rexroth

A Bosch Company

Remote Agent App

Connecting the ctrlX Device to the ctrlX Device Portal 01VRS

Copyright

Disclaimer

The data specified above only serve to describe the product. As our products are constantly being further developed, no statements concerning a certain condition or suitability for a certain application can be derived from our information. The information given does not release the user from the obligation of own judgment and verification. It must be remembered that our products are subject to a natural process of wear and aging.

Table of contents

1   About this documentation

Editions of this documentation

Edition	Release date	Note
01	2020-06	First edition Remote Agent App version RMA-V-0102
02	2020-10	Revision Remote Agent App version RMA-V-0104
03	2021-05	Revision Remote Agent App Version RMA-V-0108
04	2021-09	Revision Remote Agent App Version RMA-V-0110 ● ↪ Chapter 4.1 Remote Agent on page 9 Revision/internet sources added ● Revision of the ctrlX Device Portal documentation. User documentation for the ctrlX Device Portal added, see ↪ Chapter 5.2 Additional documentations on page 11 ● ↪ Chapter 6.1.2 Window – Activity Overview on page 22 Updated (modifications of the web interface)
05	2021-12	Revision Remote Agent App Version RMA-V-0112 ● Updated (modifications of the web interface)
06	2022-08	Revision Remote Agent App Version RMA-V-0116 ● Updated (modifications of the web interface)
07	2023-01	Revision Remote Agent App Version RMA-V-0118 Revision: ● ↪ Network configuration specifications
08	2023-08	Revision Remote Agent App Version RMA-V-0120 Revision: ● ↪ Network configuration specifications

2   Important directions on use

2.1   Intended use

2.1.1   Introduction

Rexroth products are developed and manufactured to the state-of-the-art.

The products are tested prior to delivery to ensure operational safety and relia-
bility.

⚠ WARNING	**Personal injury and damage to property due to incorrect use of products!**
	The products may only be used as intended.
	Failure to use the products as intended may cause situations resulting in property damage and personal injury.

NOTICE	**Damages resulting from unintended use**
	Rexroth As the manufacturer does not assume any warranty, liability or compensatory claims for damages resulting from unintended use of the products. The user alone shall bear the risks of an unintended use of the products.
	Before using Rexroth products, make sure that all the prerequisites for an intended use of the products are met:
	– Personnel that in any way, shape or form uses Rexroth products must first read and understand the relevant safety instructions and be familiar with their intended use
	– Leave hardware products in their original state, i.e., do not make any structural modifications. It its not permitted to decompile software products or alter source codes
	– Do not install damaged or defective products or commission them
	– It has to be ensured that the products have been installed as described in the relevant documentation

2.1.2   Areas of use and application

Products of the ctrlX series are suitable for Motion/Logic applications.

NOTICE	Products of the ctrlX series may only be used with the accessories, mounting parts, and other components specified in this documentation. Components that are not expressly mentioned must neither be attached nor connected. The same applies to cables and lines.
	Only to be operated with the hardware component configurations and combinations expressly specified and with the software and firmware specified in the corresponding documentations and functional descriptions.

Products of the ctrlX series are suitable for single-axis as well as for multi-axis
drive and control tasks. Device types with different equipment and interfaces
are available for using the system in specific applications.

Typical areas of application:

● Building automation

● IoT and Security Gateway or Device

● Handling & Robotic

Controls of the ctrlX CORE series may only be operated under the mounting and installation conditions, in the position of normal use and under the ambient conditions (temperature, degree of protection, humidity, EMC, etc.) specified in the related documentations.

2.2 Unintended use

"Unintended use" refers to using the ctrlX products outside of the above-mentioned areas of application or under operating conditions and technical data other than described and specified in the documentation.

ctrlX products must not be used if they are exposed to following conditions:

● Operating conditions that do not meet the specified ambient conditions. Operation under water, under extreme temperature fluctuations or under extreme maximum temperatures is prohibited

● Applications that have not been expressly authorized by Rexroth

3 Safety instructions

The Safety instructions contained in the available application documentation feature specific signal words (DANGER, WARNING, CAUTION or NOTICE) and, where required, a safety alert symbol (in accordance with ANSI Z535.6-2006).

The signal word is meant to draw the reader's attention to the safety instruction and identifies the hazard severity.

The safety alert symbol (a triangle with an exclamation point), which precedes the signal words DANGER, WARNING and CAUTION, is used to alert the reader to personal injury hazards.

The Safety instructions in this documentation are designed as follows:

⚠ DANGER	In case of non-compliance with this safety instruction, death or serious injury **will** occur.
⚠ WARNING	In case of non-compliance with this safety instruction, death or serious injury **could** occur.
⚠ CAUTION	In case of non-compliance with this safety instruction, minor or moderate injury could occur.
NOTICE	In case of non-compliance with this safety instruction, property damage could occur.

4 Remote Agent

4.1 Remote Agent

The Remote Agent is a software package to connect to the central ctrlX Device Portal. The software inventory of the control can be updated using the Remote Agent.

The ctrlX Device Portal is a fee-based cloud service for the worldwide management of ctrlX devices, see ↪ Chapter 5.1 Introduction on page 11.

ℹ️ On ctrlX CORE Virtual, the Remote Agent functions are not supported.

