



Integration Guide | PUBLIC

Document Version: 2311 – 2023-12-01

Cloud Integration Guide

Content

1	Introduction.	3
2	Prerequisites for Installing the Software Components.	6
2.1	Installing the SAP Java Virtual Machine	7
3	Installation of the Production Connector.	9
4	Settings in the Control Center of the Production Connector.	10
4.1	Adding an Administrator User.	11
4.2	Server Certificate.	13
4.3	Key Usage for Server Certificate.	14
5	Installing the Cloud Connector.	16
6	Upgrade of the Cloud Connector.	18
7	Configuration of the Cloud Connector.	19
7.1	Assisted Configuration of the Cloud Connector.	19
7.2	Setting Up the Cloud Connector Manually.	21
	Starting the Cloud Connector.	22
	Defining the Subaccount.	24
	Mapping Virtual to Internal System.	27
	Adding Accessible Resources.	31
	Creating the Cloud Connector System Certificate	32
	Configure Trust for the Cloud Connector.	37
	Configure Trust for the Production Connector.	37
	Recommendations for the Secure Setup of the Cloud Connector.	38
8	Settings in SAP Digital Manufacturing.	40
8.1	Configuring Production Connectivity.	40
8.2	Configuring Certificates	44
8.3	Maintaining User Groups.	47
9	Troubleshooting.	48

1 Introduction

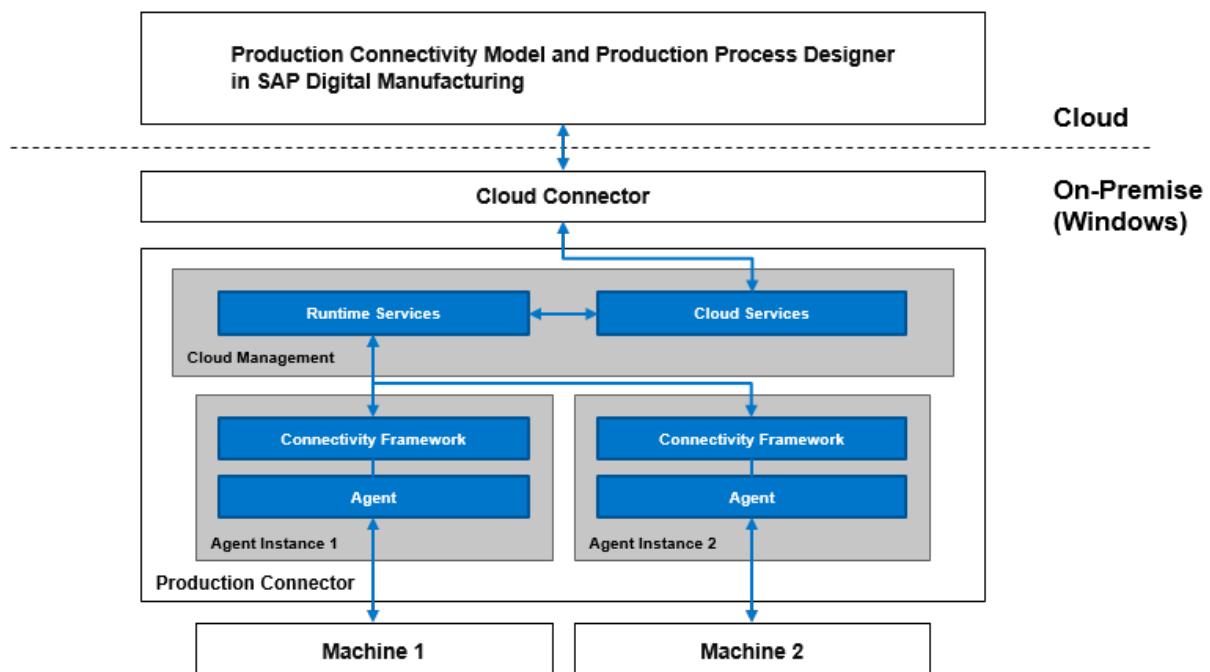
This guide provides an overview of cloud integration and how to establish the connections between SAP Digital Manufacturing, the Production Connector, and the Cloud Connector. It gives you step-by-step instructions for connecting a Windows-based Production Connector instance to SAP Digital Manufacturing using the Cloud Connector. You can use this guide for test purposes, but also for setting up the productive system landscape.

Overview

The Production Connector enables the data flow between shop floor systems in manufacturing and the SAP Digital Manufacturing applications. It is typically installed in the same network as the shop floor systems that you want to integrate with SAP Digital Manufacturing.

Integration with SAP Digital Manufacturing enables end-to-end processes from planning to execution of manufacturing processes involving physical assets or devices.

This guide supports you in connecting instances of the Production Connector with SAP Digital Manufacturing applications to enable the information exchange between, on the one hand, production related, locally installed systems or Internet-enabled devices, and on the other hand, business applications in **SAP Digital Manufacturing**.



The Production Connector hosts services that can be accessed from SAP Digital Manufacturing applications such as **Production Connectivity Model** or **Production Process Designer (PPD)** using the SAP Business Technology Platform (SAP BTP).

The SAP Business Technology Platform offers the **Cloud Connector**, which is required for securing the communication from SAP Digital Manufacturing to the Production Connector. Communication from the Production Connector to the cloud is performed directly, that is, without involving the Cloud Connector.

When you work with cloud applications to configure or operate the Production Connector, the cloud applications send requests via the SAP Business Technology Platform. The Cloud Connector redirects these requests to the endpoint hosted by the Production Connector.

You have to install the Cloud Connector in an on-premise system in your enterprise network, for example, on the same server as the Production Connector or on another server if you want to have several Production Connectors administered by one Cloud Connector.

• Example

If you have created a shop floor system for an OPC UA data source in the Production Connectivity Model, a configuration request is sent automatically to the Production Connector. The necessary objects, OPC UA source system and the corresponding agent instance, are then generated in the Production Connector.

Communication in the direction  *Cloud Application*  *Business Technology Platform*  *Cloud Connector*  *Production Connector*  and in the direction  *Production Connector*  *Cloud Application*  must be secured by using Transport Layer Security (TLS).

i Note

For security reasons, make sure that the endpoint of the cloud services hosted by the Production Connector is not exposed to the public Internet and can only be accessed by the Cloud Connector.

Services Provided by the Production Connector

The Production Connector offers the following services that can be accessed and executed by cloud applications:

- Configuration services

Services that provide the following functions:

- Create, update, and delete source systems, destination systems, and agent instances in the Production Connector
- Browse for tags and services in a data source
- Create, import, and read data types from the Production Connector data type repository

- Administration services

The Production Connector offers the following administration services:

- Start and stop a shop floor system or a service provider (triggers the starting and stopping of an agent instance in the Production Connector)
- Get the runtime status of the agent instance in the Production Connector
- Read the metadata of all services
- Create, update, and delete user groups and their roles
- Create and restore configuration backups

- Runtime services

Services that allow access to the shop floor layer:

- Retrieve tag data
- Write data to a tag of a data source
- Execute a service that you have registered in the *Manage Service Registry* app in SAP Digital Manufacturing
- Certificate services

Services that provide information for certificates:

- Browse certificate folders
- Browse certificates
- Generate self-signed certificates

More Information

For more information on integration, see:

- Migration from SAP Plant Connectivity
If you have used SAP Plant Connectivity for integration with SAP Digital Manufacturing before, the integration functions will be taken over into the Production Connector when you install it. For more information on the migration from SAP Plant Connectivity to the Production Connector, see: [Preparing the Migration from SAP Plant Connectivity](#).
- Shop Floor Integration with SAP
Digital Manufacturing: https://help.sap.com/docs/SAP_DIGITAL_MANUFACTURING/c86ca4026fae4cb3ba66ed751866175b/b39c43da65b94106a01c9d01ec81f23c.html
- Integration with SAP Digital Manufacturing: <https://help.sap.com/docs/sap-digital-manufacturing/integration-guide/integrate-with-production-connector-sap-plant-connectivity>
- SAP BTP Connectivity: https://help.sap.com/viewer/p/CP_CONNECTIVITY
- Cloud Connector: <https://help.sap.com/viewer/cca91383641e40ffbe03bdc78f00f681/Cloud/en-US/e6c7616abb5710148cf3e75d96d596.html>

2 Prerequisites for Installing the Software Components

You can install one Production Connector instance on a computer and connect it with one tenant of SAP Digital Manufacturing. To connect a Production Connector instance to SAP Digital Manufacturing, certain prerequisites need to be met for each software component:

Prerequisites for SAP Digital Manufacturing

- The subaccount ID and location of the **subaccount** containing **SAP Digital Manufacturing** must be known. You can find this information in the **SAP Business Technology Platform (SAP BTP) cockpit**.
- Depending on the **SAP BTP** environment, a user with the roles described under *Managing Subaccounts* must be available for the initial Cloud Connector connection setup. (See <https://help.sap.com/docs/connectivity/sap-btp-connectivity-cf/managing-subaccounts#prerequisites>.)
- The user performing the setup needs to exist in the cloud. He or she needs authorization for working with the **Configure Production Connectivity** app. This requires the role of the **Automation_Engineer** provided by SAP Digital Manufacturing.

Prerequisites for the Production Connector

- A **Windows** computer with an up-to-date operating system is required. The **Production Connector** and, if applicable, the **Cloud Connector** run on this computer.

i Note

The Cloud Connector can also be run on another computer and aggregate several Production Connector instances running on different computers or other on-premise systems.

- The computer on which the **Production Connector** is installed should, if possible, have a Fully Qualified Domain Name (FQDN).
- If a previous **Production Connector** version is already installed, SAP recommends updating to the current version with the latest support package and patch level.
- To download the **Production Connector**, you need access to the SAP Software Center for your S-User. If you do not have this, contact the user administrator in your company.

