

PUBLIC

Document Version: 1.0 – 2023-02-17

# Application Help for Production Connector

© 2023 SAP SE or an SAP affiliate company. All rights reserved.

THE BEST RUN SAP

# Content


**1 Production Connector for SAP Digital Manufacturing. . . . . 3**

**2 Control Center Settings. . . . . 6**

2.1 Log Display. . . . . 6

2.2 Ease of Use. . . . . 7

**3 Structure of the Control Center. . . . . 9**

3.1 Settings for Cloud Integration. . . . . 9

Port Settings. . . . . 9

User Configuration. . . . . 10

Server Security Settings. . . . . 14

Troubleshooting. . . . . 21

3.2 Certificate Overview. . . . . 21

Configured Certificates. . . . . 21

Trusted Certificates. . . . . 22

Issuer Certificates. . . . . 22

3.3 Agent Instances. . . . . 22

Log. . . . . 23

Queued Messages. . . . . 26

Messages for Bundling. . . . . 27

Message Failures. . . . . 28

Starting and Stopping Agent Instances. . . . . 28

**4 Special Functions. . . . . 29**

4.1 Audit Log. . . . . 29

# 1 Production Connector for SAP Digital Manufacturing

The Production Connector for SAP Digital Manufacturing is a Windows-based application that enables you to integrate SAP Digital Manufacturing applications with machines and equipment on the shop floor.

## Business Background

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.

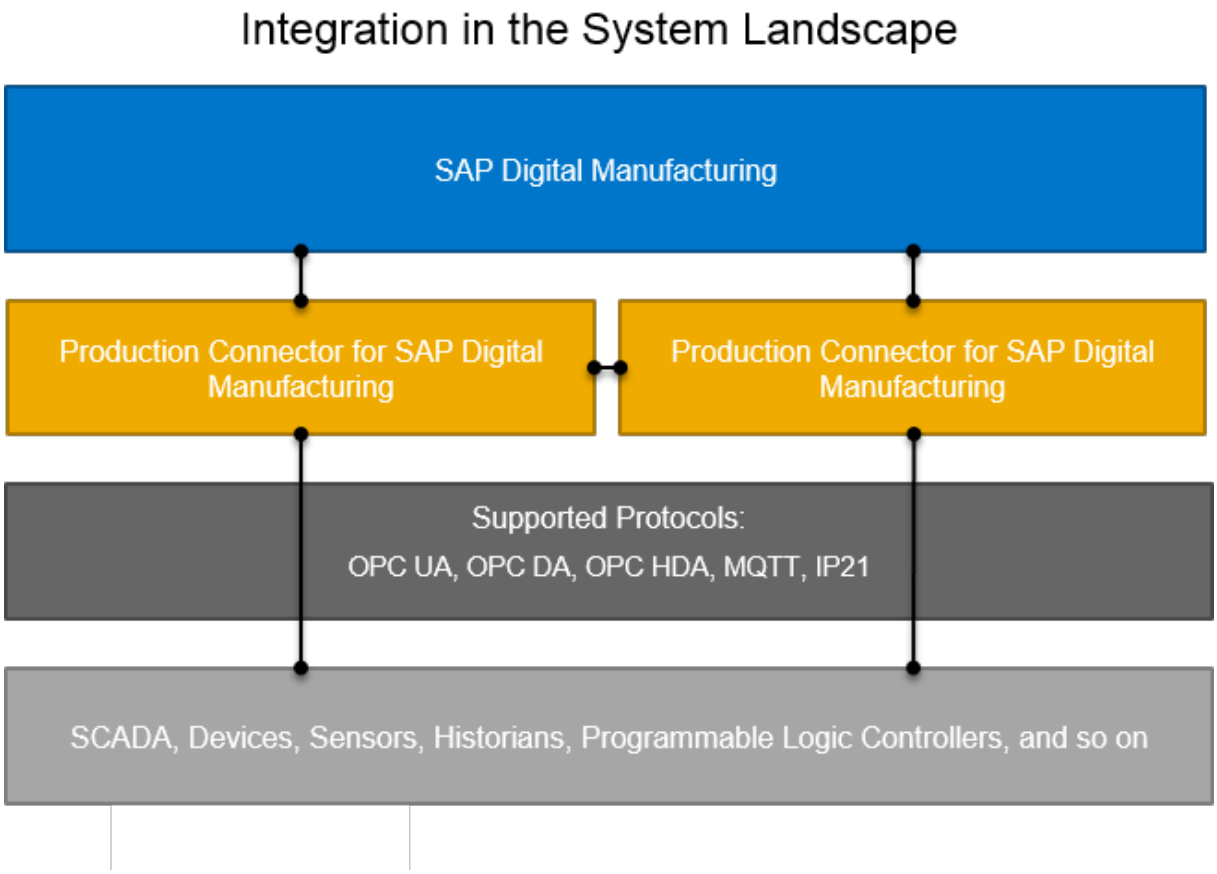
You create the configuration elements for connecting and exchanging data with manufacturing directly in the Production Connectivity apps in SAP Digital Manufacturing. After deployment, the required configuration elements are created in the Production Connector and the data flow between the systems in manufacturing and SAP Digital Manufacturing is established via the Production Connector.

## Technical Background

The Production Connector consists of two components:

- The **main service**, which is executed as a Windows service that starts automatically, provides the cloud services that are called from SAP Digital Manufacturing, and with which the Production Connector is configured, operated, and monitored.
- You use the **Control Center** to set up the connection to SAP Digital Manufacturing and to manage users and their authorizations. You can also use the Control Center to monitor the running of the Production Connector and for troubleshooting.

