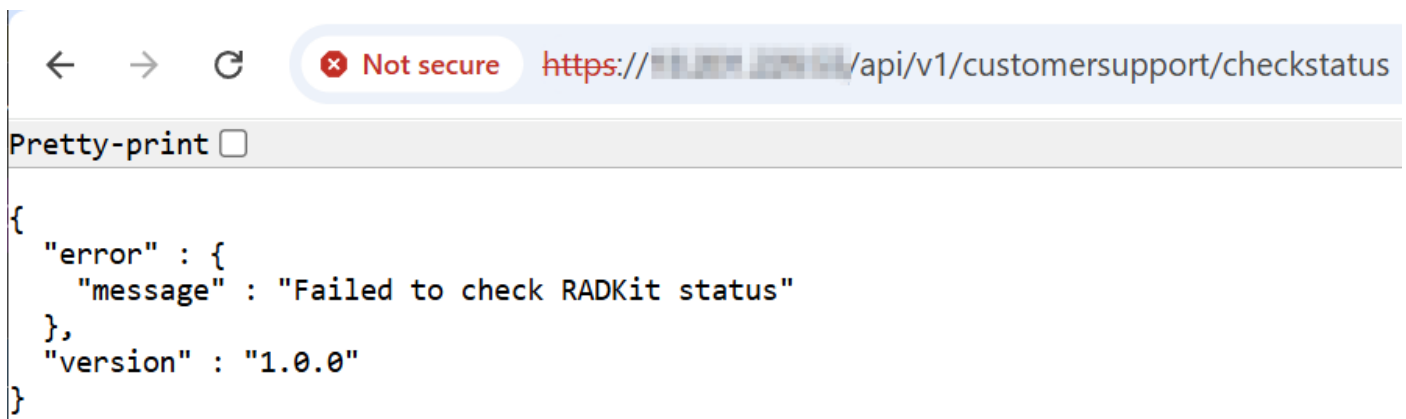
```
2025-05-20T14:21:24.800804-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] In
2025-05-20T14:21:24.804531-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] IS
2025-05-20T14:21:27.859691-05:00 ise-3-4-909-55 root: info:[application:operation:radkit-control.sh] 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
```

È inoltre possibile controllare lo stato del servizio RADKit utilizzando la chiamata API

<https://<ISE PAN>/api/v1/customersupport/checkstatus>.



Output quando il servizio RadKit è in esecuzione



Output quando il servizio RadKit non è in esecuzione

Per visualizzare i registri del servizio RADKit dopo l'avvio del Servizio di autorizzazione del supporto remoto, immettere il comando `show logging application radkit/service/service.log`. Quando il servizio viene avviato per la prima volta, viene eseguita una configurazione di base con l'applicazione RADKit.

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
```

Viene creato il servizio RADKit disponibile per le connessioni.

```
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
```

Quando si aggiunge un'autorizzazione al supporto remoto nella GUI, lo Specialist Cisco viene creato come utente remoto.

```
2025-05-20T19:24:10.599Z INFO | radkit_control/superadmin/5d496186 | MainThread DBOperationsAPI(0x7F92
2025-05-20T19:24:10.600Z INFO | radkit_control/superadmin/5d496186 | MainThread radkit_service.webserv
```

Quando lo specialista Cisco si connette al servizio e accede a un nodo ISE, viene mostrato in questi log.

```
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
```

Dopo la scadenza o la rimozione dell'autorizzazione remota, l'utente remoto viene eliminato dal servizio RADKit.

```
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
```

Informazioni correlate

- [Guida dell'amministratore di Cisco Identity Services Engine, versione 3.4](#)
- [Note sulla versione di Cisco Identity Services Engine, versione 3.4](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).