Prerequisites for the Cloud Connector

- You can find the prerequisites for Cloud Connector hardware under <https://help.sap.com/docs/connectivity/sap-btp-connectivity-cf/sizing-for-master-instance?version=Cloud>.

- Before you can install the Cloud Connector, you need to install a supported Java Development Kit (JDK). SAP recommends, using SAP Java Virtual Machine 8 (SAP JVM 8) for this purpose. You can find an overview of the usable Java Virtual Machines under <https://help.sap.com/docs/connectivity/sap-btp-connectivity-cf/prerequisites#jdks>.
For more information on installation and upgrade of SAP JVMs, see [Installing the SAP Java Virtual Machine \[page 7\]](#).
- It may also be necessary to **install the VC2013 redistributable package** upfront to the installation of the Cloud Connector. The latest 64-bit versions can be obtained here:
 - VC 2013: <https://www.microsoft.com/en-us/download/details.aspx?id=40784>

2.1 Installing the SAP Java Virtual Machine

Prerequisites

If a supported SAP Java Virtual Machine (SAP JVM) or another supported JDK is already installed, you can skip this step. This section describes how to install the recommended SAP JVM. You must execute this step before installing the Cloud Connector.

- All running processes that use the SAP JVM must be closed before you can install the SAP JVM.
- You have to install `VC2019 Redistributable Package` as a prerequisite for SAP JVM.

Procedure

1. To download the SAP JVM, go to the **SAP Development Tools** (see: <https://tools.hana.ondemand.com/#cloud>.)

i Note

You can leave the download page open after the download because it is needed right away for the download of the Cloud Connector.

2. On the [SAP Development Download](#) page, scroll down to the SAP JVM section.

In the SAP JVM overview table, you can find the latest entry for Windows, for example:

Operating System	Architecture	Version	File Size	Download
Windows	x86_64	8.1.094	162.0 MB	Link

3. Click on the download link.
4. Download the `.zip` file for Windows.
5. Unpack the `.zip` file, for example, into `C:\SAP\sap_jvm_8` and remember this path for later.

6. If the SAP JVM is already installed and you want to upgrade it, replace the existing folder with the newly downloaded one.

3 Installation of the Production Connector

The installation of the Production Connector comprises the following steps that are explained in detail in the *Installation Guide*.

- Downloading the software from the SAP Software Center.
- Downloading and installation of the required .NET runtime environments.
- Installation of the Production Connector, either using the SAP front-end installer in dialog mode or the SAP installation server for remote installations. This installation step includes the automatic migration from Plant Connectivity if it was installed before and used for the integration with SAP Digital Manufacturing.
- Postprocessing steps

Related Information

[Software Download](#)

[Installation Using the Front-End Installer](#)

[Installation Using the SAP Installation Server](#)

4 Settings in the Control Center of the Production Connector

The Production Connector provides services for the integration with SAP Digital Manufacturing. These **cloud services** are hosted by the Production Connector main service, which is a Windows service that runs automatically in the background. They can be called by applications from SAP Digital Manufacturing and can ultimately be used to access the service providers at Production Connectivity Model level.

Access to these cloud services is controlled by business-oriented roles that are defined specifically for each service call. The Production Connector only grants access to a particular service if either the user that is configured locally in the Production Connector, or the user groups maintained centrally in SAP Digital Manufacturing, contain the required role.

1. The cloud services are already activated after installation of the Production Connector. In the Control Center, choose the *Cloud Integration* button and change the port for the cloud services on the *Port Settings* tab, if required. You can keep the default port if there are no collisions with other applications using the same port.
2. To enable the deployment of **user groups from SAP Digital Manufacturing**, you must maintain at least one local administrator user with the roles **Administrator**, **CertificateAdministrator**, and **ServiceExecutor** in each Production Connector installation. This user runs the cloud services that are used to create and change the user groups. **No further users should be maintained in the Production Connector**.
3. Select the roles that you want to be assigned to the user.
4. Go to the *JWT Validation* tab.

On the *JWT Validation* tab, you can maintain the following parameters needed for validating the JSON web token:

- *URL of UAA Service*

You have to enter this URL. The URL of the User Account and Authentication service (UAA service) allows you to retrieve the public key. You can find the URL configured for your cloud system in the BTP Cockpit. For more information, see the application help.

- *Public Key*

The public key is used to decrypt the signature of the JSON web token. You can retrieve the key by entering the URL of the User Account and Authentication service (UAA service) and pressing the *Validate UAA Service URL* button.

i Note

Make sure that the computer on which the Production Connector is installed has permanent access to the UAA service. This ensures that exchanging of the signing key is supported without user interaction (key rotation).

Maintain the *Proxy Settings* in the Control Center if required.

5. Go to the *Server Security Settings* tab and maintain the following data:

Field	Description
<i>Server Certificate</i>	<p>Here you specify the server certificate that you have imported or generated for the computer on which the Production Connector is installed.</p> <p>This certificate is used as the Production Connector server certificate when you configure integration with the Cloud Connector (see section below).</p> <p>The certificate is of the type x.509-v3. It enables secure communication between the Production Connector and the Cloud Connector. It should be issued for the host name of the computer on which the Production Connector is running.</p> <p>For more information about the server certificate settings, see Key Usage for Server Certificate [page 14].</p> <p>The certificate can be self-signed for test purposes or must be embedded in a hierarchy of certificates.</p>
	<p>i Note</p> <p>For productive operations, you should always use a certificate that has been signed by a certification authority (CA).</p>
	<p>For more information, see Server Certificate [page 13].</p>
<i>Client Certificates screen area</i>	In the screen area for client certificates, you specify how the certificates, which are exchanged during communication between the Production Connector as a server and the Cloud Connector as a client, or between the Production Connector as a WebSocket server and the service providers as clients, are processed.
<i>Revocation Check</i> and <i>Revocation Check Scope</i>	Maintain the execution and scope of revocation checks for client certificates. Keep the default values <i>No Check on Revoked Certificates</i> and <i>Check End Certificate Only</i> if you are not using revocation lists in your company.

4.1 Adding an Administrator User

The administrator user is required for onboarding the Production Connector installation to SAP Digital Manufacturing and needs to be created in the Control Center. It must also exist as a user in SAP Digital Manufacturing. (See: [Prerequisites for Installing the Software Components \[page 6\]](#).)

Context

The administrator user has the rights that are required to perform the following activities in **SAP Digital Manufacturing**:

- Register the instance of the Production Connector in the [Configure Production Connectivity](#) app.
- Define user groups.
- Assign rights to user groups in the form of roles.

i Note

You should not create any further users in the Production Connector, but instead use the user groups to manage the authorization of the other users in SAP Digital Manufacturing.

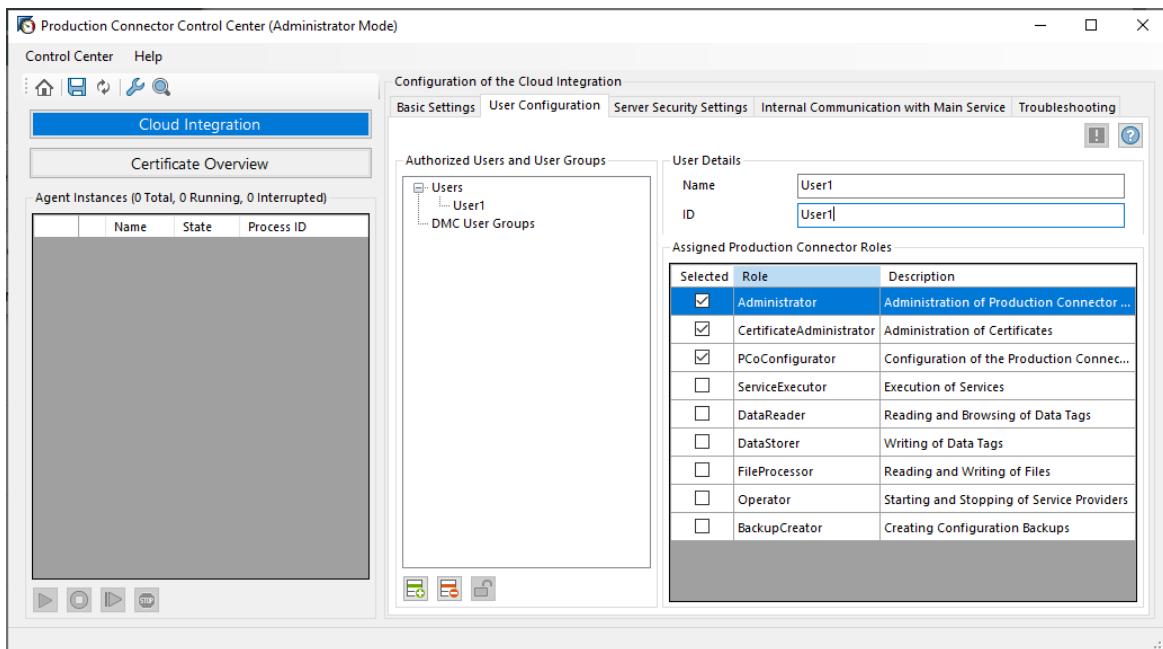
Procedure

1. On the [User Configuration](#) tab page, create the administrator user by choosing the [Add Local User](#) pushbutton and entering a unique name.
2. In the *ID* field, enter the ID provided by your identity provider. Typically, this is the user's e-mail address. The ID must also be unique.
3. To establish a connection to SAP Digital Manufacturing, assign the following roles to the new user:
 - *Administrator*
 - *CertificateAdministrator*
 - *PCoConfigurator*

i Note

Note that the authorizations of users that are specified in the Production Connector are only determined by the roles that you define for these users in the Control Center. The user groups to which this user might be assigned additionally in SAP Digital Manufacturing are not considered for the authorization check.

