Asset Manager
User Guide
Edition notice

Technical specifications and availability subject to change without notice.
This document may not be reproduced, disseminated to third parties or processed
and its contents may not be used or disclosed without express permission. Non-
compliance shall result in compensation for damages. All rights, including those
resulting from a successful patent application and registration of a utility model or
design patent, are reserved.
Edition: --
Document ID: A6V12060067_en_a

© Siemens Switzerland Ltd, 2020
Cybersecurity disclaimer

Siemens provides a portfolio of products, solutions, systems and services that includes security functions that support the secure operation of plants, systems, machines and networks. In the field of Building Technologies, this includes building automation and control, fire safety, security management as well as physical security systems.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art security concept. Siemens’ portfolio only forms one element of such a concept.

You are responsible for preventing unauthorized access to your plants, systems, machines and networks which should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. Additionally, Siemens’ guidance on appropriate security measures should be taken into account. For additional information, please contact your Siemens sales representative or visit https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html.

Siemens’ portfolio undergoes continuous development to make it more secure. Siemens strongly recommends that updates are applied as soon as they are available and that the latest versions are used. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats. Siemens strongly recommends to comply with security advisories on the latest security threats, patches and other related measures, published, among others, under https://www.siemens.com/cert/en/cert-security-advisories.htm.
# Table of Contents

1 Asset Manager User Guide ................................................................. 5
  1.1 Overview ......................................................................................... 5
  1.2 Asset Manager icons ........................................................................ 5
  1.3 Managing sites ................................................................................. 5
       1.3.1 Creating sites ........................................................................... 5
       1.3.2 Editing sites ............................................................................. 7
       1.3.3 Deleting sites .......................................................................... 7
  1.4 Managing devices ............................................................................. 8
       1.4.1 Finding devices .......................................................................... 8
       1.4.2 Adding devices ......................................................................... 9
       1.4.3 Viewing and editing device information .................................... 11
       1.4.4 Removing devices .................................................................... 13
  1.5 Working with Intelligent Valves ...................................................... 15
       1.5.1 Performing HVAC self-balancing test ....................................... 15
       1.5.2 Updating firmware .................................................................... 15
  1.6 Working with ConnectX300 devices ................................................. 16
       1.6.1 Resetting the password ............................................................ 17
       1.6.2 Viewing remote web access ...................................................... 18
       1.6.3 Updating operating system ....................................................... 19
       1.6.4 Installing and updating applications ........................................... 20
       1.6.5 Viewing service status information .......................................... 22
       1.6.6 Assigning and updating distributions ........................................ 22
       1.6.7 Rebooting device ..................................................................... 24
  1.7 Working with PXC 4/5 Controllers .................................................. 25
       1.7.1 Viewing remote web access ...................................................... 26
1 Asset Manager User Guide

1.1 Overview

Asset Manager is a service that allows you to manage your company assets. Assets are considered to be sites (the building and location the device is in) and IoT devices. This service is currently compatible with the following supported devices in Asset Manager:
- Intelligent Valve
- PXC 4 and PXC 5
- Connect X300

In particular this service offers:
- Managing Sites: Manage sites in Asset Manager by adding, editing, and deleting sites.
- Managing Devices: Manage devices in Asset Manager by finding devices by serial number, adding/removing devices, and viewing/editing device information.
- Working with Devices: Work with supported devices in Asset Manager.

The service is applicable for all cloud offerings.

The instructions in this document will cover how to manage assets in Asset Manager including how to use services available for specific devices.

1.2 Asset Manager icons

The following icons are used in Asset Manager. See the table below for icon meanings.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>Update Available</td>
</tr>
<tr>
<td>⇌</td>
<td>Remote Web Access Available</td>
</tr>
<tr>
<td>🔄</td>
<td>Device Offline</td>
</tr>
<tr>
<td>📦</td>
<td>Number of Devices</td>
</tr>
<tr>
<td>⚠</td>
<td>Number of Offline Devices</td>
</tr>
</tbody>
</table>

1.3 Managing sites

This section will cover how to manage sites, including how to create, edit, and delete sites in Asset Manager.

1.3.1 Creating sites

If you have not already created a site in Asset Manager, follow the steps below.

▶ In Asset Manager:

1. You can add a site in two ways:
   - To add a site through the Overview tab, select Sites.
To add a site through the Sites tab, select Add.

