SIEMENS

Insights Hub

Remote Services (RS)

System Manual

04/2024

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ **DANGER**
indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ **WARNING**
indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ **CAUTION**
indicates that minor personal injury can result if proper precautions are not taken.

NOTICE
indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ **WARNING**
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

4/2024 Subject to change

Table of contents

Remote Services Overview and Key Concepts 1

1.1 Remote Services Overview and Key Concepts

Introduction

Remote Services (RS) is an Xcelerator cloud-based product, which provides IP-based network-to-network connectivity from one network, often termed as *Service Network*, which hosts the apps provided by the customer (e.g. engineering applications or remote control tools) to a separate network, often termed as *Factory Network* that hosts a number of field devices.
It is also possible to connect two different *Devices* with each other which reside in two different *Factory Networks*.
For example, an HTTPS connection from a browser in a *Service Network* to a PLC in a *Factory Network* which hosts an embedded webserver. Both networks have no direct connectivity with each other. However, two tunnels can be established through which the HTTPS traffic can flow between the browser and the PLC.
These customer-owned apps may use their own specific IP-based protocols (for communication, data transfer, streaming, login, browsing or messaging) for such access. RS will route these protocols transparently from one network to another via encrypted tunnels.
Such network-to-network access is further protected by modern Fine-Grained Access Control (FGAC) mechanisms which defines which users can access which devices via which protocols in which targeted device networks.

Communication Infrastructure provided by Insights Hub

The separate networks are securely connected by a communication infrastructure provided by Insights Hub.
From each network, a secure websocket connection will be established as a *tunnel* to a backend service in Insights Hub that acts as rendezvous point that connects both the tunnels and hence, the networks.

Access endpoints to the tunnels

The key functionality of routing a customer app's IP-based protocols from one network to another is built on tunnels. Such tunnels need endpoints at either end, which allows to establish

the tunnels.
Tunnel endpoints can be downloaded from Remote Services and are available for a number of operating systems and deployment scenarios (e.g. installable binary, docker image, IE application).
These endpoints are the only Remote Services components which need to be installed by the customers. The three different types of endpoints are as follows:

- Service Endpoint
- Device Endpoint
- Preinstalled Device Endpoints

Service Endpoint

The *Remote User* needs to install this endpoint once on the desired machine to use the applications. For example, TIA Portal, VNC, RDP, SSH clients and Web Browsers that remotely connects to the *Devices*. These applications need to communicate with the endpoint on ports that are defined by the Connector configuration. With different ports, it is possible to use different applications at the same time.
The download package of the endpoint also contains a unique user specific access key to the remote tunnel. It is automatically applied when the endpoint is installed.
It is possible to use the same download package on different machines, but not simultaneously.

Device Endpoints

These endpoints must be downloaded and installed on each *Device* of type *Primary Target* or *Gateway*. The download package contains a device specific access key which identifies the Device. *Devices* behind a *Gateway* do not need an *Endpoint* as they are accessed through the *Gateway*.
The user can either manually start the *Device Endpoint* on the device or configure it in OS level to automatically start the device.
For more information, refer to the chapter Creating Device Endpoints.

Preinstalled Device Endpoints

There are also MindConnect Agents equipped with pre-installed *Device Endpoints*. These pre-installed endpoints are activated through the Agent UI. To faciliate this, the *Agent Asset ID* must be provided when the Device is created in Insights Hub.

Connectors as blueprints of communication tunnels

RS supports a number of communication protocols that can be routed through the tunnel. These protocols are called *Connector Types*.
A user can create blueprints that describe use case specific communication tunnels from a selected *Connector Type*. In RS, such a blueprint is called *Connector*. The *Connector* is pre-configured with use case specific parameters (for example, IP addresses, ports user names, passwords, etc).

It is possible to create multiple *Connectors* derived from the same *Connector Type*, but with different parameters in the same *Organization*. These *Connectors* can then later be assigned to concrete *Devices* to prepare them for establishment of a tunnel on demand.
For more information, refer to chapter Remote Services Connectors.

Users and Roles

Every Remote Services user is also a user within the Insights Hub tenant that has the Insights Hub role *serviceowner* or *orguser*.
Additionally, Remote Services has its own concept of Users and Roles. A user can be created from within Remote Services as member of an *Organization*. Each user can be assigned one or more Remote Services roles that control access to *Devices* and a defined subset of Remote Services functionality.
These user roles in Remote Services are defined as follows:

Organization Owner

The users who are not created in the scope of an *Organization* can be referred to become members of the organization. These users are known as *External Users*.
The *Organization Owner* has the authority to decide if the referral can be accepted or rejected. Additionally, *Organization Owner* can also suspend or remove the *External Users* from the organization when they are no longer required in the organization.

Organization Admin

This role enables a user to set up an *Organization* that contains all the infrastructure. This Organization can be later used by a *Remote User* to establish a connection between *Service Network* and *Factory Network*.
The *Organization Admin* has the rights to perform the following steps:

- Defines a logical structure of Nodes, Sites and Products and adds devices to that structure. The logical structure is used for *Fine Grained Access Control*.
- Creates *Connectors* with a use case specific configuration and assigns them as needed to the devices.
- Creates users within the *Organization* and assigns one or multiple *Remote Services Role(s)* to them.

Remote User

This role enables a user to select a device and establish a connection between that device and a Service network using one of the *Connectors* assigned by the *Organization Admin*. In addition, the Remote User has the File Transfer capabilities. File Transfers does not need connectors, but just need Device Endpoint.

Site Owner

A connector can be configured to require the consent of a user with *Site Owner* role to establish the tunnel.

Summary on Users and Roles

- The users with the roles *Organization Admin* and *Remote User* are the ones that perform the day-to-day work on Remote Services.
- The *Organization Admin* sets up the infrastructure and extends or removes elements as needed.
- The *Remote User* accesses the prepared sites and devices through the predefined communication tunnels to perform the business task.

Organizations

The functionality of Remote Services is built upon the concept of Organizations.
Users with the Insights Hub role `Service Provider` can create organizations as needed. The organizations are separated from each other.
An organization consists of the following:

- one or more nodes and sites
- a collection of one or more product types
- a collection of *Connectors*
- one or more devices which reside in a particular site
- a collection of users which can perform a various tasks within the organization

In order to place *Devices* into the *Organization*, at least one *Site* needs to be part of the *Organization*.
The definition of a *Product Hierarchy* is optional as each newly created Organization by default already contains the top-level Product `All`.

Service Provider Organization

This *Organization* is automatically created when the Remote Services is provisioned to the Insights Hub tenant. It is the home organization for all users with the Insights Hub role `rsv2 serviceowner`. It can be used like any other *Organization*.

Fine Grained Access Control

This concept allows to enforce separate access permissions to devices, information and Remote Services functionality for different users, even with a single tenant. This is achieved across four different dimensions of access permission.

Access Control through Organizations

Organizations provide separation of access to information and devices on tenant level.

Access Control through Remote Services Roles

The Remote Services roles control access to Remote Services functionality. Depending on the role, a user within an Organization can only perform specific tasks.

Access Control through Nodes and Sites

With *Nodes* and *Sites*, a tree structure can be defined. *Devices* are the leaves on that tree because they are directly placed under a specific site.
When a user is assigned a specific role, access has to be granted as well to specific branches of this tree. Hence, the user potentially gets access to all devices on those branches of the tree.
That concept provides an attribute that can be used to classify access to devices on an *Organization* Level.
The Nodes and Sites not necessarily have to represent geographical location, but can be used to express any desired logical structure, e.g. departments, teams etc.

Access Control through Products

Similarly, a tree of *Product* classes can be defined.
When a user is assigned a specific role, access has to be granted as well to specific branches of this Product tree. Hence, the user potentially gets access to all devices on those branches of the Product tree.
This concept provides an attribute for a *Device* within an *Organization* but independent of its relationship with *Nodes* or *Sites* and can be used to further classify access permission.
Products actually has no explicit meaning related to Product types as such, but could also be used to model any other logical grouping within the whole Organization independent of *Nodes* and/or *Sites*.

Combining the Dimensions Controls Access

When a user who is part of a certain organization is given a role, the user will also be assigned permissions to certain Products and Sites and/or Nodes.
It is the intersection of these two dimensions *Nodes* / *Sites* on one hand and *Product* on the other hand that controls the access within the organization.

Example Scenario

- There is an Organization **X**.
- Within that Organization **X**, there are users **A**, **B**, **C** and **D**.
- There is a Node **Europe**.
- There are the Sites **Germany** and **Italy**, which are placed under the Node **Europe**.
- There are the Products **Pump** and **Heater**.

- There are the following Devices:
  - **K** of Product **Pump** in Site **Germany**
  - **L** of Product **Heater** in Site **Germany**
  - **M** of Product **Pump** in Site **Italy**
  - **N** of Product **Heater** in Site **Italy**

User **A** has the role *Organization Admin* for Node **Europe** in the Organization and all *Products*.
User **B** has the role *Organization Admin* for *Site* **Germany** in the Organization and all *Products*.
User **C** has the role *Remote User* for *Site* **Italy** in the Organization and all *Products*.
User **D** has the role *Remote User* for Node **Europe** in the Organization and *Product* **Heater**.
Thereby, the following access grants are defined:

- All these users have access only for the Organization **X**.
- User **A** has access to all devices and can define and assign *Connectors* to them. **A** also can add or delete *Devices* on any *Site* within the *Organization*.
- User **B** has access to devices **K** and **L** and can define and assign *Connectors* to them. **B** also can add or delete *Devices* to/from Site **Germany**.
- User **C** has access to *Devices* **M** and **N** and can select an assigned *Connector* and establish a tunnel.
- User **D** has access to devices **L** and **N** and can select an assigned *Connector* and establish a tunnel.

Devices

Definition

The purpose of a *Device* is to provide certain functionality, e.g. a web server, a machine control system, a compute node etc. The purpose of Remote Services (RS) is to provide access to the Device from a network for which there is no direct IP connectivity.
In RS, a *Device* is the representation of a software process that operates as a *Device Endpoint*, i.e. terminates one side of a tunnel connection.
Often, it is a real piece of hardware, where a *Device Endpoint* executable is installed and running, but it could also be a Docker container on a Docker host.
Typically, the *Device* is part of a Factory Network that is connected through RS to a *Service Endpoint* in a *Service Network*. However, it is also possible to connect two *Devices* in two different *Factory Networks* via two different *Device Endpoints* using the *DTT-R* connector.

Device Types

There are three types of *Devices*:

- *Primary Target*, which has an IP address within the *Factory Network* and a *Device Endpoint* installed through which it is accessed by RS.
- *Gateway*, which also has an IP address within the *Factory Network* and a *Device Endpoint* installed through which it is accessed by RS.
  - The *Gateway* provides access to one or many *Secondary Targets*.
  - The *Gateway* is configured in RS with the IP addresses of the *Secondary Targets*. However, it is still required that on OS level in the *Gateway*, the required routing is defined.
- *Secondary Target*, which has an IP address in a network that is only accessible through the related *Gateway*. It has no *Device Endpoint* installed and is connected to RS only through the *Device Endpoint* on the related *Gateway*.
  - An example of *Secondary Targets* are PLCs that are connected to a MindConnect Nano which acts as a *Gateway*.

Defining Connectivity via Connectors

An *Organization Admin* defines the type of connectivity that will be available to *Remote Users* to a given *Device*.
This is done by assigning one or more *Connectors* to a *Device*.
An example use case is to provide SSH access to a MindConnect Nano through assignment of an *SSH Connector* to the MindConnect Nano, thereby allowing access for TIA portal to an S7-1500 that is connected as *Secondary Target* behind the MindConnect Nano which acts as *Gateway*. A *Proxy Unaware Connector* is assigned to the S7-1500. Additionally, it is possible to assign a *Web Application Connector* to the S7-1500 to provide access to an embedded webserver on the S7-1500.
The *Connectors* enable only the connectivity to a service on a *Device* but not the service functionality itself.
So in this example, it is the S7-1500 which hosts the control functionality which shall be provisioned by TIA portal and the embedded webserver.

Access Control

A *Device* is always created in a specific *Site*. As grants to access specific *Sites* are given to RS users, this implies that only those users which have grants for a specific *Site* can access the related *Devices*.
A *Device* is always classified as a specific *Product*. As grants to access specific *Products* are given to RS users, this implies that only those users which have grants for a specific *Product* can access the related *Devices*.
For more information on access control through *Sites* and *Product Types*, refer to the chapter Fine Grained Access Control.

Getting Started 2

2.1 Remote Services Getting Started

This chapter explains the usage of Remote Services. To simplify the setup, the *Service Provider Organization* which was automatically created when the Remote Services have been provisioned to the tenant will be used.

The goal is to connect two Windows machines with a Remote Desktop Protocol (RDP):

- Machine **A** acts as an RDP client in a *Service Network*.
- Machine **B** acts as a *Device* in a *Factory Network* and hosts an RDP server.

All interactions with *Insights Hub* and the *Remote Services* application shall be performed from machine **A**.

Prerequisites

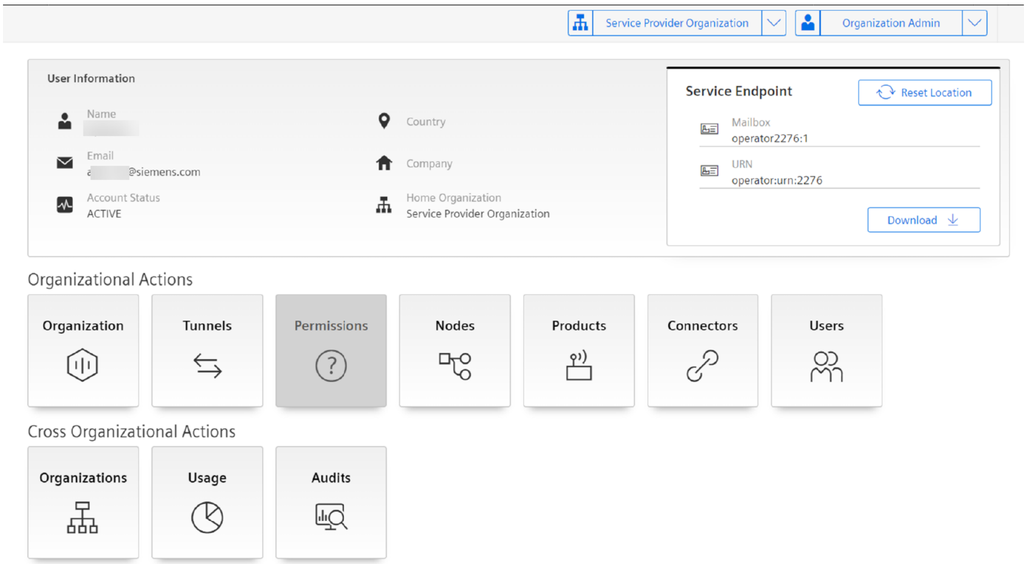
- An Insights Hub user with Insights Hub Role `rsv2 serviceowner`.
- Machine **A** has an RDP client installed.
- Machine **B** has an RDP server installed and enabled.

Procedure

Log in

1. From machine **A**, log into the tenant as a user with `rsv2 serviceower` role.

2. Open the "Remote Services" app.



User Information

Name [redacted]

Email [redacted]@siemens.com

Account Status ACTIVE

Country

Company

Home Organization Service Provider Organization

Service Endpoint

Mailbox operator2276:1

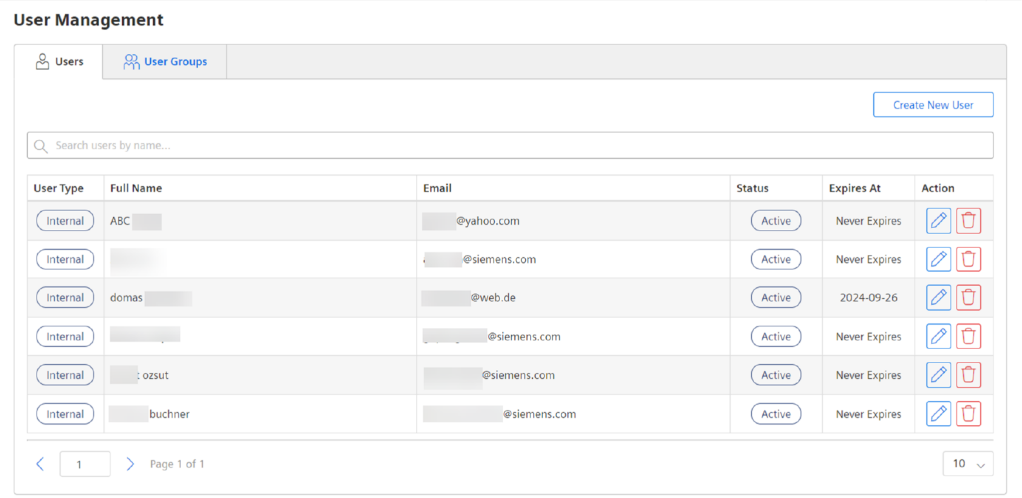
URN operator:urn:2276

3. From the "Home" screen of the app, select the *Service Provider Organization* from the Organization drop-down menu and select the *Organization Admin* role from the role drop-down menu.

Update user information

Now, the user needs to update the user information:

1. Click on the "Users" icon in the "Organizational Actions" section. The "Users" screen is displayed which displays the list of all the existing users within the organization.



User Management

User Type	Full Name	Email	Status	Expires At	Action
Internal	ABC [redacted]	[redacted]@yahoo.com	Active	Never Expires	
Internal	[redacted]	[redacted]@siemens.com	Active	Never Expires	
Internal	domas [redacted]	[redacted]@web.de	Active	2024-09-26	
Internal	[redacted]	[redacted]@siemens.com	Active	Never Expires	
Internal	[redacted] ozsut	[redacted]@siemens.com	Active	Never Expires	
Internal	[redacted] buchner	[redacted]@siemens.com	Active	Never Expires	

2. Search for the current user and click on the "Edit" icon in "Action" column. The "User Information" page opens.

3. Click "Update User Information".

4. Enter the required information and click "Update".

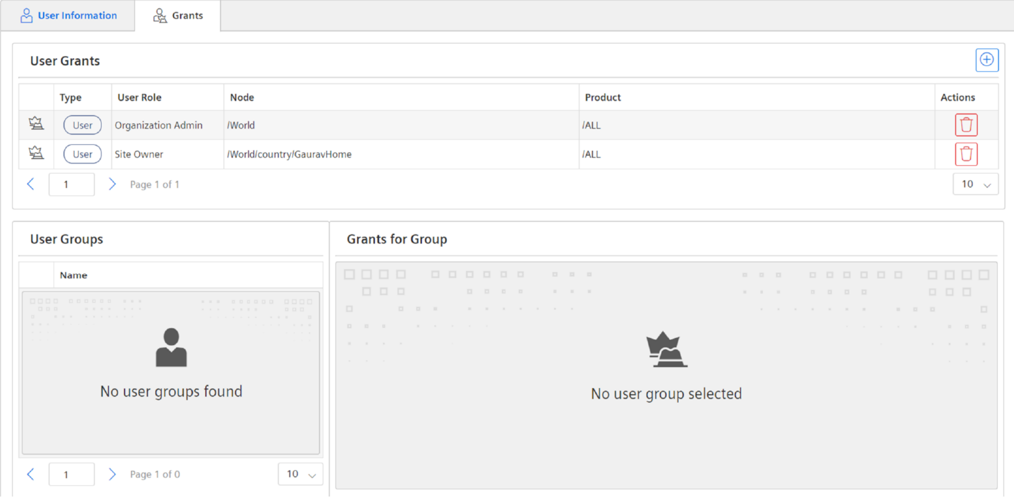
It is important to enter the Country information as this value is checked against the IP address when *Service* and/or *Device Endpoints* shall be downloaded.

For more information, refer the chapter Setting up users and access.

Acquire the additional role *Remote User*

Now, the user needs to acquire the additional role `Remote User`, as described in chapter Setup users and access.

1. In the "Users" screen, click the "Grants" tab. The "Grants" screen displays all the grants, including roles of the current user.



User Grants

	Type	User Role	Node	Product	Actions
	User	Organization Admin	/World	/ALL	
	User	Site Owner	/World/country/GauravHome	/ALL	

User Groups

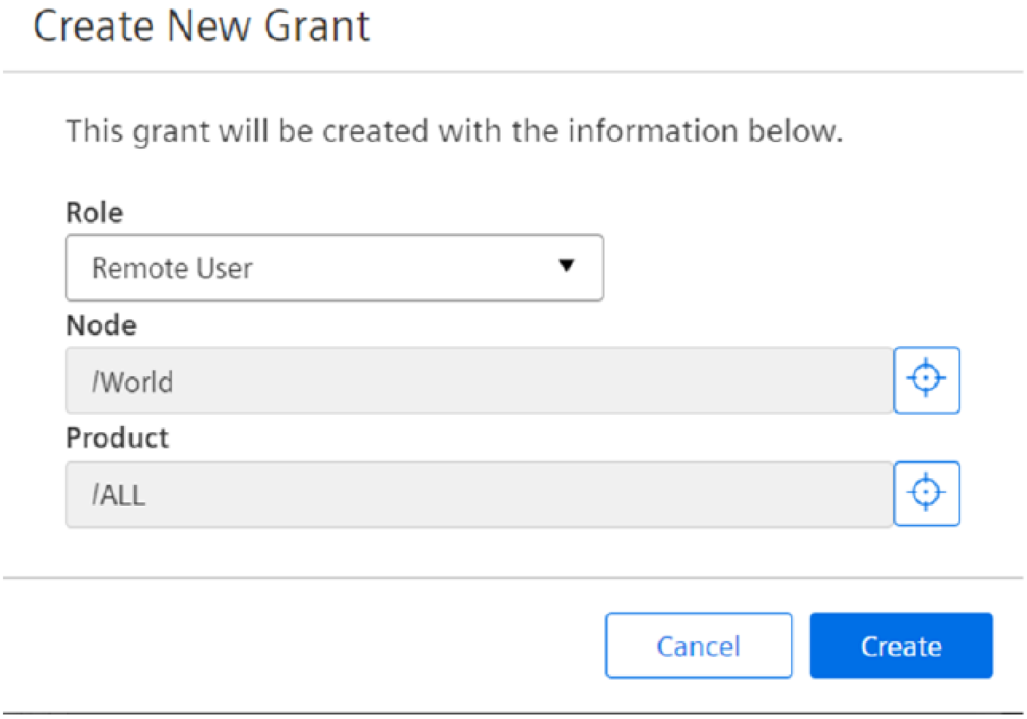
Name

No user groups found

Grants for Group

No user group selected

2. Click on the "Create" icon. The "Create New Grant" pop-up window appears.



Create New Grant

This grant will be created with the information below.

Role: Remote User

Node: /World

Product: /ALL

3. From the "Role" drop-down menu, select "Remote User".

4. Click on the "Search" icon in the "Node" field.

5. Select "World" which grants access to all *Nodes* and *Sites* in that Organization.

6. Click on the "Search" icon in the "Product" field.

7. Select "All" which grants access to all *Product* in that Organization.

8. Click "Add Grant".

Add *Site* to the Organization which will host the *Devices*

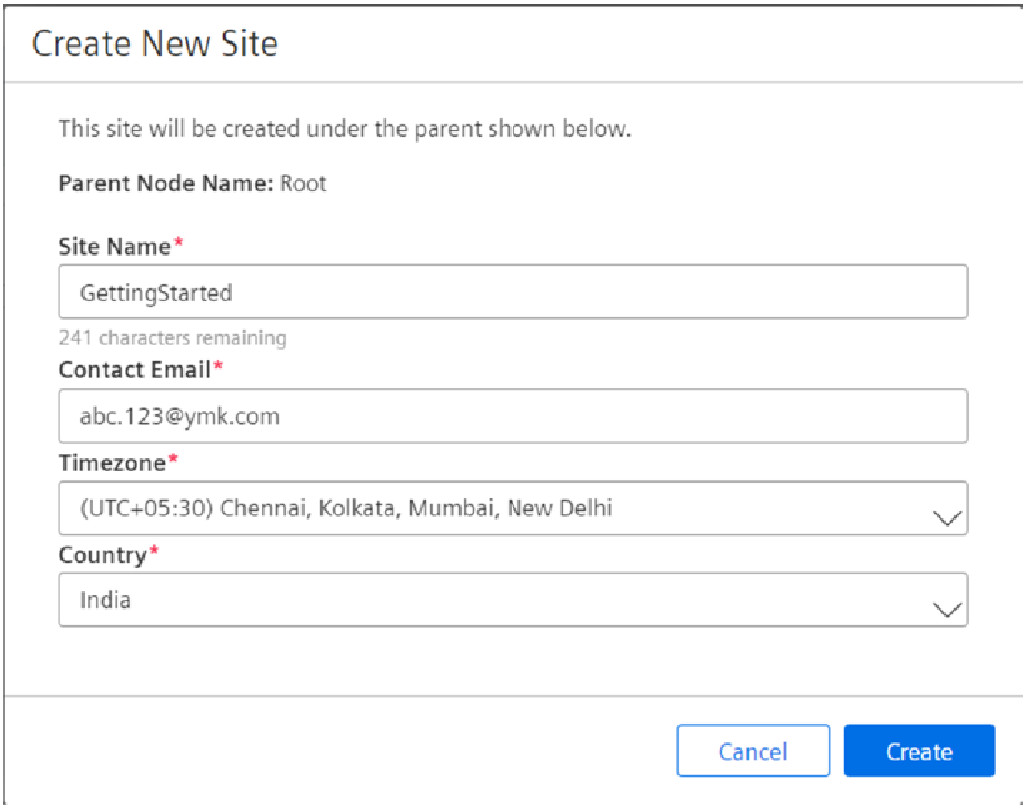
Now, a *Site* needs to be added to the Organization which will host the *Devices*, as described in the chapter Creating a structure hierarchy.

1. Click on the "Home" icon of the "Remote Services" application.

2. Click "Nodes" in the "Organizational Actions" section.

3. Click "Create New Site under Root". The "Create New Site" pop-up window appears.

4. Enter the required information. For name, use `GettingStarted` and click "Create".



Create New Site

This site will be created under the parent shown below.

Parent Node Name: Root

Site Name*

GettingStarted

241 characters remaining

Contact Email*

abc.123@ymk.com

Timezone*

(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Country*

India

Add *Device* to the *Site*

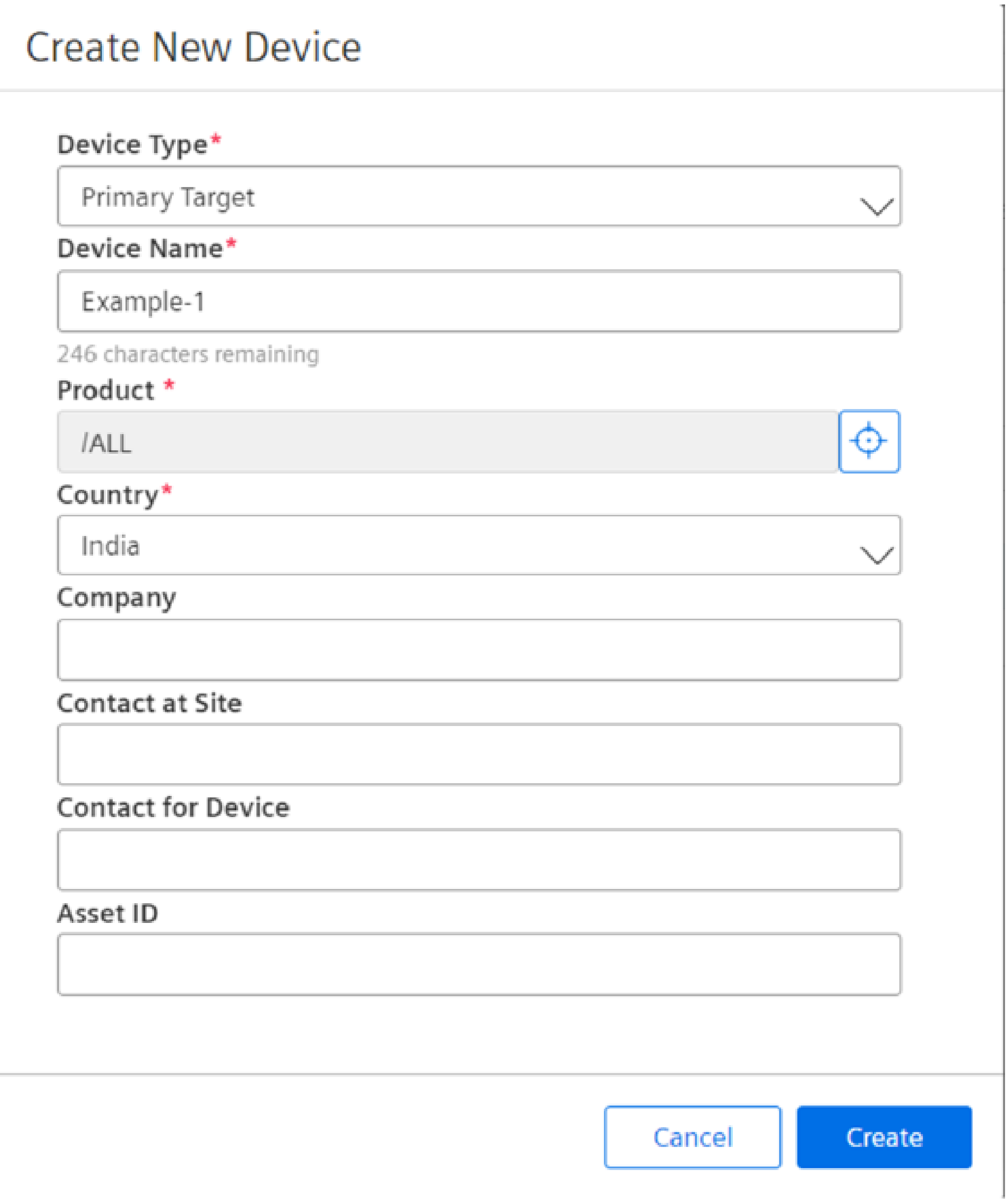
Now, a *Device* shall be added to the *Site* that was created, Adding Devices to an existing organization.