The following graphic provides an overview of the integration of instances of the Production Connector in the system landscape:



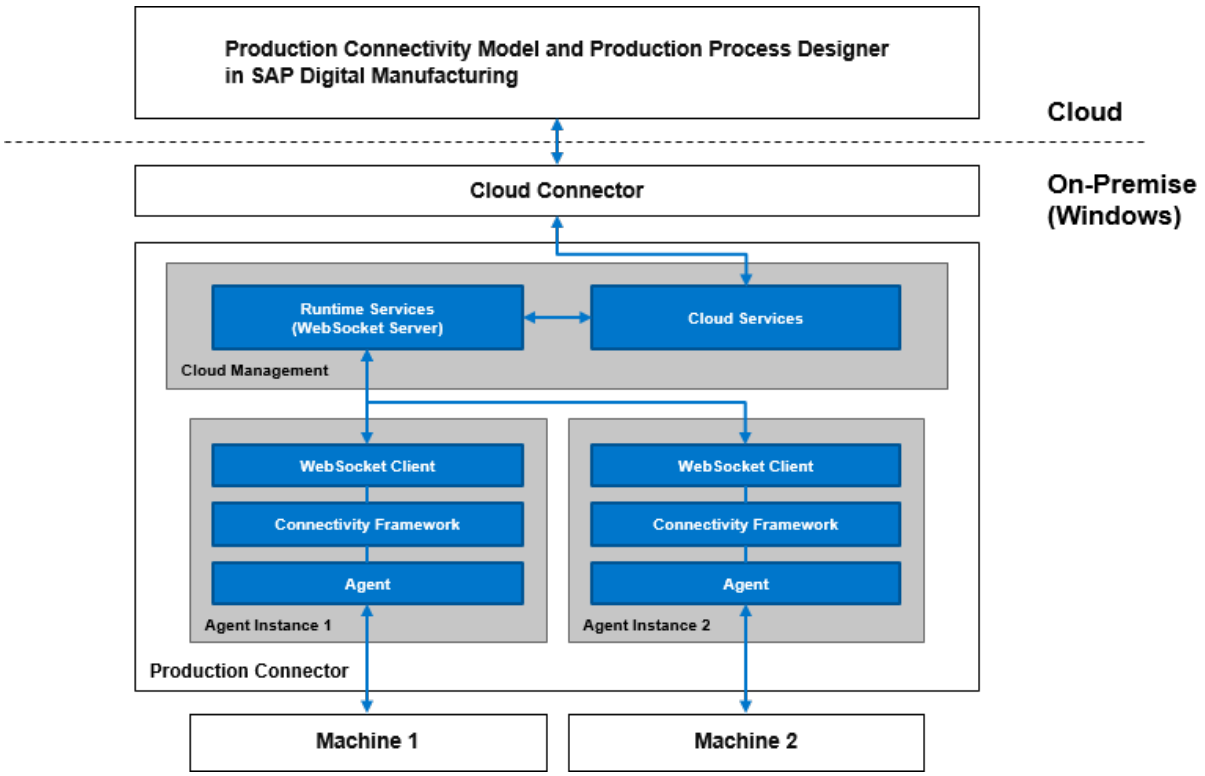

The connection of the local data sources, such as OPC DA, from the Production Connector, is performed using **agent instances**. In the Production Connectivity Model, the endpoints of the machines are mapped as shop floor systems. These shop floor systems model the tag information and the services offered by the machine.

The agent instances are the central components of the Production Connector. They establish the data flow between the data source on the shop floor and SAP Digital Manufacturing, and enable the processing and forwarding of notification messages. Moreover, they process queries and method calls. They build on a source-system-specific **agent** that encapsulates the access methods to the corresponding source system. An agent is a .NET DLL assembly component that can establish the connection between the data source and the Production Connector.

If you start agent instances using the *Configure Production Connectivity* app in SAP Digital Manufacturing or using the *Control Center*, each instance is executed as a standalone Windows service in the background. Therefore, you can run multiple agent instances at the same time and independently of each other. The number of agent instances that can be executed at the same time is only restricted by the capacity of the computer on which the Production Connector is installed. You can use the *Configure Production Connectivity* app or the Control Center to monitor the status of the individual agent instances at runtime. If there are fatal errors, the agent instance stops and is displayed as interrupted.

Communication from the cloud to the Production Connector is through the **Cloud Connector** to satisfy the security requirements for Internet communication. Communication from the Production Connector to the cloud is direct, that is, without a Cloud Connector.

The following graphic illustrates the basic architecture of the Production Connector in conjunction with the Cloud Connector and the data sources in manufacturing.




The Production Connector, in conjunction with SAP Digital Manufacturing, uses the **agents** to support common software interfaces to receive data from the shop floor systems.

Production Connector agents support the following standardized software interfaces:

- OPC Data Access (OPC DA)
- OPC Historical Data Access (OPC HDA)
- OPC Unified Architecture (OPC UA)
- MQTT
- IP21

Communication between the Production Connector, the Cloud Connector, and SAP Digital Manufacturing takes place using RESTful Web services. Internal communication between the host for the cloud services and the agent instances that function as service providers takes place using the WebSocket protocol for which the agent instances function as clients and the host as server.

You can customize the parameters of the cloud services and the main service in the Cloud Integration settings in the Control Center. (See also: Settings for Cloud Integration [page 9].)

## Implementation Considerations

The Production Connector is a Windows-based application and requires **.NET 6.0** runtime libraries to run. For more information about the installation, see the *Installation Guide*.

# 2 Control Center Settings

You can use the Control Center settings to define how individual functions are displayed in the Control Center. The settings you make are user-specific and only apply to the user who is currently logged in.

