



PUBLIC

SAP Cloud for Customer

Document Version: CLOUD – 2021-10-09

SAP Cloud for Customer Security Guide

SAP Cloud for Customer

Content

- 1 Technical System Landscape. 5**
- 2 Security Aspects of Data, Data Flow, and Processes. 7**
 - 2.1 Communication Channels. 7
 - 2.2 Business-To-Business Communication and Application Integration. 8
 - Communication Arrangements Quick Guide. 10
 - 2.3 E-Mail. 18
 - Enabling S/MIME Security. 19
 - Configuring S/MIME Security. 20
 - Security Measures for E-Mail Domains. 21
 - 2.4 File and Attachment Processing 23
 - Configure Upload Controls. 23
 - Temporary Files. 24
 - 2.5 Tax Numbers in SAP Cloud for Customer. 24
 - 2.6 Cookies. 25
- 3 User Administration and Authentication. 26**
 - 3.1 User Management. 26
 - VIDEO: Assigning User Access Rights by Roles. 28
 - Restricting Access Roles. 28
 - 3.2 User Types. 30
 - 3.3 Authentication Mechanisms. 31
 - Log on Using SAML 2.0 Assertion for Front-End Single Sign-On (SSO). 32
 - Logon Using Client Certificate (X.509). 34
 - Log On Using User ID and Password. 37
 - Creating a Security Certificate for HTTPS-Enabled Computer Telephony Integration (CTI). 38
 - 3.4 Security Policy Quick Guide. 39
 - Business Background. 39
 - Create a Security Policy. 39
 - Edit an Existing Security Policy. 40
 - Assign Security Policies. 40
 - Define the Default Security Policy. 41
 - Delete an Existing Security Policy. 41
 - 3.5 Security Settings. 42
- 4 Authorizations. 43**
 - 4.1 Authorization Assignment. 43
 - 4.2 Access Restriction. 44

	Sales: Setting up User Access Rights and Restrictions.	44
	Service: Setting up User Access Rights and Restrictions.	49
	Restricting Access for Local Administrators.	50
4.3	Segregation of Duties.	51
5	Mobile Devices.	52
5.1	SAML2 Based SSO.	53
5.2	SSO Recommendation.	53
5.3	Authorizations.	53
5.4	Secure System Access and Authentication.	54
	SAP Cloud for Customer for Android.	54
	Certificate Pinning.	54
5.5	Special Considerations.	55
5.6	Data Storage.	55
	Support Log Files.	58
	Cache Files.	59
	Local Application Data Storage.	59
5.7	Offline Mode.	59
6	Front-End Security.	61
7	Security of Data Storage and Data Centers.	62
8	Security for Additional Applications.	64
9	Other Security-Relevant Information.	65
9.1	Security for End-User Devices.	65
9.2	Service Composition Security.	66
	URL Mashup Integration.	66
	HTML Mashup Integration.	66
	Map Mashup Integration.	67
	Data Mashups.	67
9.3	Security Management and Continual Improvement of Security.	68
10	Data Protection and Privacy.	70
10.1	Disclose Personal Data.	72
10.2	Remove Personal Data.	73
10.3	Depersonalize Transactional Data.	76
10.4	Data Retention.	78
10.5	Administer Data Removal Runs.	79
10.6	Automate Removal of Obsolete Business Partners.	81
	Web Services for Business Partner End-of-Purpose.	82
10.7	Enable Read Access Logging.	83
10.8	Prerequisites for Usage Block Integration.	87

11	Security-Relevant Logging and Tracing	90
11.1	Change Logs	90
11.2	Security Monitoring and Alerting	90
	Security-Relevant Reports	91
	Security-Relevant Data Sources	91
	Security-Relevant Log APIs	93
11.3	Connectivity Errors - Troubleshooting	93

1 Technical System Landscape

SAP data centers provide the highest-quality security measures while still allowing integration and flexible access to their cloud data.

SAP Cloud solutions are hosted in data centers around the world. Customers can choose in which data center they want their solution to run.

The solutions provide optional integration with many SAP solutions, such as a full Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM) suite, including the associated server landscape and system maintenance.