Sources of information in the web

● ↪ Remote Agent website

Setup

Before using the Remote Agent application, Bosch Rexroth has to provide a certificate & encryption file. Subsequently, insert these files using the "Certificates & Keys" app, see "ctrlX CORE Runtime", Application Manual (R911403768), chapter ↪ Working with ctrlX CORE – Managing certificates and keys

ℹ️ The Remote Agent has to be installed in the apps.

Starting and operating

The Remote Agent is integrated in the web interface of the ctrlX CORE control.

The Remote Agent can be found in the ctrlX CORE side navigation: *"Remote Agent"*

The Remote Agent node in the side navigation contains the following subnodes:
● "Device Overview", see ↪ Chapter 6.1.1 Window – Device Overview on page 21
● "Activity Overview", see ↪ Chapter 6.1.2 Window – Activity Overview on page 22
● "Add Device", see ↪ Chapter 6.1.3 Window – Add Device on page 23

Further information

● ↪ Chapter 5.1 Introduction on page 11

4.2 Confirming remote activities on the ctrlX device

Via the ctrlX Device Portal, activities can be transmitted to the ctrlX device for execution; e.g. to establish a remote connection or to update software, see ↪ Chapter 5.8 Executing remote activities on the ctrlX device on page 15.

In the default setting, the execution of activities requires a confirmation by the ctrlX device or the user.

The confirmation is given in the "Activity Overview" window in the ctrlX CORE web interface, see ↪ Chapter 6.1.2 Window – Activity Overview on page 22.

Configuring the confirmation

The confirmation type cannot be configured in the ctrlX device:

- Accept
- Reject
- Ask user

The modifications are only applied when clicking on the ⬛Save interface.

Find the configuration in the ctrlX CORE web interface in the side navigation: *"Remote Agent → Device Overview → Tab Policies"*

Refer to ➡ Chapter 6.1.1 Window – Device Overview on page 21

4.3   Enabling or disabling the remote connection

Remote connections between ctrlX CORE and the ctrlX Device Portal can be controlled in the Remote Agent on ctrlX CORE.

In the ctrlX CORE web interface, open the window: *"Remote Agent → Device Overview"*

Under "Actions", the remote connections can be enabled or disabled.

Buttons:

- 🔌 Disables remote access
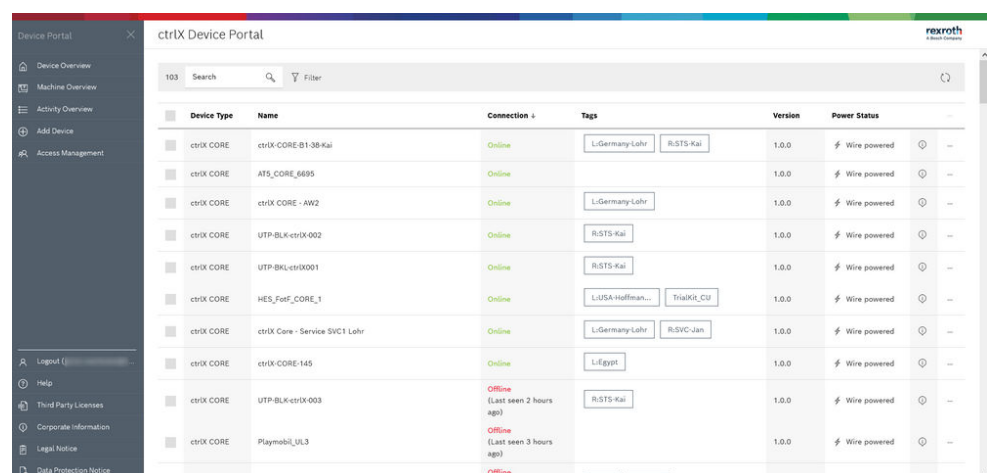- 🔌 Enables remote access

5 ctrlX Device Portal

5.1 Introduction

The ctrlX Device Portal is a fee-based cloud service for the worldwide management of ctrlX devices during the entire life cycle (Remote Device Management). By using the ctrlX Device Portal, new functions (apps) can be distributed, updates, backup and restore actions can be executed and diagnostic options are possible via remote access. The ctrlX Device Portal provides an overview of all connected ctrlX devices. Actions on the target device can be executed. The ctrlX Device Portal is user-friendly and can easily be integrated in an existing IT infrastructure.

Core features:

- Central management of all connected devices
  - Information about the device pool/type and number
  - Display of device firmware/error status
- Targeted software provision, e.g. installation of apps and licenses (also customer-specific apps possible)
- Installing updates
- Back up and restore
- Option for remote maintenance and status analysis via a secure connection

Currently, ctrlX CORE Virtual is not supported by the ctrlX Device Portal.