2. Fill in the fields on the ensuing form appropriately. Select Add.

The Address field will automatically suggest addresses. Selecting a suggested address will automatically populate the Time Zone field. If Google API is unavailable, you will need to enter in an address and time zone manually.
1.3.2 Editing sites
To edit a site in Asset Manager, follow the steps below.

1. In Asset Manager:
   - In the sites tab, select Edit in the overflow menu of the site you want to edit.

2. In the pop-up, type to change the fields you want to edit and select update.

1.3.3 Deleting sites
To delete a site in Asset Manager, follow the steps below.

In Asset Manager:
1. In the sites tab, select **Delete** in the overflow menu of the site you want to edit.

![Image of Asset Manager](image)

2. In the pop-up, verify the site that you want to delete. Click **Delete** to remove the site.

![Image of Delete site dialog](image)

Devices associated with a site must be removed prior to deleting the site.

---

1.4 Managing devices

This section will cover how to manage devices, including how to find, add, view/edit, and remove a device.

1.4.1 Finding devices

To find an existing device within your device list by serial number, follow the steps below.

- In Asset Manager:
  1. In the **Overview** tab, type in the serial number of your device in the search bar.
  2. Select **Find**.
3. The device will appear under the site that it's currently added to.

If the serial number was typed incorrectly, the serial number will appear as 'Device Not Found'. Check the serial number to make sure it's correct.

1.4.2 Adding devices

To add a device to a site, follow the steps below.

- In Asset Manager:
1. In the **Sites** tab, select the site where you want to add your device.

2. Select **Add**.

3. Enter the device activation key and select **Validate**.

   The device activation key can be found in the activation email that is sent after registering your device. The activation key can also be found in the device UI. To access the device UI, see Viewing Remote Web Access.

4. Confirm the details of your device and select **Add**.
When defining or changing the custom name of the device, it will only affect the display name in the cloud.

5. A message will appear that the device was successfully added.

1.4.3 Viewing and editing device information
To view and edit device information, follow the steps below.

▷ In Asset Manager:
1. In the **Sites** tab, select the site with the device you want to view.

2. Select the device.

3. The devices information will appear on the screen. To edit this information, select **Edit**.

4. After editing the information, select **Save**.
1.4.4 Removing devices

To remove a device, follow the steps below.

1. In Asset Manager:
   - In the Sites tab, select the site with the device you want to view.

2. Select the device.

3. Click Remove.
4. In the pop-up, click **Remove** to confirm the removal of the device.

5. A message will pop-up when the device is successfully removed.

Once a device is removed, it can be added again to the same site or a different site.
1.5 Working with Intelligent Valves

The Intelligent Valve is a 2-port pressure-independent control valve (PICV) with volume flow, temperature and power measurement for heating, ventilation, and air conditioning plants.

For more information on the Intelligent Valve, please see the Intelligent Valve – Onboarding in Building Operator (A6V11999683).

1.5.1 Performing HVAC self-balancing test

To perform an HVAC Self-Balancing Test for an Intelligent Valve, follow the steps below.

1. In Asset Manager:
   1. In the Sites tab, select the site with the Intelligent Valve you want to perform a test on.
   2. Select the Intelligent Valve in the list of devices.
   3. In the Balancing tab, click Start to begin the Self-Balancing test.

4. Once the test is finished running, you can download a report as a PDF. To download the report, click Report. The file will be downloaded to your browser's download location.

1.5.2 Updating firmware

To update the firmware of the Intelligent Valve, follow the steps below.

1. In Asset Manager:
   1. In the Sites tab, select the site with the Intelligent Valve you want to update.
   2. Select the Intelligent Valve in the list of devices.
3. In the Updates tab, verify the current installed version and available latest version. To update to the latest version, click **Update**.

The Intelligent Valve will close during the firmware update. This may take several minutes.

4. Click **Update**.

5. The update will start to execute. Once the update is installed, it will indicate if your device was successfully updated.

1.6 Working with ConnectX300 devices

The Connect device family of devices are physical devices that serve as the connecting point between the cloud and controlled or monitored devices. This can include controllers, sensors, and actuators in the building. These devices integrate BACnet/IP or Modbus/TCP devices and systems as well as FS20 fire panels.

For more information on the Connect device hardware, please see the Connect X300 Data Sheet (A6V11473182).
For information on network set-up and accessories, please see the CXG3.X300 Quick Install Guide (A6V110508811).

### 1.6.1 Resetting the password

To reset the password of the Connect device, follow the steps below.