You can find the settings in the menu under *Control Center* > *Settings*. The following options are available:

| Setting | Description |
|---|---|
| *Display Language* | In the *Language* field, you can select the language in which you want to display the Control Center. If you change the language in this field, and then close the dialog box by choosing OK, the Control Center is restarted immediately in your chosen language. |
| *Help Language* | You can define in which language you display the online help (application help), which you can call up depending on the context by choosing the help button on the Control Center screens. If you specify that you want the language of the online help to be dependent on the display language, and you are working with the display language German, you will get the help texts in German. For all other display languages, the application help is displayed in English. |
| *Status Updates* | You can define the time interval between subsequent status updates of the display of agent instances. You can select a value between 1 and 60 seconds. |
| *Log Display* | You can configure how the agent instance log is displayed. (See also: Log Display [page 6].) |
| *Ease of Use* | Settings that facilitate accessible usage of the Control Center. (See also: Ease of Use [page 7].) |

## 2.1 Log Display

You can configure how the agent instance log is displayed.

The Production Connector creates a log for each agent instance and displays this on the *Log* tab of the agent instance. (See also: Log [page 23].)

You can specify which columns and separators you want to use.

1. From the menu, choose *Control Center* and then *Settings*.
2. In the *User Settings* dialog box, choose the *Log Display* entry.
3. Select the checkboxes for the columns you want to display, or deselect those you do not wish to display. Choose OK. For more information about the meaning of the individual columns, see Log Columns [page 24].

> **i Note**
>
> All columns are selected by default and so all columns are shown in the log display.

4. If required, choose the option *Automatically Adjust Column Width* if you want to adjust the column width of the log display automatically to fit its content.
5. If required, select a different separator to use as the column separator when exporting the log to a CSV file. You can choose one of the following options:
   - Semicolon
   - Comma
   - Vertical bar
   - Tab

> **i Note**
>
> During the export, any separators in the message text are replaced with another character to prevent unwanted formatting in the CSV file.

## 2.2 Ease of Use

On this tab page, you can make settings that facilitate accessible usage of the Control Center.

If errors occur when you are displaying data or during the configuration, error icons are displayed within tables at the beginning of the row in which the error occurred. When you hold the mouse over the error icon, the error message is displayed as a quick info. Similar error handling is also often used for input fields. Errors are symbolized by an error icon next to the affected field and the error text is available as a quick info.

To support users with visual or motor impairments, you can also display such visualized errors in a separate dialog box in an overview. You can make the required settings here.

Settings for Error Handling

| Field | Description |
| --- | --- |
| *Enable Log Display for Errors* | If you select this checkbox, a pushbutton is provided next to the pushbutton for the application help (on the screens on which the function is supported). You can then display the errors in a dialog box. The pushbutton is active as soon as there are error messages on the screen. You can also use the F7 function key to call the dialog box. |
| *Start Numbering of Table Rows with Zero in Error Log* | In the speech output of tables, the first row is called row zero. You can use this option to adjust how the row numbers are displayed in the error dialog so that they also begin with zero. |

| Field | Description |
| --- | --- |
| *Show Additional Windows Notification for New Errors* | If you also select this checkbox, a Windows notification is issued when a new configuration error occurs. In the Windows system settings, you can define how long the notification is displayed. If you click on the notification, the dialog box also opens to display the error. |
| *Min. Notification Interval* | Indicates the minimum time in seconds between consecutive notifications. This helps you avoid having too many notifications issued when a screen is being maintained. The minimum value is 0. In other words, you receive a notification as soon as the error situation changes on the current screen.<br><br>**i Note**<br>The setting is only effective for the current screen. If you switch to another screen on which enhanced error handling is active, the time interval starts again. |
| *Show Additional Windows Notifications for Status Messages* | If you select this checkbox, message texts are output from the status line of the Control Center in the form of Windows notifications. These notifications are immediately recognized by the speech output and are read out. The following screens are supported:<br>• Main window of the Control Center<br>• Agent instance log<br>• All tabs for managing queued messages<br>• Audit log dialog box |
| *Enable CTRL-ENTER as Shortcut for Navigating Between Screen Groups* | If you select this checkbox, you can use the key combination CTRL + ENTER to navigate cyclically through the screen groups of the Control Center. For example, if you have selected an agent instance, you can use this key combination to jump to the pushbuttons for starting and stopping agent instances. Entering the key combination again takes you to the first tab of the details screen area on the right-hand side. Therefore, the key combination supplements the tab key, which you can use to jump from screen element to screen element. |

# 3 Structure of the Control Center

## 3.1 Settings for Cloud Integration

You use the *Cloud Integration* function key to call the tabs that contain the settings for integration with SAP Digital Manufacturing.

You can configure the following settings here:

- You can monitor the main service that hosts the cloud services and adjust the ports used.
- You can create the administrator user, which is required for the first connection of the Production Connector to SAP Digital Manufacturing.
- You can display the user groups with their assigned user roles. User groups and their roles are defined in SAP Digital Manufacturing.
- You can define the security settings that establish the trust relationship between the Production Connector, the Cloud Connector, and SAP Digital Manufacturing.

You can define the settings for integration on the following tabs:

Port Settings [page 9]

User Configuration [page 10]

Server Security Settings [page 14]

Troubleshooting [page 21]

For more information about connecting a Production Connector installation to SAP Digital Manufacturing via the Cloud Connector, see SAP Note 3271973.

### 3.1.1 Port Settings

On this tab, you can check the status of the main service and change the ports for the configuration and cloud services.

The **main service** is a Windows service and also the host for the configuration services and cloud services. The main service is started automatically during installation, and for the Production Connector to function correctly, the main service must always be executed.

> **i** Note
>
> When the main service is started, it automatically generates certificates that secure the user's logon to the configuration services. These certificates are valid for one year. If the certificates have expired, the Production Connector remains functional, but warnings are logged for the main service. The certificates

are automatically renewed when the main service is restarted, for example, when the computer is restarted or when a patch is installed for the Production Connector. The remaining runtime of the certificates is displayed in the certificate overview. (See also: Certificate Overview [page 21].)

The **ports** for the services are found automatically during installation. However, it may still be necessary to adjust the configuration of the ports because there may be a port conflict that is not detected during installation. Once you have changed one of the ports, you need to save. The main service is then restarted automatically to make the changes effective. The same applies to changes to the server certificate or user changes.