This is an example for the required role assignment for an administrator user in the Production Connector:



4.2 Server Certificate

The server certificate enables secure communication between the Production Connector and the Cloud Connector.

When a Production Connector system is created, **SAP Digital Manufacturing** requests the public key of the server certificate specified here. The Production Connector forwards the public key to the cloud. The cloud needs this public key so that it can transfer the passwords, which you have specified for specific configuration elements in the Production Connectivity Model, to the Production Connector in encrypted form. Only the Production Connector system that has the appropriate private key can decrypt the passwords.

The trusted folder can be found under: C:\ProgramData\SAP\PCo\CertificateStores\CloudServicesHost\Trusted\certs

The following functions are available for the server certificate:

- Selecting a Server Certificate

You can use this function to select a server certificate from the [Windows certificate store](#). The prerequisite is that you have already stored a suitable certificate in the certificate store of the computer on which the Production Connector is installed.

- Generate Server Certificate

You can use this function to generate a self-signed server certificate for test purposes using default values. In the subsequent dialog box, you can maintain the required parameters for the certificate. After you have closed the dialog box with the [OK](#) button, the server certificate is generated, saved in the Windows certificate store, and displayed in the [Certificate](#) field.

- Export Server Certificate

You can export the public part of the server certificate that you have assigned. To establish secure communication between the Production Connector and the Cloud Connector, you need to upload this

public part of the server certificate to the **Trust Store of the Cloud Connector**. (See: [Configure Trust for the Production Connector \[page 37\]](#).)

i Note

The trusted relationship is automatically established if you configure the Cloud Connector using the assisted configuration option in the Control Center.

4.3 Key Usage for Server Certificate

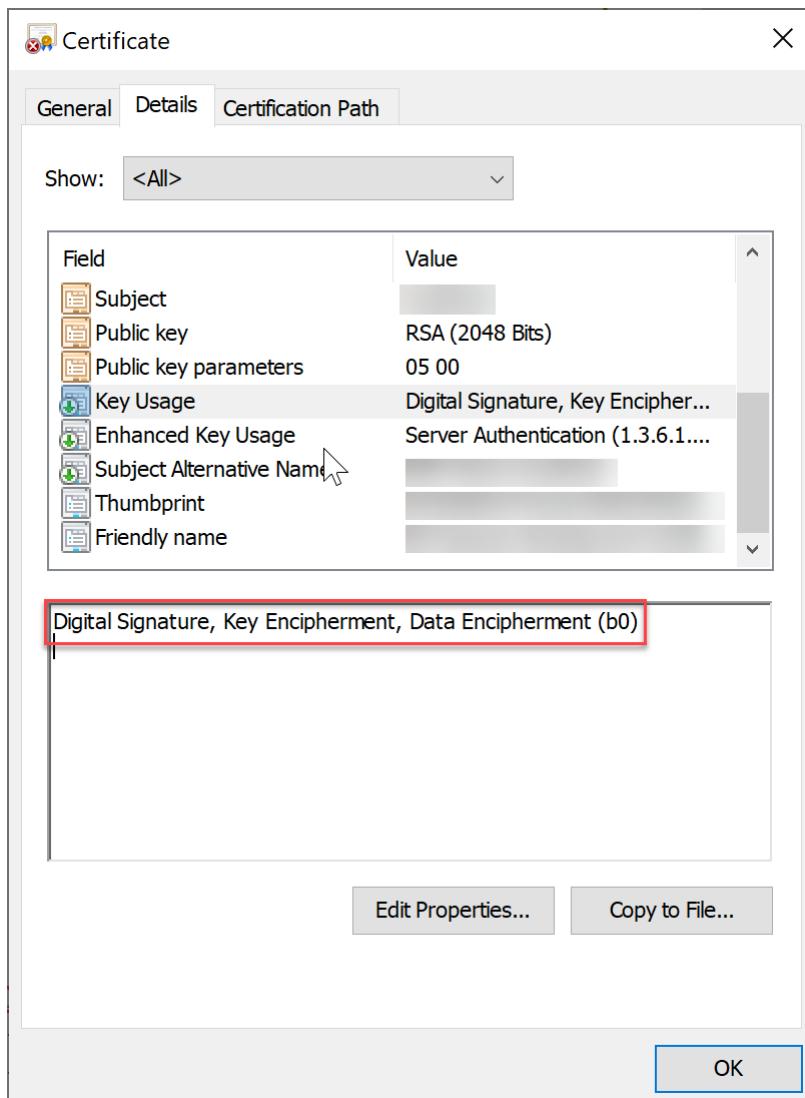
A certificate with a private key is needed for the cloud integration. In this certificate the common name (CN) must be set to the host name or fully qualified domain name (FQDN). There should be no white spaces present. In addition, the Subject Alternative Name (SAN) must have an entry of type DnsName with the same host name or FQDN as the entry. For the key usage, the following attributes are required:

- `DigitalSignature`
- `KeyEncipherment`
- `DataEncipherment`

The enhanced key usage should be `ServerAuth`. Additional attributes are optional.

Example

The screenshot shows what you need to define for the server certificate:



This example refers only to the server certificate. The `KeyUsageProperty` for the private key of the certificate cannot be displayed in the Windows dialog.

i Note

The self-signed server certificate generated by the Production Connector fulfills the requirements.

Related Information

[Generating a Self-Signed Certificate or Signing Request for Cloud Services](#)

5 Installing the Cloud Connector

This document describes the prerequisites and steps for installing the Cloud Connector.

Context

You have to install the Cloud Connector in an on-premise system in your enterprise network, for example, on the same server as the Production Connector, or on another server if you want to have several Production Connector installations administered by one Cloud Connector. (See the following documentation: <https://help.sap.com/viewer/cca91383641e40ffbe03bdc78f00f681/Cloud/en-US/57ae3d62f63440f7952e57bfcef948d3.html>.)

Before the Cloud Connector can be installed, the following prerequisites have to be met:

- A SAP Java Virtual Machine is required. (See: [Installing the SAP Java Virtual Machine \[page 7\]](#).)
- The **VC2013 Redist-package** is required. It can be downloaded from the **Microsoft Download Page** under <https://www.microsoft.com/en-us/download/details.aspx?id=40784> ↗

i Note

If you forget this download, an error message will appear when running the setup saying that a required DLL is missing.

- If the Cloud Connector is running on a separate machine, this machine can also be Linux-based. In this case, follow the installation instructions on <https://help.sap.com/docs/connectivity/sap-btp-connectivity-cf/installation-on-linux-os>.

Procedure

1. To download the **Cloud Connector**, go to the **SAP Development Tools** page: <https://tools.hana.ondemand.com/#cloud>
2. Search for the **Cloud Connector** category and download the **Windows Installer**:

SAP Development Tools

Legal Disclosure | Privacy | Terms of Use | More

HOME ABAP BW CLOUD CLOUD INTEGRATION HANA IDM ML FOUNDATION MOBILE SAPUI5

Cloud Connector

The Cloud Connector is an optional on-premise component that is needed to integrate on-demand applications with customer backend services and is the counterpart of SAP Connectivity service.

For more information, see the Cloud Connector [documentation](#).

Note: The Portable archives for Cloud Connector are meant for non-productive scenarios only. They can be used even if you don't have administrator permissions on the machine, on which you like to use the Cloud Connector. However, those variants do not support upgrades from previous versions.

Available Cloud Connectors

Operating System*	Architecture	Version	File Size	Download
Linux	ppc64le	2.14.2	73.5 MB	sapcc-2.14.2-linux-ppc64le.zip (sha1)
Linux	x86_64	2.14.2	71.9 MB	sapcc-2.14.2-linux-x64.zip (sha1)
Linux (Portable)	ppc64le	2.14.2	76.6 MB	sapcc-2.14.2-linux-ppc64le.tar.gz (sha1)
Linux (Portable)	x86_64	2.14.2	74.3 MB	sapcc-2.14.2-linux-x64.tar.gz (sha1)
Mac OS X (Portable)	x86_64	2.14.2	74.2 MB	sapcc-2.14.2-macosx-x64.tar.gz (sha1)
Windows	x86_64	2.14.2	75.8 MB	sapcc-2.14.2-windows-x64.msi (sha1)
Windows (Portable)	x86_64	2.14.2	73.6 MB	sapcc-2.14.2-windows-x64.zip (sha1)

*Read the [prerequisites](#) page of the documentation in order to inform yourself about the supported operating system versions and JVMs.

SAP JVM

The SAP JVM is a prerequisite for local profiling with the SAP JVM Profiler. It is a standard compliant certified JDK, supplemented by additional supportability and developer features and

i Note

Do not use the portable version.

- Run the setup and click through the setup steps.

If this does not work, run the installer as an administrator.

- When the [Select JDK Installation](#) page is displayed, select the path from the Installation of SAP JVM or the path of another SAP JVM that you have installed yourself. (See: [Installing the SAP Java Virtual Machine \[page 7\]](#).)

Results

After you have installed the Cloud Connector, a **Windows service** with the name **SAP Cloud Connector** is generated. This service is started automatically. The service must be running in order to receive incoming requests.

Next Steps

After the installation of the Cloud Connector, you can immediately start configuring it, for example, through the Control Center of the Production Connector. (See: [Assisted Configuration of the Cloud Connector \[page 19\]](#).)

6 Upgrade of the Cloud Connector

If you have already installed a version of the Cloud Connector and need to update it, there are a few steps to follow. You can find the upgrade steps under <https://help.sap.com/docs/connectivity/sap-btp-connectivity-cf/upgrade>.

i Note

If you don't use a shadow instance, you can skip the section *Avoid Connectivity Downtime*.