1. Click on the "Home" icon of the "Remote Services" application.

2. Click on "Organization" icon in the "Organizational Actions" section.

3. In the "Node and Site hierarchy", navigate to the site `GettingStarted`.

4. In the "Site Information" section, click "Create Device". The "Create New Device" pop-up window appears.



Create New Device

Device Type*
Primary Target

Device Name*
Example-1

246 characters remaining

Product *
/ALL

Country*
India

Company

Contact at Site

Contact for Device

Asset ID

5. From the "Device Type" drop-down, select "Primary Target". For "Product", select "All" from the drop-down and enter all the other mandatory information. For the "Device Name", use `Example-1` and click "Create".

Create *Device* and download *Device Endpoint*

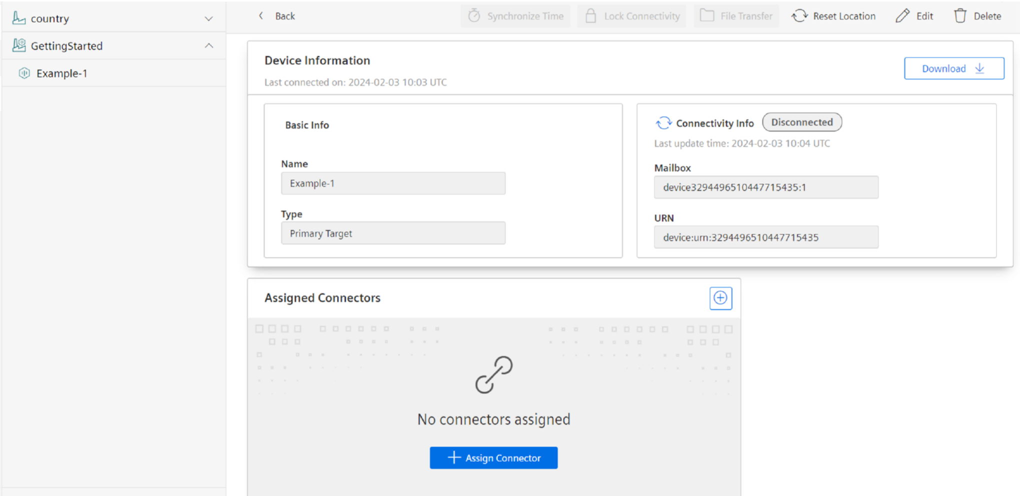
Now, the *Device* is created and the *Device Endpoint* needs to be downloaded, as described in the chapter Download the device endpoint.

1. Click on the "Home" icon of the "Remote Services" application.

2. Click on "Organization" icon in the "Organizational Actions" section.

3. In the "Node and Site hierarchy", click on `Example-1`. The "Device Information" screen for `Example-1` is displayed.

4. Click on the "Download" button.



Device Information

Last connected on: 2024-02-03 10:03 UTC

Basic Info

Name: Example-1

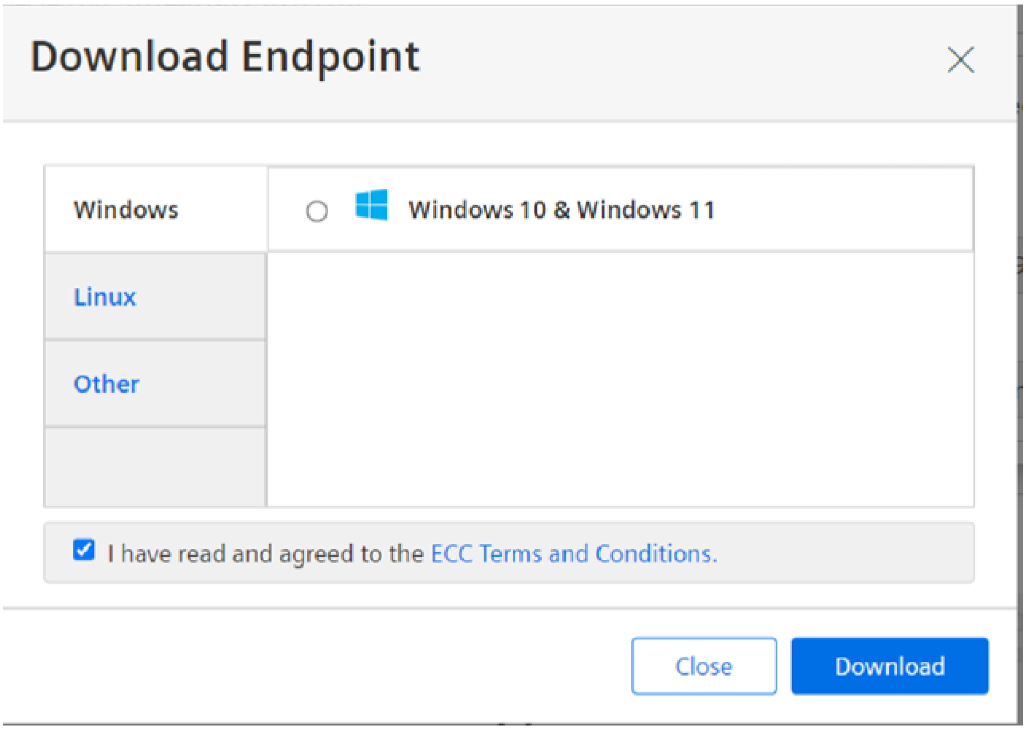
Type: Primary Target

Last update time: 2024-02-03 10:04 UTC

Mailbox: device32944965104477715435:1

URN: device:urn:32944965104477715435

5. The "Download Endpoint" pop-up appears which offers various versions of *Device Endpoints*.



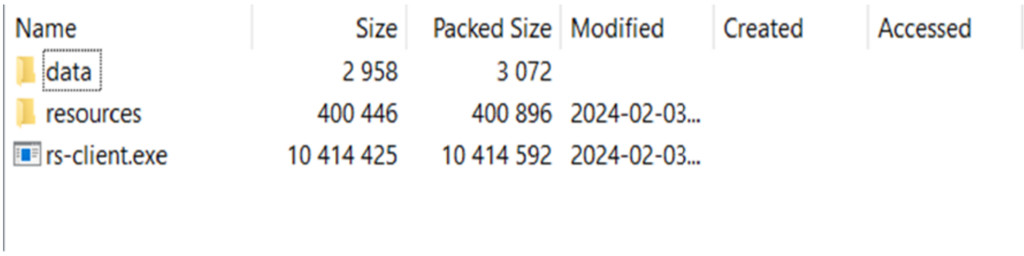
○ Windows 10 & Windows 11

☑ I have read and agreed to the ECC Terms and Conditions.

6. Accept the ECC terms and conditions by checking the checkbox next to it.

7. In this example, let us assume the *Device* is a Windows 10/11 machine. Select "Windows 10 & Windows 11" and click "Download".

8. An archive is downloaded which not only contains the *Device Endpoint* executable, but also the device and tenant specific authentication information.



Name	Size	Packed Size	Modified	Created	Accessed
data	2 958	3 072			
resources	400 446	400 896	2024-02-03...		
rs-client.exe	10 414 425	10 414 592	2024-02-03...		

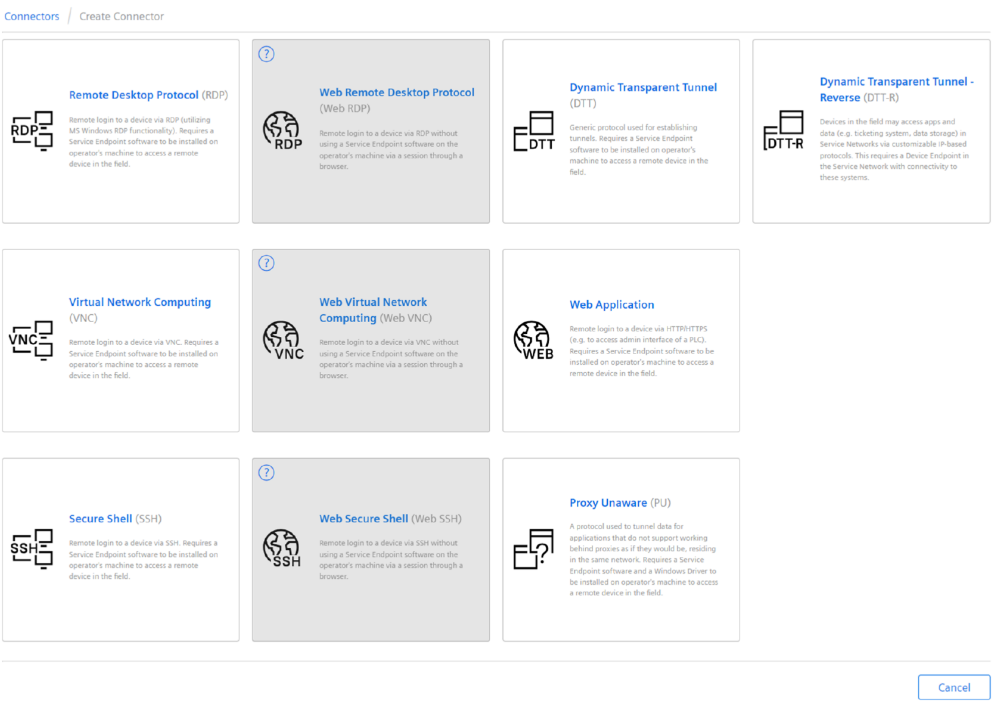
Define *RDP Connector* in the *Organization*

Now, a *Connector* needs to be defined in the *Organization* so that it can be later assigned to the *Device*, as described in chapter Adding a connector.

1. Click on the "Home" icon of the "Remote Services" application.

2. Click on "Connectors" icon in the "Organizational Actions" section. The "Connectors Overview" screen appears.

3. Click "Create New Connector". The "Create Connector" screen with a selection of protocols is displayed.



Remote Desktop Protocol (RDP)
Remote login to a device via RDP (utilizing MS Windows RDP functionality). Requires a Service Endpoint software to be installed on operator's machine to access a remote device in the field.

Web Remote Desktop Protocol (Web RDP)
Remote login to a device via RDP without using a Service Endpoint software on the operator's machine via a session through a browser.

Dynamic Transparent Tunnel (DTT)
Generic protocol used for establishing tunnels. Requires a Service Endpoint software to be installed on operator's machine to access a remote device in the field.

Dynamic Transparent Tunnel - Reverse (DTT-R)
Devices in the field may access apps and data (e.g. ticketing system, data storage) in Service Networks via customizable IP-based protocols. This requires a Device Endpoint in the Service Network with connectivity to these systems.

Virtual Network Computing (VNC)
Remote login to a device via VNC. Requires a Service Endpoint software to be installed on operator's machine to access a remote device in the field.

Web Virtual Network Computing (Web VNC)
Remote login to a device via VNC without using a Service Endpoint software on the operator's machine via a session through a browser.

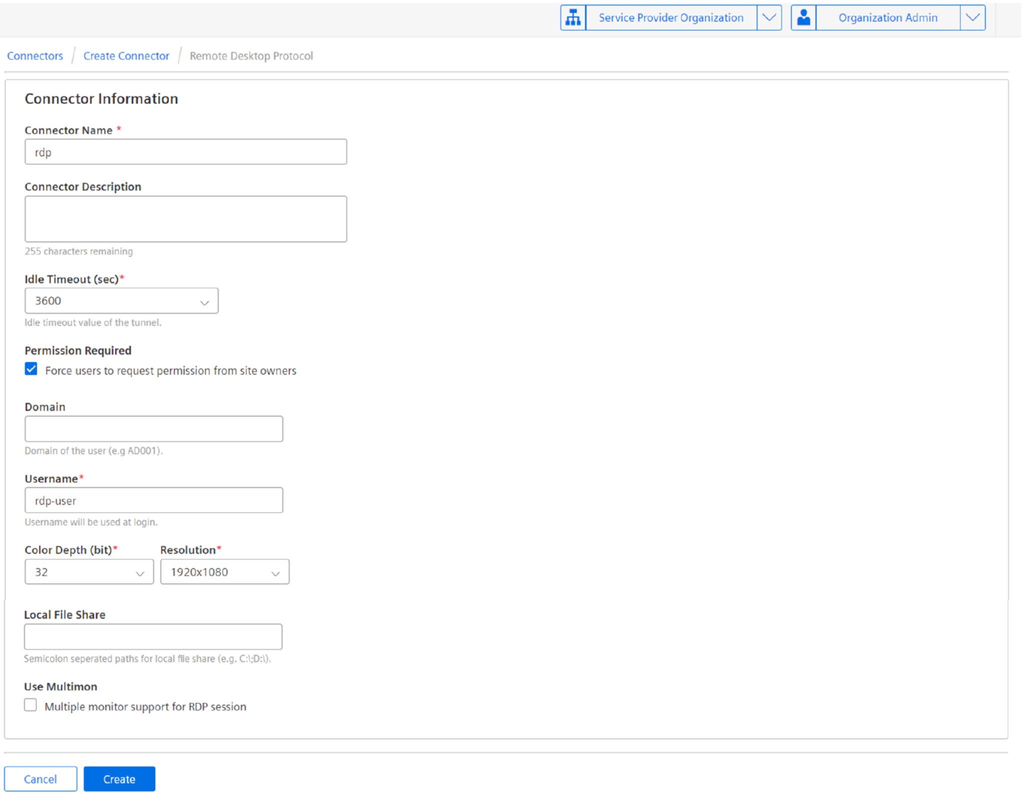
Web Application
Remote login to a device via HTTP/HTTPS (e.g. to access admin interface of a PLC). Requires a Service Endpoint software to be installed on operator's machine to access a remote device in the field.

Secure Shell (SSH)
Remote login to a device via SSH. Requires a Service Endpoint software to be installed on operator's machine to access a remote device in the field.

Web Secure Shell (Web SSH)
Remote login to a device via SSH without using a Service Endpoint software on the operator's machine via a session through a browser.

Proxy Unaware (PU)
A protocol used to tunnel data for applications that do not support working behind proxies as if they would be, residing in the same network. Requires a Service Endpoint software and a Windows Driver to be installed on operator's machine to access a remote device in the field.

4. Click on "Remote Desktop Protocol" as described in chapter Create RDP Connector.



Connectors / Create Connector / Remote Desktop Protocol

Connector Information

Connector Name *: rdp

Connector Description:

255 characters remaining

Idle Timeout (sec)*: 3600

Idle timeout value of the tunnel.

Permission Required

☑ Force users to request permission from site owners

Domain:

Domain of the user (e.g AD001).

Username*: rdp-user

Username will be used at login.

Color Depth (bit)*: 32

Resolution*: 1920x1080

Local File Share:

Semicolon seperated paths for local file share (e.g. C:\;D:\).

Use Multimon

□ Multiple monitor support for RDP session

5. A screen to configure the RDP connection is displayed.

6. Enter the required values and click "Create".

Assign RDP Connector to the Device

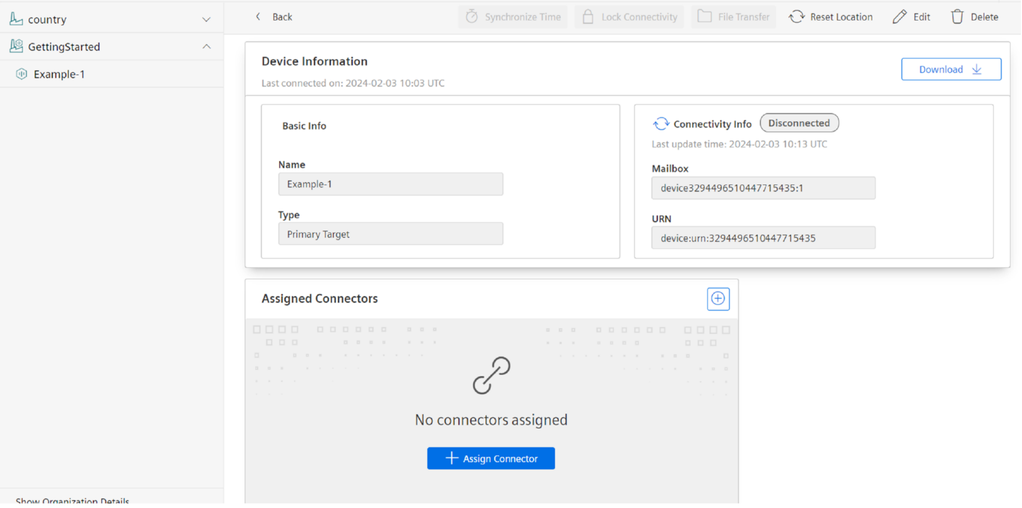
Now, the configured RDP *Connector* needs to be assigned to the *Device*, as described in chapter Assign Connectors

1. Click on the "Home" icon of the "Remote Services" application.

2. Click on "Organization" icon in the "Organizational Actions" section.

3. In the "Node and Site hierarchy", click on `Example-1`. The "Device Information" screen for `Example-1` is displayed.

4. Click on the "Assign Connector" button.



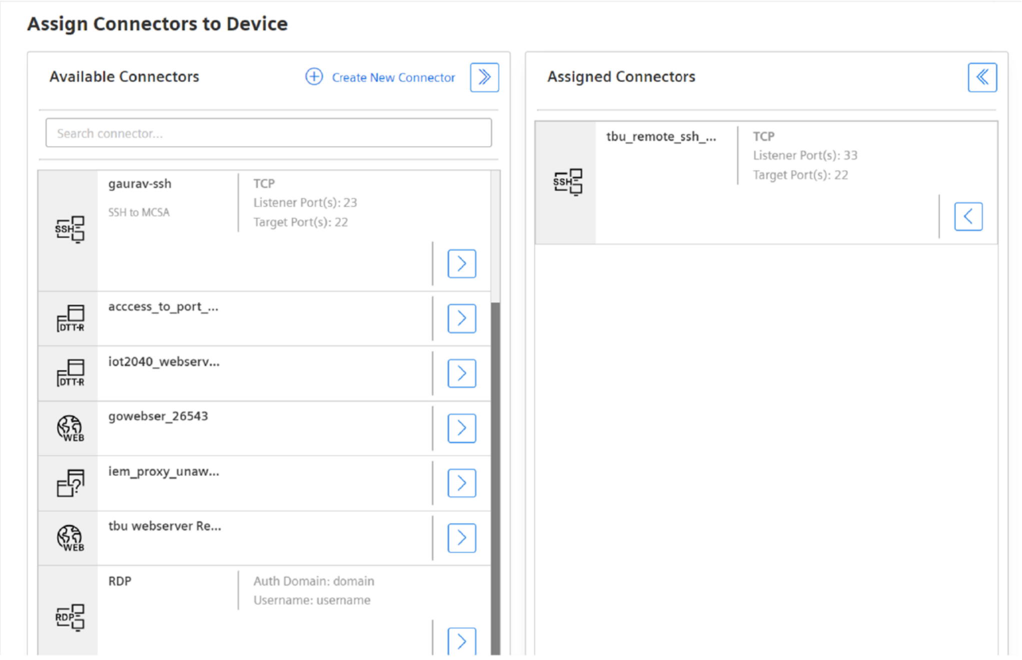
Device Information
Last connected on: 2024-02-03 10:03 UTC

Name: Example-1
Type: Primary Target

Last update time: 2024-02-03 10:13 UTC
Mailbox: device3294496510447715435:1
URN: device:urn:3294496510447715435

5. The "Available Connectors" screen for the *Organization* and `Example-1` is displayed.

6. Select the entry for the RDP *Connector* in the section "Available Connectors" and click on > button to add it to the "Assigned Connectors" section.



Available Connectors:
- gaurav-ssh — SSH to MCSA — TCP, Listener Port(s): 23, Target Port(s): 22
- acccess_to_port_...
- iot2040_webserv...
- gowebser_26543
- iem_proxy_unaw...
- tbu webserver Re...
- RDP — Auth Domain: domain, Username: username

Assigned Connectors:
- tbu_remote_ssh_... — TCP, Listener Port(s): 33, Target Port(s): 22

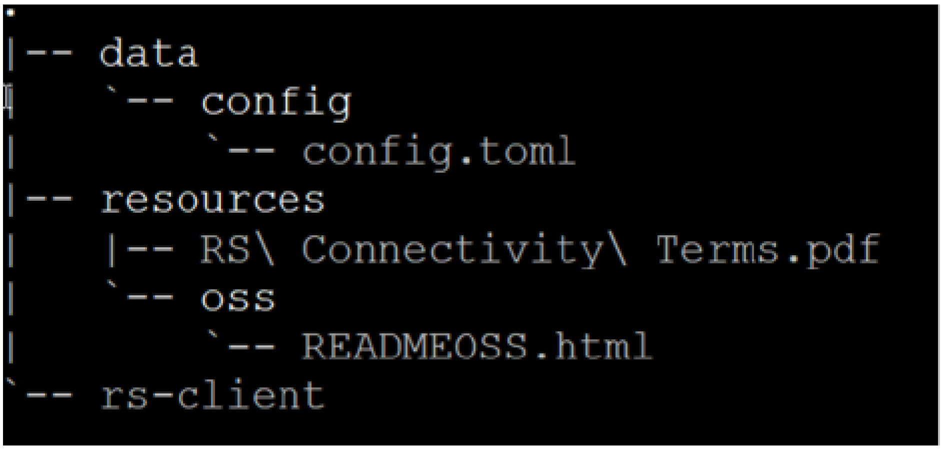
7. Click "Save".

Install Device Endpoint on machine B

Now, the *Device Endpoint* needs to be installed on machine **B**, as described in chapter 4.3. This can be done by anyone who has access to machine B and does not require a user in Insights Hub.

1. Copy the archive to machine **B** which shall be used as *Device*.

2. On that *Device*, extract the archive. A folder structure will be created which contains the executable `rs-client.exe` at the top level.



```
.
|-- data
|   `-- config
|       `-- config.toml
|-- resources
|   |-- RS\ Connectivity\ Terms.pdf
|   `-- oss
|       `-- READMEOSS.html
`-- rs-client
```

3. Click on `rs-client.exe` to start the *Device Endpoint*. If required, you can use Windows auto-start capabilities to start the *Device Endpoint* whenever the user logs into machine **B**.

Now, the Service Endpoint needs to be downloaded as described in chapter Download the service endpoint and installed as described in chapter Installing and Starting the Service Endpoint on machine **A**. This is done with the Role **Remote User** and needs to be done only once.

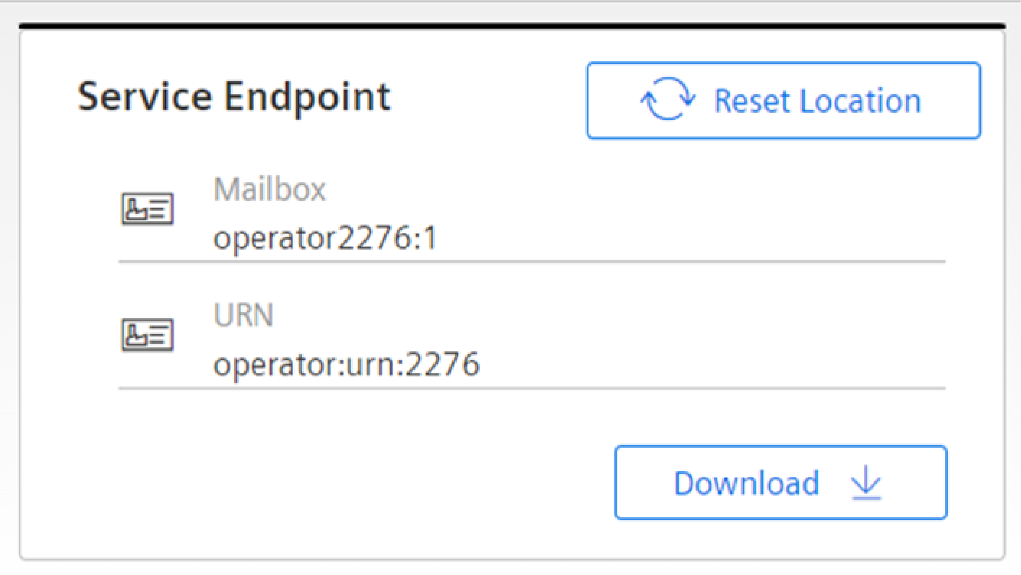
Download Service Endpoint

Now, the Service Endpoint needs to be installed on machine **A**. This is done with the Role `Remote User` and needs to be done only once.

1. Click on the "Home" icon of the "Remote Services" application.

2. Select the "Remote User" role in the "Roles" drop-down menu.

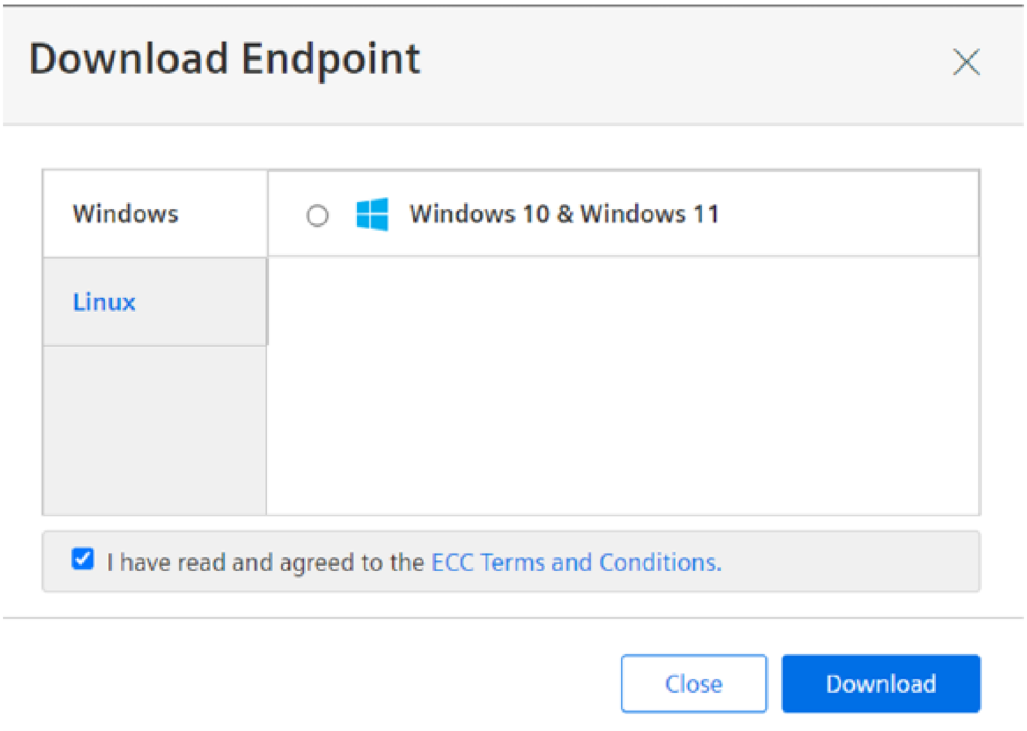
3. In the "Service Endpoint" section, click on "Download".