Description of Settings

| Field | Description |
|---|---|
| *Service Status* of the main service | The main service is started automatically when the Production Connector is installed. The status is displayed in this field, for example, `Running`.<br><br>You cannot stop the main service from the UI. However, if it was stopped for technical reasons, you can start it. In this case, the *Start* button becomes active. |
| *Port* of configuration services | Specifies the port used for the configuration services. The configuration services provide access to the configuration elements of SAP Digital Manufacturing.<br><br>If there is an undetected port conflict during installation, you can find a free port by using the *Propose Free Port for Configuration Services* button. |
| *Port* of cloud services | Specifies the port used for the cloud services. The cloud services enable integration with SAP Digital Manufacturing.<br><br>If there is an undetected port conflict during installation, you can find a free port by using the *Propose Free Port for Cloud Services* button. |

## 3.1.2 User Configuration

On the *User Configuration* tab, you can create the administrator user locally, and monitor the rights of the users and user groups that can access the cloud services provided by the Production Connector.

On this tab page, you can do the following:

- Create a user with the administrator role.
  This user runs the cloud services that are used later in SAP Digital Manufacturing to create and change the user groups. (See also: Adding an Administrator User [page 11].)
- Check the user groups that you have created in SAP Digital Manufacturing. (See also: User Groups [page 11].)
- Check the assignment of the Production Connector roles. (See also: Production Connector Roles [page 12].)

### 3.1.2.1 Adding an Administrator User

After installing the Production Connector, you need to create a user on the *User Configuration* tab, to which you assign the administrator role.

This user later has the user rights 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 users in SAP Digital Manufacturing.

**Procedure**:

1. On the *User Configuration* tab page, create a user by choosing the *Add Local User* pushbutton and entering a user name. The name must be a real name.
2. In the *ID* field, enter the ID provided by your identity provider. Typically, this is the user's e-mail address.
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 roles are not hierarchical. Therefore, an administrator does not have all rights, but only certain rights. They can create and manage users and user groups. The other rights are acquired later through user groups in SAP Digital Manufacturing. Note, however, that the configuration for a specific user overwrites the user groups. Therefore, check whether the administrator user might require more rights if he or she is to be able to perform other actions.

### 3.1.2.2 User Groups

In the *User Groups* screen area you can check the user groups that you have defined in SAP Digital Manufacturing.

You define the user groups, the assignment of roles, and the assignment of user groups to the SAP Digital Manufacturing users centrally using the *Configure Production Connectivity* app in SAP Digital Manufacturing.

For more information about user groups in SAP Digital Manufacturing, see the production connectivity documentation under https://help.sap.com/docs/SAP_DIGITAL_MANUFACTURING/76070b83a9954174b76a3411ad31f034/2398ea32c7934c089c1c834e329bb425.html.

To enable the deployment of user groups from the cloud, you need to have created at least one local user with the `Administrator` role in each Production Connector installation. This user runs the cloud services that are used to create and change the user groups. (See also: Adding an Administrator User [page 11].)

The user groups defined in SAP Digital Manufacturing are displayed in the Production Connector after they have been deployed. The master data and assigned roles of these user groups are protected against changes made via the Control Center. In exceptional cases, you can remove the write protection by choosing *Unlock User Group* and then making the necessary changes.

> **i** Note
>
> If you have registered and configured a new Production Connector system in SAP Digital Manufacturing, the technical user group `SAP_Technical_UG` with the roles `DataReader` and `BackupCreator` is created automatically and displayed in the Production Connector.

## 3.1.2.3 Production Connector Roles

By assigning roles, you can control the authorizations of users and user groups.

You can assign the roles to the users created locally. Roles are assigned to the individual user groups using the *Configure Production Connectivity* app in **SAP Digital Manufacturing**. You can display the user groups and their assigned roles here.

Role Descriptions

| Role | Description |
|---|---|
| `Administrator` | This role is for the administration of users and authorizations. The administrator can also trigger the generation and recovery of data backups of the configuration via SAP Digital Manufacturing.<br><br>Users with the **Administrator** role can **only be created locally in the Production Connector**. |
| `CertificateAdministrator` | A user or user group with this role is allowed to manage certificates. In particular, he or she can establish the trust relationship with communication partners. |
| `PCoConfigurator` | A user or a user group with this role can create and change configuration elements, in particular, service providers and their dependent configuration elements, such as source and destination systems. |
| `ServiceExecutor` | This role is required to execute machine methods of the Production Connectivity Model. |
| `DataReader` | This role is required to read data from a source system using a query. |
| `DataStorer` | A user or a user group with this role can use a store query to write data back to a source system. |

| Role | Description |
| --- | --- |
| `FileProcessor` | A user or a user group with this role can read and write files. This allows files to be written via SAP Digital Manufacturing for handover to a print server to a folder that you have configured for this purpose. For more information about setting up the print function in SAP Digital Manufacturing, see https://help.sap.com/viewer/97c9e9b9fac74be2a023638cd1700b46/latest/en-US/800486f1fd8e4d97bd062c4694c30772.html. |
| `Operator` | A user or a user group with this role can start and stop agent instances and query their runtime status. |
| `BackupCreator` | A user or user group with this role can trigger the generation of data backups of the configuration in SAP Digital Manufacturing. |

### 3.1.2.4 Process Flow for the Authorization Check

At the runtime of the main service, when a cloud service is called, SAP Digital Manufacturing either transfers the **user information** directly, or transfers a **JSON web token (JWT)** that contains information about the identity of the user and the user groups assigned to it. During the authorization check, the Production Connector first determines the Production Connector roles that are assigned to the transferred user, and checks whether they correspond to the roles required by the service call. If you have not created a suitable local user in the Production Connector, this check is executed for the roles assigned to the transferred user groups.