7 Configuration of the Cloud Connector

There are two options for configuring the Cloud Connector:

- Assisted configuration in the Control Center of the Production Connector.
This is the recommended way of setting up the integration.
- Manual configuration step-by-step.
You must configure the Cloud Connector manually, for example, if the Cloud Connector is installed on a different computer than the Production Connector and you cannot access the administration UI from the Production Connector computer.

7.1 Assisted Configuration of the Cloud Connector

You can set up the Cloud Connector in the Control Center of the Production Connector. The assisted configuration option offered by the Production Connector guides you step-by-step through the configuration. This is more convenient than carrying out the configuration manually in the Cloud Connector.

Prerequisites

Before starting the assisted configuration, the following prerequisites have to be met:

- You have already installed the Cloud Connector in an on-premise system in your company network, for example, on the same server as the Production Connector, or on a different server if you want to manage multiple on-premise systems with one Cloud Connector.
- You are logged on to the computer, where the Production Connector is installed as a Windows administrator.
- In the Control Center, you have configured the server certificate for the cloud services. You have assigned this server certificate in the *Certificate* field of the server security settings in the Control Center. For more information, see [Settings in the Control Center of the Production Connector \[page 10\]](#).
- You have defined the following Production Connector roles for the administrator user who is executing the onboarding of the Production Connector in SAP Digital Manufacturing:
 - Administrator
 - PCoConfigurator
 - CertificateAdministrator
- You have maintained the security parameters on the *JWT Validation* tab page in the Control Center.
- In the SAP BTP cockpit, you have determined the ID of the subaccount that you are using for your SAP Digital Manufacturing system. (See: <https://help.sap.com/docs/connectivity/sap-btp-connectivity-cf/find-your-subaccount-id-cloud-foundry-environment?version=Cloud.>)

Performing the Configuration

Open the Control Center of the Production Connector. On the *Server Security Settings* tab, choose the *Assisted Configuration* pushbutton to start the user-guided dialog. You are guided through the settings required for the Cloud Connector. You also get support when setting up the certificates that you can use to establish the trust relationship between the Cloud Connector and the Production Connector.

The user-guided configuration is subdivided into the following steps:

Configuration Steps in the Assisted Configuration

Step	Activity	Description
1	Logging on to the Cloud Connector	Log on to the Cloud Connector with the initial user data.
2	Trusting the cloud API certificate	If the Cloud Connector API uses a certificate that is not trusted, you can find all details about this certificate on the UI. Choose the <i>Trust</i> button.
3	Selecting the setup type	<p>There are three options:</p> <ul style="list-style-type: none">• Set Up Integration with the Cloud Connector You choose this option to fully set up a new or existing Cloud Connector.• Manage Cloud Connector Certificate and Establish Trust You choose this option, if you want to update the Cloud Connector certificate or if you want to upload the result of a certificate signing request (CSR).• Establish Trust Between Cloud Connector and Production Connector You select this option if you have updated the Production Connector server certificate.
4	Defining a subaccount	In the first setup, you need to add the subaccount on which your SAP Digital Manufacturing system is running. You can also select an existing subaccount in the first run. For each further configuration run, you only need to select the subaccount.

Step	Activity	Description
5	Establishing the trust relationships	<p>The system certificate is the certificate with which the Cloud Connector identifies itself to the Production Connector. You choose the <i>Trust Certificate</i> button to trust this certificate from the Production Connector perspective.</p> <p>The Production Connector certificate is the certificate that you previously assigned as a server certificate on the <i>Server Security Settings</i> tab in the Control Center. The system selects this certificate automatically. The Production Connector uses this certificate to identify itself to the Cloud Connector. You choose the <i>Trust Certificate</i> button to trust this certificate from the Cloud Connector perspective.</p>
6	Summary of the configuration result	<p>If your configuration has been successful, you receive a success message. In addition, the <i>Internal Host</i>, the <i>Virtual Host</i> and the <i>Location ID</i> are displayed with the configured content. You can copy and store the content of these fields for later usage in SAP Digital Manufacturing in the <i>Configure Production Connectivity</i> app.</p>

7.2 Setting Up the Cloud Connector Manually

This section shows the configuration steps necessary for setting up the Cloud Connector version 2.15. You can use this alternative method, if you cannot execute the user-guided dialog in the Production Connector Control Center.

You may have to choose the manual configuration, for example, if the Cloud Connector runs on a different machine than the Production Connector and the port for configuring the Cloud Connector (typically 8443) is not open.

Configuration Steps

Step	Configuration Activity	Description
1	Starting the Cloud Connector [page 22]	Open the Cloud Connector and log on for the first time.

Step	Configuration Activity	Description
2	Defining the Subaccount [page 24]	Define the subaccount and user data. A subaccount user is needed for establishing the connection between the SAP BTP subaccount and the Cloud Connector.
3	Mapping Virtual to Internal System [page 27]	In this step, you define a virtual system that addresses the endpoint of cloud services running on the Production Connector.
4	Adding Accessible Resources [page 31]	In this step, you specify the resources that are accessible from the cloud. Additionally, you can specify the access authorizations for the resources of the endpoint, for example, authorization for creating a service provider.
5	Creating the Cloud Connector System Certificate [page 32]	The system certificate of the Cloud Connector is the certificate with which the Cloud Connector identifies itself to the Production Connector.
6	Configure Trust for the Cloud Connector [page 37]	To establish a secure connection between the Cloud Connector and the Production Connector, the Production Connector needs to trust the system certificate that you have provided in step 5.
7	Configure Trust for the Production Connector [page 37]	You have to enter a certificate in the <i>Configuration Trust Store</i> section of the Cloud Connector. You can use the server certificate from the Production Connector.

7.2.1 Starting the Cloud Connector

Open the Cloud Connector and log on for the first time.

Procedure

1. Enter the URL `https://localhost:8443` into the browser on the machine where the Cloud Connector is installed.

i Note

If the Cloud Connector is installed on a different computer, enter the host name of this computer instead of **localhost**.

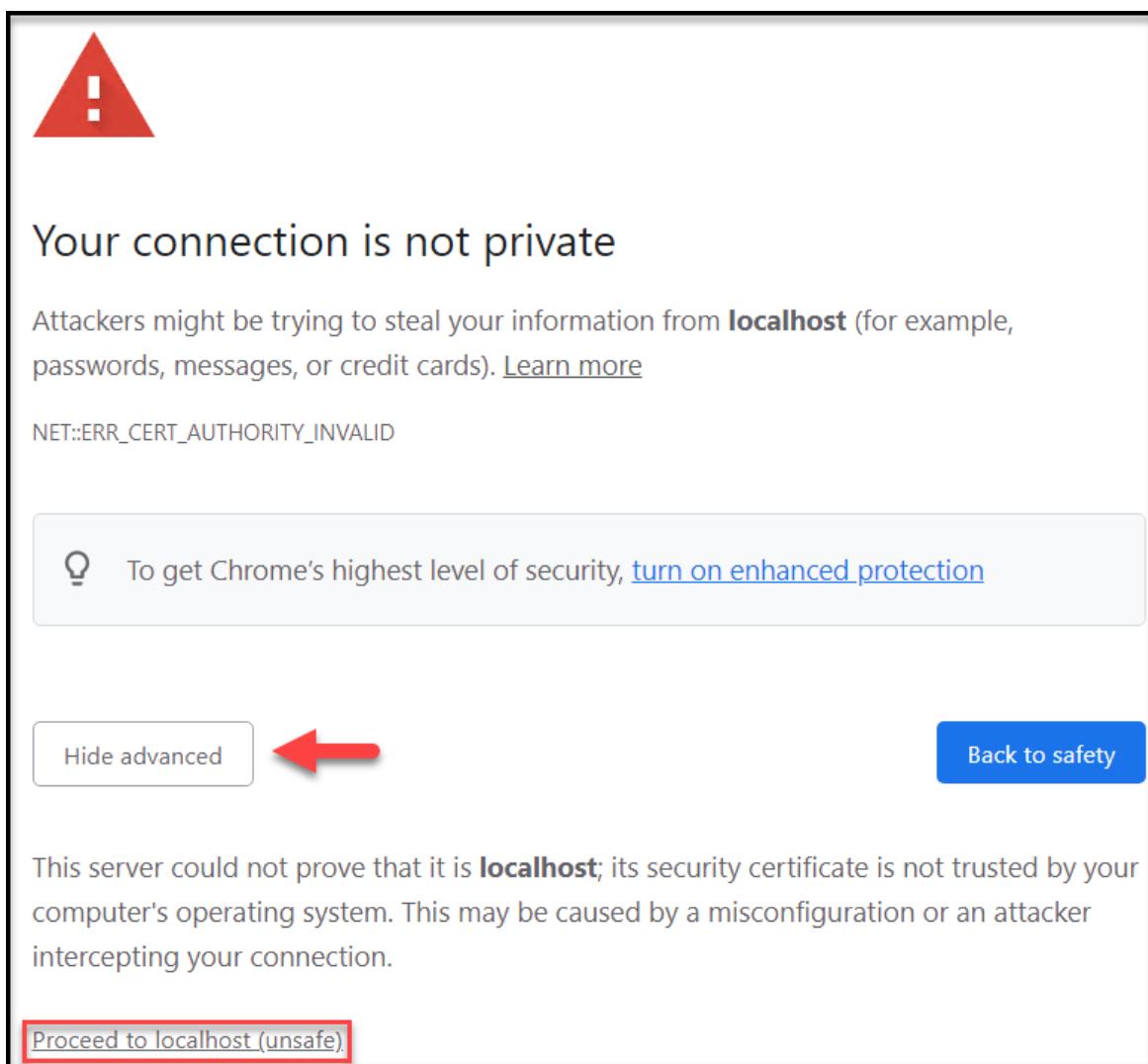
Enter the port that you maintained during the installation of the Cloud Connector; **8443** is the default port.