Mailbox
operator2276:1

URN
operator:urn:2276

4. The "Download Endpoint" pop-up is displayed.



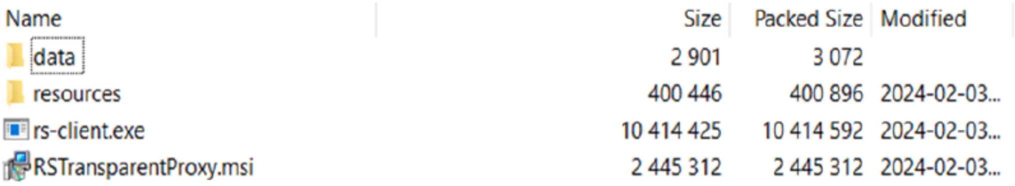
☑ I have read and agreed to the ECC Terms and Conditions.

5. Check the acceptance of the ECC terms and conditions.

6. Select the Windows version of the endpoint and click "Download".

7. An archive is downloaded which not only contains the *Service Endpoint* executable but also the endpoint and tenant specific authentication information. The archive contains also an Windows installer for a transparent proxy which is only required for the *Proxy Unaware Connector*.

8. Extract the archive. A folder structure will be created which contains the executable `rs-client.exe` at top-level.



Name	Size	Packed Size	Modified
data	2 901	3 072	
resources	400 446	400 896	2024-02-03...
rs-client.exe	10 414 425	10 414 592	2024-02-03...
RSTransparentProxy.msi	2 445 312	2 445 312	2024-02-03...

All the steps until now needs to be performed only once to set up the desired infrastructure for future use.

Create Remote Services tunnel between machines A and B

Now, the Remote Services tunnel can be created between machines **A** and **B** as described in chapter Establish Connections.
This is done with the Role `Remote User` and needs to be performed every time such a connection is required. This assumes that the *Device Endpoint* on machine **B** has been manually

started by someone who has access to machine **B** or is automatically started by Windows.

1. Navigate to the folder on machine **A** where the *Service Endpoint* was installed.

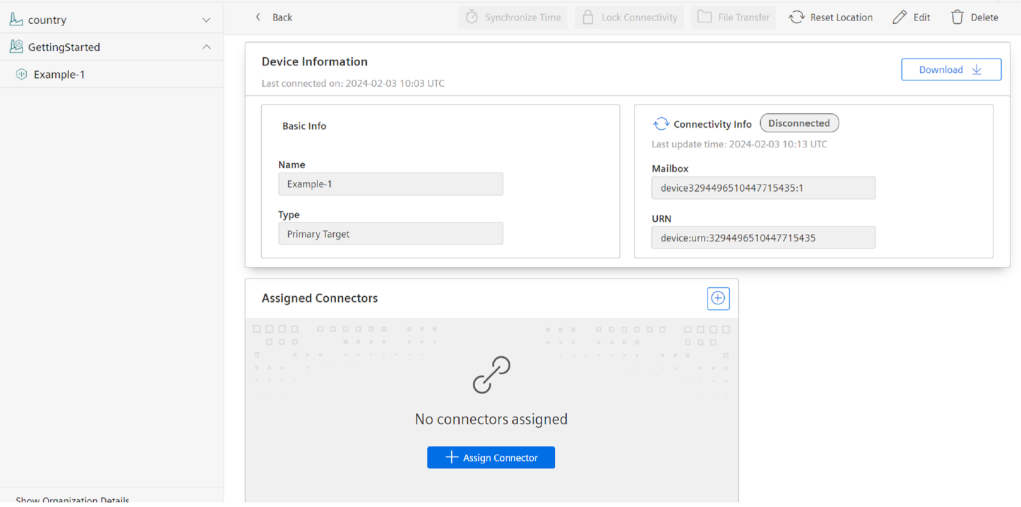
2. Click on `rs-client.exe` to start the *Service Endpoint*.

3. Click on the "Home" icon of the "Remote Services" application to come back to the "Home" screen.

4. Select the `Remote User` role in the "Roles" drop-down menu.

5. Click on the "Organization" icon in the "Organizational Actions" section.

6. In the "Node and Site hierarchy", click on `Example-1`. The "Device Information" screen for `Example-1` is displayed.



Device Information

Last connected on: 2024-02-03 10:03 UTC

Basic Info

Name: Example-1

Type: Primary Target

Connectivity Info: Disconnected

Last update time: 2024-02-03 10:13 UTC

Mailbox: device3294496510447715435:1

URN: device:urn:3294496510447715435

Assigned Connectors

No connectors assigned

7. In the "Assigned Connectors" section, search for the "RDP Connector".

8. Click on the "Connect" icon.

The RDP Client application starts automatically.

Setting up a New Organization 3

3.1 Setting up a new organization

Create an organization

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` is required.

Procedure

To create a new organization, follow these steps:

1. Log into tenant as a user with `rsv2 serviceowner` role.

2. Open the "Remote Services" app.

3. From the "Home" screen of the app, click the "Organizations" icon in the "Cross Organizational Actions" area. The "Manage Organizations" app screen opens.

4. Click on the "Create New Organization" button.

5. In the pop-up, enter a name for the new organization and click "Create".

Result

- A new empty organization is created.
- The user who created the organization becomes `Organization Owners` and *Organization Admin* of this organization. Currently, this is the only user in the organization.
- The new organization becomes visible in the Organizations drop-down list of the home screen, but only for that particular user.

Creating a structure hierarchy

The structure hierarchy consists of a tree of Nodes and Sites. Nodes can appear anywhere in the hierarchy while Sites are the leaves of the tree. It is possible to have also *Sites* at the root level of the organization.
Nodes and Sites form one dimension of Fine Grained Access Control (FGAC) to devices.

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser` is required.
- An organization must already exist.
- The user must have the Remote Services role `Organization Admin` granted with access to this organization.

Procedure

To create a structure hierarchy within an organization, follow these steps:

1. Log into tenant as one of the users mentioned above.

2. Open the "Remote Services" app.

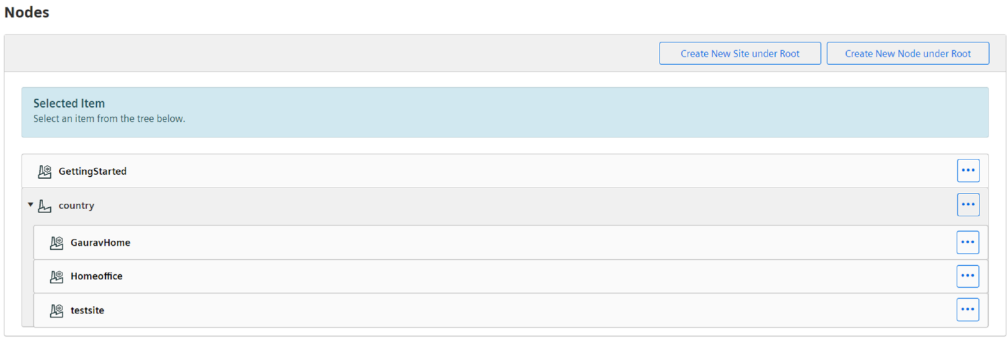
3. From the "Home" screen, select the required organization from the "Organizations" drop-down list and from the "RS Roles" drop-down, select the `Organization Admin` role.

4. Click on the "Nodes" icon.

5. The "Nodes" app screen appears. Either,
    - Click on the "Create New Site To Root" button to add a "Site" to the top level of the organization or,
    - Click on the "Create New Node To Root" button to add a "Node" to the top level of the organization or,
    - Select an existing Node and click on the *3 horizontal dots* icon to display a sub-menu and add a new "Site" or "Node" below the selected Node.

Result

- A structure hierarchy within the organization is created.
- The Nodes and Sites can be used to specify Fine Grained Access Control for devices within the organization.
- *Devices* can be assigned to the *Sites*.



Nodes

Selected Item
Select an item from the tree below.

Creating a product hierarchy

The product hierarchy consists of a tree of *Products*. *Products* form one dimension of *Fine Grained Access Control* to devices.

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser` is required.
- An organization must already exist.
- The user must have the Remote Services role `Organization Admin` granted with access to this organization.

Procedure

To create a product hierarchy within an organization follow these steps:

1. Log into tenant as one of the users mentioned above.

2. Open the "Remote Services" app.

3. From the "Home" screen, select the desired organization from the "Organizations" drop-down list and from the "RS Roles" drop-down select the *Organization Admin* role.

4. Click on the "Products" icon.

5. The "Products" app screen appears. Either,
   - Click "Create New Product To Root" to add a *Product* to the top level of the organization. Or
   - Select an existing Product and click on the *3 horizontal dots* icon to display a submenu where one can select to add a new *Product* below the selected Product.

Result

- A product hierarchy within the organization is created.
- The Products can be used to specify Fine Grained Access Control for devices within the organization.

Adding a Connector to the Organization

Connectors are the building blocks for the communication Tunnels to and from Devices. A Connector is an instance of a particular Connection Protocol class configured with the desired values for protocol parameters required for the usage of the connection (e.g. usernames, passwords, IP addresses, ports etc). It is merely a blueprint of a *Tunnel* that shall be established on demand.

It is possible to have multiple *Connectors* of the same *Connection Protocol* class in the organization with different parameters to fullfill different use cases.

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser` is required.
- An organization must already exist.
- The user must have the Remote Services role `Organization Admin` granted with access to this organization.

Procedure

To add *Connectors* to an organization follow these steps:

1. Log into tenant as one of the users mentioned above.

2. Open the "Remote Services" app.

3. From the "Home" screen, select the desired organization from the "Organizations" drop-down list and from the "RS Roles" drop-down select the `Organization Admin` role.

4. Click on the "Connectors" icon.

5. The "Connectors Overview" app screen opens which shows the list of already existing connectors within the organization.
    - Click on the "Create New Connector" button to add a "Connector" to the organization

6. The "Add Connector" app screen opens which shows the list of supported Connection Protocols.
    - Click on the icon that represents the desired "Connection Protocol".

7. The configuration app page for the selected "Connection Protocol" opens.
    - Enter the parameter values of the selected protocol according to the required use case.

Result

- A new Connector is available throughout the organization which can be assigned to any of the Devices within the organization. The same Connector can be assigned to multiple Devices.

Handing over an organization

The Service Provider who has created an organization automatically becomes an External User in that organization with Remote Services Roles `Organization Owner` and `Organization Admin`. This `Service Provider` has full control over the new organization.

In some cases, this might not be applicable. For example, when an organization belongs to another legal entity.

The following procedure describes how the organization can be handed over to an internal user of the organization.

Prerequisites

- An Insights Hub user **A** with Insights Hub Role `rsv2 serviceowner`.
- An organization **X** must already exist.
- The user must have created this organization.
- An internal user must have been created within that organization.

Procedure

1. Log into tenant as one of the user **A**.

2. Open the "Remote Services" app.

3. From the "Home" screen, select organization **X** from the "Organizations" drop-down list and from the "RS Roles" drop-down, select the `Organization Owner` role.

4. In the section "Organizational Actions", click on the "Organization" icon. The "Organization Owner Overiew" screen appears.

5. Click on the "Add New Organization Owner" button. The "Add new Organization Owner" screen appears where all users of the organization are listed.

6. Select the line with the user that shall become `Organization Owner` for that organization and click "Select". The details of the selected user is displayed.

7. Click on the "Add" button to promote this user to `Organization Owner`. The "Organization Owner Overiew" screen opens again.

8. Select the line with user **A** and click on the "Delete" button to remove the `Organization Owner` of organization **X**. However, this does not remove user **A** from the organization X.

To remove the user **A** completely from organization **X**, refer to Remove an external user from an organization by a Service Provider.

Summary

In this chapter, it has been shown how to set up an organization with all the elements required to manage access to devices and prepare connections to a from the devices:

- Nodes and Sites form the structure of the organization
- Products allow to classify potential Devices

These elements appear in the definition of users grants which control on which devices a particular user within the organization can establish connection Tunnels.

- Connectors are the blueprints of Tunnels that shall be established on Devices.

After all these procedures the organization is ready to be populated by Devices.

For more information, refer to the chapter Working with devices.

Working with Devices 4

4.1 Working with Devices

Adding Devices to an existing Organization

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser` is required.
- An organization must already exist.
- The user must have the Remote Services role *Organization Admin* granted with access to this organization.
- There is at least one *Site* defined in the Organization.
- There is at least one *Product* defined in the Organization. By default, this can be the top level *Product* **ALL**.

Procedure

To add *Devices* to an organization, follow these steps:

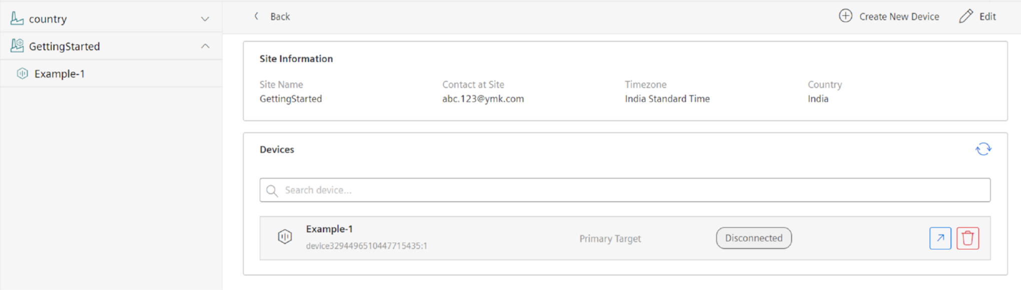
1. Log into tenant as one of the users mentioned above.

2. Open the "Remote Services" app.

3. From the "Home" screen, select the required organization from the "Organizations" drop-down list and from the "RS Roles" drop-down select the *Organization Admin* role.

4. Click on the "Organization" icon. The *Organization* and *Devices page* opens where there is also a hierarchical view of the *Nodes* and *Sites*.

5. Select the desired *Site* in the hierarchical view. The "Site Info" page is displayed.



Site Information

Site Name	Contact at Site	Timezone	Country
GettingStarted	abc.123@ymk.com	India Standard Time	India

Example-1
device3294496510447715435:1
Primary Target

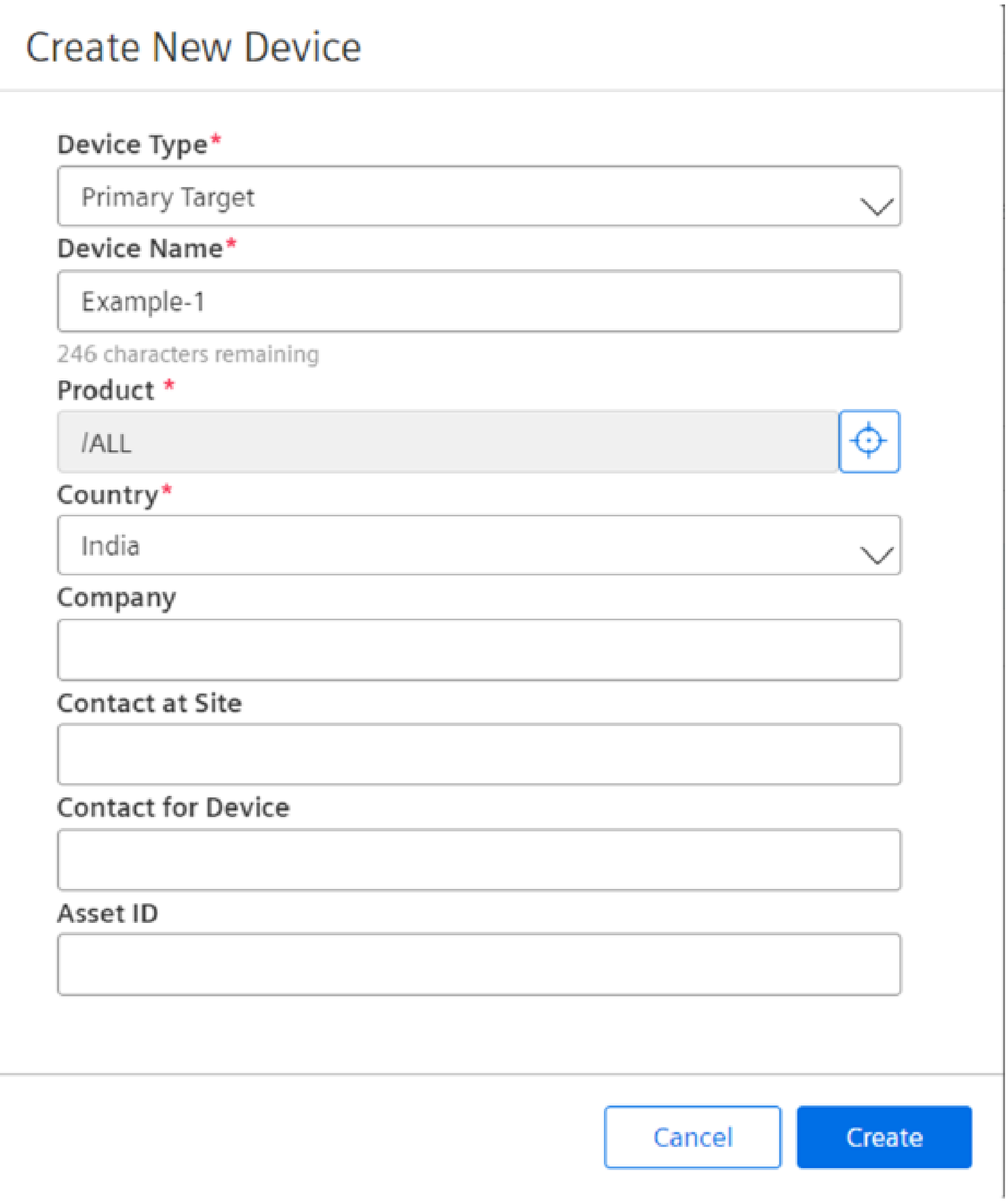
6. Click "Create New Device". The "Create New Device" pop-up window is displayed.

7. Select the "Device Type" from the drop-down, either "Primary Target" or "Gateway".

8. Enter the "Device Name". Select the "Product" and "Country" from the drop-down.

9. Enter the "Company" name and "Contact" details for the Device and *Site*.

10. If the device is an *Insights Hub Agent* where the activation of *Device Endpoint* is controlled through Insights Hub *Agent UI*, enter the "Agent's AssetID" which can be read from the Insights Hub application "Asset Manager".



Create New Device

Device Type*
Primary Target

Device Name*
Example-1
246 characters remaining

Product *
/ALL

Country*
India

Company

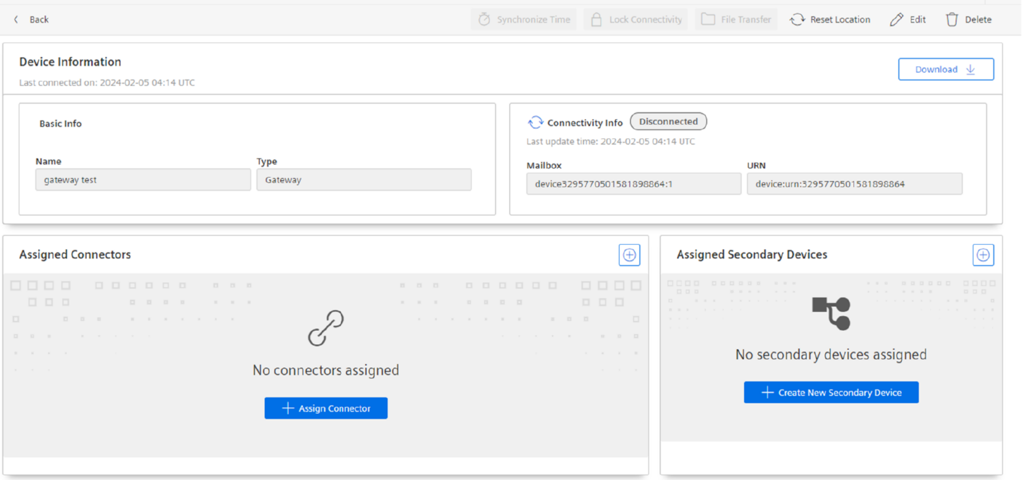
Contact at Site

Contact for Device

Asset ID

If *Primary Devices* is selected as the device type, then the new device with the entered details will be created. If *Gateway* was selected as *Device Type*, it is possible to add *Secondary Devices* that shall be reachable through this gateway. Follow the below steps:

1. Select the "Gateway Device" in the hierarchy.



Device Information
Last connected on: 2024-02-05 04:14 UTC

Basic Info

Name: gateway test
Type: Gateway

Connectivity Info
Last update time: 2024-02-05 04:14 UTC

Mailbox: device3295770501581898864:1
URN: device:urn:3295770501581898864

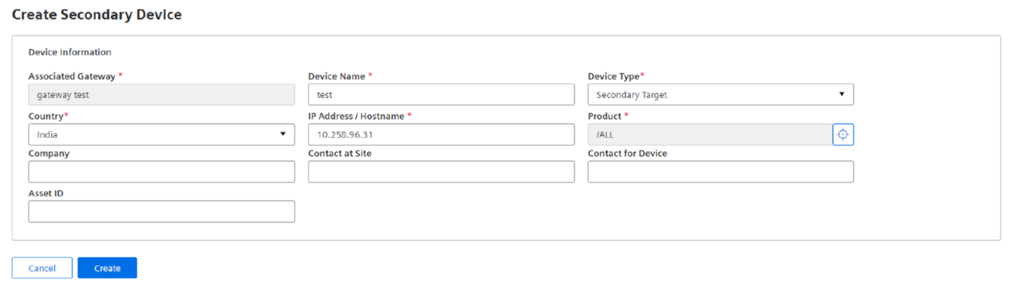
Assigned Connectors
No connectors assigned

Assigned Secondary Devices
No secondary devices assigned

The "Device Information" screen is displayed.

2. Click the "Add" icon in the "Assigned Secondary Device" section. The "Create Secondary Device" screen is displayed.

3. Enter the mandatory information.
The "IP Address/Hostname" is the *Secondary Devices's* IP address within the Gateway's network.



Create Secondary Device

Device Information

Associated Gateway *: gateway test
Device Name *: test
Device Type*: Secondary Target
Country*: India
IP Address / Hostname *: 10.258.96.31
Product *: /ALL
Company:
Contact at Site:
Contact for Device:
Asset ID:

Alternatively, it is possible to use the hostname of the device, but only if the gateway is able to translate this hostname into an IP address.

4. Click "Create".

5. The *Secondary Device* is now displayed in the "Assigned Devices" section, in the "Device Information" screen opens again.

Result

- The new device is now available in the organization and is visible in the Node/Site hierarchy under the selected site.

Download the Device Endpoint

Every device that shall be reachable through the Remote Services needs to have a *Device Endpoint* installed.
This *Device Endpoint* can be downloaded from through the *Remote Services UI*. The download package not only contains the executable of the endpoint but also a device specific

authentication key which identifies the Device and authenticates it to communicate within the given tenant.

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser` is required.
- An organization must already exist
- The *Device* must exists in the organization.
- The user must have the Remote Services role *Organization Admin* granted with access to this *Organization*, the *Site* and the *Product* of the *Device*.
- The user must log in from an IP address which is in the country that is given in his user details because per *Terms-and-Conditions* downloads are only allowed from countries which are not blacklisted as embargo countries.

Procedure

To download the *Device Endpoint* for the desired *Device* follow these steps:

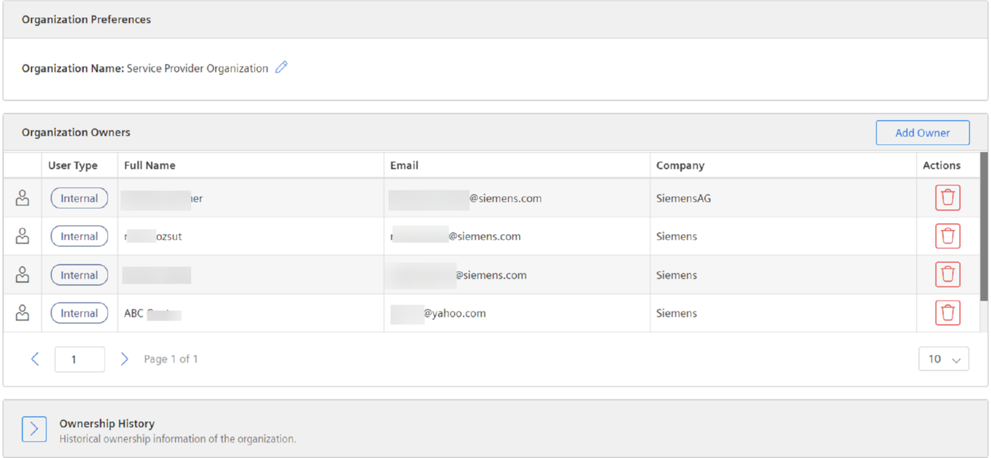
1. Log into tenant as one of the users mentioned above.

2. Open the "Remote Services" app.

3. From the "Home" screen select the desired organization from the "Organizations" drop-down list and from the "RS Roles" drop-down select the *Organization Admin* role.

4. Click on the "Organization" icon.

5. The *Organization* and *Devices page* is displayed, where there is also a hierarchical view of the *Nodes* and *Sites*.



Organization Preferences

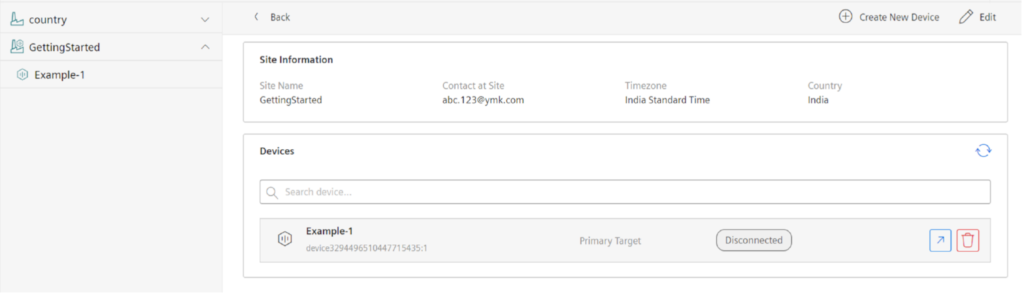
Organization Name: Service Provider Organization

Organization Owners

	User Type	Full Name	Email	Company	Actions
	Internal	[redacted]er	[redacted]@siemens.com	SiemensAG	
	Internal	r[redacted]ozsut	r[redacted]@siemens.com	Siemens	
	Internal	[redacted]	[redacted]@siemens.com	Siemens	
	Internal	ABC [redacted]	[redacted]@yahoo.com	Siemens	

Ownership History
Historical ownership information of the organization.