> **i** Note
>
> For background tasks, the JSON web token does not contain user information or user group information. In this case, the default user group `SAP_Technical_UG` provided for the execution of background tasks is used for the authorization check.

## 3.1.3 Server Security Settings

On the *Server Security Settings* tab, you define the settings that apply for communication between the host for the cloud services and the Cloud Connector. The main service, which hosts the cloud services, takes the role of the server, and the Cloud Connector takes the role of a client.

Settings in the Upper Screen Area

| Field | Description |
|---|---|
| *Session Timeout* | Time interval in minutes after which an inactive session is terminated automatically. |
| *Certificate* | Here you specify the server certificate that you have imported or generated for the computer on which the Production Connector is installed.<br><br>Choose the *Select Server Certificate* pushbutton to select a suitable certificate in the Windows certificate store (see also: Selecting a Server Certificate [page 15]).<br><br>Alternatively, you can choose the *Generate Server Certificate* pushbutton to generate a suitable self-signed certificate. You should only use the self-signed certificate for test purposes. (See also: Generating a Server Certificate [page 15].) |

For more information, see Server Certificate [page 14].

In the screen area for **client certificates**, you define how the certificates used in the communication between the Production Connector as a server and the Cloud Connector as client are to be handled.

For more information, see Client Certificates [page 18].

### 3.1.3.1 Server Certificate

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

The server certificate must be of type X.509-v3. It should be issued for the host name of the computer on which the Production Connector is installed. The certificate can be self-signed for test purposes or must be embedded in a hierarchy of certificates.

> **i** Note
>
> For productive operations, you should always use a certificate that has been signed by a Certification Authority (CA).

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

You can find the folder for the certificates that the host for the cloud services trusts under:
`C:\ProgramData\SAP\PCo \CertificateStores\CloudServicesHost\Trusted\certs`

The following functions are available for the server certificate:

- Selecting a Server Certificate [page 15]
- Generating a Server Certificate [page 15]
- Exporting a Server Certificate [page 18]
- Remove Server Certificate
  You use this function to remove the selected server certificate. However, it remains in the certificate store. You can then select a different certificate.

## 3.1.3.1.1 Selecting a Server Certificate

You can use this function to select a server certificate from the Windows certificate store.

You have already stored a suitable certificate in the certificate store of the computer on which the Production Connector is installed.

For productive operations, SAP recommends that you obtain a certificate from a Certification Authority (CA) and import this certificate. For the import, you can use the Microsoft app for managing computer certificates.

You can then select this certificate as the server certificate in the Production Connector by choosing *Select Server Certificate*.

## 3.1.3.1.2 Generating a Server Certificate

You can use this function to generate a self-signed server certificate for test purposes using default values. After you have filled in the fields in the dialog and chosen OK, the server certificate is generated, saved in the Windows certificate store, and automatically entered in the *Certificate* field.

### Mandatory Subject Components

This screen area contains the required entry field *Common Name (CN=)*, which is needed for generating the certificate. The field is prefilled with the computer name. The abbreviation CN= is generated automatically so do not enter this.

> **i** Note
>
> Each certificate has the attribute subject of type `X.509DistinguishedName` in which the entity, to which the certificate is assigned, is described in more detail.

## Optional Subject Components

This screen area contains additional fields with attributes that you can fill or leave empty.

Define Optional Attributes

| Field | Description |
| --- | --- |
| *Locality (L=)* | Freely definable |
| *Country (C=)* | Enter, for example, DE for Germany. A valid two-character country code is expected. |
| *Organizational Unit (OU=)* | Freely definable |
| *Domain Component (DC=)* | Enter the host name or the fully qualified host name of the computer here. |
| *State or Province (S=)* | Freely definable |
| *Friendly Name* | A name of your choice that you can assign to the certificate.<br>The friendly name can make it easier to recognize the certificate (for example, in the certificate store). There is a separate column for this in the selection dialog for certificates. |

## Technical Settings

In this screen area, you can specify the size of the private key and the validity period of the certificate.

Define the Technical Settings

| Field | Description |
| --- | --- |
| *Key Size (bit)* | Specifies the size of the private key. 2048 bit is the default value. |
| *Valid From Today Until* | You define the validity end date of the certificate here. The default validity is one year. |

## Microsoft Certificate Store

The server certificate to be generated is stored in the Microsoft Certificate Store.

Settings for the Microsoft Certificate Store

| Field | Description |
| --- | --- |
| *Certificate Store* | The certificates are always stored as server certificates with a private key in the Microsoft Certificate Store. You can decide whether you want to store the certificate in the private user area or in the machine-specific storage area:<br>• Current user<br>• Local computer<br>For productive use, you should store the certificate in the *Local Computer* storage area. |
| *Private Key Is Exportable* | If you select this checkbox, the certificate and the private key can be exported.<br>If you do **not** select this checkbox, you **cannot** save the certificate with the private key outside the Microsoft Certificate Store. This means greater security because the key cannot be stolen and therefore cannot be used on another device.<br>The disadvantage of this setting is that you cannot make a backup of the private key. If the computer is defective, for example, you have to generate new certificates and also set up new trust relationships for the certificates. |

## Alternative Names

For a valid certificate, the server on which the Production Connector is running must be specified in the certificate. To do so, you need to provide a DNS name or an IP address in the *Alternative Names* screen area. You can enter one or more DNS names or IP addresses here that need to match the endpoints of the server. Multiple entries must be separated with a comma.

Settings for Alternative Names

| Field | Description |
| --- | --- |
| *DNS* | You enter the name or names for the domain name system here. For the server on which the Production Connector is running, a value for the domain name is prefilled with the current server name. |
| *IP Address* | Enter the IP address(es) of your computer here if you are using the IP address for the endpoint definition of the Production Connector server. It must then match the endpoint of the server on which the Production Connector is running.<br>The IP address is the unique identification characteristic of a computer that defines its location in the Internet. |

## 3.1.3.1.3 Exporting a Server Certificate

After you have selected a server certificate or generated and saved a self-signed certificate in the Production Connector, you can use the *Export Server Certificate* pushbutton to export the public part of the certificate and save it on your computer.