Your browser will display a warning: `Your connection is not private`.

The reason for this warning is that the Cloud Connector initially uses a self-signed certificate for the website. This can be replaced later, making it more secure to access the Cloud Connector website from another computer.

2. Skip the warning by clicking on [Show advanced](#) and then choose [Proceed to localhost \(unsafe\)](#).

You can see an example of this in the following screenshot, but it may look different, depending on your browser.



i Note

If the Cloud Connector website is not available, run the [Start Cloud Connector](#) app as an administrator from the Windows start menu.

The [Cloud Connector Login](#) screen appears.

- Enter the following initial login data on the *Login* screen:

Login Data

Field	User Input
User Name	Administrator
Password	manage

Note
You have to change the password after the first login.

You will see the information: Installation has neither master nor shadow role. Administrator rights are required.. This information can be ignored for the initial setup.

After you have successfully entered the login data, you will be redirected to a page called *Initial Setup*:

The screenshot shows the SAP Cloud Connector Administration interface. At the top, it says "Cloud Connector Administration" and "Administrator". Below that is the "Initial Setup" section. It contains two main sections: "Mandatory Password Change" and "Choose Installation Type". In the "Mandatory Password Change" section, there are three input fields: "Current Password" (containing "*****"), "New Password" (containing "*****"), and "Repeat New Password" (containing "*****"). In the "Choose Installation Type" section, there are two radio buttons: "Master (Primary Installation)" (selected) and "Shadow (Backup Installation)". There is also a "Description" field with a placeholder. At the bottom left, a note says "You are required to change your password before being permitted to continue". At the bottom right are "Save" and "Cancel" buttons.

- On this initial screen change the password and select the installation type. Leave it at *Master (Primary Installation)*.

Afterwards, you can optionally perform a "Shadow" installation on another computer, which will take over the tasks in case the primary installation fails. For more information on how to install a failover instance, see: <https://help.sap.com/docs/connectivity/sap-btp-connectivity-neo/install-failover-instance-for-high-availability>

7.2.2 Defining the Subaccount

A subaccount is needed for establishing the connection between the SAP BTP subaccount and the Cloud Connector.

This procedure explains how to set up the subaccount for the Cloud Connector:

- Find out the SAP BTP role, the subaccount ID, and the region of your SAP Digital Manufacturing tenant. You can find this information on the overview page of the **Business Technology Platform Cockpit**, or you can ask your administrator.

The screenshot shows the SAP BTP Cockpit interface. On the left, there's a sidebar with links like Overview, Services, HTML5 Applications, Connectivity, Security, Entitlements, and Usage Analytics. The main area has tabs for General, Cloud Foundry Environment, and Entitlements. Under General, there are sections for Entitlements and Instances and Subscriptions. A subaccount configuration form is displayed, with fields for Subdomain, Tenant ID, Provider, Region (which is highlighted with a red box), Used for Production, Beta Features, Subaccount ID (also highlighted with a red box), Created By, Created On, and Modified On.

2. On the **Cloud Connector** web page, choose *Subaccount*.

The following page opens, on which you can set up the first subaccount and a proxy configuration:

The screenshot shows the 'Define Subaccount' page. At the top, there's a message: 'Cloud Connector is not configured and remains inoperative unless you define at least one subaccount'. Below this, there are two sections: 'First Subaccount' and 'HTTPS Proxy'. The 'First Subaccount' section contains fields for Region, Subaccount, Display Name, Subaccount User, Password, Location ID (with placeholder 'Enter location ID to overwrite default'), and Description. The 'Region' field is highlighted with a red box. The 'HTTPS Proxy' section contains fields for Host, Port, User, and Password.

3. Enter the following data for the new subaccount:

Field	User Input
<i>Region</i>	Specify the SAP Business Technology Platform (BTP) host that should be used. You can choose a region from the dropdown list. See also: https://help.sap.com/viewer/65de2977205c403bbc107264b8eccf4b/Cloud/en-US/350356d1dc314d3199dca15bd2ab9b0e.html

Field	User Input
<i>Subaccount</i>	<p>Enter the value you obtained when you registered your subaccount on SAP BTP. See also: <i>Managing Subaccounts</i>: under https://help.sap.com/viewer/cca91383641e40ffbe03bdc78f00f681/Cloud/en-US/f16df12fab9f4fe1b8a4122f0fd54b6e.html</p> <p>In the Cloud Foundry environment, you must enter the subaccount ID as <Subaccount>, rather than its actual name. For information on getting the subaccount ID, see section <i>Find Your Subaccount ID</i> (<i>Cloud Foundry Environment</i>) under https://help.sap.com/viewer/cca91383641e40ffbe03bdc78f00f681/Cloud/en-US/b43eff2df3f84124995f6acbc9e5c55b.html.</p>
<i>Display Name</i>	<p>The display name is how the subaccount will be displayed in the Cloud Connector. This simplifies management in case several different subaccounts are used on one computer.</p>
<i>Subaccount User / Login E-Mail</i>	<p>Enter your login e-mail for your Business Technology Platform user, which has the user rights defined in <i>Managing Subaccounts</i> (see: https://help.sap.com/docs/CP_CONNECTIVITY/%20cca91383641e40ffbe03bdc78f00f681/f16df12fab9f4fe1b8a4122f0fd54b6e.html?version=Cloud.)</p> <p>The rights for this user can be removed after the connection has been established, because the user is only used for the initial connection setup.</p>
<i>Password</i>	<p>Enter your password.</p> <p>If you have configured two-factor authentication for your account, enter your password followed by the one-time passcode. In this case, it is recommended that you make all the other settings on the current screen, before you complete your password entry to prevent the passcode expiring before you submit your input.</p>

Field	User Input
<i>Location ID</i>	<p>The Location ID uniquely identifies the Cloud Connector on the Business Technology Platform and in SAP Digital Manufacturing for a specific subaccount. This entry is mandatory.</p> <p>You can enter an ID of your choice. Use characters A-Z, a-z, 0-9 only.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> i Note <p>The location ID is used in the <i>Configure Production Connectivity</i> app later. (See also, Configuring Production Connectivity [page 40].)</p> </div>
<i>Description</i>	Enter a description.

4. Define the proxy settings. These settings are only required if you are using a proxy server in your network.

Field	Entry
<i>Proxy Host</i>	example: proxy
<i>Proxy Port</i>	example: 8080
<i>User</i>	example: proxypassword
<i>Password</i>	example: proxypassword

5. Choose **Save**.

The overview page of the subaccount should appear, showing that a connection has been established.

For more information, see **Initial Configuration** in the SAP BTP Connectivity documentation: https://help.sap.com/viewer/cca91383641e40ffbe03bdc78f00f681/Cloud/en-US/db9170a7d97610148537d5a84bf79ba2.html#loiodb9170a7d97610148537d5a84bf79ba2__configure_proxy

7.2.3 Mapping Virtual to Internal System

With these settings, you define a virtual system that addresses the endpoint of the cloud service running on the Production Connector. This virtual system will be used to connect the Cloud Connector with the Production Connector in **SAP Digital Manufacturing**.

1. Access the Cloud Connector web interface: <https://localhost:8443>.

i Note

If you have customized the WebUI certificate or copied the self-signed WebUI certificate manually, you can safely access it from other computers. In this case, enter the host name or the FQDN instead of local host.

2. On the *Cloud Connector Administration* screen, select *Cloud To On-Premise* (in the menu on the left). Then press the **+** button to add the system mapping as shown in the following screenshot:

A wizard appears asking you for all the required settings.

3. Enter the following data:

Field	Entry
<i>Back-end Type</i>	Other SAP System
<i>Protocol</i>	HTTPS
<i>Internal Host</i>	Enter the FQDN or host name of the machine on which the Production Connector is installed. The FQDN or host name should match the Common Name (CN) of the Production Connector system certificate.
<i>Internal Port</i>	Enter the port of the endpoint for the cloud services of the Production Connector.
<i>Virtual Host</i>	Enter the virtual host, for example, prodconccms . This is a unique name for this Production Connector instance and used for its identification.
i Note Do not use special characters for the host name. Only use characters A-Z, a-z, 1-9 and periods.	

Field	Entry
<i>Virtual Port</i>	Enter the virtual port, for example, 50066 . The URL will look like this: <code>https://prodconccms:50066</code>
	<p>i Note</p> <p>Internal port and virtual port can be the same.</p>
<i>Principal Type/ Principal Propagation</i>	<p>Principal propagation is no longer used in favor of certificate-based OAuth authentication.</p> <p>Therefore, configure the following (depending on the Cloud Connector version):</p> <ul style="list-style-type: none"> • If you are using Cloud Connector version 2.14.x, set the <i>Principal Type</i> to None. • If you are using Cloud Connector version 2.15.0 or higher, deselect the <i>Principal Propagation</i> checkbox.
<i>Check Internal Host</i>	Select the checkbox.
<i>System Certificate for Logon</i> (only Cloud Connector version 2.15.x)	Select the checkbox.

Choose **Save**.

4. You can display your settings:

Edit System Mapping

Virtual host and port cannot be changed

Back-end Type:	Other SAP System
Protocol:	HTTPS
Virtual Host:	
Virtual Port:	50060
Internal Host: *	
Internal Port: *	50060
SAProuter:	
Principal Type:	None
System Certificate for Logon:	<input checked="" type="checkbox"/>
SNC Partner Name:	
Host In Request Header:	Use Virtual Host
Description:	
Check Internal Host:	<input type="checkbox"/> 

Save **Cancel**

5. After you have saved your settings successfully, the dialog should close and an entry with the check result **Reachable** should appear.