6. In the hierarchical view, select the required *Site*.

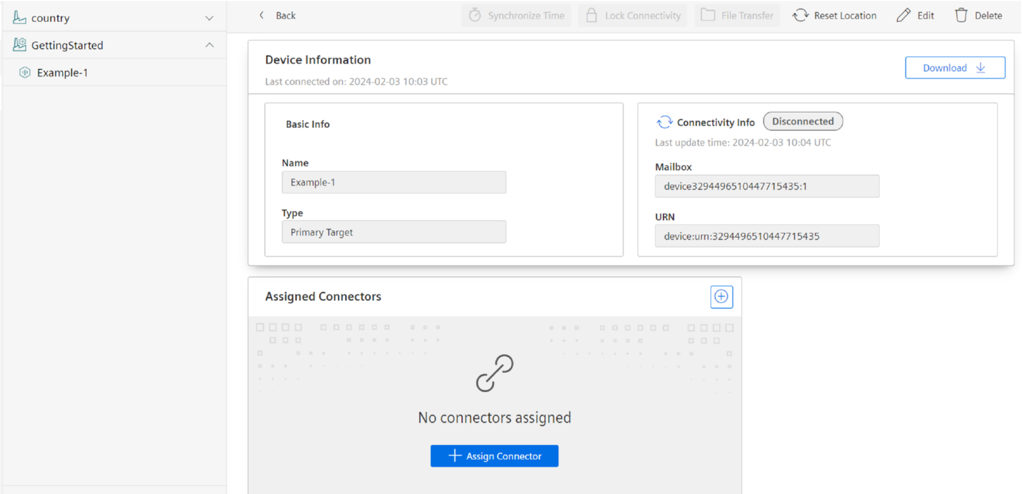


Site Information

Site Name: GettingStarted
Contact at Site: abc.123@ymk.com
Timezone: India Standard Time
Country: India

Example-1
device32944965104477715435:1
Primary Target
Disconnected

7. In the hierarchical view, select the *Device* and click the "Download" button.



Device Information

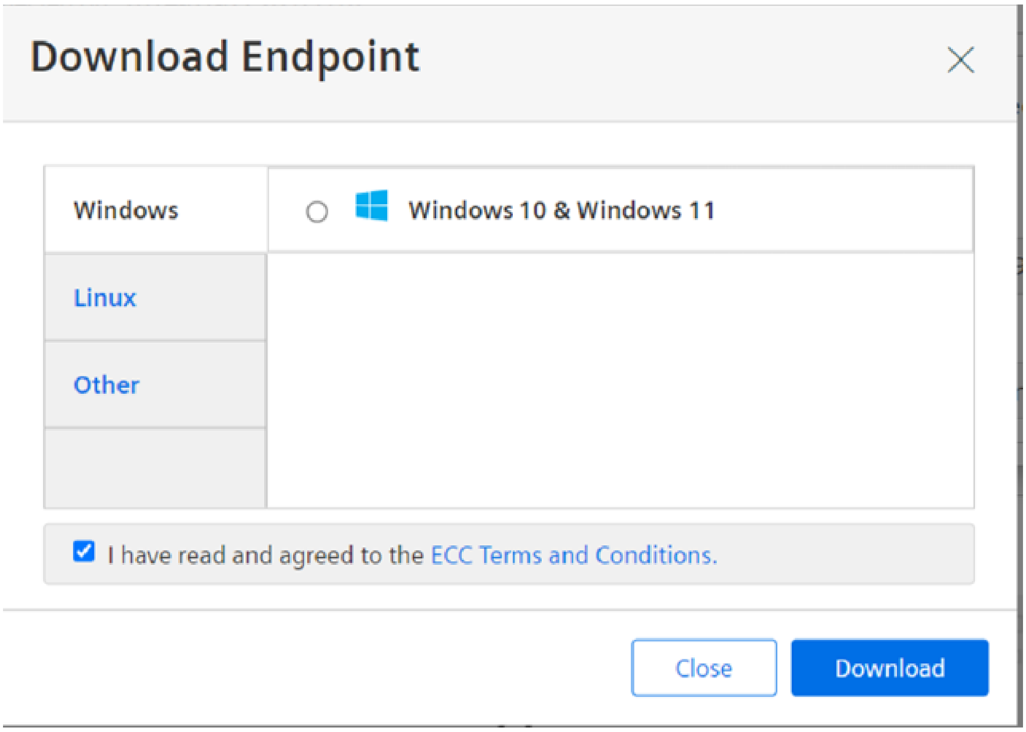
Last connected on: 2024-02-03 10:03 UTC

Basic Info

Name: Example-1
Type: Primary Target

Connectivity Info: Disconnected
Last update time: 2024-02-03 10:04 UTC
Mailbox: device32944965104477715435:1
URN: device:urn:32944965104477715435

8. The "Download Endpoint" dialog is displayed. Read "ECC Terms and Conditions" and confirm the acceptance.



☑ I have read and agreed to the ECC Terms and Conditions.

9. Select the installation package that is applicable for your target operating system and click "Download".

Result

The required device endpoint is downloaded.

Installing and starting the Device Endpoint

In order to make a system **A** which resides in a *Factory Network* accessible to a system **B** in a *Service Network*, a *Device Endpoint* must be installed and executed on the system **A**.
The Linux versions require **root** privileges to execute the *Device Endpoint*.

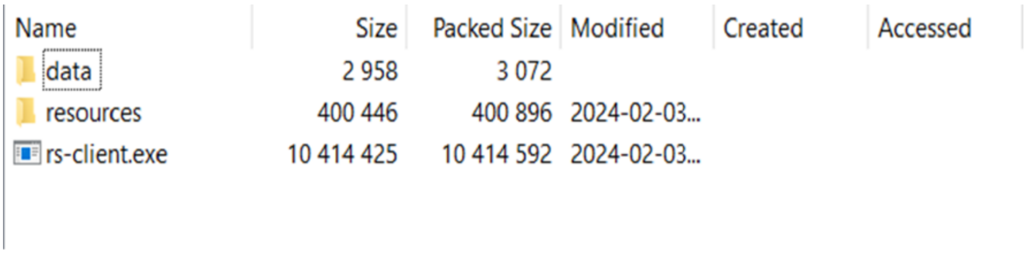
Prerequisites

- The *Device Endpoint* must already downloaded as described in the chapter Download the device endpoint.

Procedure

1. Copy the *Device Endpoint* archive package to the system that needs to be made accessible through the *Device Endpoint*.

2. Extract the archive. A folder structure will be created.



Name	Size	Packed Size	Modified	Created	Accessed
data	2 958	3 072			
resources	400 446	400 896	2024-02-03...		
rs-client.exe	10 414 425	10 414 592	2024-02-03...		

The name of the executable file depends on the target operating system, *rs-client.exe - Windows* or *rs-client - Linux*.

3. Start the executable file either manually or by using the autostart mechanisms of the target operating system.

Result

The *Device Endpoint* is connected to the Remote Services. The Device is shown as Connected in the "Device Information" screen.

Download the Service Endpoint

Any user who wants to connect to *Devices* through Remote Services needs to have a single *Service Endpoint* installed on their system.
The network where this system resides is considered as the *Service Network*. The network where the *Device* is located is considerered as a *Factory Network*.
A typical use case would be a user's Engineering Tool (e.g. TIA Portal) on the laptop in the home office that is used to remotely configure a PLC in a *Factory Network* at a customer site.

This *Service Endpoint* acts as a proxy on the user's system through which user's applications can reach through a secure tunnel to *Devices* in the *Factory Network*.
This *Service Endpoint* can be downloaded through the *Remote Services UI*. The download package not only contains the executable of the endpoint, but also a user specific authentication key which identifies the user and authenticates him to communicate within the given tenant.
The same package can be installed on multiple systems because it is only user specific. However, it cannot be used simultaneously on multiple systems.

Transparent Proxy

For Windows Systems, the download package also contains the installer for the *Transparent Proxy* which is required to use *Proxy Unaware Connector*.

Prerequisites

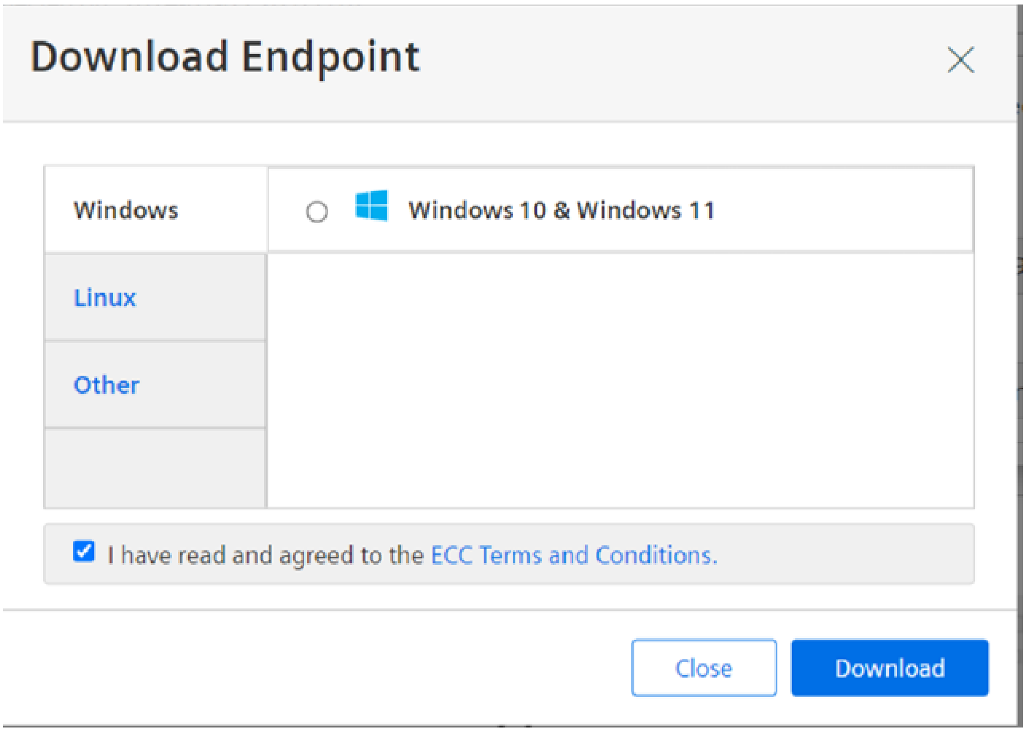
- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser`.
- The user must have one of the Remote Services roles`Remote User`, `Organization Admin` or `Organization Owner`.
- The user must log in from an IP address which is in the country that is entered in their user details because, as per *Terms-and-Conditions*, the downloads are only allowed from countries which are not blacklisted as embargo countries.

Procedure

To download the *Service Endpoint*, perform the following steps:

1. Log into tenant as one of the users mentioned above.
2. Open the "Remote Services" app.

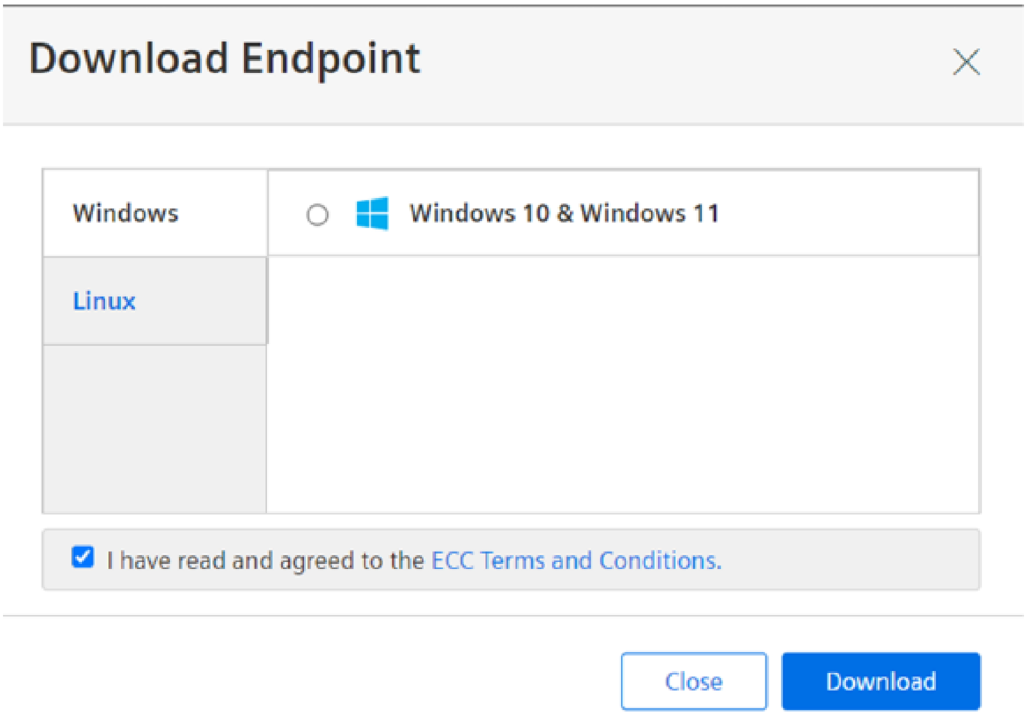
3. From the "Home" screen, click on the "Download" button in the "Service Endpoint" section.



Download Endpoint

☑ I have read and agreed to the ECC Terms and Conditions.

4. The "Download Endpoint" dialog appears. Read the "ECC Terms and Conditions" and confirm the acceptance.



Download Endpoint

☑ I have read and agreed to the ECC Terms and Conditions.

5. Select the installation package that is suitable for your target operating system and click "Download".

Result

The required Service Endpoint is stored in the download folder of the user.

Installing and starting the Service Endpoint

In order to make a system **A** which resides in a *Factory Network* accessible to a system **B** in a *Service Network*, a *Service Endpoint* must be installed and executed on the system **B**.
The Linux versions require **root** privileges to execute the *service Endpoint*.

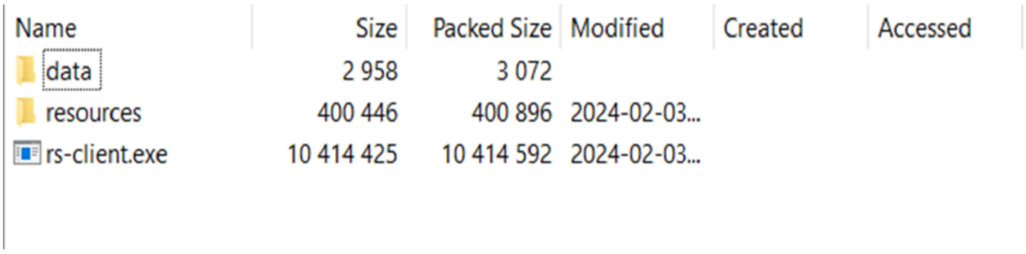
Prerequisites

The *Service Endpoint* for the operating system of the system to be used must have been downloaded as described in chapter Download the service endpoint.

Procedure

1. Copy the *Service Endpoint* archive package to the system which shall be used in the *Service Network*.

2. Extract the archive. A folder structure will be created.



Name	Size	Packed Size	Modified	Created	Accessed
data	2 958	3 072			
resources	400 446	400 896	2024-02-03...		
rs-client.exe	10 414 425	10 414 592	2024-02-03...		

The executable name depends on the target operating system, *rs-client.exe* - *Windows* or *rs-client* - *Linux*.

3. On Windows, install the `RSTransparentProxy.msi` which provides the *Transparent Proxy*.

4. At the first time, the *Service Endpoint* shall be used on a given system. Log in from that system into Remote Services Tenant as a user you want. Later, use it for Remote Connection and click on "Reset Location" in the "Service Endpoint" section. This will register the system with the RS backend and ensure that only a single instance of the endpoint is in use.

5. Start the executable either manually or by using the autostart mechanisms of the target operating system.

Result

The *Service Endpoint* is connected to the Remote Services. The Device is shown as "Connected" in the "Device Information" screen.

File transfer from Device to Service Network and vice versa

With Remote Services, it is possible to transfer files which reside on a *Device* to the location where the *Service Endpoint* is installed and vice versa.
Besides the direct transfer between the *Endpoints*, it is also possible to transfer the files temporarily to the Remote Services backend so that they can later be transferred in case the

target *endpoint* is currently not active.

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser`.
- An organization must already exist.
- The *Device* must exist in the organization.
- The user must have the Remote Services role *Remote User* granted with access to this *Organization*, the *Site* and the *Product* of the *Device*.
- The user must have a *Service Enpoint* installed and started.
- A *Device Endpoint* must have been installed on the *Device* and started.

Procedure

To add *Devices* to an organization, perform the following steps:

1. Log into tenant as one of the users mentioned above.

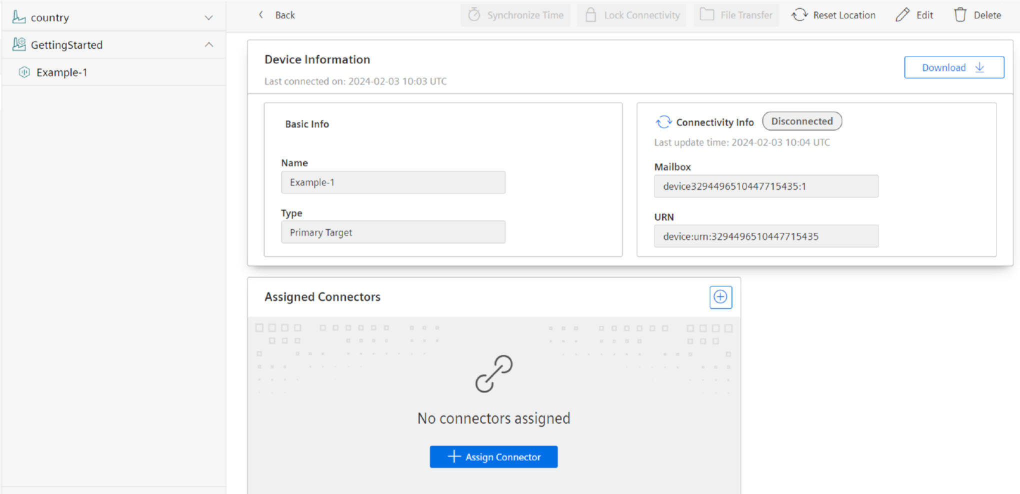
2. Open the "Remote Services" app.

3. From the "Home" screen, select the required organization from the "Organizations" drop-down list and from the "RS Roles" drop-down, select the *Remote User* role.

4. Click on the "Organization" icon. The "Organization Overview" is displayed, where there is also a hierarchical view of the *Nodes* and *Sites*.

5. In the hierarchical view, select the desired *Site* and expand it so that the *Devices* become visible.

6. Select the required Device. The "Device Information" screen appears.



Device Information

Last connected on: 2024-02-03 10:03 UTC

Basic Info

Name: Example-1

Type: Primary Target

Connectivity Info: Disconnected

Last update time: 2024-02-03 10:04 UTC

Mailbox: device32944965104477154351

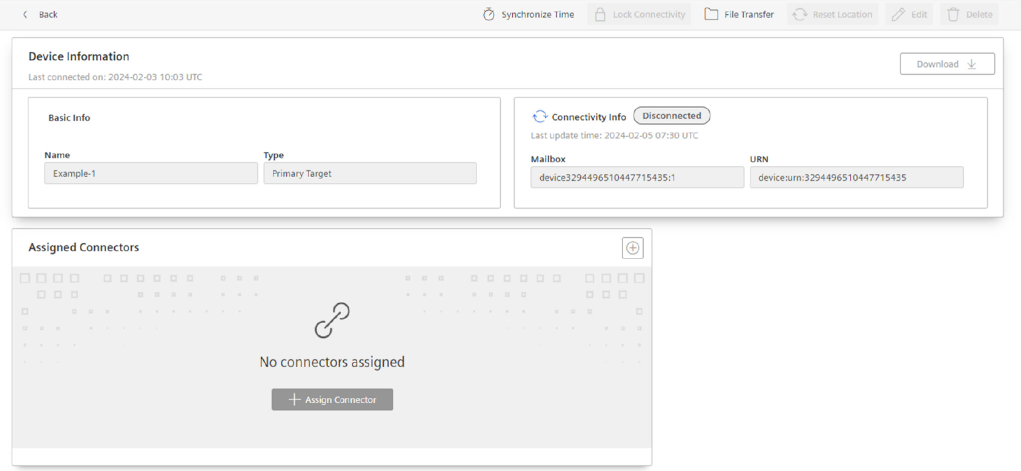
URN: device:urn:3294496510447715435

Assigned Connectors

No connectors assigned

7. Verify that the Device is shown as "Connected".

8. Click on the "File Transfer" icon in top region of the screen. The "File Transfer" screen appears.



Device Information
Last connected on: 2024-02-03 10:03 UTC

Basic Info
Name: Example-1
Type: Primary Target

Connectivity Info
Last update time: 2024-02-05 07:30 UTC
Mailbox: device3294496510447715435:1
URN: device:urn:3294496510447715435

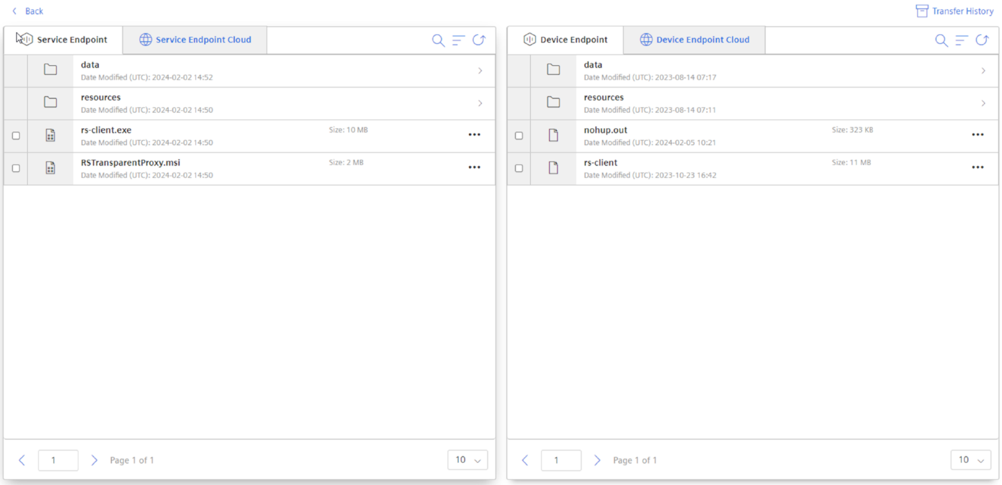
Assigned Connectors
No connectors assigned

This screen shows two file browsers. On the left, the files at the location of the *Service Endpoint* executable and below. On the right, the files on the *Device Endpoint* exectuable and below.

9. Select one or more files in one of the file browsers and click the *3 dots* which indicate more options and select the desired transfer target.

   - Either the opposite endpoint for direct transfer between the endpoints.

   - Or, Cloud for temporary storage of the file for later transfer to an *Endpoint*.



Service Endpoint:
- data – Date Modified (UTC): 2024-02-02 14:52
- resources – Date Modified (UTC): 2024-02-02 14:50
- rs-client.exe – Date Modified (UTC): 2024-02-02 14:50 – Size: 10 MB
- RSTransparentProxy.msi – Date Modified (UTC): 2024-02-02 14:50 – Size: 2 MB

Device Endpoint:
- data – Date Modified (UTC): 2023-08-14 07:17
- resources – Date Modified (UTC): 2023-08-14 07:11
- nohup.out – Date Modified (UTC): 2024-02-05 10:21 – Size: 323 KB
- rs-client – Date Modified (UTC): 2023-10-23 16:42 – Size: 11 MB

Result

- The selected file is transferred to the desired target destination. The selected file will not be deleted from the source location.
- The file is visible in the file browser of the target destination.

MindConnect Elements with preinstalled Device Endpoint

The following MindConnect Elements have a preinstalled Device Endpoint:

- MindConnect Nano

- MindConnect IoT2050
- MindConnect IoT2040

To use these elements as a Gateway in a *Factory Network*, it is required to define them as *Device* of type *Gateway* as described in this procedure. In that case, the `AssetID` needs to be read from the Asset Manager according to the following procedure and entered in the "Create Device" screen.

Read AssetId from Asset Manager

Prerequisites

- The MindConnect Element must be created in Asset Manager.
- An Insights Hub user with access to Asset Manager is required.

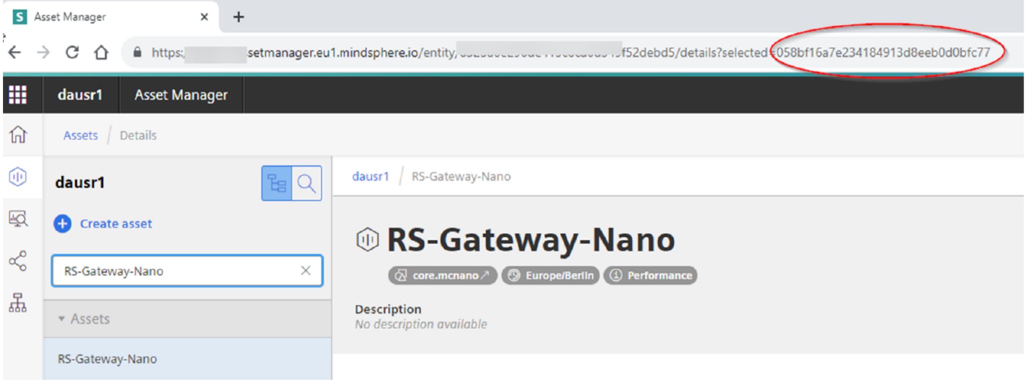
Procedure

To read the AssetId of the MindConnect Element that shall be created as *Gateway Device* in Remote Services, perform the following steps:

1. Log into tenant as the user mentioned above.

2. Open the "Asset Manager" app.

3. Find the Asset by its name.



https:[redacted]setmanager.eu1.mindsphere.io/entity,[redacted]f52debd5/details?selected=058bf16a7e234184913d8eeb0d0bfc77

4. From the browsers's address bar note the highlighted number which is the AssetID.

Result

The `AssetId` is identified and can be used to create a *Gateway Device* according to this procedure.

Enable pre-installed Device Endpoint

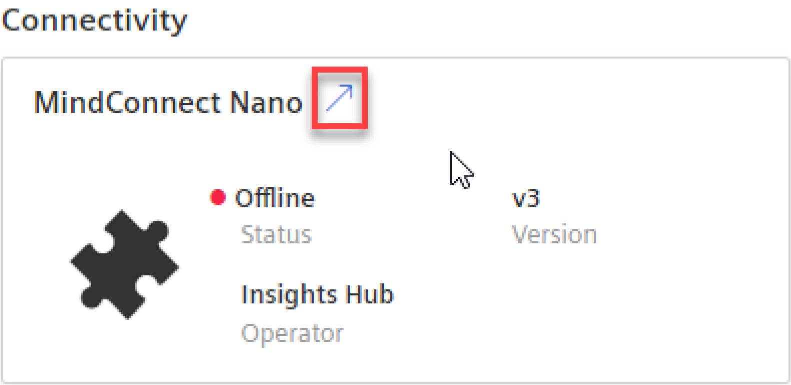
The pre-installed *Device Endpoint* on the *MindConnect Element* is by default disabled and must be explicitly enabled in the Asset Manager. It is also possible to disable it again later again in the Asset Manager.

Prerequisites

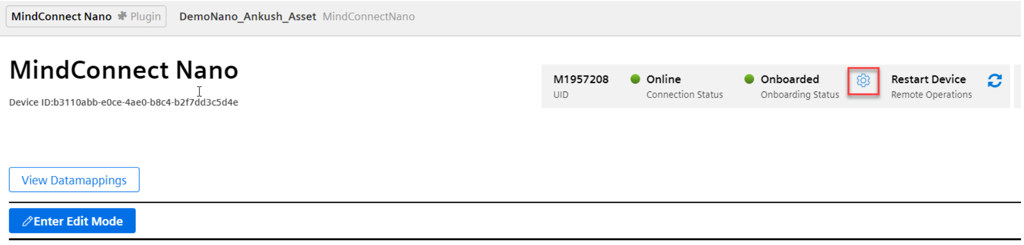
- The MindConnect Element must be created in "Asset Manager".
- The MindConnect Element must be onboarded.
- A *Gateway Device* must have been created according to this procedure using the `AssetId` of the *MindConnect Element*.
- An Insights Hub user with access to *Asset Manager* is required.

Procedure

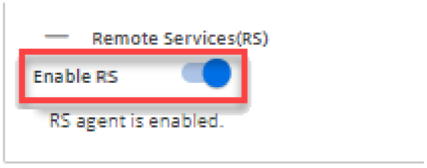
1. Log into tenant as the user mentioned above.
2. Open the "Asset Manager" app.
3. Find the Asset by its name.
4. Open the MindConnect Element plugin as shown in "Asset Manager".



5. Click ⚙



6. In the Remote Services section, enable MRS toggle.



RS agent is enabled.