If you establish the trust relationship between the Cloud Connector and the Production Connector when configuring the Cloud Connector, you can then simply upload the exported certificate file from your computer to the trust store of the Cloud Connector.

> **i** Note
>
> As of Cloud Connector version 2.15, the server certificate must be uploaded to the trust store.

### Related Information

Selecting a Server Certificate [page 15]
Generating a Server Certificate [page 15]
Configure Trust for the Production Connector

## 3.1.3.2 Client Certificates

In the *Client Certificates* screen area, you specify how the certificates, which are exchanged during communication between the Production Connector as a server and the Cloud Connector as a client, and between the Production Connector as a WebSocket server and the service providers as clients, are to be processed.

The client certificate of the Cloud Connector is stored in the **file system** of the computer on which the Production Connector is installed, in order to establish the trust relationship. Choose *Open Selected Folder in Windows Explorer* to go to the default directory (directory for trusted certificates).

Directories for the Client Certificates

| Certificate | Directory |
| --- | --- |
| Trusted Certificates | `C:\ProgramData\SAP\ProdCon\CertificateStores\CloudServicesHost\Trusted\certs`<br><br>If the host for the cloud services wants to set up a secure connection to a Cloud Connector as a client, it gets a certificate with a public key from the Cloud Connector (client). The Production Connector accepts this certificate if it regards it as trustworthy.<br><br>If the client (the Cloud Connector) is using a self-signed certificate, you can, after an unsuccessful connection attempt, move the certificate from the store location for rejected certificates to the directory for trusted certificates. This establishes the trust relationship between the server and client on the Production Connector side. This is the `Trusted` directory in the directory named here. |
| Certificates from Trusted Issuers | `C:\ProgramData\SAP\ProdCon\CertificateStores\CloudServicesHost\Issuer\certs`<br><br>If the client certificate is embedded in a certificate hierarchy, the related root certificate also needs to be available to establish a trust relationship to the server. You must store this root certificate under `certs` of the directory specified here. |
| Rejected Certificates | `C:\ProgramData\SAP\ProdCon\CertificateStores\CloudServicesHost\Rejected\certs`<br><br>If the host for the cloud services wants to set up a secure connection to a Cloud Connector as a client, it gets a certificate with a public key from the Cloud Connector (client). If the Production Connector **does not** accept this certificate, the certificate is stored in the directory specified here for rejected client certificates. You can move the certificate from here to the trusted certificates folder to establish the trust relationship between the Cloud Connector and the Production Connector. |

## Extended Field Description

Settings in the Client Certificates Screen Area

| Field | Description |
| --- | --- |
| *Access to Folder* | The storage locations in the file system for the client certificates, which the Production Connector is to trust, are preconfigured in the system. You can use the pushbutton to the right of this field to open the Windows Explorer directly for the storage locations (directories) for trusted certificates, for trusted issuer certificates, and for rejected certificates.<br>The following options are available:<br>• Folder for trusted certificates<br>• Folder for certificates from trusted issuers<br>• Folder for rejected certificates |
| *Revocation Check* | In this field, you define how the revocation check of the client certificate is to be performed.<br>The following options are available:<br>• No check on revoked certificates<br>No check is carried out. This is the default setting.<br>• Check online revocation lists<br>The online check is a secure procedure but it can have a negative impact on performance.<br>• Check offline revocation lists<br>In this procedure, you need to copy all related certificate revocation lists into the revocation list folder as .crl files. |
| *Revocation Check Scope* | You specify here how you want the Production Connector (as a server) to perform the check for revoked certificates. The following options are available:<br>• Check end certificate only<br>Only the last certificate in a certificate chain is checked. This is the recommended setting.<br>• Check entire chain<br>All certificates in a certificate chain are checked.<br>• Exclude root certificate from check |
| *Accept Invalid Host Name* | If you choose this option, the Production Connector accepts an invalid host name in the client certificate.<br>Select this checkbox for test purposes only. |
| *Accept Expired Validity Period* | With this option, the Production Connector also accepts expired client certificates. Select this checkbox for test purposes only. |

### 3.1.4 Troubleshooting

This tab provides access to the logs of the main service, the installation logs of the Production Connector, and the log of the Cloud Connector. You can also compile information here that SAP Support needs to analyze problems.

## 3.2 Certificate Overview

The *certificate overview* gives you an overview of all certificates that are stored in the Production Connector configuration. The certificate overview evaluates the security configuration of all relevant configuration elements and checks the certificates that are found.

The certificate overview helps you to monitor the validity of the configured certificates.

To call the certificate overview, choose the *Certificate Overview* function key.

The certificate overview supports the following certificate usages:

- **Host for the cloud services**: Server certificate and certificate for internal Web socket communication
- **Main service**: Certificate for transport security of configuration services (Transport Layer Security TLS)
- **OPC UA client:** Application certificate
- **Client proxy (universal Web service destination system):** Certificate for authentication

The certificate overview informs you **when a certificate is going to expire**. An error symbol is displayed beside the certificates whose validity is due to end within a defined time interval.

At the lower edge of the certificate overview, you can define the length of this *time interval*. The default time interval is 30 days. This allows you to identify at an early stage which certificates need to be renewed.

Select a certificate and choose the *Display Certificate Details* pushbutton to display all information about the selected certificate.

### 3.2.1 Configured Certificates

On the *Configured Certificates* tab, you can see the application certificates that you have defined yourself for specific configuration elements, for example, the application certificates for the OPC UA source systems or the server certificates of the OPC UA server. The main details are displayed for each certificate. The error icon at the beginning of each table row informs you of any issues with the respective certificate.