5.2 Additional documentations

5.2.1 ctrlX Device Portal Application Manual

Contents

- General product description of the ctrlX Device Portal
- System requirements
- Generating a Bosch ID and a tenant ID
- User interface of the ctrlX Device Portal
- Adding devices
- Access Management (user management)
- Private Artifact Repository (rolling out and managing individual software components)

Download

→ PDF for download (EN / provided by Bosch Connected Industry)

5.2.2 ctrlX Device Portal website

→ Link to the ctrlX website

5.2.3 ctrlX Device Portal FAQ

→ Link to the ctrlX Device Portal FAQ
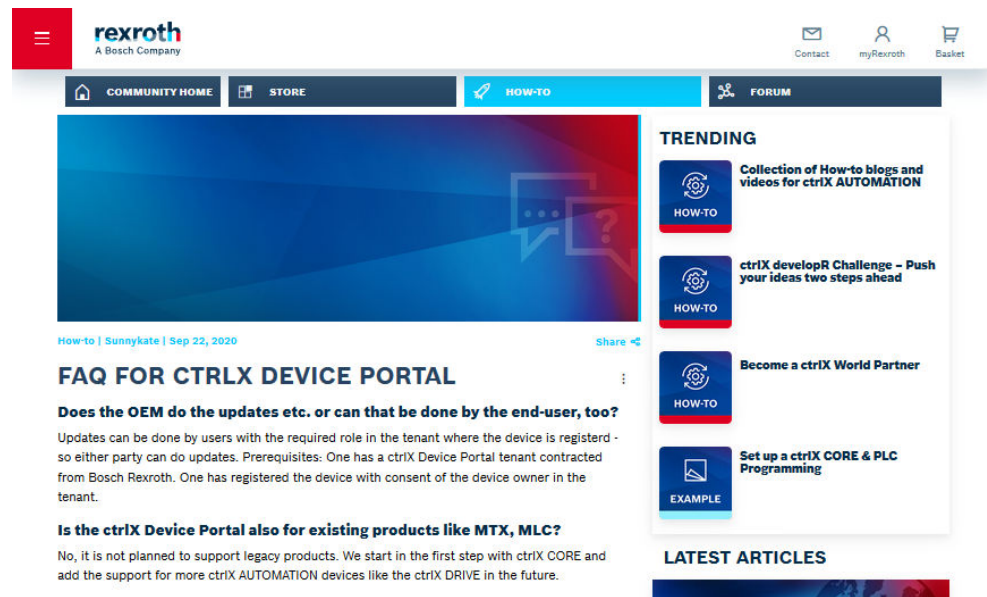
5.3   Access to the ctrlX Device Portal

Applying for access

The access to the ctrlX Device Portal can be applied for via the ctrlX Support & Service website ➜ Link

Requirements for use of the ctrlX Device Portal

Required access data:

- **Bosch-ID**
  For login at the ctrlX Device Portal.
  The Bosch ID can be generated on the following Bosch page by registering:
  ➜ https://identity-myprofile.bosch.com/ids/login
- **Tenant ID**
  For unique identification of an enterprise or an organization.
  The tenant ID is created by the Bosch Connected Industry and is provided together with the URL.

For more information about the Bosch ID or the tenant ID, refer to the application manual for the ctrlX Device Portal ➜ PDF for download (EN)

5.4   Adding the device to the ctrlX Device Portal

The basic requirement for remote access to a ctrlX device is that the target device is known or registered in the ctrlX Device Portal.

Registering a ctrlX device at the ctrlX Device Portal is referred to as "Add Device" and is realized in 5 steps, refer to ➜ Chapter 6.1.3 Window – Add Device on page 23.

Ensure that you have access to the ctrlX Device Portal before starting the "Add Device" process, see ➜ Chapter 5.3 Access to the ctrlX Device Portal on page 13.

5.5   Establishing a remote connection to the ctrlX device

Go to the ctrlX Device Portal to access the web interface of ctrlX CORE using a remote connection, e.g. for remote maintenance.

ctrlX Device Portal

Requirement: ctrlX CORE is registered in the ctrlX Device Portal, see process "Add Device" ➜ Chapter 5.4 Adding the device to the ctrlX Device Portal on page 13.

Activity to establish a remote connection

The user can start to establish a remote connection in the ctrlX Device Portal by transferring the "UPDATE_TUNNEL" activity to ctrlX CORE for execution. The activity requests ctrlX CORE to establish a remote connection to the ctrlX Device Portal.

Depending on the configuration, it can be required that a pending activity first has to be confirmed by the user at the device before executing the activity, see ➜ Chapter 4.2 Confirming remote activities on the ctrlX device on page 9.

Related topics

- ➜ Chapter 5.8 Executing remote activities on the ctrlX device on page 15
- ➜ Chapter 4.3 Enabling or disabling the remote connection on page 10

5.6   Monitoring the device status

Use the ctrlX Device Portal to monitor the ctrlX device status.

If the device is known in the ctrlX Device Portal (claiming process) and if it is active, the device transfers information to the ctrlX Device Portal. The information includes:

- Firmware version
- Firmware version bootloader
- Available software
- Online status

Related topics

- ➜ Chapter 5.4 Adding the device to the ctrlX Device Portal on page 13

5.7   Software provision on ctrlX devices

The ctrlX Device Portal has a central server allowing to install or uninstall apps or to install updates on the ctrlX device via remote access.

If the device is connected to the ctrlX Device Portal, it can receive and execute activities of the ctrlX Device Portal, see ➜ Chapter 5.5 Establishing a remote connection to the ctrlX device on page 13.

Activities to manage the software on the device:

- ➜ Installing software
- ➜ Installing a software update
- ➜ Uninstalling software

On the ctrlX device, the activities are displayed in the "Activity Overview" window, see ➜ Chapter 6.1.2 Window – Activity Overview on page 22.