If the Production Connector is reachable from the Cloud Connector it is not necessarily reachable from the cloud yet. You have to establish trust between the communication partners first.

If the Production Connector is not reachable, check the following possible reasons for failures:

- The internal port is wrong or already used. Please check and change this again as described above.
- The cloud integration settings have not been saved in the Production Connector.
- The Production Connector main service has not been started. Please check if the service **SAP Production Connector (ProdConMainService)** is running.

- A firewall is preventing the connection. Check this with your IT administrator.

7.2.4 Adding Accessible Resources

Define the resources that SAP Digital Manufacturing can access via the Cloud Connector.

The prerequisite for defining the resources is that the connection to the Cloud Connector has been successfully established.

1. Go to the *Cloud To On-Premise* screen.
In the screenshot below you can see the list for those resources. The list is currently still empty.
2. To add an accessible resource, choose the **+** button in the *Access Control* section as shown in the following screenshot:

Cloud To On-Premise - Access Control

The *Add Resource* screen appears.

3. Enter the following data on the *Add Resource* screen:

Add Resource

Field	Entry
URL Path	/cloudservices

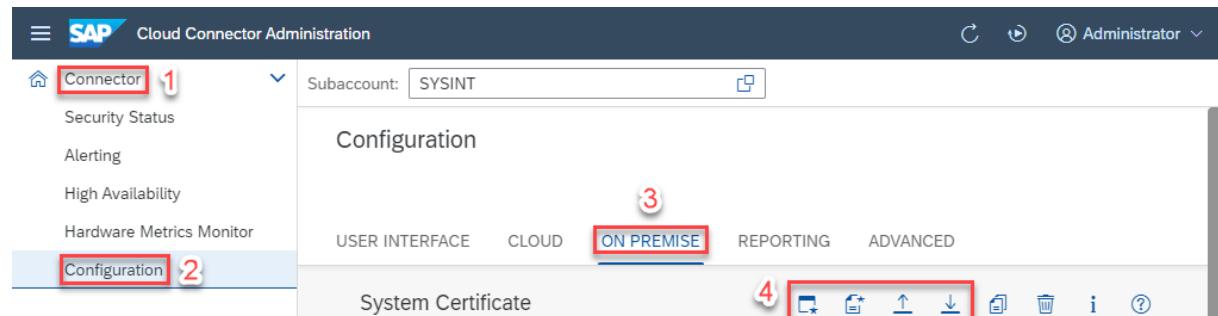
Field	Entry
Active	Select the checkbox. Active means that the resource can be used.
WebSocket	Do not select this checkbox.
Path and all sub-paths	Select the checkbox. This is the Access Policy.

- Save your entries.

7.2.5 Creating the Cloud Connector System Certificate

The system certificate of the Cloud Connector is the certificate with which the Cloud Connector identifies itself to the Production Connector. You have to specify a system certificate for establishing a secure connection between the two communication partners.

Follow the steps as shown in the picture:



- On the *Cloud Connector Administration* screen go to *Connector* in the menu on the left.
- Choose *Configuration*.
- Choose the *On Premise* tab.
- Use the pushbuttons to create a system certificate. You have the following options:
 - You can create a certificate signing request (CSR) and import the signed certificate later. (See: [Create a CSR and Import the Signed Certificate \[page 33\]](#).)
 - You can create a self-signed certificate (second button) and import it. (See: [Create and Import a Self-Signed Certificate \[page 34\]](#).)

Related Information

[Troubleshooting \[page 48\]](#)

7.2.5.1 Create a CSR and Import the Signed Certificate

In this step, you create a certificate signing request (CSR) and then import the generated certificate.

1. Choose the *Configuration* option in the menu on the left and then click on the *On Premise* section.
2. On the *On Premise* screen, choose the button to generate a certificate signing request as shown in the screenshot:

The screenshot shows the SAP Cloud Connector Administration interface. The left sidebar has sections like Connector, Security Status, Alerting, High Availability, Hardware Metrics Monitor, Configuration, Cloud To On-Premise, On-Premise To Cloud, Monitor (Cloud to On-Premise), Monitor (On-Premise to Cloud), Audits, Log And Trace Files, Important Links, and Legal Information. The main area is titled 'Configuration' and has tabs for USER INTERFACE, CLOUD, ON PREMISE (which is selected), REPORTING, and ADVANCED. Under 'ON PREMISE', there's a 'System Certificate' section with fields for Subject DN, Issuer, Valid From, and Valid To. It also includes a 'Subject Alternative Names' table with one row: Type (No data). Below this is a 'Trust Store' section with a warning message: 'No trusted backends are configured — HTTPS communication is not possible'. At the bottom is an 'Allowlist (0)' section with a table for X.509 Certificates. A red box highlights the 'upload' icon in the top right corner of the 'System Certificate' section.

The *Generate CSR* dialog box appears.

3. Enter the following **data for generating a certificate signing request** in the dialog box:

Data for Generating a Certificate Signing Request

Field	Description
Common Name (CN)	Enter the fully qualified domain name of the server where the Cloud Connector is installed.
Email-Address (EMAIL)	Optional. You can enter the e-mail address of the user.
Organizational Unit (OU)	Optional. Enter your organizational unit.
Country (C)	Optional. Enter your country, for example, DE.

4. Choose the *Generate* button in the dialog box.

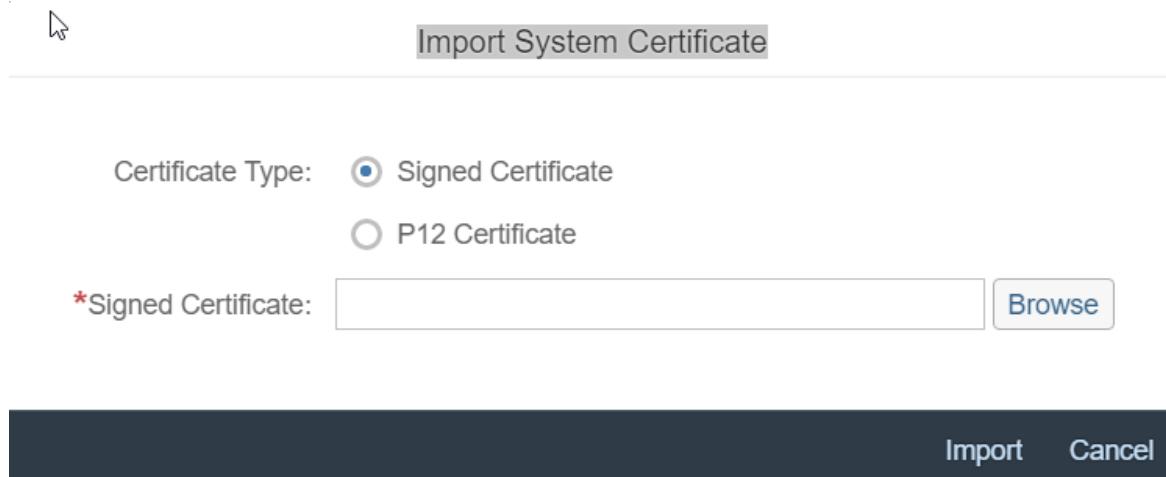
The certificate signing request is created automatically.

i Note

As a customer, you have to generate a trusted certificate from the signing request using your own public-key infrastructure (PKI). As an alternative, you can also use a certificate from a public certification authority (CA). Export the signed certificate to a `.pem` file or a PKCS#7 keystore. Optimally, include the entire certificate chain.

5. Choose **Connector > Configuration > On Premise > System Certificate** in the Cloud Connector and press the button for importing a certificate (icon with arrow pointing up).

The dialog box *Import System Certificate* is displayed. Here you have to browse for the certificate that has been created:



6. Select the certificate and choose the *Import* button.

Now the system certificate is added and displayed. See the following screenshot:

Cloud Connector Administration

Configuration

USER INTERFACE CLOUD **ON PREMISE** REPORTING ADVANCED

System Certificate

Subject DN:	CN= [REDACTED]	Subject Alternative Names
Issuer:	CN= [REDACTED]	Type Value
Valid From:	2022-10-20 16:41:14 +0200	DNS [REDACTED]
Valid To:	2023-10-20 16:51:14 +0200	DNS [REDACTED]
		DNS [REDACTED]

Trust Store

No trusted backends are configured — HTTPS communication is not possible

Determining Trust Through Allowlist:

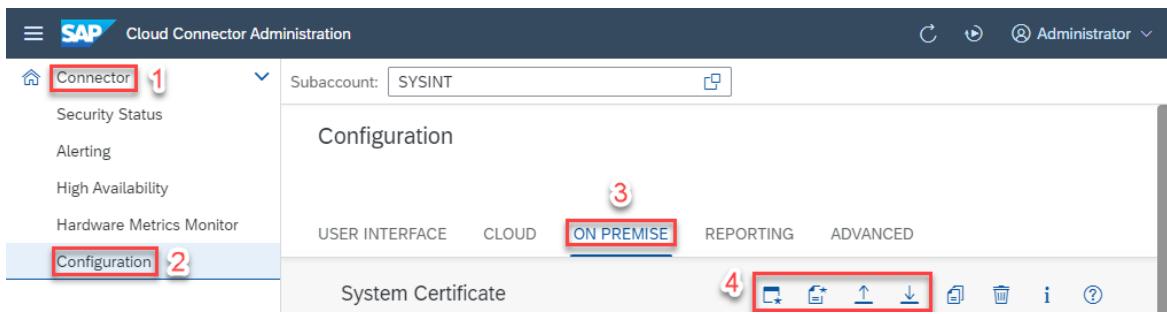
Allowlist (0)

Status	X.509 Certificate	Actions
No data		

7.2.5.2 Create and Import a Self-Signed Certificate

For test purposes, you can also use a self-signed certificate as system certificate for the Cloud Connector. SAP recommends using only CA-issued certificates in productive environments.