Since SAP Cloud solutions deal with business data from your core business processes, SAP adheres to the highest security and quality requirements, as follows:

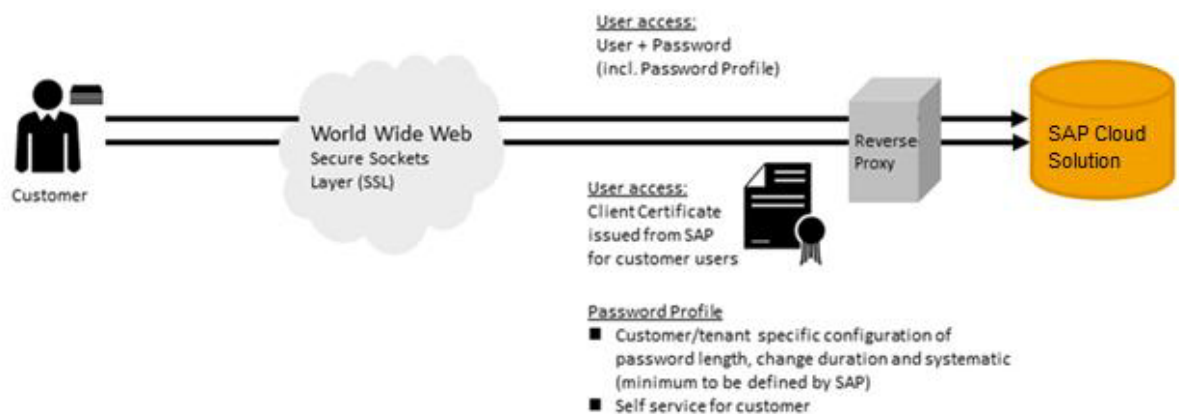
- The business data is stored securely in SAP data centers.
- Customers share physical hardware, but their data is separated into tenants.
- Users who require access to the business data must authenticate themselves, and their identity must be verified by user and access management.
- Customer data always belongs to the customer.

You can access your SAP Cloud solution in the following ways:

- Desktop computer: browser-based Internet access from any network with internet access
- Portable computers: browser-based Internet access from any network with internet access
- Mobile devices: native apps

Industry best practices and state-of-the-art open cryptographic standards secure and protect communications between customer devices and the system landscapes of your SAP Cloud solution in the SAP data center.

The following diagram summarizes the technical system landscape for standard access:



To access SAP Cloud solutions, you must enter a unique, customer-specific URL.

Communication is carried out via the Reverse Proxy (RP) component in the SAP data center.

The Reverse Proxy is the SAP Web Dispatcher, which is developed and maintained by SAP Cloud Support.

The communication channels that require mutual authentication are secured by using standard Transport Layer Security (TLS) protocols. For more information about connectivity, see the **Technical Connectivity Guide for SAP Cloud Applications**, on the SAP Help Portal: <https://help.sap.com/cloud4customer>.

The communication channels for monitoring and maintaining instances of your SAP Cloud solution instances in the SAP data center network are also encrypted and authenticated.

Related Information

[SAP Data Center Locations](#) 

[Integration with SAP Solutions](#)

2 Security Aspects of Data, Data Flow, and Processes

[Communication Channels \[page 7\]](#)

Learn about the different communication channels used by SAP Cloud solutions.

[Business-To-Business Communication and Application Integration \[page 8\]](#)

Business-to-Business (B2B) communication and application integration refers to the exchange of business-related data across administrative domains. These domains need not necessarily belong to different entities, such as companies; they can also represent different geographic subsidiaries of the same company.

[E-Mail \[page 18\]](#)

SAP Cloud solutions enable you to encrypt outgoing e-mails and check the signature of incoming e-mails by using the Secure/Multipurpose Internet Mail Extensions (S/MIME) standard.

[File and Attachment Processing \[page 23\]](#)

Define the allowed file types for attachments and discover how to handle temporary files.

[Tax Numbers in SAP Cloud for Customer \[page 24\]](#)

Your SAP ERP or SAP S/4HANA system can contain various identification numbers, such as tax ID numbers or social security numbers. Some of these identification numbers can be sensitive information and special data protection policies could apply to them. To safeguard such information, you must filter out this information so that these numbers aren't replicated to SAP Cloud for Customer.

[Cookies \[page 25\]](#)

A list of cookies and their functions in SAP Cloud for Customer.

2.1 Communication Channels

Learn about the different communication channels used by SAP Cloud solutions.

The table shows the communication channels used by SAP Cloud solutions, the protocol used for the connection, and the type of data transferred.

Communication Path	Protocol Used	Technology Used	Type of Data Transferred	Data Requiring Special Protection
Web browser acting as front-end client to access the hosted SAP Cloud solution system	HTTPS	REST services	Application data	User IDs, passwords

Communication Path	Protocol Used	Technology Used	Type of Data Transferred	Data Requiring Special Protection
Apple® iPad® application, Apple® iPhone®, BlackBerry® player, Android™ (SAP Cloud for Customer)	HTTPS	REST services	Application data	User IDs, passwords, application data
E-mail	SMTP	SMTP server	Application data	Confidential data
Business-to-business communication and application integration	HTTPS	Web services	Application data	Application data

Cryptographic Protocols

Inbound Communications

For all inbound communications, TLS 1.2 is required. The following list shows a subset of supported cipher suites, in server-preferred order:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

i Note

SAP Cloud for Customer solutions use port 443 for HTTPS connectivity.