Depending on the configuration, it can be required that a pending activity first has to be confirmed by the user at the device before executing the activity, see ➜ Chapter 4.2 Confirming remote activities on the ctrlX device on page 9.

The software is either provided by Bosch Rexroth or developed by the user, refer to "Private Artifact repository" in the ctrlX Device Portal Application Manual: ➜ PDF for download (EN / provided by Bosch Connected Industry)

Related topics

- ➜ Chapter 5.4 Adding the device to the ctrlX Device Portal on page 13

5.8 Executing remote activities on the ctrlX device

Via the ctrlX Device Portal, activities can be transmitted to the ctrlX device for execution; e.g. to update software or for installing applications.

The following table lists the available activities and establishes a reference between the initial activity in the ctrlX Device Portal and the executing activity in the Remote Agent on the ctrlX device.

Overview on the activities

Initial Activity in the ctrlX Device Portal		Executing Activity in the Remote Agent
↪ Enabling/disabling a remote connection	→	UPDATE_TUNNEL
↪ Enabling/disabling the "Service mode"	→	UPDATE_SERVICE_MODE
↪ Creating a backup	→	CREATE_BACKUP
↪ Restoring a backup	→	RESTORE_BACKUP
↪ Installing software	→	INSTALL_SOFTWARE
↪ Installing a software update	→	UPDATE_SOFTWARE
↪ Uninstalling software	→	UNINSTALL_SOFTWARE

Depending on the configuration, it can be required that a pending activity first has to be confirmed by the user at the device before executing the activity, see:

↪ Confirming remote activities on the ctrlX device.

On the ctrlX device, the activities are displayed in the "Activity Overview" window, see:

↪ Window – Activity Overview.

Related topics

- ↪ Establishing a remote connection to the ctrlX device
- ↪ Enabling or disabling the remote connection

5.8.1 Enabling/disabling a remote connection

To execute activities on the ctrlX device via the ctrlX Device Portal, the remote connection between device and ctrlX Device Portal has to be enabled.

There are two options to enable the remote connection:

- Via the ctrlX device, in the web interface of the Remote Agent
- Via the ctrlX Device Portal as remote activity to be executed on the ctrlX device

Enabling the device via the ctrlX Device Portal

1. Open the "Device Overview" and navigate to the ctrlX device in the list
2. In the list entry, right-click on ⋯ to show more options.
3. Select the option "Configure Remote Access"
   ➡ The dialog "Configure Remote Access" opens.
   Options:
   - **Remote Access "Enabled"**
     Remote access to the ctrlX device is permitted.
   - **Remote access "Disabled"**
     Remote access to the ctrlX device is not permitted.
4. For activation, select the option **Remote Access "Enabled"** and confirm the dialog with "Submit"

5.   ▸   The action is transmitted to the ctrlX device for execution.

➡ The execution on the device is realized according to the Remote Agent configuration:

Options:

- Accept
- Reject
- Ask user

Refer to ➡ Confirming remote activities on the ctrlX device

5.8.2   Enabling/disabling the "Service mode"

The "Service mode" is required to implement changes at the ctrlX device, e.g. to install apps or updates.

There are two options to enable the "Service mode":

- Via the web interfacet of the ctrlX device
- Via the ctrlX Device Portal as remote activity to be executed on the ctrlX device

Procedure in the ctrlX Device Portal

NOTICE	To switch from "Operation mode" to "Service mode", real-time data processing on the ctrlX device is stopped.
	Prior to enabling the "Service mode", it has to ensured that the ctrlX device or the system is in a safe state!

1.   ▸   Open the "Device Overview" and navigate to the ctrlX device in the list.

2.   ▸   In the list entry, right-click on ⋯ to show more options.

3.   ▸   Select the option "Configure Service Mode" and select the desired option:

- **Service mode "Enabled"**
  The ctrlX device switches from "Operation mode" to "Service mode".
  The real-time data processing on the ctrlX device is stopped.
  Changes at the device are now possible, e.g. installation or app updates.
- **Service mode "Disabled"**
  The ctrlX device switches from "Service mode" to "Operation mode".
  The real-time data processing on the ctrlX device is started.
  Changes at the device are not possible.

4.   ▸   For activation, select the option **Service Mode "Enabled"** and confirm the dialog with "Submit".

5.   ▸   The action is transmitted to the ctrlX device for execution.

➡ The execution on the device is realized according to the Remote Agent configuration:

Options:

- Accept
- Reject
- Ask user

Refer to ➡ Confirming remote activities on the ctrlX device

5.8.3   Creating a backup

The scope of the backup file corresponds to the standard function for saving and restoring on the ctrlX device, see:

➡ Back up and restore – Introduction

Prerequisites:

- The remote connection the ctrlX device is enabled, see:
  ➡ Enabling/disabling a remote connection
- To create backups, the ctrlX device has to be in "Operation mode", see:
  ➡ Enabling/disabling the "Service mode"
  When executing the backup activity in "Service mode", an error message is output.