Result

- The preinstalled *Device Endpoint* on the *MindConnect Element* is activated and the Gateway *Device* connects to Remote Services.

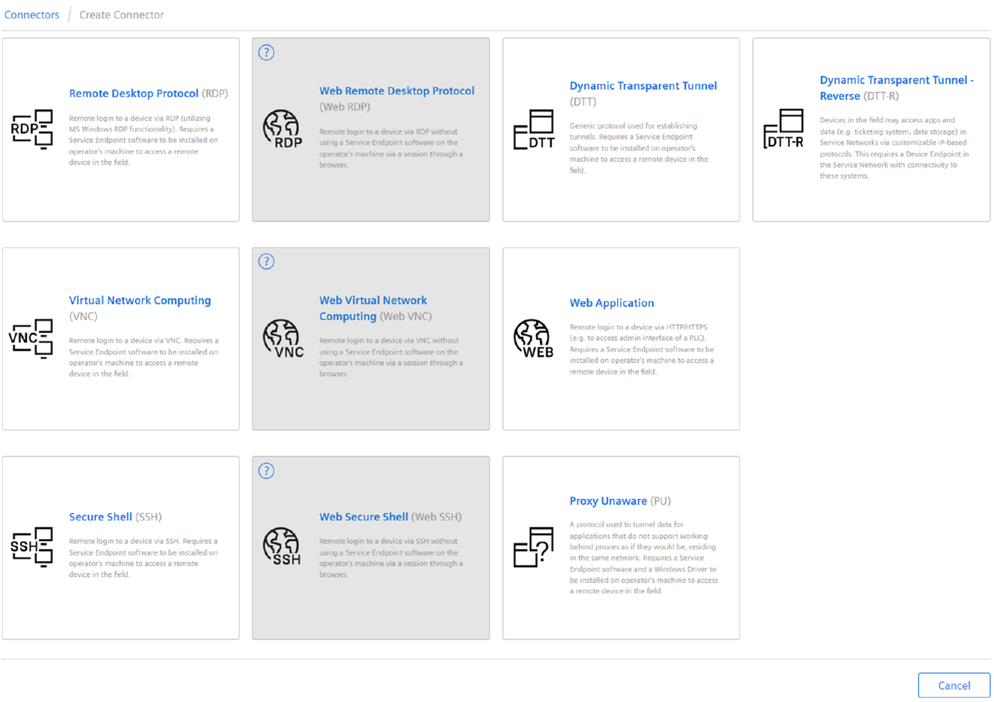
Remote Services Connectors

5

5.1 Creating, Assigning and Using Connectors

Introduction

The Connector Type Overview Page shows a list of *Connector Types*.



Connectors / Create Connector

Remote Desktop Protocol (RDP)
Remote login to a device via RDP (utilizing MS Windows RDP functionality). Requires a Service Endpoint software to be installed on operator's machine to access a remote device in the field.

Web Remote Desktop Protocol (Web RDP)
Remote login to a device via RDP without using a Service Endpoint software on the operator's machine via a session through a browser.

Dynamic Transparent Tunnel (DTT)
Generic protocol used for establishing tunnels. Requires a Service Endpoint software to be installed on operator's machine to access a remote device in the field.

Dynamic Transparent Tunnel - Reverse (DTT-R)
Devices in the field may access apps and data (e.g. ticketing system, data storage) in Service Networks via customizable IP-based protocols. This requires a Device Endpoint in the Service Network with connectivity to these systems.

Virtual Network Computing (VNC)
Remote login to a device via VNC. Requires a Service Endpoint software to be installed on operator's machine to access a remote device in the field.

Web Virtual Network Computing (Web VNC)
Remote login to a device via VNC without using a Service Endpoint software on the operator's machine via a session through a browser.

Web Application
Remote login to a device via HTTP/HTTPS (e.g. to access admin interface of a PLC). Requires a Service Endpoint software to be installed on operator's machine to access a remote device in the field.

Secure Shell (SSH)
Remote login to a device via SSH. Requires a Service Endpoint software to be installed on operator's machine to access a remote device in the field.

Web Secure Shell (Web SSH)
Remote login to a device via SSH without using a Service Endpoint software on the operator's machine via a session through a browser.

Proxy Unaware (PU)
A protocol used to tunnel data for applications that do not support working behind proxies as if they would be, residing in the same network. Requires a Service Endpoint software and a Windows Driver to be installed on operator's machine to access a remote device in the field.

The ones in the middle which are grayed out are planned to be supported in future releases of Remote Services.
All Connector Types except the **DTT-R Connector** require a *Service Endpoint* to be installed on the *Remote User's* machine.
The **DDT-R Connector** is meant to connect two *Devices*, hence no *Service Endpoint* is required.

Create *DTT Connector*

Usecase

This is the most generic connector type that allows tunneling of TCP traffic originating from the service endpoint towards a device where the connector is assigned to.

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser`.
- An organization must already exist.
- The user must have the Remote Services role *Organization Admin* granted with access to this organization.
- Usage of this Connector requires a *Service Endpoint* to be installed on the machine of the *Remote User*.

Procedure

To create a new *DTT Connector* to an existing organization, perform the following steps:

1. Log into tenant as one of the users mentioned above.

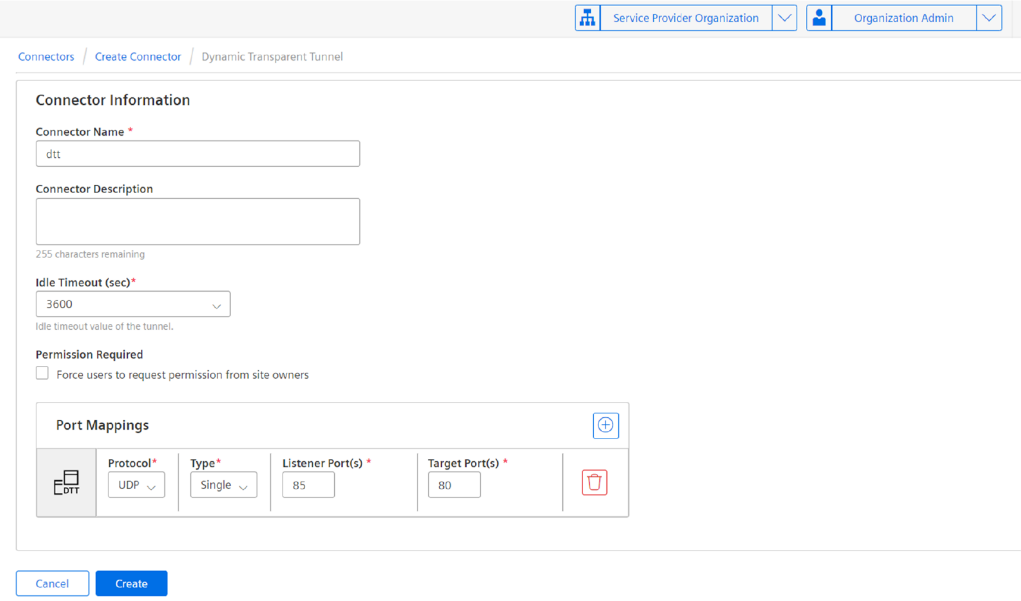
2. Open the "Remote Services" app.

3. From the "Home screen", select the required organization from the "Organizations" drop-down list and from the "RS Roles" drop-down select the "Organization Admin" role.

4. Navigate to the "Connectors" page.

5. Click "Create New Connector". The overview page to select the connector is displayed.

6. Select "Dynamic Transparent Tunnel Protocol".


Service Provider Organization
Organization Admin
Connectors / Create Connector / Dynamic Transparent Tunnel
DTT
Cancel
Create

Connector Information

Connector Name *: dtt

Connector Description:

255 characters remaining

Idle Timeout (sec)*: 3600

Idle timeout value of the tunnel.

Permission Required

□ Force users to request permission from site owners

Port Mappings

Protocol*	Type*	Listener Port(s) *	Target Port(s) *
UDP	Single	85	80

7. Enter the necessary information for the connector, ensuring to provide port mapping, for routing of TCP/UDP data packets using custom port settings.

8. Click "Create".

Result

The connector is created and is available by Organization Admin for assignment to *Devices* of the current organization.

Create *RDP Connector*

Use case

This is a connector type that builds on top of DTT to provide additional convenience to users by providing RDP related properties such as domain name, user name, resolution, etc.
This *Connector* will automatically start the Windows Remote Desktop Client on the machine where the *Service Endpoint* is installed and offers a connection to the Remote Desktop Server on the *Device* where the connector is assigned to.

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser`.
- An organization must already exist.
- The user must have the Remote Services role *Organization Admin* granted with access to this organization.
- A *Service Endpoint* to be installed on the machine of the *Remote User*.

Procedure

To create a new *RDP Connector* to an existing organization, perform the following steps:

1. Log into tenant as one of the users mentioned above.

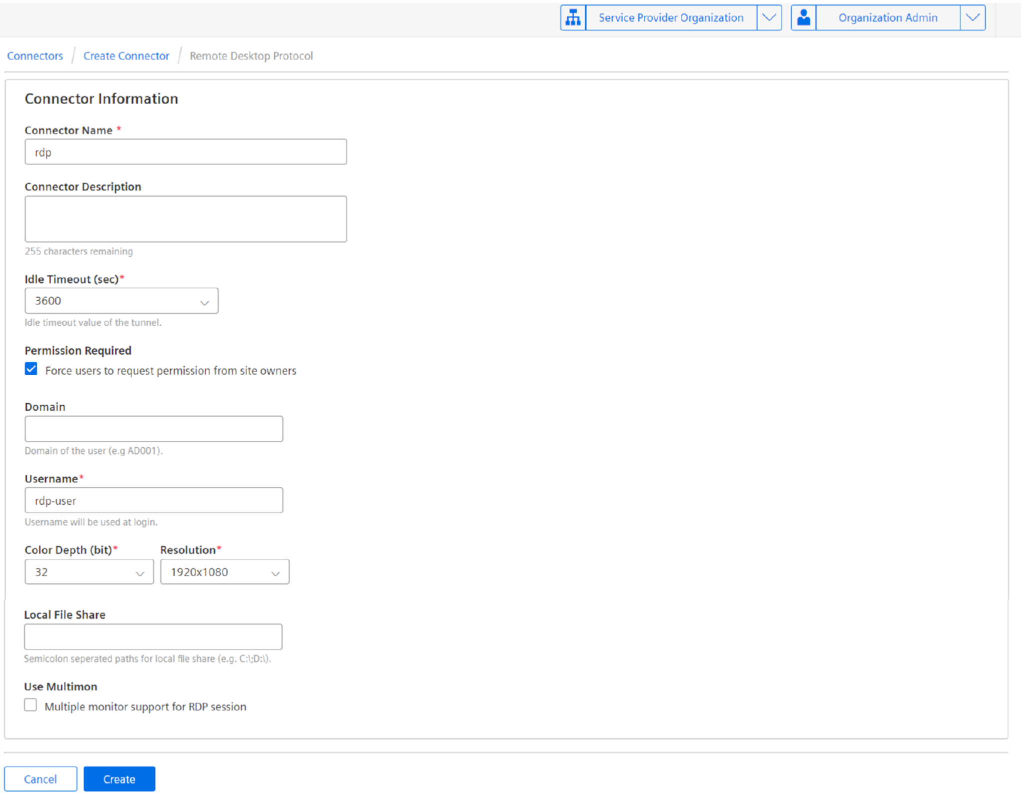
2. Open the "Remote Services" app.

3. From the "Home" screen, select the required organization from the "Organizations" drop-down list and from the "RS Roles" drop-down, select the "Organization Admin" role.

4. Navigate to the "Connectors" page.

5. Click "Create New Connector". The overview page to select the connector is displayed.

6. Select "Remote Desktop Protocol".



Service Provider Organization
Organization Admin
Connectors / Create Connector / Remote Desktop Protocol

Connector Information

Connector Name *: rdp

Connector Description:

255 characters remaining

Idle Timeout (sec)*: 3600

Idle timeout value of the tunnel.

Permission Required

☑ Force users to request permission from site owners

Domain:

Domain of the user (e.g AD001).

Username*: rdp-user

Username will be used at login.

Color Depth (bit)*: 32

Resolution*: 1920x1080

Local File Share:

Semicolon seperated paths for local file share (e.g. C:\;D:\).

Use Multimon

☐ Multiple monitor support for RDP session

7. Enter the necessary information for the connector. Note that the entered username will be used for RDP login in the system.

8. Click "Create".

Result

The connector is created and is available by the Organization Admin for assignment to *Devices* of the current organization.

Create *VNC Connector*

Usecase

This is a connector type that builds on top of DTT to provide additional convenience to users by providing VNC related properties.

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser`.
- An organization must already exist.
- The user must have the Remote Services role *Organization Admin* granted with access to this organization.
- A *Service Endpoint* to be installed on the machine of the *Remote User*.

Procedure

To create a new *VNC Connector* to an existing organization, perform the following steps:

1. Log into tenant as one of the users mentioned above.

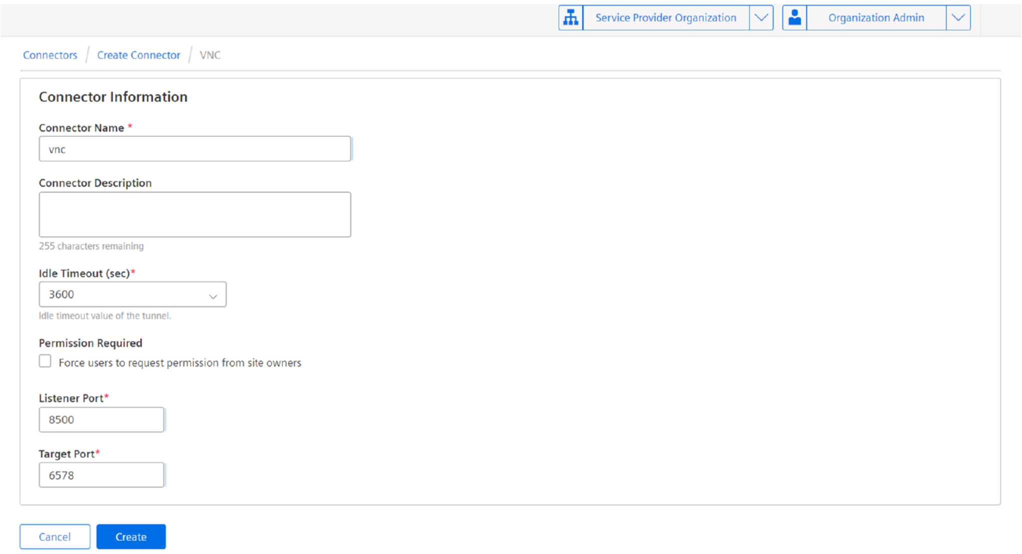
2. Open the "Remote Services" app.

3. From the "Home" screen, select the required organization from the "Organizations" drop-down list and from the "RS Roles" drop-down, select the "Organization Admin" role.

4. Navigate to the "Connectors" page.

5. Click "Create New Connector". The overview page to select the connector is displayed.

6. Select "Virtual Network Computing Protocol".


Service Provider Organization
Organization Admin
Connectors / Create Connector / VNC
Cancel
Create

Connector Information

Connector Name *: vnc

Connector Description:

255 characters remaining

Idle Timeout (sec)*: 3600

Idle timeout value of the tunnel.

Permission Required

□ Force users to request permission from site owners

Listener Port*: 8500

Target Port*: 6578

7. Enter the necessary information for the connector, ensuring to provide listener and target port, which is meant for connecting to devices via VNC-based remote login.

8. Click "Create".

Result

The connector is created and is available by Organization Admin for assignment to *Devices* of the current organization.

Create *SSH Connector*

Usecase

This is a connector type that builds on top of DTT to provide additional convenience to users by providing SSH related properties.

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser`.

- An organization must already exist.
- The user must have the Remote Services role *Organization Admin* granted with access to this organization.
- Usage of this Connector requires a *Service Endpoint* to be installed on the machine of the *Remote User*.

Procedure

To create a new *SSH Connector* to an existing organization, perform these steps:

1. Log into tenant as one of the users mentioned above.

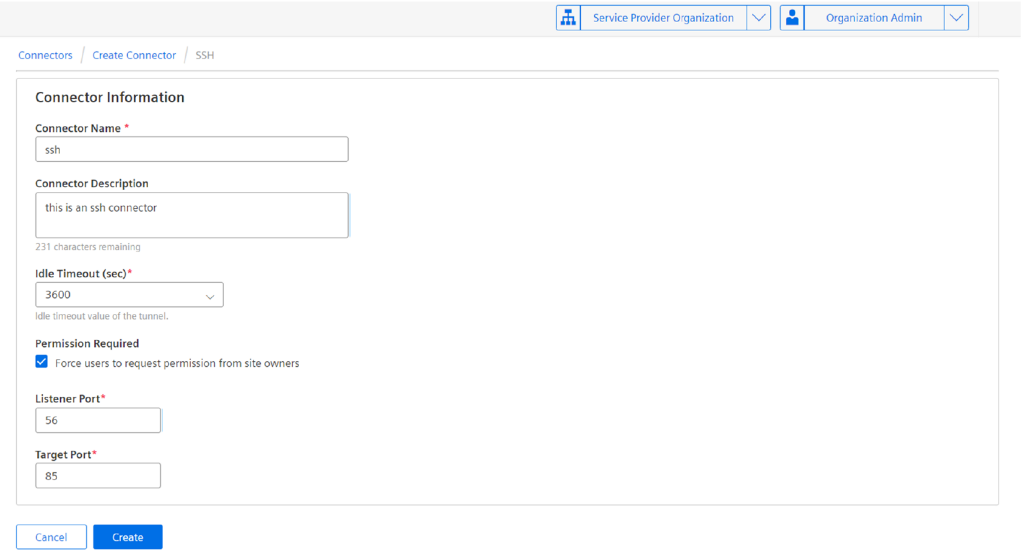
2. Open the "Remote Services" app.

3. From the "Home" screen, select the required organization from the "Organizations" drop-down list and from the "RS Roles" drop-down, select the "Organization Admin" role.

4. Navigate to the "Connectors" page.

5. Click "Create New Connector". The overview page to select the connector is displayed.

6. Select "Secure Shell Protocol".


Service Provider Organization
Organization Admin
Connectors / Create Connector / SSH
Cancel
Create

Connector Information

Connector Name *
ssh

Connector Description
this is an ssh connector
231 characters remaining

Idle Timeout (sec)*
3600
Idle timeout value of the tunnel.

Permission Required
☑ Force users to request permission from site owners

Listener Port*
56

Target Port*
85

7. Enter the necessary information for the connector, ensuring to provide listener and target port, which is meant for connecting to devices via SSH.

8. Click "Create".

Result

The connector is created and is available by Organization Admin for assignment to *Devices* of the current organization.

Create *Web Application Connector*

Usecase

This connector type allows tunneling of HTTP/HTTPS based applications to be accessed by remote users.

Once a tunnel of this *Connector Type* is successfully established, a Web Browser on the system where the *Service Endpoint* is installed will automatically open and display the start page specified in the *Connector* definition.

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser`.
- An organization must already exist.
- The user must have the Remote Services role *Organization Admin* granted with access to this organization.
- Usage of this Connector requires a *Service Endpoint* to be installed on the machine of the *Remote User*.

Procedure

To create a new *Web Application Connector* to an existing organization, perform the following steps:

1. Log into tenant as one of the users mentioned above.

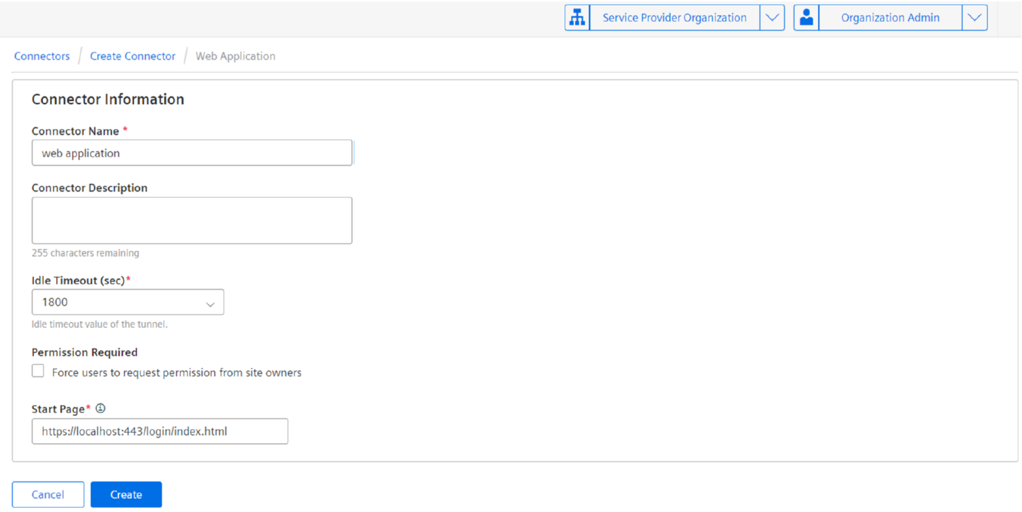
2. Open the "Remote Services" app.

3. From the "Home" screen, select the required organization from the "Organizations" drop-down list and from the "RS Roles" drop-down, select the "Organization Admin" role.

4. Navigate to the "Connectors" page.

5. Click "Create New Connector". The overview page to select the connector is displayed.

6. Select "Web Application Protocol".



Service Provider Organization

Organization Admin

Connectors / Create Connector / Web Application

Connector Information

Connector Name *

web application

Connector Description

255 characters remaining

Idle Timeout (sec)*

1800

Idle timeout value of the tunnel.

Permission Required

□ Force users to request permission from site owners

Start Page*

https://localhost:443/login/index.html

7. Enter the necessary information for the connector, ensuring to use localhost while specifying the Start Page. The localhost keyword will be automatically replaced by actual IP address of the target device.

8. Click "Create".

Result

The connector is created and is available by *Organization Admin* for assignment to *Devices* of the current organization.

Create *Proxy Unaware Connector*

Usecase

This is a connector type that allows clients/applications to connect to remote devices seamlessly even if the clients/applications cannot cope with intermediate proxies. One of the most prominent application is TIA portal.
If this *Connector* is assigned to a *Device* of type *Primary Target*, the client/application will have to connect to IP address 127.0.0.1 or localhost at the port given as target port in the *Connector* definition.
If this *Connector* is assigned to a *Device* of type *Secondary Target*, the client/application will have to connect to the IP address assigned for the *Secondary Target* at the port given as target port in the *Connector* definition. In this case, the *Transparent Proxy* mentioned in the following section will perform an IP address translation that is transparent to the client/application.

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser`.
- An organization must already exist.
- The user must have the Remote Services role *Organization Admin* granted with access to this organization.
- The operating system on the machine of the Remote User is Windows 10 or Windows 11.
- Usage of this Connector requires a *Service Endpoint* to be installed on the machine of the *Remote User*.
- Usage of this Connector requires installation of the *Transparent Proxy* from the *Service Endpoint Installation Package* on the machine of the *Remote User*.

Procedure

To create a new *Proxy Unaware Connector* to an existing organization, perform the following steps:

1. Log into tenant as one of the users mentioned above.

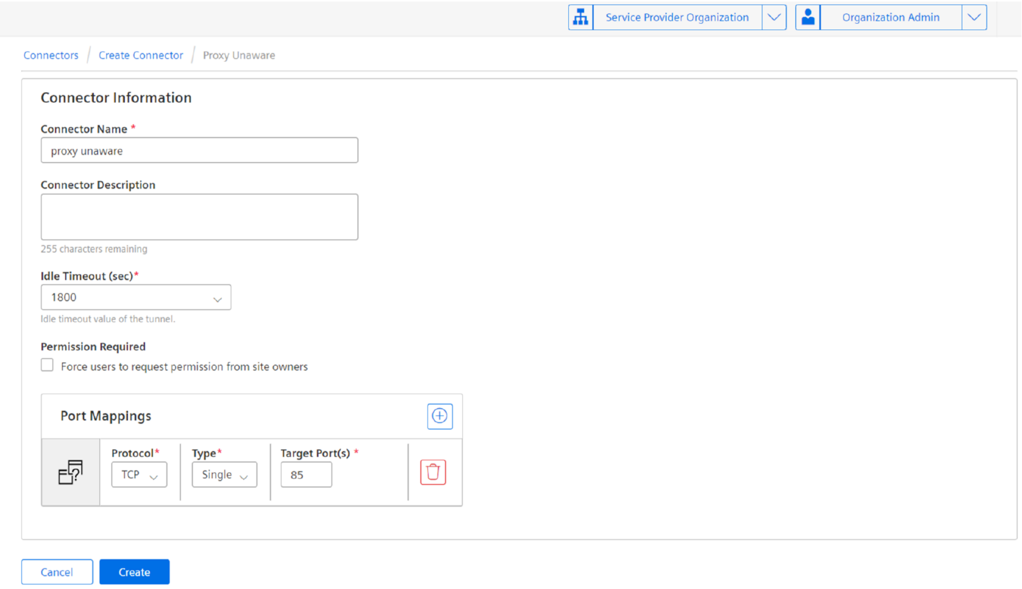
2. Open the "Remote Services" app.

3. From the "Home" screen, select the required organization from the "Organizations" drop-down list and from the "RS Roles" drop-down, select the *Organization Admin* role.

4. Navigate to the "Connectors" page.

5. Click "Create New Connector". The overview page to select the connector is displayed.

6. Select "Proxy Unaware Protocol".


Service Provider Organization
Organization Admin
Connectors / Create Connector / Proxy Unaware
Cancel
Create

Connector Information

Connector Name *: proxy unaware

Connector Description

255 characters remaining

Idle Timeout (sec)*: 1800

Idle timeout value of the tunnel.

Permission Required

□ Force users to request permission from site owners

Port Mappings

Protocol*	Type*	Target Port(s) *
TCP	Single	85

7. Enter the necessary information for the connector, ensuring to provide Port Mappings for TCP/UDP protocol with single/range of target device ports.

8. Click "Create".

Result

The connector is created and is available by *Organization Admin* for assignment to *Devices* of the current organization.

Create *DTT-R Connector*

Usecase

DTT-R stands for DTT-Reverse. This is similar to DTT. However, to provide device to device tunneling, it requires two *Device Endpoints* to be installed. The *Service Endpoint* is not required. The *Connector* is assigned to the source *Device*, i.e. the one that initiates the connection. In the *Connector* definition, the *Device Endpoint* id of the target *Device* needs to be given.

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser`.
- An organization must already exist.

- The user must have the Remote Services role *Organization Admin* granted with access to this organization.
- There must be a target *Device* defined in the same Organization, typically it will be in a different network than the *Device* to which the DDT-R connector is assigned.

Procedure

To create a new *Dynamic Transparent Tunnel - Reverse Connector* to an existing organization, perform the following steps:

1. Log into tenant as one of the users mentioned above.

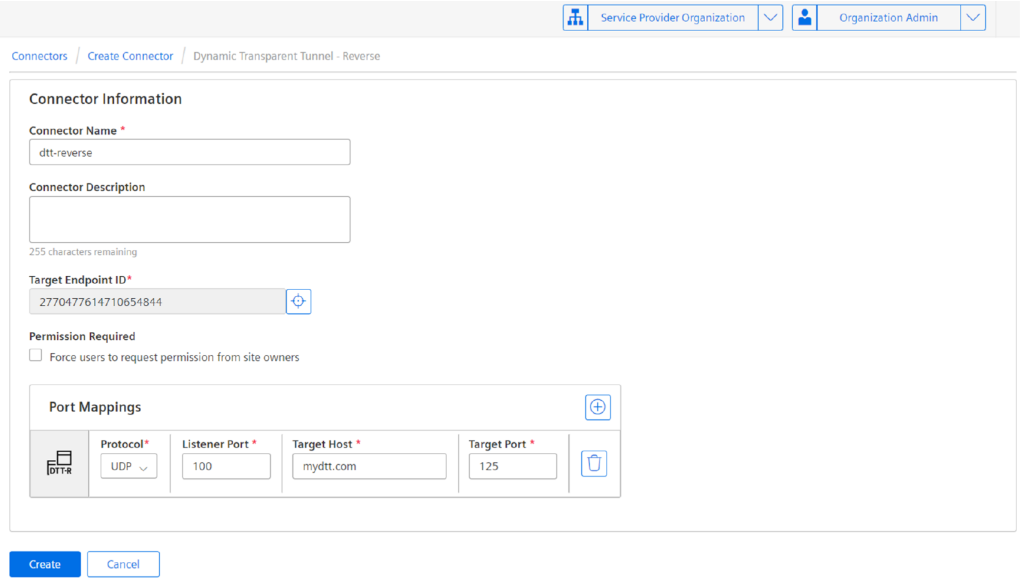
2. Open the "Remote Services" app.