1. Choose the *Configuration* option in the menu on the left and then click on the *On Premise* section
2. On the *On Premise* screen choose the button *Create and Import a Self-Signed Certificate*.



The following dialog box is displayed:

Create Self-Signed Certificate

Key Size

2048 Bits 4096 Bits

Subject DN

Common Name (CN):*	<input type="text"/>
E-Mail Address (EMAIL):	<input type="text"/>
Locality (L):	<input type="text"/>
Organizational Unit (OU):	DMC
Organization (O):	SAP SE
State or Province (ST):	BW
Country (C):	DE

Subject Alternative Names +

Type	Value	Actions
DNS	<input type="text"/>	
DNS	<input type="text"/>	
DNS	<input type="text"/>	

Create Cancel

- Enter the required data and press the *Create* button.

i Note

You have to enter the Fully Qualified Domain Name (FQDN) or the host name of the Cloud Connector computer in the *CN* field or in the *Subject Alternative Name* field.

As a result, the self-signed certificate is created.

- Choose the *Download* button (see arrow icon in image) to download the public part of the generated certificate.

You need this certificate later on the computer where the Production Connector is installed. (See: [Configure Trust for the Production Connector \[page 37\]](#).)

7.2.6 Configure Trust for the Cloud Connector

To establish a secure connection between the Cloud Connector and the Production Connector the Production Connector needs to trust the system certificate of the Cloud Connector.

The Cloud Connector system certificate can be a self-signed certificate or a certificate that was signed by a certification authority (CA). SAP recommends using only CA-issued certificates in productive environments. (See: [Creating the Cloud Connector System Certificate \[page 32\]](#).)

Depending on whether the system certificate is a self-signed certificate or a certificate signed by a CA, you proceed differently:

- The system certificate of the Cloud Connector is self-signed:**

Copy the self-signed certificate to
C:\ProgramData\SAP\ProdCon\CertificateStores\CloudServicesHost\Trusted\certs.

- The system certificate of the Cloud Connector is signed by a CA:**

Copy the system certificate of the intermediate CA to:
C:\ProgramData\SAP\ProductionConnector\CertificateStores\CloudServicesHost\Trusted\certs.
In addition, all intermediate CA certificates (including the one that may be in the Trusted folder) and the root certificate must be copied to the following folder:
C:\ProgramData\SAP\ProductionConnector\CertificateStores\CloudServicesHost\Issuer\certs.

For more information about root and intermediate certificates, see: <https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/77a609451dbd46a58991e685c37350d8.html?q=Certificate%20chain>

7.2.7 Configure Trust for the Production Connector

In this step, you configure trust in the *Configuration Trust Store* of the Cloud Connector so that the Production Connector is accepted as a trusted communication partner.

Upload the server certificate of the Production Connector into the *Configuration Trust Store* section of the Cloud Connector.

- If the certificate is self-signed, upload the public part of the certificate to the trust store .

i Note

You can export the public part of the **server certificate** that you have selected or generated in the **Production Connector** under *Cloud Integration* on the *Server Security Settings* tab. You can use the *Export Server Certificate* pushbutton to save this data on your computer. The button is located on the

Server Security Settings tab to the right of the selected server certificate. (See also: [Server Certificate \[page 13\]](#).)

- If the server certificate is issued by a CA, upload the public part of the root certificate of the CA or of the intermediate CA into the trust store.

When one of these certificates is uploaded to the *Trust Store* of the Cloud Connector, the Production Connector server certificate becomes trustworthy.

i Note

The server certificate must be uploaded to the trust store as of Cloud Connector version 2.15. Earlier versions of the Cloud Connector do not require this step.

The screenshot shows the SAP Cloud Connector Administration interface. The left sidebar has sections like Connector, Security Status, Alerting, High Availability, Hardware Metrics Monitor, Configuration (which is selected), and Audit logs. The main content area has tabs for USER INTERFACE, CLOUD, ON PREMISE (which is selected), REPORTING, and ADVANCED. Under ON PREMISE, there's a 'System Certificate' section with fields for Subject DN, Issuer, Valid From, and Valid To, along with a table for Subject Alternative Names (IP, DNS). Below that is a 'Trust Store' section with a note about listed backends and an 'Allowlist' table. The Allowlist table has columns for Status, X.509 Certificate, and Actions. There are '+' and '-' buttons at the top of the table.

7.2.8 Recommendations for the Secure Setup of the Cloud Connector

To increase security, follow the instructions in the SAP BTP Connectivity documentation.

Related Information

<https://help.sap.com/docs/connectivity/sap-btp-connectivity-cf/recommendations-for-secure-setup>

8 Settings in SAP Digital Manufacturing

This section describes the steps for configuring the connection between the Production Connectivity Model in SAP Digital Manufacturing and the Production Connector.

Prerequisites:

The role `Automation_Engineer` is assigned to your user.

Configuration Steps

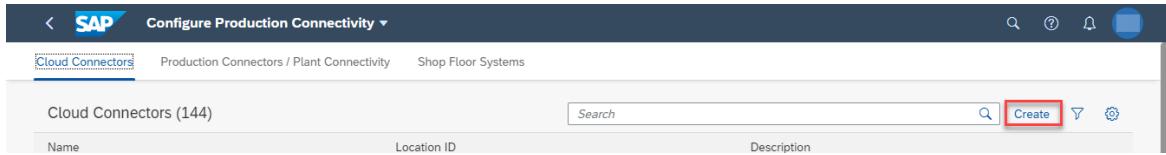
Step	Configuration Activity	Description
1	Configuring Production Connectivity [page 40]	You configure the connection between the Cloud Connector and the individual Production Connector installations.
2	Configuring Certificates [page 44]	You define the certificates for communication between the Production Connectivity Model and the Production Connector.
3	Maintaining User Groups [page 47]	You assign Production Connector roles to the user groups that you have defined in the cloud. The user groups are then distributed to the pertaining Production Connector installation.

8.1 Configuring Production Connectivity

You configure the connections between SAP Digital Manufacturing, the Cloud Connector and the Production Connector by executing the following activities:

1. Log on to **SAP Digital Manufacturing** using the same user for which the user ID was added as administrator in the Production Connector.
2. Choose the *Configure Production Connectivity* app.

The *Cloud Connector* screen area of this app appears:



Configure Production Connectivity - Cloud Connector

3. Choose the *Create* button to enter the parameters of the Cloud Connector.

The screen for the new Cloud Connector appears.

4. Enter the following data:

Cloud Connector Data

Field	Description
<i>Name</i>	Enter the name for the Cloud Connector, that you have installed.
<i>Description</i>	Enter a description for the Cloud Connector.
<i>Location ID</i>	Enter the location ID of the Cloud Connector. This ID identifies the location of this Cloud Connector for a specific subaccount. (See also: Defining the Subaccount [page 24] .)

5. Go back to the overview screen and choose the *Production Connectors / Plant Connectivity* tab. Then choose the *Create* button to add the data for the Production Connector system that you want to connect.

The following dialog appears:

SAP Configure Production Connectivity

New Production Connector

Production Connector / Plant Connectivity

Header Connections Certificates

Name: * demoProdCon Internal Host: * https://:50060

Description: Plant: 0001

Connections

Cloud Connector: * DemoCloudConnector Test Connection

Production Connector / PCo Virtual Host URL: * http://:50060

Certificates

Company Name: SAP SE

Create Cancel

New Production Connector

6. Enter the data for the Production Connector system:

Production Connector Header Data

Field	Description
Name	Enter the name of the Production Connector system.

Note
You cannot create multiple Production Connector systems that have the same internal host URL.

Field	Description
<i>Internal Host (URL)</i>	<p>Enter the URL of the internal host of the Production Connector server in the following format: <code>https://<internal host>:<internal port></code></p> <div style="background-color: #f0f0f0; padding: 10px;"> <p>i Note</p> <p>A valid URL should be in the following format: <code>https://<Fully Qualified Domain Name>:<port></code>. The FQDN should be the same as the common name (CN) of the server certificate used in the Production Connector.</p> </div>
<i>Plant</i>	Enter the plant for which the Production Connector instance is used.
Connections (Cloud Connector)	
Field	Description
<i>Cloud Connector</i>	Select the previously entered Cloud Connector.
<i>Virtual Host (URL)</i>	<p>Enter the URL of the virtual host of the Cloud Connector in the format <code>http://<virtual host>:<virtual port></code>. (See also: Mapping Virtual to Internal System [page 27].)</p>
<i>Certificate - Company Name</i>	Enter the company name that should appear on the certificates.

7. Choose the *Test Connection* button.

If the system certificate of the Cloud Connector has been copied correctly before, the connection will be established successfully.

If this is not the case, an error message will appear. For more information, see [Troubleshooting \[page 48\]](#).)