Procedure in the ctrlX Device Portal

1. ⟩ Open the "Device Overview" and navigate to the ctrlX device in the list.
2. ⟩ Click in the line to open the ctrlx device view.
3. ⟩ In the view, change to the "Backup & Restore" tab.
4. ⟩ Execute the action ▭ **Backup device** in the command bar.
5. ⟩ The action is transmitted to the ctrlX device for execution.
   - ➡ The execution on the device is realized according to the Remote Agent configuration:
     Options:
     - Accept
     - Reject
     - Ask user

     Refer to ➡ Confirming remote activities on the ctrlX device
6. ⟩ The backup file is now generated on the ctrlX device, and subsequently uploaded and saved in the ctrlX Device Portal. The process can take several minutes, depending on the scope of the data to be backed up.

   Saved backup files can be found in the *"Device Overview → Backup & Restore"* tab.

5.8.4   Restoring a backup

The scope of the backup file corresponds to the standard function for saving and restoring on the ctrlX device, see:

➡ Back up and restore – Introduction

Previously generated backups are saved in the ctrlX Device Portal and are available in the "Device Overview → Backup & Restore" tab.

Prerequisites:

- The remote connection the ctrlX device is enabled, see:
  ➡ Enabling/disabling a remote connection
- To restore backups, the ctrlX device has to be in "Service mode".
  ➡ Enabling/disabling the "Service mode"
  When executing the restore activity in the "Operation mode", an error message is output.

Procedure in the ctrlX Device Portal

1. ⟩ Open the "Device Overview" and navigate to the ctrlX device in the list.
2. ⟩ Click in the line to open the ctrlx device view.
3. ⟩ In the view, change to the "Backup & Restore" tab.
4. ⟩ Select the backup file to be restored on the ctrlX device from the list.
   In the list entry, right-click on ⋯ to show more options.
5. ⟩ Execute the action **Restore device to this state**.

6. ▸ The action is transmitted to the ctrlX device for execution.

➡ The execution on the device is realized according to the Remote Agent configuration:

Options:

- Accept
- Reject
- Ask user

Refer to ➥ Confirming remote activities on the ctrlX device

7. ▸ After the action has been confirmed on the ctrlX device, the restore activity automatically starts in the following order:

- Uploading the backup file from the ctrlX Device Portal to the ctrlX device
- Restoring the backup file on the ctrlX device
- Restart of the ctrlX device

Note:

The remote connection to the ctrlX Device Portal is interrupted by a ctrlX device restart.

To re-establish the connection to the ctrlX device, please execute the following activities:

➥ Enabling/disabling a remote connection

If it is not possible to establish the connection to the ctrlX device, the reason might be in the network settings responsible for re-establishing the connection to the device. In this case check the correct setting of the network settings via the web interface of the ctrlX device.

5.8.5   Installing software

Via the ctrlX Device Portal, software can be installed on a ctrlX device via remote access.

Depending on the device type, the ctrlX Device Portal provides a matching selection of software products, e.g. apps or system software.

Prerequisites:

- The remote connection the ctrlX device is enabled, see:
  ➥ Enabling/disabling a remote connection
- The ctrlX control is in "Service mode".

Procedure in the ctrlX Device Portal

1. ▸ Open the "Device Overview" and navigate to the ctrlX device in the list.

2. ▸ Open the ctrlX device view by clicking in the relevant column.

➡ The "Software" tab is opened.

The tab lists all software projects available on the ctrlX device, including the software already installed on the device.

3. ▸ From the list, select the software you want to install on the device and right-click on the ☁ interface

➡ The dialog "Install Software" opens.

The dialog shows all available software versions available on the device.

4. ▸ Select the version and confirm the dialog with "Install".

5. ▸ The action is transmitted to the ctrlX device for execution.
   ➡ The execution on the device is realized according to the Remote Agent configuration:
   Options:
   ● Accept
   ● Reject
   ● Ask user
   Refer to ➡ Confirming remote activities on the ctrlX device

5.8.6 Installing a software update

Via the ctrlX Device Portal, software updates can be installed on a ctrlX device via remote access.

Prerequisites:
● The remote connection the ctrlX device is enabled, see:
  ➡ Enabling/disabling a remote connection
● The ctrlX control is in "Service mode".

Procedure in the ctrlX Device Portal

1. ▸ Open the "Device Overview" and navigate to the ctrlX device in the list.
2. ▸ Open the ctrlX device view by clicking in the relevant column.
   ➡ The "Software" tab is opened.
   The tab lists all software projects available on the ctrlX device, including the software already installed on the device.
3. ▸ From the list, select the software you want to install an update for and right-click on ↻
   ➡ The "Change update channel" dialog is opened.
   The dialog shows all available software versions available on the device.
4. ▸ Select the version and confirm the dialog with "Update"
5. ▸ The action is transmitted to the ctrlX device for execution.
   ➡ The execution on the device is realized according to the Remote Agent configuration:
   Options:
   ● Accept
   ● Reject
   ● Ask user
   Refer to ➡ Confirming remote activities on the ctrlX device

5.8.7 Uninstalling software

Via the ctrlX Device Portal, software can be uninstalled on a ctrlX device via remote access.

Prerequisites:
● The remote connection the ctrlX device is enabled, see:
  ➡ Enabling/disabling a remote connection
● The ctrlX control is in "Service mode".

Procedure in the ctrlX Device Portal

1. ▸ Open the "Device Overview" and navigate to the ctrlX device in the list.

2. ▸ Open the ctrlX device view by clicking in the relevant column.
   ➡ The "Software" tab is opened.

   The tab lists all software projects available on the ctrlX device, including the software already installed on the device.