3. From the "Home" screen, select the required organization from the "Organizations" drop-down list and from the "RS Roles" drop-down. select the *Organization Admin* role.

4. Navigate to the "Connectors" page.

5. Click "Create New Connector". The overview page to select connector is displayed.

6. Select "Dynamic Transparent Tunnel - Reverse Protocol".


Service Provider Organization
Organization Admin
Connectors / Create Connector / Dynamic Transparent Tunnel - Reverse
Create
Cancel

Connector Information

Connector Name *: dtt-reverse

Connector Description:

255 characters remaining

Target Endpoint ID*: 2770477614710654844

Permission Required

□ Force users to request permission from site owners

Port Mappings

	Protocol*	Listener Port *	Target Host *	Target Port *
DTT-R	UDP	100	mydtt.com	125

7. Enter the necessary information for the connector, ensuring to provide Target Endpoint and Port Mapping between Listener Port and Target Host port.

8. Click "Create".

Result

The connector is created and is available by *Organization Admin* for assignment to *Devices* of the current organization.

Assign Connectors

To establish a connection to a particular *Device* to fulfill a particular use case, for example RDP, VNC, SSH, access to web-server, etc, the prepared required *Connector* needs to be assigned by the *Organization Admin* to that *Device* so that the *Remote User* can later activate that connection.

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser`.
- An organization must already exist.
- The *Connector* **c** must exist.
- A *Device* **A** must exist to which the *Connector* **c** shall be assigned.
- The user must have the Remote Services role *Organization Admin* granted with access to this organization and the *Device* **A**.

Procedure

To assign *Connector* **c** to **Device a**, perform the following steps:

1. Log into tenant as one of the users mentioned above.

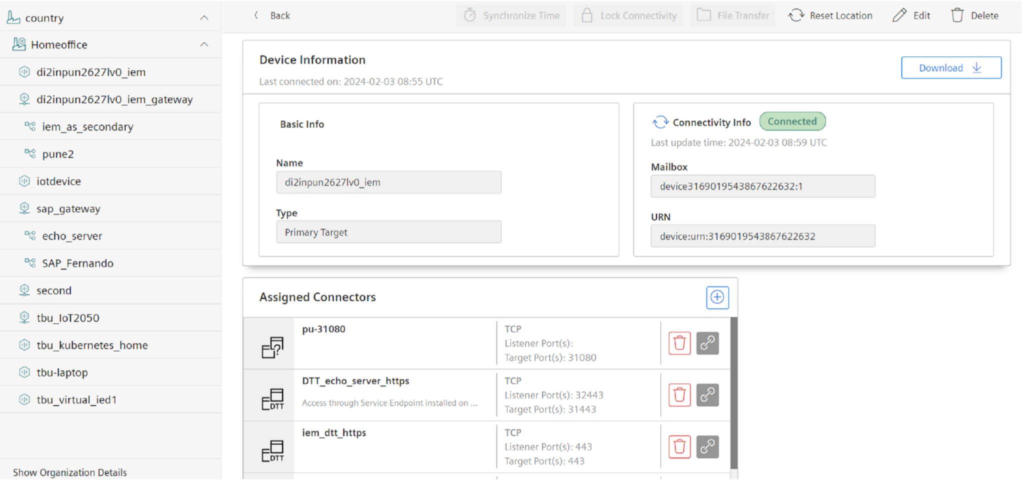
2. Open the "Remote Services" app.

3. From the "Home" screen, select the required organization from the "Organizations" drop-down list and from the "RS Roles" drop-down, select the *Organization Admin* role.

4. Click on the "Organization" icon. The *Organization* and *Devices page* is displayed, where there is also a hierarchical view of the *Nodes* and *Sites*.

5. In the hierarchical view, select the required *Site* and expand it so that the *Devices* are displayed.

6. Select the required *Device*. The *Device Information* screen is displayed which shows a list of assigned *Connectors*.



Device Information

Last connected on: 2024-02-03 08:55 UTC

Name: di2inpun2627lv0_iem

Type: Primary Target

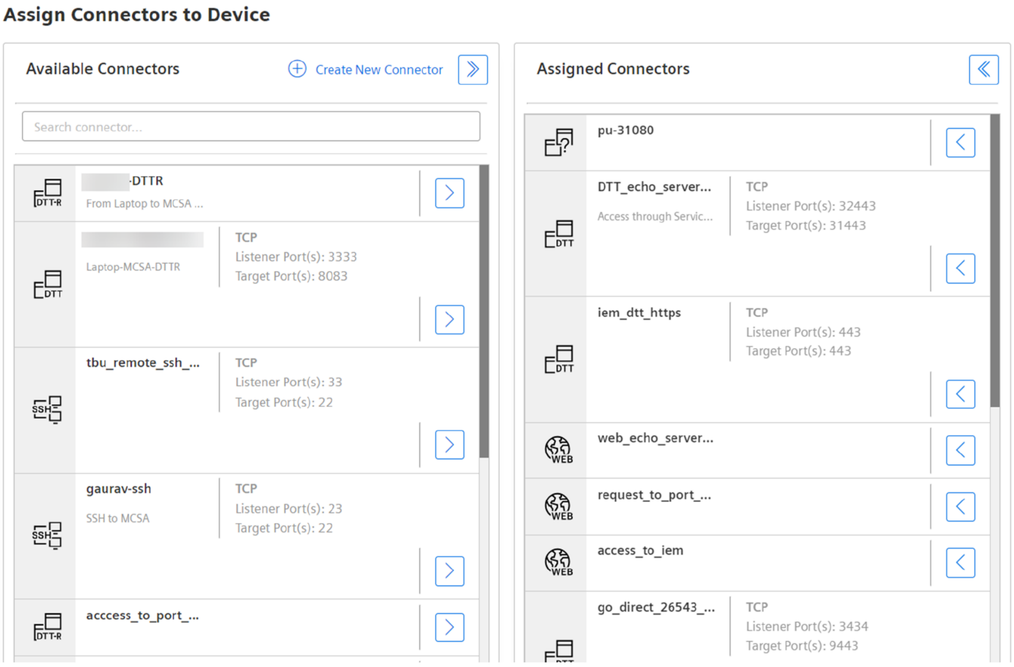
Last update time: 2024-02-03 08:59 UTC

Mailbox: device3169019543867622632:1

URN: device:urn:3169019543867622632

pu-31080	TCP Listener Port(s): Target Port(s): 31080
DTT_echo_server_https Access through Service Endpoint installed on ...	TCP Listener Port(s): 32443 Target Port(s): 31443
iem_dtt_https	TCP Listener Port(s): 443 Target Port(s): 443

7. In the "Assigned Connectors" list, click on the "plus" icon to display the list of *Connectors* which are ready to be assigned.



Assign Connectors to Device

Available Connectors

Search connector...

[redacted]-DTTR
From Laptop to MCSA ...

[redacted]
Laptop-MCSA-DTTR
TCP
Listener Port(s): 3333
Target Port(s): 8083

tbu_remote_ssh_...
TCP
Listener Port(s): 33
Target Port(s): 22

gaurav-ssh
SSH to MCSA
TCP
Listener Port(s): 23
Target Port(s): 22

acccess_to_port_...

Assigned Connectors

pu-31080

DTT_echo_server...
Access through Servic...
TCP
Listener Port(s): 32443
Target Port(s): 31443

iem_dtt_https
TCP
Listener Port(s): 443
Target Port(s): 443

web_echo_server...

request_to_port_...

access_to_iem

go_direct_26543_...
TCP
Listener Port(s): 3434
Target Port(s): 9443

8. In the "Available Connectors" column, search for the required *Connector* **c** and click on the **>** icon to move it to the "Assigned Connectors" column.

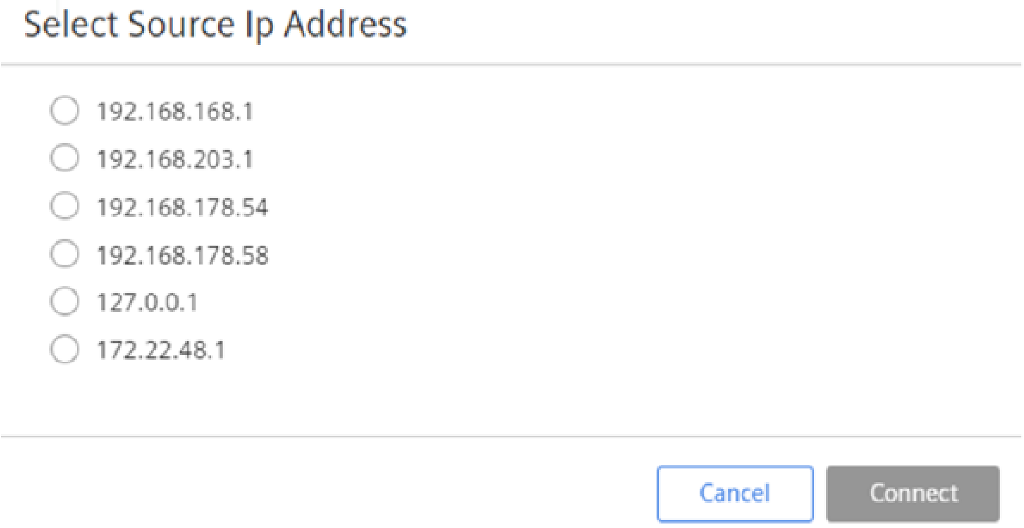
9. Click "Save" to save your selection and navigate back to the *Device Information* screen.

Result

- *Connector* **c** is assigned to the *Device* **A** and ready for use by the *Remote User*.

Establish Connection

The Remote User can establish a connection to a particular Device using the Connectors assigned by the `Organization Admin`.
When the *Proxy Unaware Connector* is used, there will be a pop-up which allows to select the source IP of the connection.



Select Source Ip Address

○ 192.168.168.1
○ 192.168.203.1
○ 192.168.178.54
○ 192.168.178.58
○ 127.0.0.1
○ 172.22.48.1

It will list all IP addresses of NICs available on the system with the *Service Endpoint*. Select the IP address used by your client/application. If this is not known, use the value 127.0.0.1 (localhost).

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser`.
- An organization must already exist.
- The *Connector* **c** must exist.
- A *Device* **A** must exist to which the *Connector* **c** is already assigned.
- The user must have the Remote Services role *Remote User* granted with access to this organization and the *Device* **A**.
- The user must have the *Service Endpoint* installed and started.

Procedure

To establish a connection, perform the following steps:

1. Log into tenant as one of the users mentioned above.

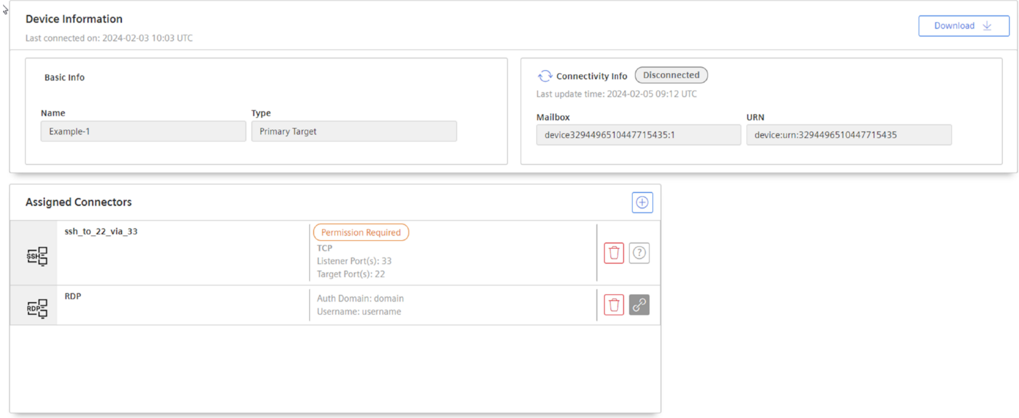
2. Open the "Remote Services" app.

3. From the "Home" screen, select the required organization from the "Organizations" drop-down list and from the "RS Roles" drop-down, select the *Remote users* role.

4. Click on the "Organization" icon. The *Organization* and *Devices page* is displayed where there is also a hierarchical view of the *Nodes* and *Sites*.

5. In the hierarchical view, select the required *Site* and expand it so that the *Devices* are displayed.

6. Select the required *Device* **A**. The *Device Information* screen is displayed which shows a list of assigned *Connectors*.



Device Information
Last connected on: 2024-02-03 10:03 UTC

Basic Info

Name: Example-1
Type: Primary Target

Last update time: 2024-02-05 09:12 UTC

Mailbox: device3294496510447715435:1
URN: device:urn:3294496510447715435

Assigned Connectors

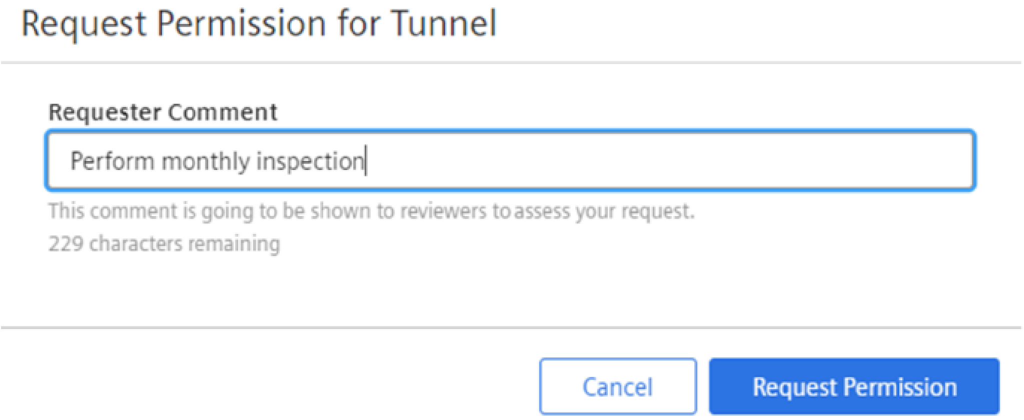
SSH	ssh_to_22_via_33	Permission Required TCP Listener Port(s): 33 Target Port(s): 22
RDP	RDP	Auth Domain: domain Username: username

7. Search for the required *Connector* **c**. Depending on whether the "Permission Required" is configured or not, click:

   - The **chain** icon to establish the connection, if no permission by *Site Owner* is required.

- The **?** icon to establish the connection, if the permission by *Site Owner* is required.
  If **?** icon is clicked to establish the connection, perform the following step:

8. The "Request Permission for Tunnel" screen is displayed. Enter the "Requester Comment" to inform the *Site Owner* about the request.



Request Permission for Tunnel

Requester Comment

Perform monthly inspection

This comment is going to be shown to reviewers to assess your request.
229 characters remaining

For more information about granting permission, refer to the chapter Grant permission.

Result

The connection is established.

Request Permission to Establish Connection

For additional security, the *Organization Admin* can optionally configure a *Connector* to require a *Site Owner* to confirm permission to establish a connection with the given *Connector*.
For that purpose, all the configuration screens for the various *Connector Types* provide an option "Permission Required".

Prerequisites

- Two Insights Hub users **R** and **P** with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser`.
- An organization must already exist.
- The *Connector* **c** must exist.
- The *Connector* **c** must be configured with the option "Permission required".
- A *Device* **A** must exist to which the *Connector* **c** is already assigned.
- The user **R** requesting permission must have the Remote Services role *Remote User* granted with access to this organization and the *Device* **A**.
- The user **P** deciding on permission must have the Remote Services role *Site Owner* granted with access to this organization and the *Device* **A**.

Request Permission

In order to request permission from a site owner, proceed with all the steps as described above.

Accept, Reject or Withdraw Permission Requests

A *Remote User* **R** or *Service Provider* **P** can check the status and history of pending, accepted and rejected permission requests.
The *Remote User* can withdraw their request even when the permission has already been granted.
The *Site Owner* can accept or reject the request, or withdraw the permission granted to the *Remote User*. If the *Site Owner* accepts the request, it is required to specify a time period for which the connection shall be active. After this time period exceeds, the conection will be automatically terminated.

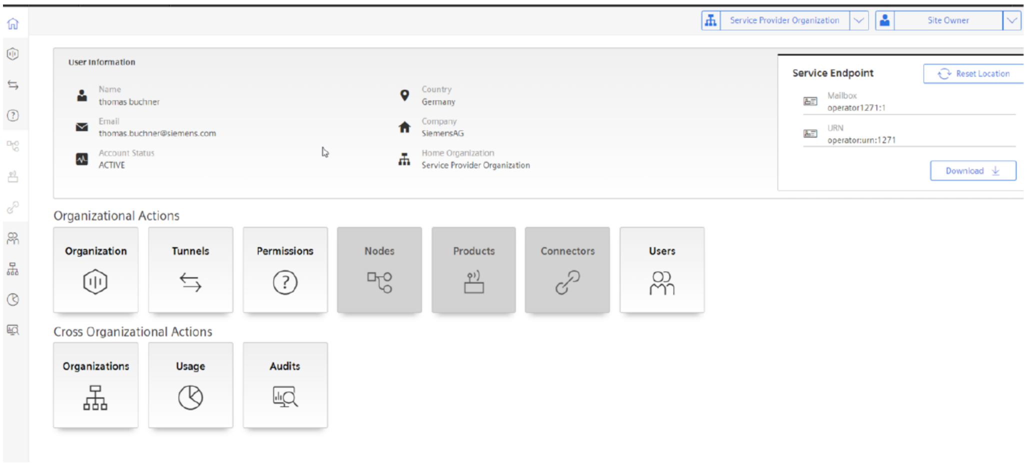
Prerequisites

- Two Insights Hub users **R** and **P** with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser`.
- An organization must already exist.
- The *Connector* **c** must exist.
- The *Connector* **c** must be configured with the option "Permission Required".
- A *Device* **A** must exist to which the *Connector* **c** is already assigned.
- The user **R** requesting permission must have the Remote Services role *Remote User* granted with access to this organization and the *Device* **A**.
- The user **P** deciding on on permission must have the Remote Services role *Site Owner* granted with access to this organization and the *Device* **A**.

Procedure

To check for the status of pending permission requests perform the following steps:

1. Log into tenant as one of the users mentioned above.
2. Open the "Remote Services" app.
3. From the "Home" screen, select the required organization from the "Organizations" drop-down list and from the "RS Roles" drop-down, select the *Remote User* or *Site Owner* role.



User Information

Name: thomas buchner

Email: thomas.buchner@siemens.com

Account Status: ACTIVE

Country: Germany

Company: SiemensAG

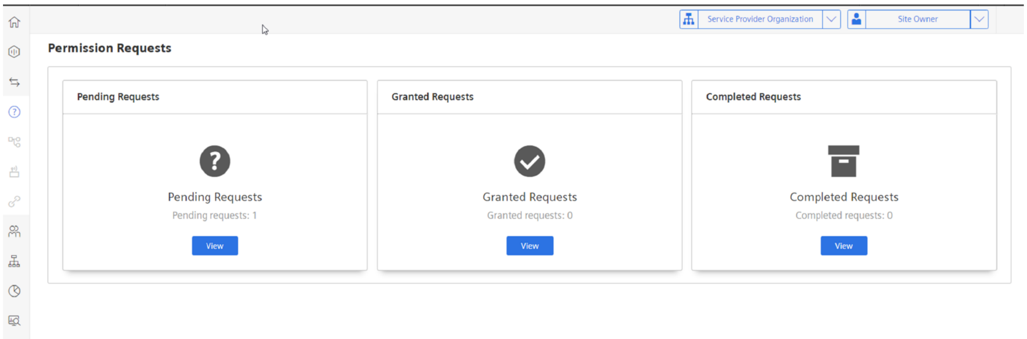
Home Organization: Service Provider Organization

Service Endpoint

Mailbox: operator1271:1

URN: operator:urn:1271

4. Click on the "Permissions" icon. The "Permission Request" screen is displayed.

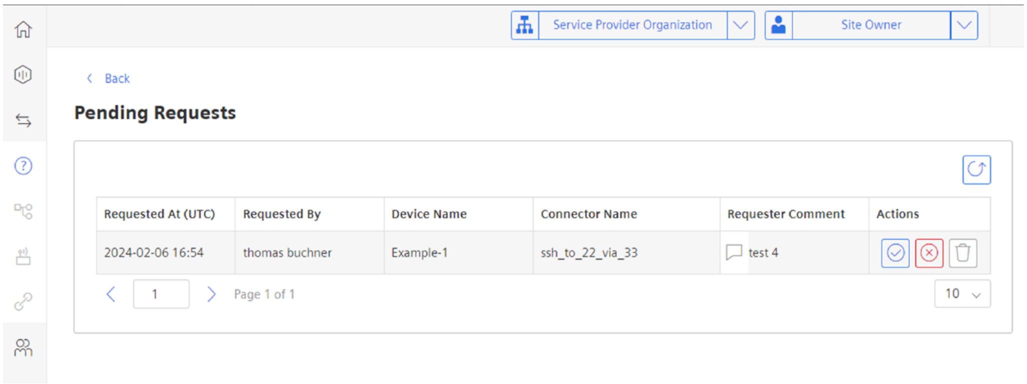


Permission Requests

Pending Requests	Granted Requests	Completed Requests
Pending Requests Pending requests: 1	Granted Requests Granted requests: 0	Completed Requests Completed requests: 0

5. Click on the "View" button in one of the following sections in that screen:

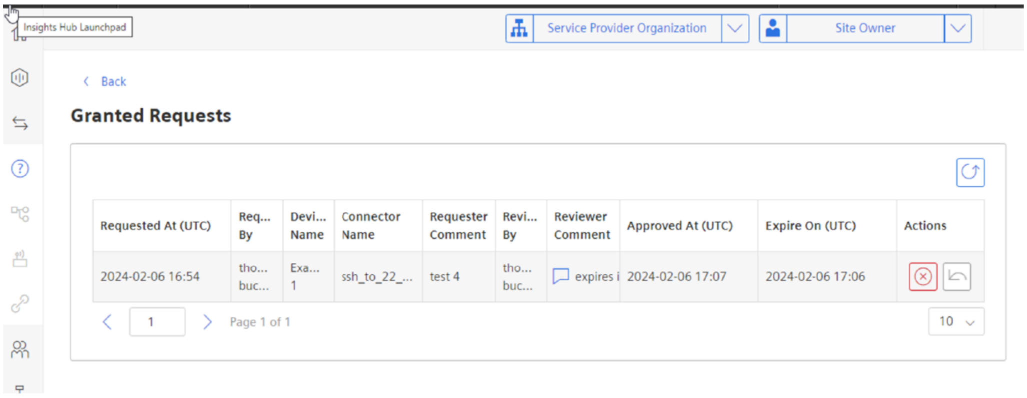
- "Pending Requests" - To approve/reject (*Site Owner* role required) or withdraw (*Remote User* role required) the request.



Pending Requests

Requested At (UTC)	Requested By	Device Name	Connector Name	Requester Comment	Actions
2024-02-06 16:54	thomas buchner	Example-1	ssh_to_22_via_33	test 4	

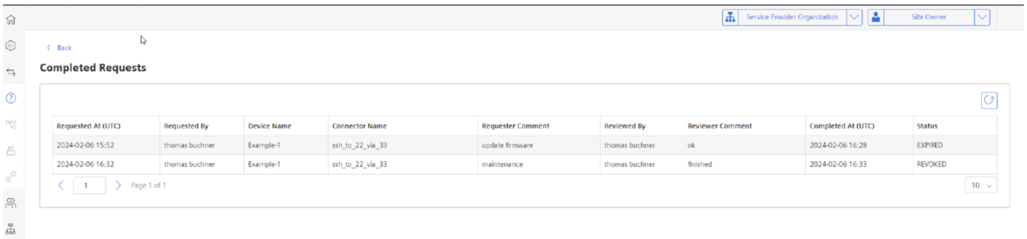
- "Granted Requests" - To view the approved requests and as a Service Owner eventually withdraw the permission.



Granted Requests

Requested At (UTC)	Req... By	Devi... Name	Connector Name	Requester Comment	Revi... By	Reviewer Comment	Approved At (UTC)	Expire On (UTC)	Actions
2024-02-06 16:54	tho... buc...	Exa... 1	ssh_to_22_...	test 4	tho... buc...	expires i	2024-02-06 17:07	2024-02-06 17:06	

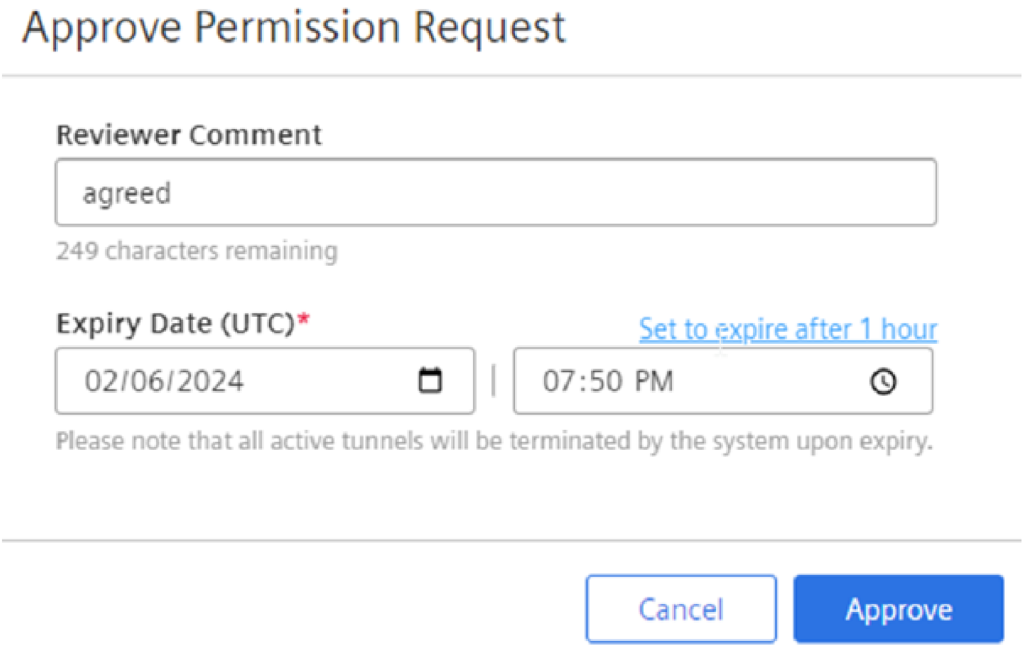
- "Completed Requests" - To view the requests which have been withdrawn, rejected or expired.