## 3.2.2 Trusted Certificates

On the *Trusted Certificates* tab, you see, for each store location, the certificates that you trusted explicitly when configuring the connections by moving them from the store location for rejected certificates to the store location for trusted certificates.

For each store location, you see the configuration elements that refer to this store location.

### Related Information

Certificate Overview [page 21]

## 3.2.3 Issuer Certificates

On the *Issuer Certificates* tab, you see, for each store location, the issuer of the certificates that you have trusted explicitly. The functions on this tab are the same as those on the *Trusted Certificates* tab.

### Related Information

Certificate Overview [page 21]

# 3.3 Agent Instances

The agent instances are created using the *Configure Production Connectivity* app in SAP Digital Manufacturing. You can start and stop and monitor the agent instances in SAP Digital Manufacturing. In addition, after deployment, you can display and monitor them using the Production Connector.

Agent instances are the central components of the Production Connector. They define the data flow and enable the processing and forwarding of notification messages. Moreover, they process queries and method calls.

The following functions are provided for the agent instances in the Control Center:

- You can monitor the status of agent instances.
- You can start and stop agent instances.
  When you start agent instances, each instance is executed as a standalone Windows service in the background.
- You can evaluate logs to troubleshoot issues with agent instances.
- You can monitor the queues of the notification messages.

## 3.3.1 Log

On the *Log* tab page, you can display the log of the selected agent instance. The Production Connector writes a separate log for each agent instance. This log logs the activities or errors of the agent instance.

Messages from agent instances are written to an agent-instance-specific Windows event log. They are called SAP_<log ID>, where the log ID is a four-character sequence of uppercase letters and numbers, for example, A3XU.

The raw data from the log is saved in the Windows event log. The Windows event log is a Microsoft component with which you can display and manage event logs of the individual agent instances.

The name of the Windows event log that is assigned to the agent instance is displayed in the status bar. You can evaluate the relevant log for each agent instance via the Control Center.

> **i** Note
>
> Log data is only written by agent instances that are running. However, you can access the logs regardless of the agent instance's operation status.

The following functions are available:

- A separate event log, whose name is generated automatically when the agent instance is created, is created for each agent instance.
- You can use selection criteria to restrict how the logged entries are displayed.
- You can export the log in the form of a CSV file.
- If required, you can also delete old log entries.
- You can use the functions provided by Windows event logs to configure their lifecycle and maximum size.

### Related Information

Calling the Log of an Agent Instance [page 23]
Log Columns [page 24]
Log Functions (Pushbuttons) [page 26]

## 3.3.1.1 Calling the Log of an Agent Instance

On the *Log* tab page, you can call the log for a specific agent instance.

### Context

You can use selection criteria to restrict the log data.

## Procedure

1. In the Control Center, select the required agent instance and click on the *Log* tab page.
2. With the help of the following table, enter the data needed to restrict the log data displayed:

| Field | Description |
|---|---|
| *Start Date* | Date and time from which log entries are to be displayed.<br>Activate the selection field by selecting the checkbox or pressing the spacebar if the focus is on this field.<br>If you deselect the checkbox, all entries in the log since the start of record keeping are selected. |
| *End Date* | Date and time until which log entries are to be displayed.<br>Activate the selection field by selecting the checkbox or pressing the spacebar if the focus is on this field.<br>If you deselect the checkbox, all logs available since the start date are displayed. |
| *Filter Level* | Defines the entry types to display.<br>For example, if you only want to display the logged error messages for the event type *Error* and *Critical*, choose the *Error* entry. If you do not specify anything, all message types are selected from the log. |
| *Number of Entries* | Indicates the number of entries that are selected by default. This allows you to shorten the runtime when selecting the log. In the status bar, you see whether there are further entries, in addition to the displayed entries, that satisfy the selection conditions. |

3. Click Refresh.

   The log entries are now selected according to the above dates and filter conditions. The log is always sorted in descending order according to the time of the logged events; in other words, the most recent events are displayed first. (See also: Log Columns [page 24].)

# 3.3.1.2 Log Columns

The agent instance log contains the following columns:

| Column | Meaning |
|---|---|
| *Date/Time* | Time at which the event was registered by the agent instance. The last three digits represent the milliseconds. The time displayed refers to the time zone of the user that is logged on. |

| Column | Meaning |
| --- | --- |
| *Event Type* | Severity of the registered event. The Production Connector distinguishes between the following event types:<br>• *Critical*<br>Serious errors that mostly lead to a running agent instance being stopped<br>• *Error*<br>Common errors<br>• *Warning*<br>Warnings that indicate an unusual agent instance status<br>• *Information*<br>• *Verbose*<br>Diagnostic messages that can be used in error analysis |
| *Server Name* | Name of the server on which the messages were registered. This is usually the name of the computer on which the Production Connector is installed. |
| *Thread ID* | ID of the thread in which the event was registered. As a rule, notifications from the data source and queries by the agent instance are processed in parallel in different threads to increase the data throughput. Using the thread ID, you can group together and assign to each other the events that originate from a specific notification or a specific query. |
| *Process ID* | ID of the Windows process that has been assigned to the running agent instance. The process ID does not change during the runtime of the agent instance. Changes to the process ID in the log will let you recognize if the agent instance has been stopped in the meantime. |
| *Process Name* | Name of the Windows process that has been assigned to the running agent instance. |
| *Source* | Module of the Production Connector program in which the event has been triggered. This information is mainly of importance for SAP development. |
| *Event ID* | Indicates the point in the program at which the event was logged. This information is mainly of importance for SAP development. |
| *Message* | Message text. The message text is issued in English in most cases. |
| *Stack Trace* | Call hierarchy up until the error occurred. The stack trace is only written to the log for exceptions. |