3. ▸ From the list, select the software you want to uninstall from the device and right-click on 🗑
   ➡ The dialog "Uninstall software" opens.

4. ▸ Confirm the dialog with "Uninstall".

5. ▸ The action is transmitted to the ctrlX device for execution.
   ➡ The execution on the device is realized according to the Remote Agent configuration:

   Options:
   - Accept
   - Reject
   - Ask user

   Refer to ➡ Confirming remote activities on the ctrlX device

5.9 Network configuration specifications

ctrlX Device Portal

Device	Domain	IP
Access to a ctrlX Device Portal as device with interdependent TLS	cert.device.device-portal.bosch.com	108.142.158.253

The connection to the ctrlX Device Portal uses the TCP network ports 80 and 443 as outgoing port.

Online store

The connection to the online store is ➡ https://snapstore.boschrexroth.com and ➡ https://serialvault.boschrexroth.com with port 443.

6　ctrlX UI – Elements

6.1　Windows

6.1.1　Window – Device Overview

Function:

The window "Device Overview" shows an overview on manageable devices.

Call:

ctrlX CORE side navigation *"Remote Agent → Device Overview"*

Elements of the "Device Overview" **window**

GUI element	Description
Table "Device Overview"	"Name": Device name
	"State" The column shows whether the device is currently active or if it used to be active
	"Description" The description of the device can be selected individually
	"Actions" The configuration of the ctrlX Device Portal connection can be adjusted in this column: ● Go to ✎ to modify the device name and the device description and to enable or disable the connection to the ctrlX Device Portal ● Go to "Policies" to configure the activities that can be executed in the device by the ctrlX Device Portal. These activities include: 　– UPDATE_TUNNEL 　　To request the remote access channel between the ctrlX Device Portal and the device 　– UPDATE_SOFTWARE 　　To update software 　– INSTALL_SOFTWARE 　　To install software 　– UNINSTALL_SOFTWARE 　　To uninstall software 　– ACTIVATE_SERVICE_MODE 　　To disable the service mode 　Refer to ➡ Chapter 4.2 Confirming remote activities on the ctrlX device on page 9 ● Use ⌀ to disable an existing remote access or use ⌀ to enable a new remote access ● 🗑 Delete device

Further information

- ➡
- ➡
- ➡
- ➡

6.1.2   Window – Activity Overview

The window shows the activity record which the ctrlX device received for execution from the ctrlX Device Portal:

- Time of execution of the activity
- Pending activities
- Involved devices and their status
- Activities in execution
- Executed activities

If the ctrlX device is claimed in the Device Portal and is active, the device sends device information to the Device Portal. The device information includes information such as firmware version, firmware version bootloader, existing firmware and online status, etc.

Related topics

➡
➡

Call:

ctrlX CORE side navigation *"Remote Agent → Activity Overview"*

Elements of the *"Activity Overview"* **window**

GUI element	Description
Table "Activity Overview"	⟳ Refresh view
	"Timestamp" Time stamp of the device
	"Activity" Device activity
	"Device" Device name
	"Status" Activity status: - TRANSMITTED: Command to be processed - ACCEPTED: Confirmed command - REJECTED: Rejected command - SUCCESSFUL: Successful command - FAILED: Failed command

GUI element	Description
	"Actions"
Depending on the "Policies" (see ➡ Chapter 6.1.1 Window – Device Overview on page 21), the activity has to be confirmed manually: ● ✓: Confirm activity ● ✕: Reject activity ● 🔍: More information can be shown for this activity

6.1.3   Window – Add Device

Function:

In window "Add Device", a new device can be added to the ctrlX Device Portal. The process "Add Device" has to be completed. This process ensures that you can access the device physically. Ensure that you have access to the ctrlX Device Portal before starting the "Add Device" process. The note "Add device to ctrlX Device Portal by claiming the device" contains an info link that links to a website with more information about the Device Portal.

Call:

ctrlX CORE side navigation *"Remote Agent → Add Device"*

The "Add Device" process is executed in 5 steps in the Remote Agent:

1. ▶ Welcome

   For the first step, accept "Software as a Service Terms and Conditions of Use" of the Bosch Rexroth AG. You agree to the terms and conditions

2. ▶ Establish Connection

   For managing purposes using the ctrlX Device Portal, the device has to be connected to the internet. The current connection status between the device and the ctrlX Device Portal is shown under "Establish Connection"

3. ▶ Log into Device Portal

   To start the claiming, log into the ctrlX Device Portal. Execute the following steps in the ctrlX Device Portal:

   ● Select "Add Device" ctrlX CORE in the menu.
   ● Select a name for the device and add the communication identifier to your ctrlX.
     The communication identifier is shown in the device and can then be copied
   ● Start the claiming in the ctrlX Device Portal

4. ▶ Confirm claiming

   To complete the claiming, make an approval on the device

5. ▶ Finished

   Upon completion, the message that the "Add Device" process has been completed successfully is reported

Adding new devices to the Remote Agent.