Completed Requests

Requested At (UTC)	Requested By	Device Name	Connector Name	Requester Comment	Reviewed By	Reviewer Comment	Completed At (UTC)	Status
2024-02-06 15:52	thomas buchner	Example-1	ssh_to_22_via_33	update firmware	thomas buchner	ok	2024-02-06 16:28	EXPIRED
2024-02-06 16:32	thomas buchner	Example-1	ssh_to_22_via_33	maintenance	thomas buchner	finished	2024-02-06 16:33	REVOKED

6. In one of the screens above, perform the required action:
   - "Approve request" - Specify an expiry time.



Approve Permission Request

Reviewer Comment

agreed

249 characters remaining

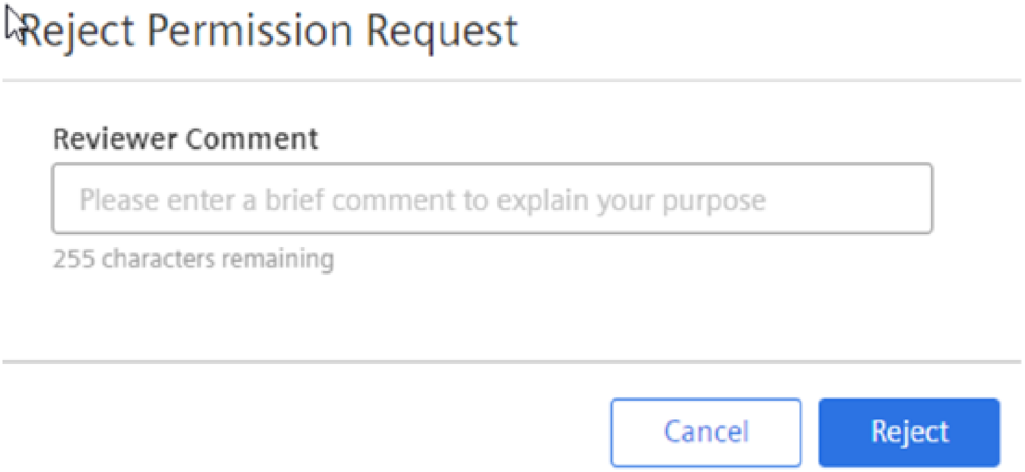
Expiry Date (UTC)*

Set to expire after 1 hour

02/06/2024 | 07:50 PM

Please note that all active tunnels will be terminated by the system upon expiry.

  - "Reject request" - Enter the reason for rejecting the request.



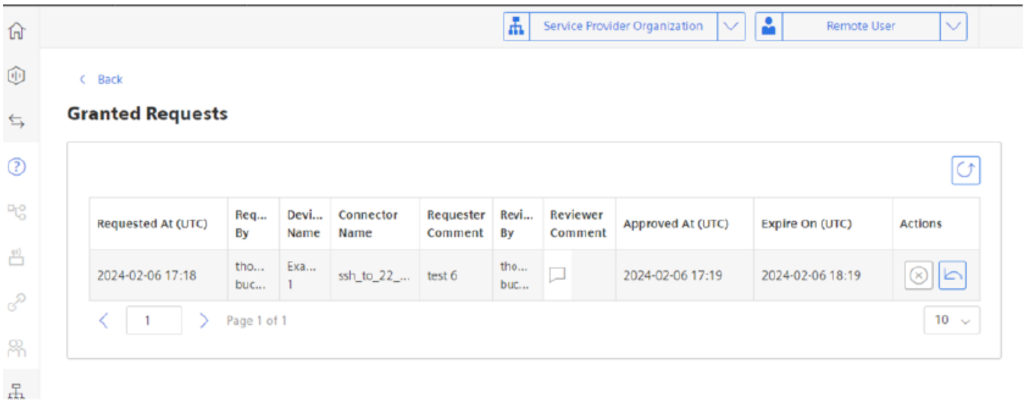
Reject Permission Request

Reviewer Comment

Please enter a brief comment to explain your purpose

255 characters remaining

  - "Withdraw request" - Click on the "Return" icon.



Granted Requests

Requested At (UTC)	Req... By	Devi... Name	Connector Name	Requester Comment	Revi... By	Reviewer Comment	Approved At (UTC)	Expire On (UTC)	Actions
2024-02-06 17:18	tho... buc...	Exa... 1	ssh_to_22_...	test 6	tho... buc...		2024-02-06 17:19	2024-02-06 18:19	

Result

- If the request is approved, the connection will be established.
- If a request is withdrawn while the connection is alredy established, the connection will be terminated. The request will be moved from the "Granted Requests" list to the "Completed Requests" list.
- If a request is withdrawn while it is not yet approved, it will be moved from the "Pending Requests" list to the "Completed Requests" list.

Setting up Users and Access 6

6.1 Setting up Users and Access

Create new user in existing organization

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser` is required.
- An organization must already exist.
- The user must have the Remote Services role *Organization Admin* granted with access to this organization.

Procedure

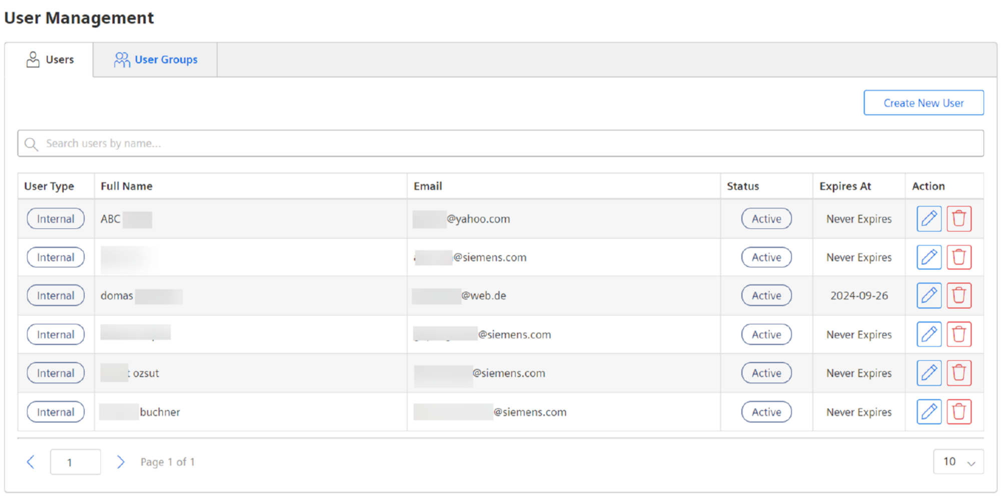
To create a new user to an existing organization, perform the following steps:

1. Log into tenant as one of the users mentioned above.

2. Open the "Remote Services" app.

3. From the "Home" screen, select the required organization from the "Organizations" drop-down list and from the "RS Roles" drop-down, select the *Organization Admin* role.

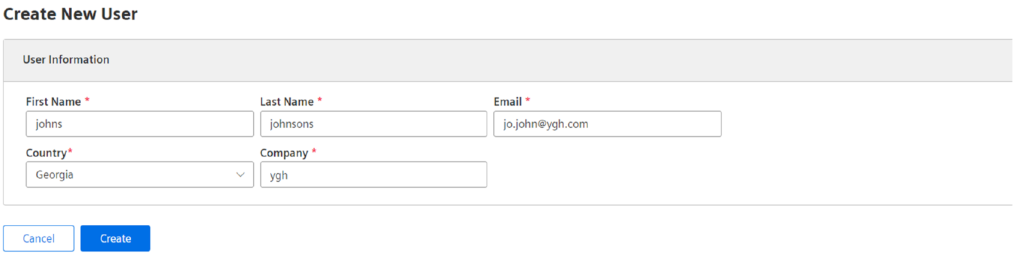
4. Navigate to the "Users" page.



User Type	Full Name	Email	Status	Expires At	Action
Internal	ABC [redacted]	[redacted]@yahoo.com	Active	Never Expires	✎ 🗑
Internal	[redacted]	[redacted]@siemens.com	Active	Never Expires	✎ 🗑
Internal	domas [redacted]	[redacted]@web.de	Active	2024-09-26	✎ 🗑
Internal	[redacted]	[redacted]@siemens.com	Active	Never Expires	✎ 🗑
Internal	[redacted] ozsut	[redacted]@siemens.com	Active	Never Expires	✎ 🗑
Internal	[redacted] buchner	[redacted]@siemens.com	Active	Never Expires	✎ 🗑

5. Click "Create New User".

6. Enter the necessary information for the user. Ensure that the email id is unique in the system.



Create New User

User Information

First Name * johns

Last Name * johnsons

Email * jo.john@ygh.com

Country* Georgia

Company * ygh

7. Click "Create".

- If a user is not an Insights Hub user, this user will be created as a *Standard User* in Insights Hub. This user will get an invitation mail to Insights Hub to confirm the creation of the account and choose a password to log into Insights Hub.
- The Insights Hub user will be granted the Insights Hub role `rsv2 orguser`.

Result

The user is automatically created in "Remote Services" app as an *Internal user* of the current organization. However, the user has no grants assigned yet.

Assign roles and device access rights to existing user within an organization

By default, a newly created Organization user does not have Remote Services Roles and access rights for devices in the hierarchy of the organization.
The roles which can be assigned by this procedure are:

- Organization Admin
- Remote User
- Site Owner

Prerequisites

- An Insights Hub user with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser`.
- An organization with structure and product hierarchy must already exist.
- The user must have the Remote Services role *Organization Admin* granted with access to this organization.
- A user must have been created according to above procedure.

Procedure

To assign roles and access rights for a user in an existing organization, perform the following steps:

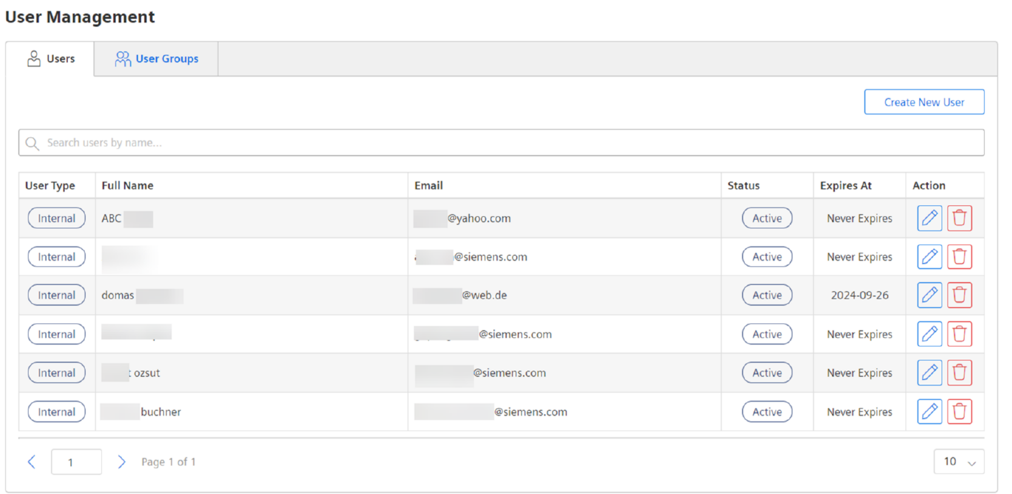
1. Log into tenant as one of the users mentioned above.

2. Open the "Remote Services" app.

3. From the "Home" screen, select the required organization from the "Organizations" drop-down list and from the "RS Roles" drop-down, select the *Organization Admin* role.

4. In the "Home" screen of the Organization, click on the "Users" icon. The "Users" overview page is displayed.

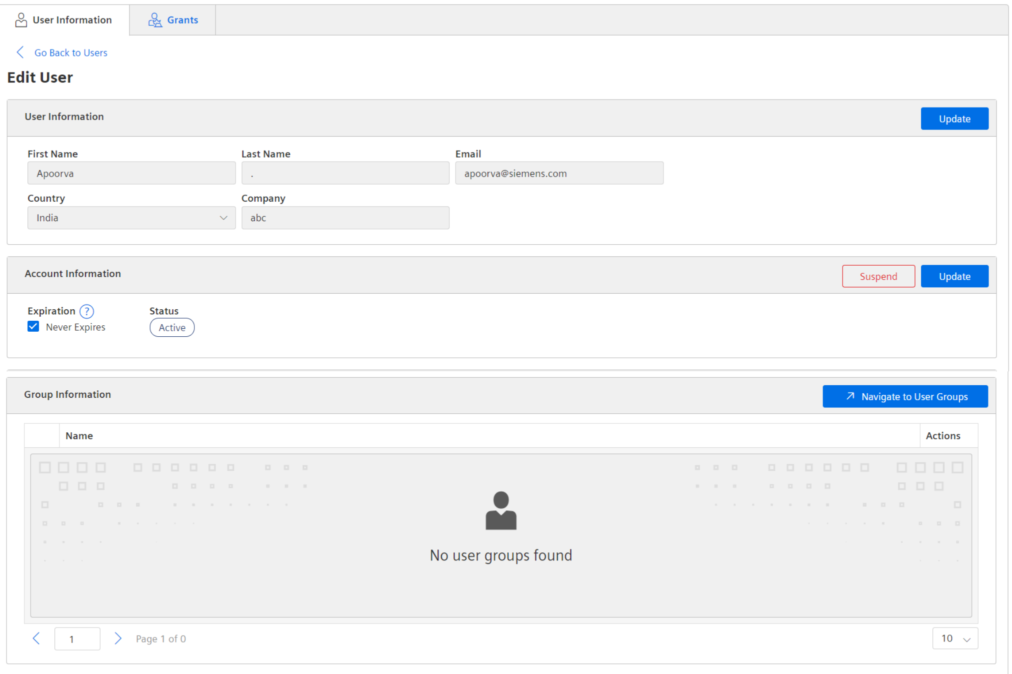
5. Select the required user and click the "Edit" icon.



User Management

User Type	Full Name	Email	Status	Expires At	Action
Internal	ABC [redacted]	[redacted]@yahoo.com	Active	Never Expires	✎ 🗑
Internal	[redacted]	[redacted]@siemens.com	Active	Never Expires	✎ 🗑
Internal	domas [redacted]	[redacted]@web.de	Active	2024-09-26	✎ 🗑
Internal	[redacted]	[redacted]@siemens.com	Active	Never Expires	✎ 🗑
Internal	[redacted] ozsut	[redacted]@siemens.com	Active	Never Expires	✎ 🗑
Internal	[redacted] buchner	[redacted]@siemens.com	Active	Never Expires	✎ 🗑

6. A page with the user's details is displayed.



Edit User

User Information

First Name: Apoorva
Last Name: .
Email: apoorva@siemens.com
Country: India
Company: abc

Account Information

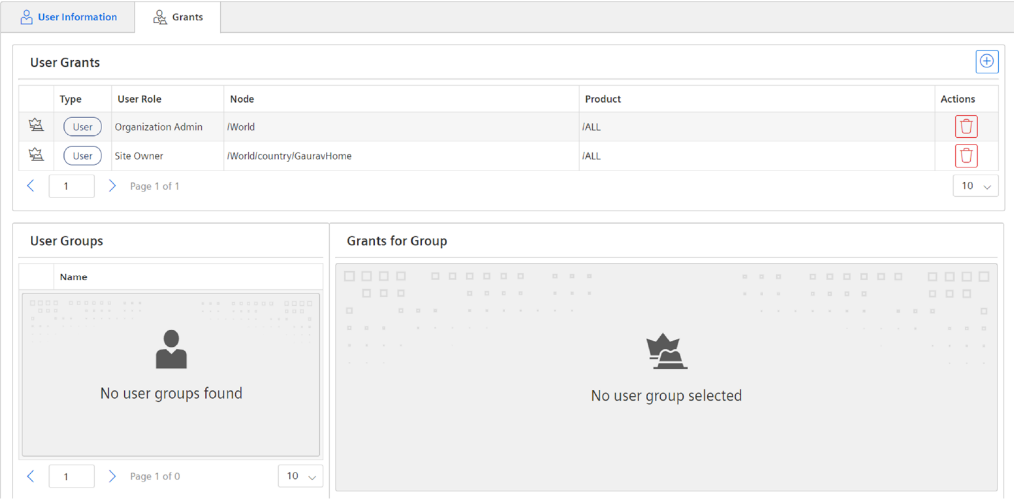
Expiration ?
☑ Never Expires
Status: Active

Group Information

Name	Actions

No user groups found

7. Click on the "Grants" tab. The Grants overview page is displayed.



User Information | Grants

User Grants

	Type	User Role	Node	Product	Actions
	User	Organization Admin	/World	/ALL	
	User	Site Owner	/World/country/GauravHome	/ALL	

1 Page 1 of 1 10

User Groups

	Name

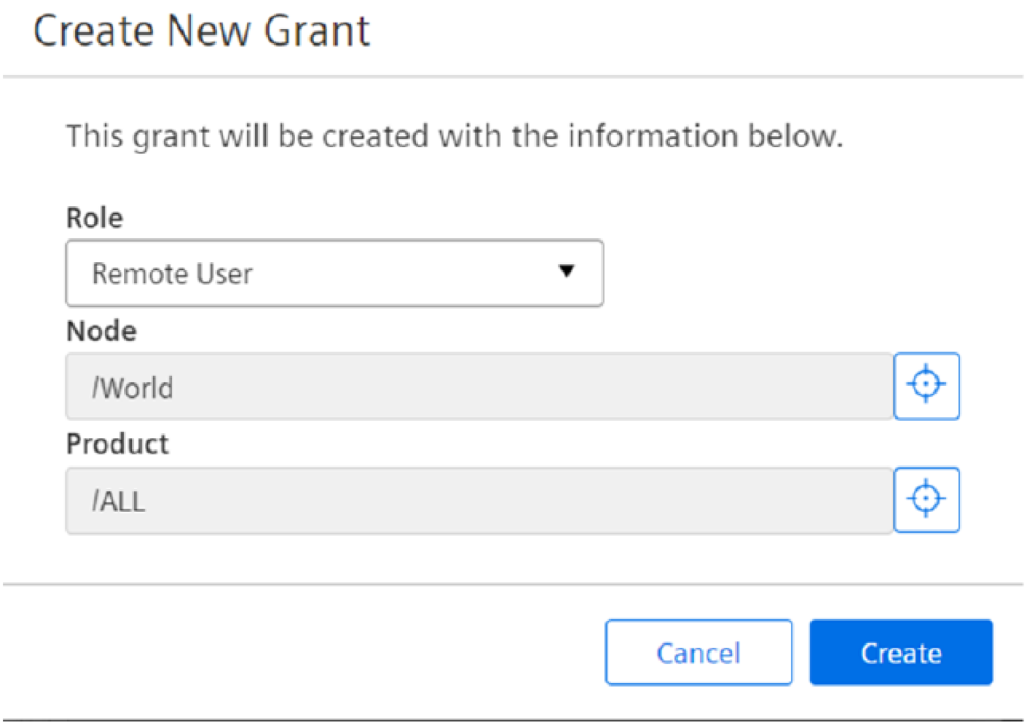
No user groups found

1 Page 1 of 0 10

Grants for Group

No user group selected

8. Click on the *plus* icon. A Pop-up window "Create New Grant" is displayed.



Create New Grant

This grant will be created with the information below.

Role: Remote User

Node: /World

Product: /ALL

9. Select the required Remote Services Role* to be granted to the user.

10. Select the required level in the "Node or Site hierarchy".

11. Select the required level in the "Product hierarchy".

12. Click "Create".

To grant the same user role on different levels of the hierarchies, repeat the above procedure.

Result

The user has been granted the required Remote Services Role and has access to devices that match the specified structure and product level in the respective hierarchies.

Grant or revoke Organization Owner Role to/from Organization User

The Service Provider who created the Organization automatically becomes a user in that Organization and is also assigned the RS role Organization Owner of that Organization.
As an Organization Owner, it is possible to assign the Organization Owner role to other internal or external users in the Organization.
Additionally, the other Organization Owners can also be removed. This is useful when it is required to hand over an Organization after it has been created.

Prerequisites

- An Insights Hub user **A** with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser`.
- An organization **O** must already exist.
- The user must have the Remote Services role *Organization Owner* granted with access to organization **O**.
- Another user **B** must have been created for **O** as described in the section Creating a new user or successfully been referred as external user to *Organization* **O** as described in the section Referring an external user.

Procedure to grant Organization Owner Role

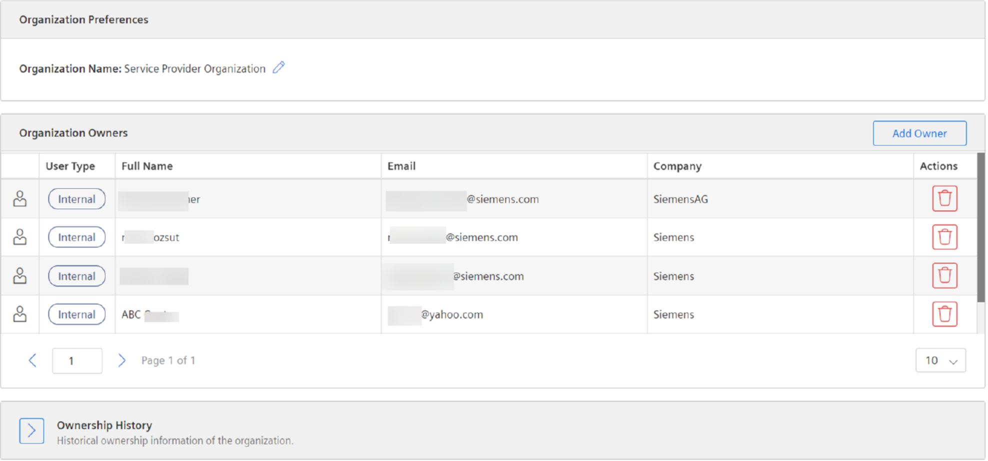
To grant user **B** the Organization Owner role for Organization **O**, perform the following steps:

1. Log into tenant as users **A**.

2. Open the "Remote Services" app.

3. From the "Home" screen, select the required organization from the "Organizations" drop-down list and from the "RS Roles" drop-down, select the `Organization Owner` role.

4. In the "Home" screen of the organization, click on the "Organization" icon in the "Organizational Actions" section. The "Organization Preferences" screen is displayed.



Organization Preferences

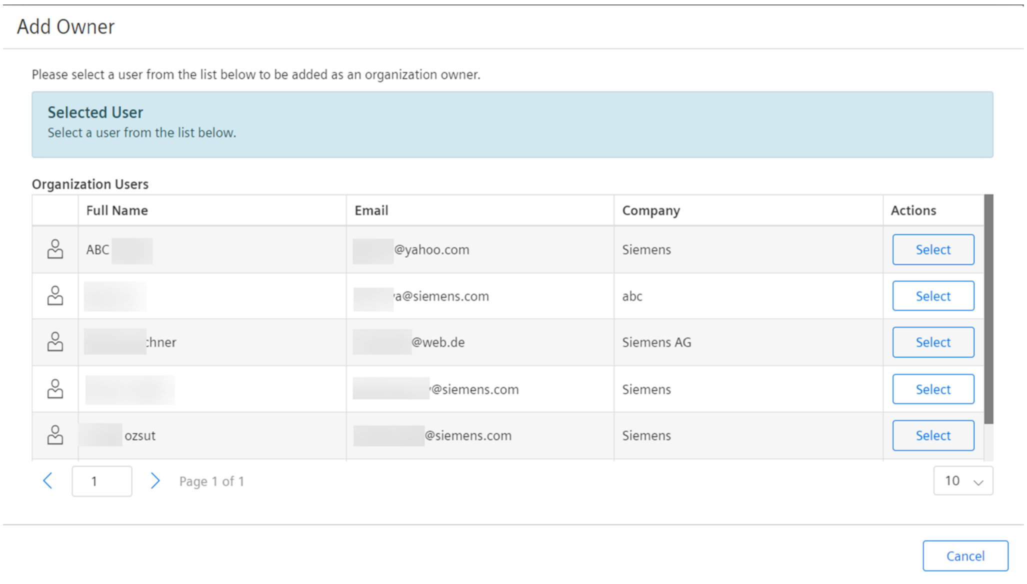
Organization Name: Service Provider Organization

Organization Owners

	User Type	Full Name	Email	Company	Actions
	Internal	[redacted] ıer	[redacted]@siemens.com	SiemensAG	🗑
	Internal	r [redacted] ozsut	ı [redacted]@siemens.com	Siemens	🗑
	Internal	[redacted]	[redacted]@siemens.com	Siemens	🗑
	Internal	ABC [redacted]	[redacted]@yahoo.com	Siemens	🗑

Ownership History
Historical ownership information of the organization.

5. Click on the "Add Owner" button. The "Add Owner" screen is displayed.



Add Owner

Please select a user from the list below to be added as an organization owner.

Selected User
Select a user from the list below.

Organization Users

	Full Name	Email	Company	Actions
	ABC [redacted]	[redacted]@yahoo.com	Siemens	Select
	[redacted]	[redacted]a@siemens.com	abc	Select
	[redacted]hner	[redacted]@web.de	Siemens AG	Select
	[redacted]	[redacted]@siemens.com	Siemens	Select
	[redacted]ozsut	[redacted]@siemens.com	Siemens	Select

6. Select user **B** from the list of the organization's users and click "Add".

7. The "Organization Preferences" screen is displayed again and shows the user **B** as additional `Organization Owner`.

Result

User **B** is now `Organization Owner` of Organization **O**.

Procedure to revoke Organization Owner Role

To revoke user **B**'s `Organization Owner` role for Organization **O**, perform the following steps:

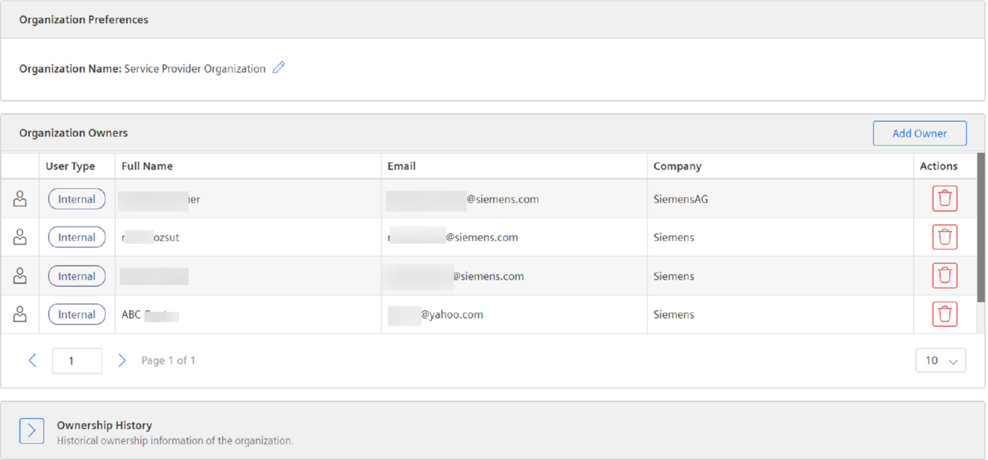
1. Log into tenant as user **A**.

2. Open the "Remote Services" app.

3. From the "Home" screen, select Organization **O** from the "Organizations" drop-down list and from the "RS Roles" drop-down, select the `Organization Owner` role.

4. In the "Home" screen of the organization, click on the "Organization" icon in the "Organizational Actions" section.

5. The "Organization Preferences" screen opens.



Organization Preferences

Organization Name: Service Provider Organization

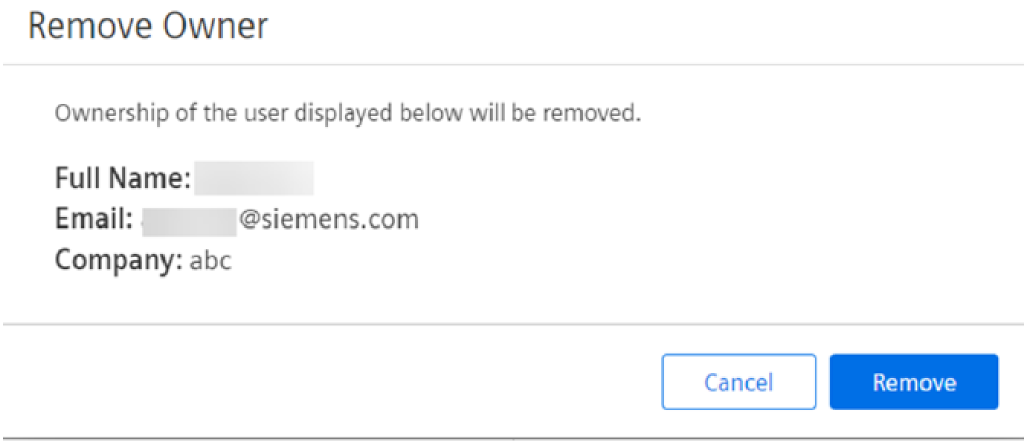
Organization Owners

User Type	Full Name	Email	Company	Actions
Internal	[redacted]	[redacted]@siemens.com	SiemensAG	🗑
Internal	[redacted]	[redacted]@siemens.com	Siemens	🗑
Internal	[redacted]	[redacted]@siemens.com	Siemens	🗑
Internal	ABC [redacted]	[redacted]@yahoo.com	Siemens	🗑

Ownership History
Historical ownership information of the organization.