### 3.3.1.3 Log Functions (Pushbuttons)

The following functions are provided for the log by means of pushbuttons that are located beside the selection criteria:

| Function | Meaning |
| --- | --- |
| *Delete All Log Entries* | You can use this pushbutton to delete all log data in the assigned Windows event log. |
| *Export to CSV File* | With this pushbutton, you can export log data using **<agent name>_yyyy.mm.dd_hh.mm.ss.csv** to a CSV log file into a folder of the user's choice. You can choose the time period and the filter level of the log data that is to be exported.<br><br>In the user-specific settings, if required, you can change the separator used to separate the columns of the CSV file. The semicolon is the default separator. (See also: Log Display [page 6].) |
| *Manage Windows Event Log* | By choosing this pushbutton, you start the *Windows Event Viewer* for the Windows log that is assigned to the agent instance. In the *Properties* of this log, you can specify, for example, the maximum size of the log and what should happen when this maximum size is reached. |

## 3.3.2 Queued Messages

All notification messages that are currently in the queue are displayed on the *Queued Messages* tab.

Before notification messages are delivered within a tag-based notification process/subscription process or an asynchronous method call, they are placed in a queue. On the one hand, the queue decouples source system events from the delivery of notification messages to the destination systems. So if there is a delay in delivery to a destination system, this doesn't block processing of further notification events at the source system. On the other hand, the queue makes sure that delivery retries can be started even if delivery attempts have failed.

Messages that are currently being sent are not displayed. If the Production Connector does not succeed in sending a notification message, the message is displayed on this tab with entries in the *Last Attempt* and *Current Attempt* columns.

For each agent instance, individual queues are used for sending notification messages. The queues are set up automatically as soon as you start an agent instance. The following queues are created:

- Main queue
- Queue for failed messages
- Queue for expired messages
- Queue for messages that are waiting to be bundled

The queues for an agent instance are removed when you delete the agent instance.

The parameters for the queues of an agent instance are set when they are created and cannot be changed:

- Queues only exist at the runtime of the agent instance in the main memory of the computer and are not persisted.
- A maximum of 1000 notification messages are put into the active queue and into the message failures queue. If this value is exceeded, the agent instance is interrupted. As soon as 80% of this number of messages is reached, messages of the type *Critical* are written to the log of the agent instance.
- The number of threads for sending notification messages asynchronously is limited to five times the number of processor cores of the computer.
- The notification messages are processed in parallel and not in the sequence in which they are registered in the queue (no Exactly Once in Order processing).
- Expired notification messages are not retained, but are automatically deleted after one day.
- Failed notification messages are not automatically resent.

### Displaying Queued Messages

1. Select an agent instance, click on the *Queued Messages* tab, and choose the *Refresh* pushbutton.
   The system displays the list of queued messages.

   > ⚠ Caution
   >
   > The entries in the *Last Attempt* and *Current Attempt* columns are only up-to-date if the agent instance is running or has paused. If the agent instance has been stopped, the entries are not up-to-date.

2. Click on *Display* to display the details for a notification message.
3. If you choose the *Delete All* pushbutton, you can remove a notification message from the queue.

## 3.3.3 Messages for Bundling

On the *Messages for Bundling* tab page, you can display bundled notification messages.

Message bundling is a procedure in which notification messages can no longer be sent individually. Instead, they are bundled in one large notification message and sent together to the connected client proxy (universal Web service destination system).

The prerequisite for this is that you have activated message bundling in SAP Digital Manufacturing.

### Display Messages for Bundling

To be able to display the messages that are to be bundled, do the following:

1. In the Control Center, select an agent instance, click on the *Messages for Bundling* tab page, and choose the *Refresh* pushbutton.

The Production Connector displays all the notification messages that are to be bundled into one larger notification message.

2. To send one or more notification messages manually, select the message or messages and choose the *Send All Messages* pushbutton.
3. To delete the notification messages, choose the *Delete All Messages* pushbutton.

## 3.3.4 Message Failures

On this tab, you can display notification messages that could not be delivered even after multiple attempts.

1. Select an agent instance, click on the *Message Failures* tab, and choose the *Refresh* pushbutton.
   The Production Connector displays all notification messages that could not be sent, even after multiple attempts.
2. To send one or more notification messages manually, select the message or messages and choose the *Resend All Messages* pushbutton. To delete the notification messages, choose the *Delete All Messages* pushbutton.

## 3.3.5 Starting and Stopping Agent Instances

In the Agent Instances screen area, you can start and stop agent instances using pushbuttons.

Start and Stop Functions

| Function | Description |
| --- | --- |
| Start Selected Agent Instances | To set up the data flow between the data source, the Production Connector, and the destination system, or in order that you can use the agent instance as a server, you need to start the agent instance. You can select multiple agent instances and start them simultaneously. |
| Stop Selected Agent Instances | If you want to stop the data flow or stop the server, you need to stop the agent instance.<br>Note<br>You can change the log level of the agent instance at runtime using SAP Digital Manufacturing.<br>Select at least one agent instance and choose *Stop Selected Agent Instances*. |
| Stop All Agent Instances | If you choose this pushbutton, you can stop all active agent instances in one step after you have confirmed a security question. |
| Restart Interrupted Agent Instances | You can use this pushbutton to first stop and then restart interrupted agent instances. |

# 4 Special Functions

## 4.1 Audit Log

Log for tracking changes to the configuration objects.

The audit log documents all changes that a user has made to the configuration of the Production Connector.

To display the audit log, choose *Control Center* > *Display Audit Log* from the Control Center menu.

The following information is displayed for the selected time period:

- Date/time of change
- User that made the change
- Object changed
- The operation that was carried out, for example, add or update
- Group name
- Old value and new value
- Error message

> **i Note**
>
> If changes were made in the background using SAP Digital Manufacturing, the recorded changes are not assigned to a special user.

# 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.

www.sap.com/contactsap

© 2023 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see https://www.sap.com/about/legal/trademark.html for additional trademark information and notices.

THE BEST RUN SAP