Further information

ctrlX UI – Elements

7   Related documentation

7.1   Overview
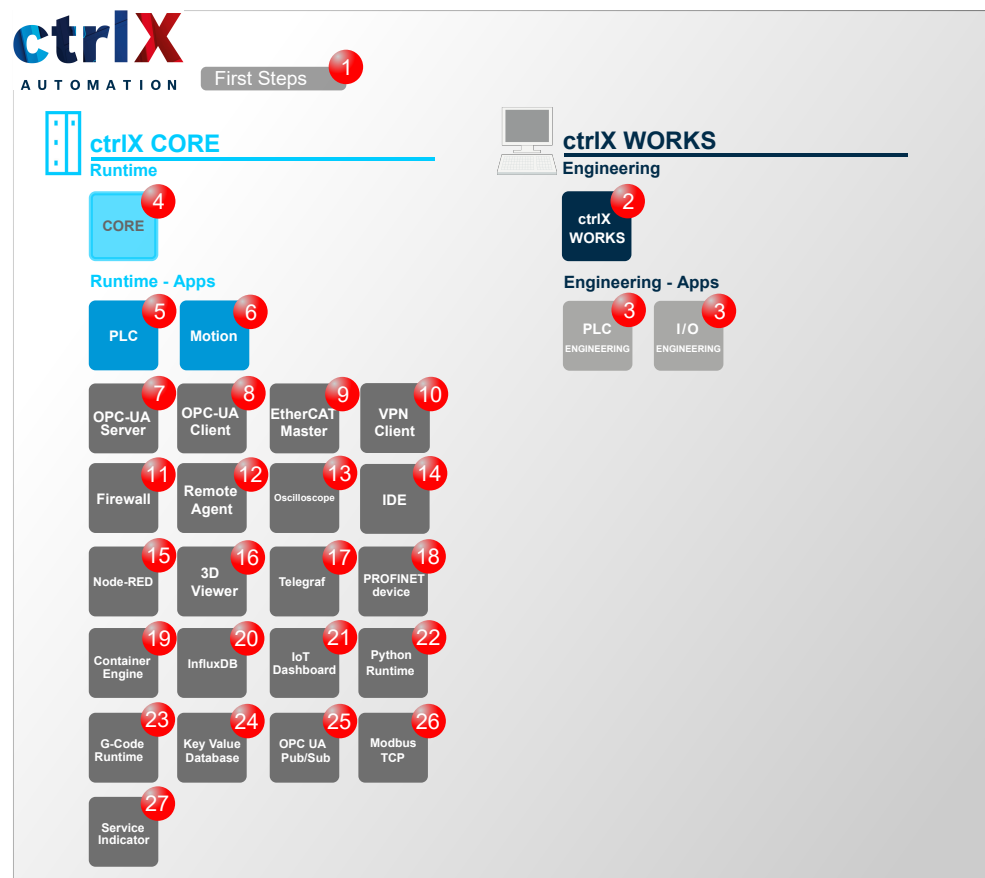
Fig. 1: Overview on further documentations

7.2   ctrlX AUTOMATION

No.	Documentation
1	**ctrlX WORKS First Steps 01VRS** Quick Start Guide ➡ Web documentation link Ordering information: • DOK-XWORKS-F*STEP**V01-QURS-EN-P • R911403760

7.3   ctrlX WORKS

No.	Documentation
2	**ctrlX WORKS Basic System 01VRS** Application Manual → Web documentation link Ordering information: ● DOK-XWORKS-********V01-APRS-EN-P ● R911403761
3	**ctrlX PLC Engineering - PLC Programming System 01VRS** Application Manual → Web documentation link Ordering information: ● DOK-XPLC**-ENG*****V01-APRS-EN-P ● R911403764
3	**ctrlX PLC Engineering - PLC Libraries 01VRS** Reference → Web documentation link Ordering information: ● DOK-XPLC**-LIBRARY*V01-RERS-EN-P ● R911403766

7.4   ctrlX CORE

No.	Documentation
4	**ctrlX CORE - Runtime 01VRS** Application Manual → Web documentation link Ordering information: ● DOK-XCORE*-BASE****V01-APRS-EN-P ● R911403768
	ctrlX CORE - Nodes of the Data Layer 01VRS Reference → Web documentation link Bestellinformationen: ● DOK-XCORE*-BASE*DL*V01-RERS-EN-P ● R911420072
	ctrlX CORE - Diagnostics 01VRS Reference → Web documentation link Ordering information: ● DOK-XCORE*-DIAG****V01-RERS-EN-P ● R911403770

7.5   ctrlX CORE Apps

No.	Documentation
5	**PLC App - PLC Runtime Environment for ctrlX CORE 01VRS** Application Manual ➟ Web documentation link Ordering information: ● DOK-XCORE*-PLC*****V01-APRS-EN-P ● R911403787
6	**Motion App - Motion Runtime Environment for ctrlX CORE 01VRS** Application Manual ➟ Web documentation link Ordering information: ● DOK-XCORE*-MOTION**V01-APRS-EN-P ● R911403791
7	**OPC UA Server App - OPC UA Server for ctrlX CORE 01VRS** Application Manual ➟ Web documentation link Ordering information: ● DOK-XCORE*-OPCSERV*V01-APRS-EN-P ● R911403778
8	**OPC UA Client App - OPC UA Client for ctrlX CORE 01VRS** Application Manual ➟ Web documentation link Ordering information: ● DOK-XCORE*-OPCCLIENV01-APRS-EN-P ● R911403781
9	**EtherCAT Master App - EtherCAT Master for ctrlX CORE 01VRS** Application Manual ➟ Web documentation link Ordering information: ● DOK-XCORE*-ETHERCATV01-APRS-EN-P ● R911403773
10	**VPN Client App - Remote Support Software for ctrlX CORE 01VRS** Application Manual ➟ Web documentation link Ordering information: ● DOK-XCORE*-VPN*****V01-APRS-EN-P ● R911403775
11	**Firewall App - Security Functions for ctrlX CORE 01VRS** Application Manual ➟ Web documentation link Ordering information: ● DOK-XCORE*-FIREWALLV01-APRS-EN-P ● R911403783