- In Asset Manager:
  1. In the Sites tab, select the site with the Connect device.
  2. In the list of devices, select the Connect device you want to reset the password for.
  3. In the Information tab, select Reset Password.

4. Confirm to reset the password by clicking **Reset** in the pop-up.
5. A message will appear that the password has been successfully reset.

6. After resetting the password, log in to the Connect Device Remote Web Access to change the password.

If the password is not changed after it is reset, the old password will still be valid if not changed.

1.6.2 Viewing remote web access

To view remote access for a Connect device, follow the steps below.

Remote web access can be configured and other endpoints can be specified on the device user interface.

1. In Asset Manager:
   1. In the sites tab, select the Connect device you want to access.
   2. In the list of devices, select the device.
   3. In the Remote access tab, click Remote access.

4. After clicking, a new tab will pop up. Enter your log in information to complete remote web access.
1.6.3 Updating operating system

To update the operating system of the Connect device, follow the steps below.

In Asset Manager:

1. In the sites tab, select the site with the Connect device you want to update.
2. In the list of devices, select the device.

The device list will indicate if an update is available for your device.

3. Select the updates tab and click **Update** to update the device to the latest version.

4. Select update to confirm.
5. After the update is executed, an update success message will appear on the screen.

1.6.4 Installing and updating applications

Installing applications
To install applications on your device, follow the steps below.

- In Asset Manager:
  1. In the sites tab, select the site with the Connect device you want to install an application on.
  2. In the list of devices, select the device.
  3. In the Applications tab, navigate to the application you want to install.
4. To install the application, select **Install** and click **Apply**.

5. After applying, a message will indicate if the application was successfully installed.

### Updating applications

To update application on your device, follow the steps below.

- **In Asset Manager:**
  1. In the sites tab, select the site with the Connect device you want to install an application on.
  2. In the list of devices, select the device.
  3. In the Applications tab, navigate to the application you want to update.
  4. To update the application, click **Update**.

5. To verify the update, navigate to the services tab, and find the status of your application.
1.6.5 Viewing service status information

To view service status information, follow the step below.

In Asset Manager:
1. In the sites tab, select the site with the Connect device you want to view.
2. Select the Connect device.
3. Select the Services tab to view the service status of services installed on the device.

1.6.6 Assigning and updating distributions

Assigning distributions

To assign a distribution to a device, follow the steps below.

Assigning a distribution set will only need to be done once.

In Asset Manager:
1. In the sites tab, select the site with the Connect device you want to assign a distribution to.
2. In the list of devices, select the device.
3. Navigate to the Applications tab. A pop up will appear.
4. In the pop-up, select the distribution set and set version. Click Save.
5. After saving, a message will indicate if the distribution was successfully assigned.

**Updating distributions**

To update a distribution on a device, follow the steps below.

▷ In Asset Manager:

1. In the sites tab, select the site with the Connect device you want to install an application on.
2. In the list of devices, select the device.
3. Navigate to the Applications tab.
4. To update the distribution, click **Update**.
5. Verify the applications and distribution set you want to update. Click **Update** to confirm.

6. To verify the update, navigate to the services tab, and find the status of your application.

1.6.7 **Rebooting device**

To reboot a Connect device, follow the steps below.

- In Asset Manager:
1. In the Sites tab, select the site with the Connect device.
2. In the list of devices, select the Connect device you want to reboot.
3. In the Information tab, select Reboot.
4. In the pop-up, click Reboot to confirm to reboot the device.
5. Once the reboot is completed, a message will indicate if your device was successfully rebooted.

1.7 Working with PXC 4/5 Controllers

The Desigo PXC4 controller is designed as a compact device with 16 onboard I/Os that can be expanded to a maximum of 40 I/Os with additional TX-I/O modules.

The Desigo PXC5 is a programmable controller used for system-level functions like alarm routing, system-wide scheduling and trending, device supervision, stronger integration capabilities, and embedded BACnet routing.
For more information on the Desigo PXC4 Controller, please see the Automation Station PXC4.E16 (A6V11646018) and Automation Station PXC4.M16 (A6V11937668).

For more information on the Desigo PXC5 Controller, please see the System Controller PXC5.E003 (A6V11646020).

1.7.1 Viewing remote web access

To view remote web access for a PXC 4/5 Controller, follow the steps below.

1. In the Sites tab, select the site with the controller you want to access.

2. In the list of devices, select the device.

3. In the Remote access tab, click Remote access.

4. After clicking, a new tab will pop up. Enter your log in information to complete remote web access.