8. Choose the *Create* button.

As a result, the Production Connector instance is created in SAP Digital Manufacturing and linked to the Cloud Connector. The following overview should display the status **Connected**, as shown in the following screenshot:

The screenshot shows the SAP Configure Production Connectivity application interface. At the top, there's a header with the SAP logo, the title 'Configure Production Connectivity' and 'Plant: HOME (HOME)', and several navigation icons. Below the header, a 'Production Connector' card is displayed. The card has a 'Status:' section showing 'Connected'. It also includes fields for 'Internal Host URL:' (https://...:50060), 'Plant:' (HOME), 'Description:' (empty), 'Type:' (Production Connector on Windows), 'Version:' (1.0.0), and 'Data Ingestion Enabled:' (No). There are 'Edit', 'Delete', 'Refresh', and 'Enable Data Ingestion' buttons at the top right of the card. Below the card, there are tabs for 'Connections' (which is selected), 'Certificates', 'User Groups', 'Backup', and 'Monitoring'. Under the 'Connections' tab, there are sections for 'Cloud Connector:' (greyed out) and 'Production Connector Virtual URL:' (http://...:50060). Under the 'Certificates' tab, there's a section for 'Cloud to Production Connector Certificate'.

You will also see the *Certificate Overview* where you have to create the required certificates. (See: [Configuring Certificates \[page 44\]](#).)

8.2 Configuring Certificates

You define the certificates for communication between the Production Connectivity Model and the Production Connector in the *Configure Production Connectivity* app.

1. Choose the *Configure Production Connectivity* app to define the certificates.
2. Choose the *Production Connector / Plant Connectivity* tab.
All Production Connector systems that you have already maintained are displayed in the list.
3. Choose an existing Production Connector system or choose the *Create* button to add a new Production Connector system.
4. Enter *Name* and *Description* for the Production Connector system that you want to create.

5. Add the certificates on the *Certificates* tab:

Certificates for communication with the Production Connector

Certificate	Description
<i>Cloud to Production Connector Certificate</i>	<p>The purpose of this certificate is to encrypt information that is sent from SAP Digital Manufacturing to the Production Connector system.</p> <p>After the Production Connector system has been created in the <i>Configure Production Connectivity</i> app in the cloud, the public key of the server certificate that you have defined in the corresponding Production Connector is retrieved from the Production Connector and the certificate details are displayed here, for example, the validity dates of the certificate.</p> <p>After you have renewed the server certificate in the Production Connector, choose the <i>Refresh Certificate</i> button in the cloud to upload the current certificate.</p>

Certificate	Description
<i>Production Connector to Cloud Certificate (X.509 OAuth)</i>	<p>You need this certificate if you want to use a subscription process with a client proxy in the cloud.</p> <p>The authentication process for communication between the Production Connector and SAP Digital Manufacturing uses the X.509 certificate authentication. The X.509 certificate is generated on connection of the respective Production Connector system with the SAP Digital Manufacturing web server.</p> <p>The authentication type is automatically switched from SAML OAuth to X.509 OAuth for any new client proxy that is created for a Production Connector system.</p> <p>Choose the <i>Regenerate Certificate</i> button to generate a new X.509 certificate if the existing certificate has expired or if a certificate needs to be revoked. The new certificate is valid without any further action.</p>
<i>Internal Production Connector Certificate</i>	<p>i Note</p> <p>Certificate rotation is supported. The agent instance of the shop floor system automatically picks up the latest certificate identified by the subject of the certificate. The certificate is regenerated automatically when a client proxy is generated.</p> <p>Refer to SAP Note 3194709 if you are operating the Production Connector on the operating system Windows Server 2016 or older. In this case, you have to adapt the certificate before it can be used in the integration with SAP Digital Manufacturing.</p>
	<p>This certificate is optional. It is used for the Production Connector internal communication. This certificate is used to protect internal communication between the Production Connector agent instances and the cloud integration server.</p> <p>You can choose the <i>Create Certificate</i> button in the cloud to generate an internal Production Connector certificate. When the system has created the certificate, it displays the certificate name and validity period.</p>

- Choose the *Refresh* button in the upper right corner of the screen.
As a result, the certificate data is updated. Additionally, the term *Plant Connectivity* is removed from the field names of the certificates as the certificates are only relevant for the Production Connector.

8.3 Maintaining User Groups

You assign the Production Connector roles to your user groups in **SAP Digital Manufacturing**. You can do this per Production Connector instance. The user groups maintained in the cloud are then distributed to this particular Production Connector instance.

Prerequisites

- The **user groups** for SAP Digital Manufacturing are created and users are assigned to the user groups. For more information, see *Manage Users and Authorization* under https://help.sap.com/docs/SAP_DIGITAL_MANUFACTURING/34f67db3b755405e8145c578221f012c/3ff12b4052784626b128f7012d048b09.html
- SAP Digital Manufacturing role collections are assigned to the user groups.
- You have set the *Principal Type* to *None* or you have deactivated principal propagation in the mapping of the Virtual to Internal System of the Cloud Connector. This enables authorization checks based on user groups. (See also: [Mapping Virtual to Internal System \[page 27\]](#).)
- You have created one local user in the Production Connector to which you have assigned the Administrator role. For more information, see [Settings in the Control Center of the Production Connector \[page 10\]](#).

Procedure

1. In the *Production Connector* section of the *Configure Production Connectivity* app, select the Production Connector system for which you want to maintain user groups.
2. Choose the *User Groups* tab.
You can see the list of existing user groups, with the assigned roles and description.

i Note

If a new Production Connector system is configured in SAP Digital Manufacturing, the technical user group `SAP_Technical_UG` with the `Data Reader` role will be created automatically.

3. Choose the *Add* button to select the user group(s) to which you want to assign Production Connector roles.
4. Choose *Show Advanced Search* to enter the user role collection and/or user role as the search criteria. A list of user groups that meet the search criteria is displayed.
5. Select the relevant user group.
6. Select the user rights that you want to assign to this user group and enter a description for the user group. For more information, see *User Groups* in the Production Connectivity Model documentation under <https://help.sap.com/viewer/76070b83a9954174b76a3411ad31f034/latest/en-US/2398ea32c7934c089c1c834e329bb425.html>.
7. After the user groups have been deployed to the Production Connector system, you can **display the user groups in the Production Connector** under  *Cloud Integration*  *User Configuration*  tab.

9 Troubleshooting

This section helps you to solve connection issues.

Troubleshooting of Connection Problems

If the Production Connector in SAP Digital Manufacturing does not show the status **Connected**, you should check the configured certificates first.

1. If the **system certificate of the Cloud Connector** has not been copied into the **folder for trusted certificates**, the connection will not be established. If you refresh the Production Connector page, an error message informs you about any missing authorization. The same error message can occur if the Production Connector Cloud system certificate was not issued correctly, for example, if the Common Name (CN) does not correspond to the server name.
2. Check if there is a **rejected certificate** in the following location:
`C:\ProgramData\SAP\ProdCon\CertificateStores\CloudServicesHost\Rejected\certs`
Check if it is the Cloud Connector system certificate. To assess this, download the Cloud Connector system certificate and open it with a double-click. Check if the thumbprint of the downloaded certificate corresponds to the thumbprint of the rejected certificate.
3. Move the rejected certificate to the following location:
`C:\ProgramData\SAP\ProdCon\CertificateStores\CloudServicesHost\Trusted\certs`

i Note

If this step has to be done, it means that something was not configured correctly earlier. Therefore, first check the following steps:

[Configure Trust for the Cloud Connector \[page 37\]](#) and [Configure Trust for the Production Connector \[page 37\]](#)

4. If there is no rejected certificate, check that the **administrator user** was created correctly in the Production Connector. (See: [Settings in the Control Center of the Production Connector \[page 10\]](#)). Check, that the **administrator user** has the required roles assigned. Check that the ID of the administrator user matches the one provided by the identity provider.
5. Check the system certificate of the Cloud Connector and the server certificate of the Production Connector. Check, that the respective Common Name (CN) or the Subject Alternative Name matches the host names or the FQDN. Check that the certificates are not expired and that their key usage is correct.
6. Make sure that the Microsoft certificate store *Local Computer/Personal* does not contain multiple valid certificates with the same subject name as the Production Connector server certificate. This could hamper establishing the trusted relationship between the Production Connector and the Cloud Connector because you could easily confuse the certificates.
7. If you have configured the validation for JSON Web Tokens, check that the Production Connector has connection to the UAA service. On the *JWT Validation* tab of the *Cloud Integration* settings in the Control Center, press the [Validate UAA Service URL](#) button to check the connectivity and to retrieve the active public key.

8. If a proxy server is configured to control the connections to the Internet, you must maintain the corresponding proxy settings in the Control Center. These proxy settings will also apply when contacting the UAA service, as described in the step before.
9. Finally, check the **logs of the main service** that are located at:
C:\Program Files (x86)\SAP\Production
Connector\Logs\ProdConMainService_yyyy.mm.dd.csv
These logs can also help to isolate the problem.

i Note

Instead of manually checking the integrity of the certificates, you can also open the Control Center and execute the guided procedure for configuring the Cloud Connector again. Perform the activity for establishing trust between the Cloud Connector and the Production Connector. (See: [Assisted Configuration of the Cloud Connector \[page 19\]](#).)

Expert Knowledge

This section provides expert knowledge for solving **issues that are caused by CA certificates and self-signed certificates** that are used as system certificates.

The Cloud Connector might not return a valid client certificate if the cloud services of the Production Connector request it. It might be that the certificate chain of this certificate is incomplete and does not contain the CA certificate that signed the Cloud Connector's system certificate.

When the cloud services in the Production Connector are requesting the system certificate (client certificate) from the Cloud Connector, the Cloud Connector might not return a client certificate. The reason for this behavior might be that the **Cloud Management Service** is sending an issuer list that does not contain the CA certificate that issues the system certificate.

The behavior of sending CA lists, when requesting the client certificate, is controlled by the following entry in the system hosting the Production Connector installation:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Send TrustedIssuerList

i Note

CA certificates must have a **Basic Constraint** attribute with the following value: Subject Type=CA so that the Production Connector can accept these CA certificates.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.

About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
 - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
 - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