6. Select Owner **B** in the `Organization Owners` section and click the "Delete" icon.

7. A confirmation dialog is displayed. Click on the "Remove" button.



Remove Owner

Ownership of the user displayed below will be removed.

Full Name: [redacted]
Email: [redacted]@siemens.com
Company: abc

Result

The `Organization Owner` role of user **B** is revoked, but user **B** still remains a user with all other assigned RS Roles in Organization **B**.

Referring an External user to an Organization

It is possible to refer users which are created within the *Service Provider Organization* to another organization. In the other organization, they are considered as *External Users*.

Prerequisites

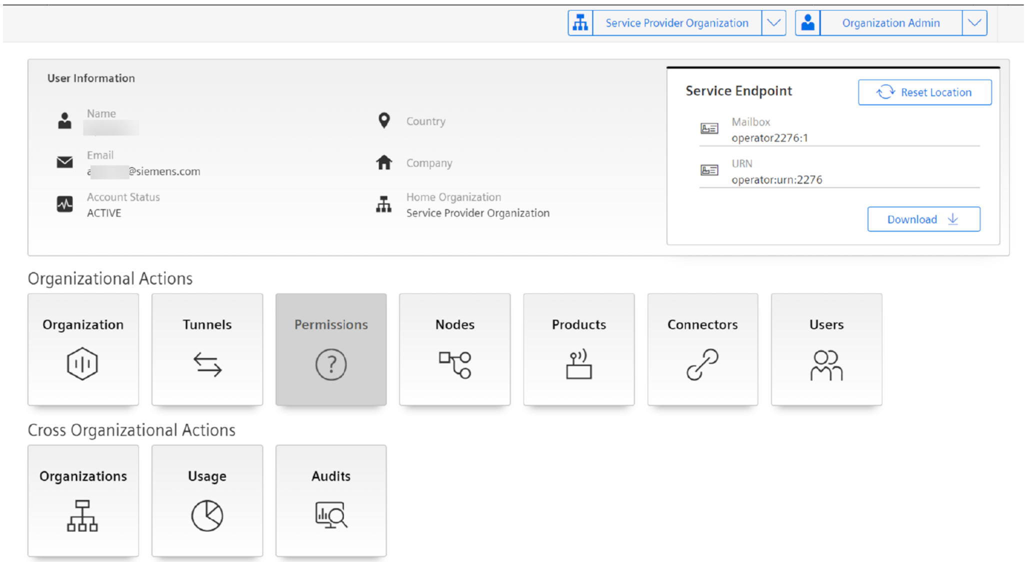
- Two Insights Hub users **A** and **B** with Insights Hub Role `rsv2 serviceowner` are required.
- A target organization must already exist.

Procedure

To refer user **B** to an existing organization, perform the following steps:

1. Log into tenant as user **A**.

2. Open the "Remote Services" app. The Home screen is displayed.



Service Provider Organization | Organization Admin

User Information

Name [redacted]

Email [redacted]@siemens.com

Account Status ACTIVE

Country

Company

Home Organization Service Provider Organization

Service Endpoint — Reset Location

Mailbox operator2276:1

URN operator:urn:2276

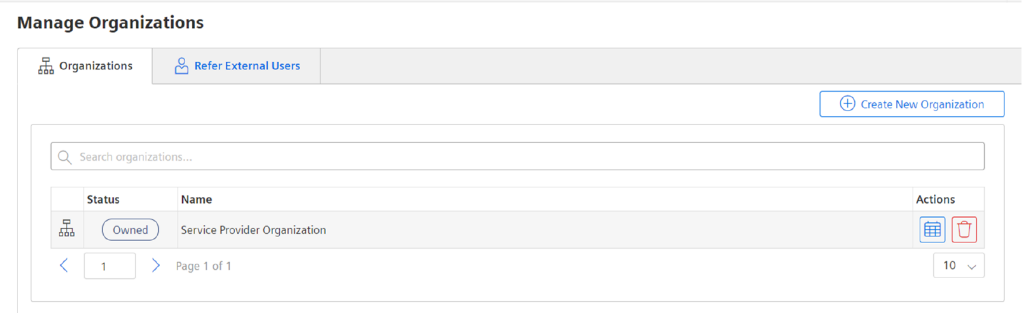
Download

Organizational Actions

Cross Organizational Actions

3. In the "Home" screen, select the "Organizations" icon from the "Cross Organizational Actions".

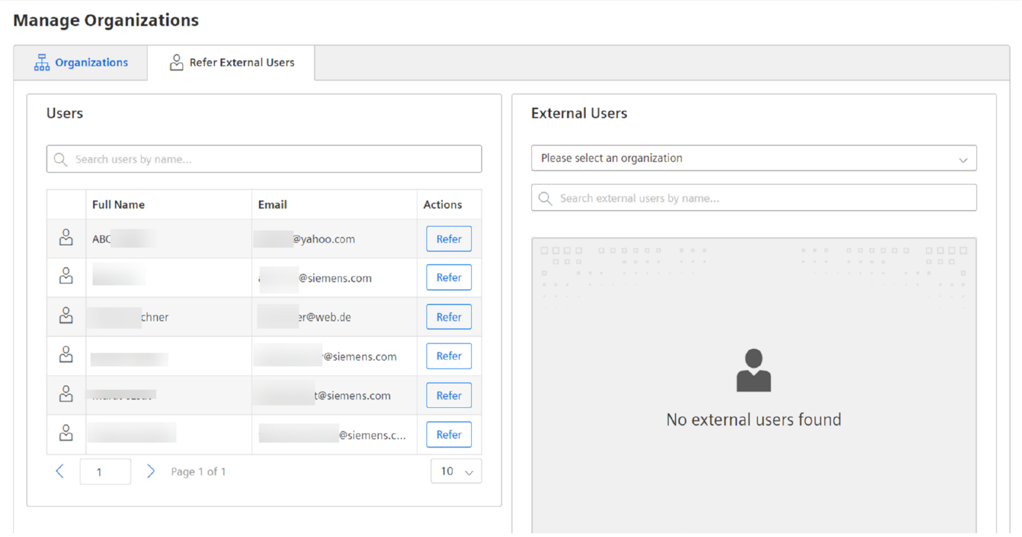
4. The "Manage Organizations" screen is displayed.



Manage Organizations

	Status	Name	Actions
	Owned	Service Provider Organization	

5. Select the "Refer External Users" tab. The referral screen is displayed which shows an overview of users which can be referred to other organizations. Click "Refer" next to the user **B** who needs to be referred to another organization.



Manage Organizations

Users

	Full Name	Email	Actions
	ABC[redacted]	[redacted]@yahoo.com	Refer
	[redacted]	[redacted]@siemens.com	Refer
	[redacted]chner	[redacted]er@web.de	Refer
	[redacted]	[redacted]@siemens.com	Refer
	[redacted]	[redacted]t@siemens.com	Refer
	[redacted]	[redacted]@siemens.c...	Refer

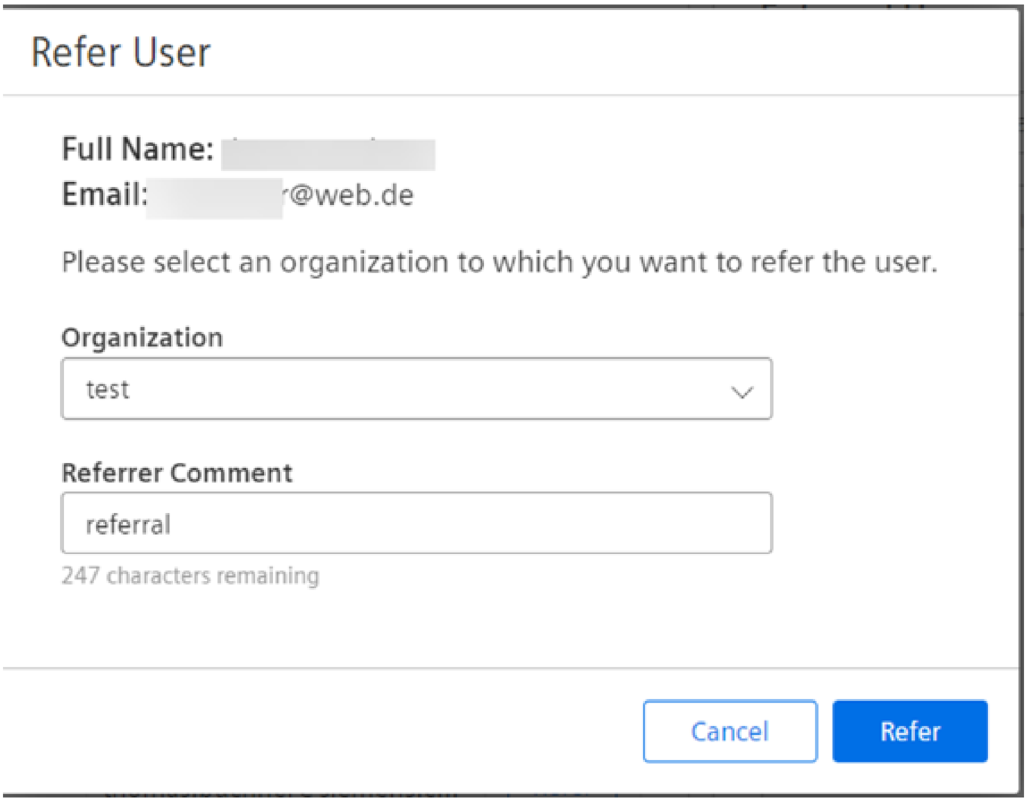
External Users

Please select an organization
Search external users by name...

No external users found

6. A pop-up window appears with a drop-down list of organizations.

7. Select the required organization. Enter a comment which explains the purpose of the referral and click "Refer".



Refer User

Full Name: [redacted]
Email: [redacted]@web.de

Please select an organization to which you want to refer the user.

Organization: test

Referrer Comment: referral

247 characters remaining

Result

- User **B** has been referred to the required organization.
- User **B** will appear in the external users screen of the organization in the section "Referred Users".
- The *Organization Owner* has the rights to accept or reject that referral.

Accepting or rejecting referrals of external user to organization

An external user becomes a member of an organization only when the referral is accepted by the `Organization Owner`. However, the `Organization Owner` has all the rights to reject the referral.
The following procedures explains how to perform these actions:

Prerequisites

- An Insights Hub user **A** with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser`.
- An organization **X** must already exist.
- User **A** has the Remote Services role *Organization Owner* for the target organization **X**.

- An external user **B** has been referred to organization X.

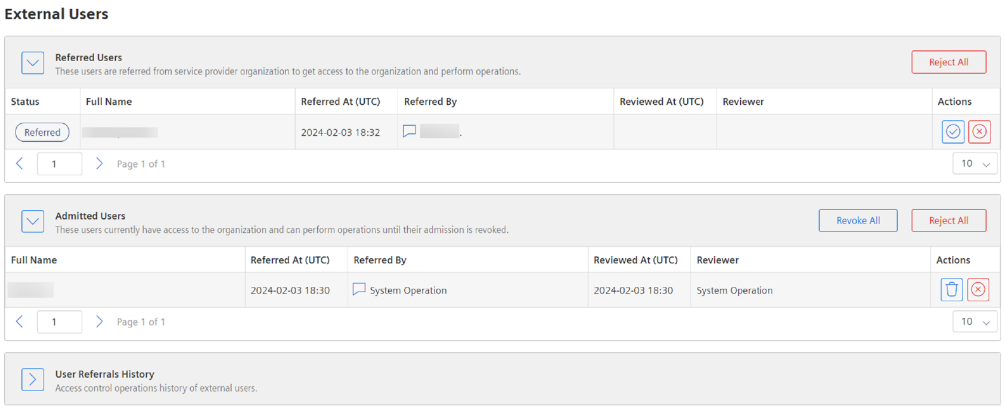
Procedure

1. Log into tenant as user **A**.

2. Open the "Remote Services" app.

3. In the "Home" screen, select "Organization X" from the Organization drop-down menu and select the role `Organization Owner` from the Roles drop-down menu.

4. Click "External Users". The "External Users" screen is displayed.



External Users

Referred Users
These users are referred from service provider organization to get access to the organization and perform operations.

Status	Full Name	Referred At (UTC)	Referred By	Reviewed At (UTC)	Reviewer	Actions
Referred	[redacted]	2024-02-03 18:32	[redacted].			✓ ⊗

Admitted Users
These users currently have access to the organization and can perform operations until their admission is revoked.

Full Name	Referred At (UTC)	Referred By	Reviewed At (UTC)	Reviewer	Actions
[redacted]	2024-02-03 18:30	System Operation	2024-02-03 18:30	System Operation	🗑 ⊗

User Referrals History
Access control operations history of external users.

5. In the "Referred Users" section, select the line with the referral of user **B** that you want to accept or reject.

6. Click "Accept" to accept the referral or "Reject" to reject the referral.

Result

- If you had clicked "Accept",
  - User **B** becomes a user of organization **X**.
  - User B has no *grants* yet within organization **X**.
  - User **B** will be shown in the "Admitted Users" section of the "External Users" screen.
- If you had clicked "Reject",
  - User **B** is not a user of organization **X**.
  - User **B** will disappear from the "External Users" screen of organization **X**.

Suspend or remove an external user from within an organization

An external user which has been accepted to an organization can be suspended (i.e. brought back into the referred state) or completely be removed by the `Organization Owner` of the organization.
The following procedures explain how to perform these actions:

Prerequisites

- An Insights Hub user **A** with Insights Hub Role `rsv2 serviceowner` or `rsv2 orguser`.
- An organization **X** must already exist.
- User **A** has the Remote Services role *Organization Owner* for the target organization **X**.
- An external user **B** has been accepted to organization **X**.

Procedure

1. Log into tenant as user **A**.

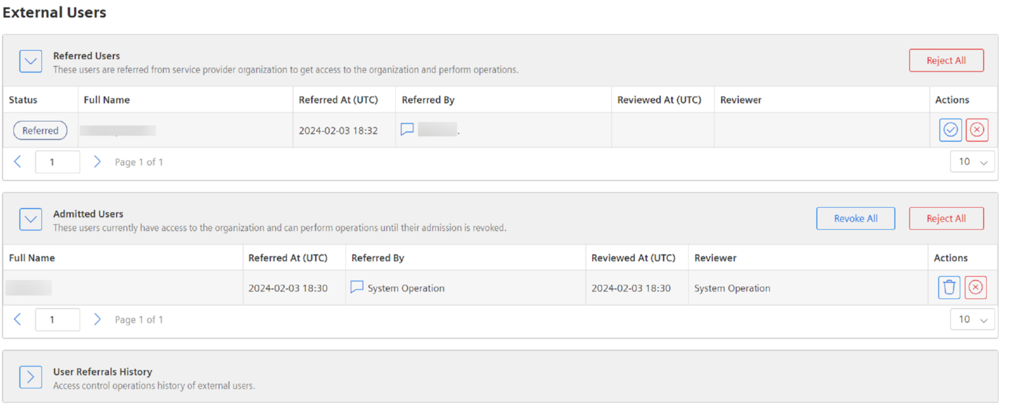
2. Open the "Remote Services" app.

3. The "Home" screen opens.

4. In the "Home" screen select "Organization X" from the organization drop-down menu and select role "Organization Owner" from the role drop-down menu.

5. Click on the "External Users" icon.

6. The "External Users" screen opens.



External Users

Referred Users

These users are referred from service provider organization to get access to the organization and perform operations.

Status	Full Name	Referred At (UTC)	Referred By	Reviewed At (UTC)	Reviewer	Actions
Referred	[redacted]	2024-02-03 18:32	[redacted]			

Page 1 of 1

Admitted Users

These users currently have access to the organization and can perform operations until their admission is revoked.

Full Name	Referred At (UTC)	Referred By	Reviewed At (UTC)	Reviewer	Actions
[redacted]	2024-02-03 18:30	System Operation	2024-02-03 18:30	System Operation	

Page 1 of 1

User Referrals History

Access control operations history of external users.

7. In the "Admitted Users" section, select the line with the details of user **B** that you want to suspend or remove.

8. Click on the "Revoke" icon to suspend user **B** or on the "Reject" icon to remove user **B**.

Result

- User **B** is no longer a user of organization **X**.
- If "Revoke" has been clicked,
  - User **B** will be shown in the "Referred Users" section of the "External Users" screen and can be later admitted again.
- If "Reject" has been clicked,
  - User **B** will disappear from the "External Users" screen of organization **X**.

Remove an external user from organization by a Service Provider

An external user which has been accepted to an organization can be removed by any *Service Provider* even if he is not a user of that organization.
The following procedure describe how to perform this:

Prerequisites

- An organization **X** must already exist
- An external user **B** has been accepted to organization X.
- An Insights Hub user **A** with Insights Hub Role `rsv2 serviceowner` is required. It is is not required that user **A** is a user of organization **X**.

Procedure

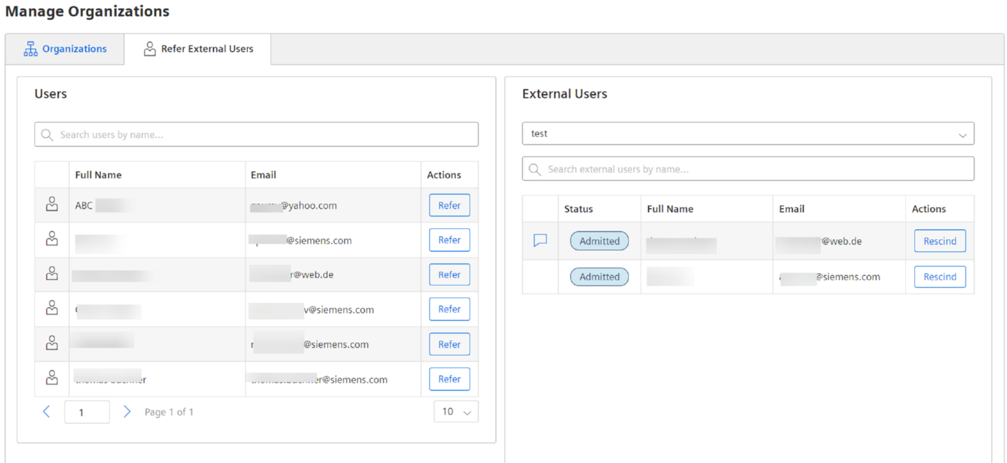
1. Log into tenant as user **A**.

2. Open the "Remote Services" app.

3. In the "Home" screen, under the section "Cross Organizational Actions", click "Organizations" icon. The "Manage Organizations" screen is displayed.

4. Click the "Refer External Users" tab.

5. The **Refer External Users** screen is displayed. In the "External Users" section, select the organization **X** from the drop-down menu.



Manage Organizations

Users

Search users by name...

	Full Name	Email	Actions
	ABC [redacted]	[redacted]@yahoo.com	Refer
	[redacted]	[redacted]@siemens.com	Refer
	[redacted]	[redacted]r@web.de	Refer
	[redacted]	[redacted]v@siemens.com	Refer
	[redacted]	[redacted]@siemens.com	Refer
	[redacted]r	[redacted]r@siemens.com	Refer

1 Page 1 of 1 10

External Users

test

Search external users by name...

	Status	Full Name	Email	Actions
	Admitted	[redacted]	[redacted]@web.de	Rescind
	Admitted	[redacted]	[redacted]@siemens.com	Rescind

6. A list with all the *External Users* in that organization is displayed. Search for the external user **B** and click on the "Remove" button.

Result

User **B** is removed from the organization **X**.

Add a new ServiceOwner to tenant

Prerequisites

- An Insights Hub user with Insights Hub Role `Tenant Admin`.
- **Remote Services** must be provisioned to the tenant.

Procedure

To create a new `ServiceOwner` to the tenant, perform the following steps:

1. Log into tenant as the user mentioned above.
2. Open the Insights Hub "Settings" app.
3. In the "Users" section, click "Check Users". The *Users* page is displayed.
4. Click "Create User". The "Create User" screen is displayed.
5. Enter the new users's details.
6. In the "Assign roles" section, select atleast "StandardUser".
7. In the "Assign roles" section, select also the Application Role `rsv2 service owner`.
8. Click "Create User".

The procedure for the `Tenant Admin` is completed.

Result

- The new user will get an invitation via the email address provided during creation.
- The user will be prompted to create the account details in response to that email and to confirm the eMail address.
- After the user has logged in for the first time into Remote Services and acknowledged acceptance to the business rules, the user is considered as a user of Remote Services.
- The user is automatically created in Remote Services app as an *Internal user* of the "Service Provider Organization" with the Remote Services Roles `Organization Owner` and `Organization Admin`.

Remote Services Network Settings 7

7.1 Network Settings

Network connections used by Remote Services

To use the "Remote Services" application, access to Insights Hub is required to log into the tenant and to access supporting applications like "Settings", "Asset Management" and "MindConnect Agent" UIs.
In order to connect a *Service Network* with a *Factory Network*, Remote Services establishes two encrypted tunnels:

- A tunnel between the **Service Network** and the **Insights Hub Backend**. This tunnel is established by the *Service Endpoint*.
- A tunnel between the **Factory Network** and the **Insights Hub Backend**. This tunnel is established by the *Device Endpoint*.

RS uses the WebSocket Secure (WSS) protocol for these tunnels.

Configuration Guidelines for Firewalls

In case a firewall is used, the following configurations are needed to enable access to and from the network locations that are used for Remote Services.
For Outbound traffic:

- Destination Server Port: **443**
- URLs to be white listed for Remote Services:
  - https://connectivity.eu1.vpnrts.mindsphere.io/uaa/oauth/token
  - https://s3restriction.eu1.vpnrts.mindsphere.io:443
  - https://wss.eu1.vpnrts.mindsphere.io:443/mts/
  - https://wss.eu1.vpnrts.mindsphere.io:443/ccf/
- Access to Insights Hub domain must be whitelisted:
  - *.eu1.mindsphere.io
- Protocol WebSocket Secure (WSS)

For Inbound Traffic:

- Protocol WebSocket Secure (WSS)

Configuration Guidelines for Network Proxies

In case a proxy is used, the following configurations are needed to enable access to and from the network locations that are used for Remote Services:

For Outbound traffic:

- Destination Server Port: **443**
- URLs to be whitelisted:
    - https://connectivity.eu1.vpnrts.mindsphere.io/uaa/oauth/token
    - https://s3restriction.eu1.vpnrts.mindsphere.io:443
    - https://wss.eu1.vpnrts.mindsphere.io:443/mts/
    - https://wss.eu1.vpnrts.mindsphere.io:443/ccf/
- Access to Insights Hub domain must be whitelisted:
    - *.eu1.mindsphere.io
- Protocol WebSocket Secure (WSS)

Proxy timeout settings

The value of the proxy timeout setting determines the maximum duration a WSS session will remain active. Hence, this value must be greater or equal than the desired session time out that is configured in the *Connector* setup for a specific connection.

Troubleshooting 8

8.1 Troubleshooting

This section provides tips and tricks for guiding users towards resolution of setup of communication issues.

General information

Please consider:

- Remote Services (RS) was designed to deliver network-to-network access to customer-owned apps, that communicate via IP-based protocols (OSI layer 3), but it does not comprise any apps using the provided access. For instance, if Remote Login protocols such as RDP or VNC are going to be used, the required client and server apps are typically provided by the Operating Systems of the Service Device (hosting the Service Endpoint) and a corresponding Device (hosting the Device Endpoint), where RDP is typically delivered with Windows®. In a similar way, the user would provide engineering tools or other apps, that want to integrate across network boundaries.
- The download package of the Service Endpoint contains a Windows® 10 driver (installer file `RSTransparentProxy.msi`). This driver must be installed on Service Devices to use them for remote engineering leveraging ISO protocol over TCP (RFC-1006), which underlies the Proxy-Unaware protocol supported by RS.

Setup issues

Please consider:

- Release notes cover RS and inform about recommended or validated hardware and software configurations such as Operating Systems or suggested device characteristics.
- Download of Service Endpoints and Device Endpoints is subject to export control (ECC). Please eensure, that the public IP address of a computer initiating an Endpoint download must match the country of the user operating the download. Using VPNs might have an impact here by relocating a user's IP address to another country. It is possible for an *Organization Admin* to temporarily modify the user's registered location following this procedure.
- Downloaded Service Endpoints have individual configurations, that bind them to a particular Siemens cloud tenant and users. Thus, they cannot be shared among users. A given user can

however use the same *Service Endpoint* on multiple computers. If the same *Service Endpoint* shall be used of different computers it is required to Reset Location according to this procedure each time when switching the computers.

- To establish tunnel-based network-to-network connectivity, there must be RS-compliant Endpoints at either end. Please ensure, that *Service Endpoints* and *Device Endpoints* are up and running and that your network is configured appropriately enabling them to connect to Siemens cloud as outlined below.
- Linux systems typically require `root` privileges to execute the Endpoints.

Access issues

Please consider:

- Remote Services apply Fine-Grained Access Control and enforces a RS-specific role model as outlined in section Remote Services: Overview and Key Concepts. In such setup, users typically may use only certain *Organizations* or *Sites* or *Products* of the RS device tree. See Remote Services: Setup Users and Access for details. If certain functionalities seem to be unusable or not even visible, please check your access rights or have them checked by *Organization Admin*.
- Please ensure, that an *Organization Admin* granted your user account with all necessary access rights and roles required to perform a particular operation as per your Siemens cloud tenant's or its owner's policies. This implies, that only those users, who have the required access rights, may perform certain operations such as deleting a particular *Device* from a particular *Site*.
- Users having multiple roles, may explicitely switch between them, because only one role will be active at a time to avoid unintended tampering or changes.
- If *Service Endpoints* are used on a computer connecting to the Internet via VPN, then the geo-location of that PC's public IP address might be different from the registered physical geo-location of the PC and its user. That impacts the behavior of certain functions such as the download of *Device Endpoints*, because the user's registered physical geo-location and the IP-addresses' geo-location do not match. In such cases either deactivate the VPN or adapt the user's geo-location to the geo-location of the public VPN IP address by means of RS user management as described in this procedure. Public services such as `https://WhatIsMyIP.com` may help with determining the geo-location of a PC's public IP address.
- *Connectors* will be assigned to certain *Devices* and only users with the the role *Remote User* can establish connections. However not every *Remote User* may have access to a given *Site* or *Product*. This depends on the grants the *Organization Admin* has given to that *Remote User*.

Network issues

Please consider:

- Ensure that network and firewall setups do permit tunnel-based connections to MindSpere Remote Services. Further details are given in section Remote Services Network Settings.
- For native Remote Login (not using a browser) and all custom connections using Remote Engineering Option it is necessary to launch the Service Endpoint before issuing any connection requests to *Devices* via the user interface. Connection Requests also demand targeted Device Endpoints to be up and running.
- When launching a Service Endpoint on Windows® then Powershell should be used instead of the Command Prompt. When using the Command Prompt press "Return" a few times to ensure that the Endpoint starts.
- Engineering protocols: please match the targeted remote web server's protocol (HTTP vs. HTTPS) when using "Web Application".
- *Connectors* will be assigned to certain *Devices* and only users with the the role *Remote User* can establish connections. However not every *Remote User* may have access to a given *Site* or *Product*.
- In case of *Service or Device Endpoints* not connecting to Siemens cloud starting the respective Endpoint in diagnostic mode via the command `rs-client --diagnose` (Linux) or `remote-client.exe --diagnose` (Windows®). will give first indications on potential network configuration issues. After doing so please restart the client in regular mode - i.e. without the parameter `--diagnose`.
- For network communication with Remote Services (RS) backend, the Operating System (OS) hosting the RS Endpoint (*Service or Device Endpoint*) needs to support TLS1.2. Related to that, the Operating System (OS) hosting the RS Endpoint (*Service or Device Endpoint*) needs to support OpenSSL libraries with version 1.0.1 or later. The reason is, that the RS Endpoint has a dependency on OpenSSL dynamic link libraries (DLLs). OpenSSL is a "robust, commercial-grade, full-featured toolkit for general-purpose cryptography and secure communication.
- For proper symbolic name resolution (Domain Name Service (DNS)), please ensure that network nodes hosting RS Endpoints (*Service or Device Endpoint*) are configured with appropriate name servers (DNS servers). Please check DNS server settings in Operating System (OS) settings.

Useful links

List of references:

- Siemens Software Support Center
- OpenSSL