Related documentation

No.	Documentation
12	**Remote Agent App - ctrlX Device Portal Connection for ctrlX Devices 01VRS** Application Manual ➥Web documentation link Ordering information: ● DOK-XCORE*-REMOTE**V01-APRS-EN-P ● R911403785
13	**Oscilloscope App - Oscilloscope Function for ctrlX Devices 01VRS** Application Manual ➥Web documentation link Ordering information: ● DOK-XCORE*-OSCI****V01-APRS-EN-P ● R911409806
14	**IDE App - Integrated Development Environment 01VRS** Application Manual ➥Web documentation link Ordering information: ● DOK-XCORE*-IDE*****V01-APRS-EN-P ● R911410625
15	**Node RED App - Graphic Programming for ctrlX CORE 01VRS** Application Manual ➥Web documentation link Ordering information: ● DOK-XCORE*-NODERED*V01-APRS-EN-P ● R911403789
16	**3D Viewer App - Browser-based 3D Kinematic Simulation for ctrlX CORE 01VRS** Application Manual ➥Web documentation link Ordering information: ● DOK-XCORE*-3D*VIEW*V01-APRS-EN-P ● R911416124
17	**Telegraf App - Server Agent for Collecting Data in the Data Layer 01VRS** Application Manual ➥Web documentation link Ordering information: ● DOK-XCORE*-TELEGRAFV01-APRS-EN-P ● R911416836
18	**PROFINET Device App - PROFINET Device for ctrlX CORE 01VRS** Application Manual ➥Web documentation link Ordering information: ● DOK-XCORE*-PROFINETV01-APRS-EN-P ● R911417857

No.	Documentation
19	**Container Engine App - Use of Docker® Images on ctrlX CORE 01VRS** Application Manual ➡ Web documentation link Ordering information: ● DOK-XCORE*-DOCKER**V01-APRS-EN-P ● R911417855
20	**InfluxDB App - Influx Database Connection for ctrlX CORE 01VRS** Application Manual ➡ Web documentation link Ordering information: ● DOK-XCORE*-INFLUX**V01-APRS-EN-P ● R911418738
21	**IoT Dashboard App - Data Visualization in Dynamic, Interactive Dashboards 01VRS** Application Manual ➡ Web documentation link Ordering information: ● DOK-XCORE*-GDB*****V01-APRS-EN-P ● R911420426
22	**Python Runtime App - Python Runtime Environment for ctrlX CORE 01VRS** Application Manual ➡ Web documentation link Ordering information: ● DOK-XCORE*-PYR*****V01-APRS-EN-P ● R911420430
23	**G-Code Runtime App - G-Code Interpreter for ctrlX CORE 01VRS** Application Manual ➡ Web documentation link Ordering information: ● DOK-XCORE*-GCO*****V01-APRS-EN-P ● R911420428
24	**Key Value Database App - Managing Data in the Data Layer 01VRS** Application Manual ➡ Web documentation link Ordering information: ● DOK-XCORE*-KVD*****V01-APRS-EN-P ● R911420423
25	**OPC UA Pub/Sub App - OPC UA Pub/Sub for ctrlX CORE 01VRS** Application Manual ➡ Web documentation link Ordering information: ● DOK-XCORE*-PUBSUB**V01-APRS-EN-P ● R911418736

No.	Documentation
26	**Modbus TCP App - Modbus TCP Communication for ctrlX CORE 01VRS** Application Manual ➡Web documentation link Ordering information: ● DOK-XCORE*-MOD*TCP*V01-APRS-EN-P ● R911417926
27	**Service Indicator App - Service Indicator for ctrlX CORE 01VRS** Application Manual ➡Web documentation link Ordering information: ● DOK-XCORE*-SIN*****V01-APRS-EN-P ● R911418740

8   Service and support

Our worldwide service network provides an optimized and efficient support. Our experts provide you with advice and assistance. You can contact us **24/7**.

Service Germany

Our technology-oriented Competence Center in Lohr, Germany, is responsible for all your service-related queries for electric drive and controls.

Contact the **Service Hotline** and **Service Helpdesk** under:

Phone:	**+49 9352 40 5060**
Fax:	**+49 9352 18 4941**
Email:	➡ service.svc@boschrexroth.de
Internet:	➡ http://www.boschrexroth.com

Additional information on service, repair (e.g. delivery addresses) and training can be found on our internet sites.

Service worldwide

Outside Germany, please contact your local service office first. For hotline numbers, refer to the sales office addresses on the internet.

Preparing information

To be able to help you more quickly and efficiently, please have the following information ready:

- Detailed description of malfunction and circumstances
- Type plate specifications of the affected products, in particular type codes and serial numbers
- Your contact data (phone and fax number as well as your e-mail address)

9   Index

R911403785