2.2 Business-To-Business Communication and Application Integration

Business-to-Business (B2B) communication and application integration refers to the exchange of business-related data across administrative domains. These domains need not necessarily belong to different entities, such as companies; they can also represent different geographic subsidiaries of the same company.

Communication arrangements enable you to configure the electronic data exchange between your solution and a communication partner. A communication partner can be a business partner in a B2B communication scenario or an external communication system that is used for application integration, for example, external time recording or master data systems.

Your SAP Cloud solution provides communication scenarios for inbound and outbound communication that you can use to create communication arrangements. Inbound communication defines how business documents are received from a communication partner, whereas outbound communication defines how business documents are sent to a communication partner.

Before you can use electronic data exchange for a particular business process, you must configure and activate a communication arrangement for the corresponding communication scenario. You can do so during your solution configuration or, after configuration is complete, under [Administrator > General Settings > Integration > Communication Arrangements](#).

You can find the list of trusted certification authorities for server certificates under [Administrator > General Settings > Common Tasks > Edit Certificate Trust List](#).

Security configuration for electronic data exchange is conducted at the communication arrangements level, where you can configure the authentication method and communication security.

Like end user authentication, B2B communication and application integration can be authenticated by two mechanisms: user ID plus password, and the X.509 client certificate. For inbound communication, you can upload the communication partner's client certificate in the configuration user interface, and map it to the communication user.

Caution

You can download an X.509 key pair from your SAP Cloud solutions. These key pairs are only intended for communication with the SAP Cloud solution and must not be used for other communication. This is because the corresponding certificate can be blocked in the solution and you can make the key pair invalid for logging on to the client but you cannot invalidate its other uses.

For outbound communication, you can upload a PKCS#12 container file, consisting of a private key and the corresponding client certificate that must be trusted and mapped by the communication partner.

Administrators can monitor the validity of client certificates in the under [Administrator > General Settings > Common Tasks > Edit Certificate Trust List](#).

Certificates have a validity period and expire at a defined point in time. Before expiration, they must be renewed; if the client certificate's Subject or Issuer has changed, then the upload and mapping process must be repeated. Communication arrangements are the customer's responsibility, since their configuration reflects the specific details of their business partner. As a result, expiring certificates cannot be replaced automatically by SAP; this action must be performed by the customer.

A good security concept also includes mandatory periodic password changes. These changes must be performed synchronously by both parties involved. If an expired client certificate is renewed with the same attributes, the certificate information can be exchanged asynchronously.

→ Recommendation

We recommend authentication using Single-Sign on with SAML 2.0 for browser-based access. Please ensure that the passwords used are strong enough.

2.2.1 Communication Arrangements Quick Guide

Communication arrangements help you to configure the electronic data exchange between the solution and a communication partner.

Communication arrangements can be set up for multiple business documents and communication methods. The solution provides communication scenarios for inbound and outbound communication that you can use to create communication arrangements. Inbound communication defines how business documents are received from a communication partner, whereas outbound communication defines how business documents are sent to a communication partner.

The *Communications Arrangements* view enables administrators to create and edit communication arrangements that your company has set up with a communication partner.

You can access this view from the *Administrator* work center, under ► *General Settings* ► *Integration* ►.

In the *Communication Arrangements* view, the following communication types are supported:

- Business-to-business (B2B)
This communication type defines an electronic data exchange with a business partner.
- Application integration
This communication type defines an electronic data exchange with a communication system.

i Note

Some communication arrangements are automatically created in your solution configuration. This is indicated by the selected *Predefined* check box in the worklist of the *Communication Arrangements* view. For predefined communication arrangements with inbound communication, you only have to define the communication account.

2.2.1.1 Create a Communication Arrangement

Procedure

1. Open the *New Communication Arrangement* guided activity in the *Communication Arrangements* view by clicking *New*.
2. In the *Select Scenarios* step, select the communications scenario for which you want to create a communication arrangement and click *Next*.
Based on the communication scenario you selected, the system presets the fields in the next steps with default values. Where possible, you can change the values, if necessary.
3. In the *Define Business Data* step, enter business data. The entry fields on the screen are dependent on the communication type of the selected communication scenario.
 - a. If you have selected a B2B scenario, enter the ID of the business partner and select the associated *Identification Type*. If necessary, you can also enter the ID of the contact person at the business partner. If you have selected an application integration scenario, enter the *System Instance ID* of the communication system with which you want to set up a communication arrangement. Note that before you set up a communication arrangement, you need to create a communication system.

- b. In the *My Communication Data* section, check the default values and make changes if necessary. Enter the company that communicates with your communication partner. By default, the *Company ID* is preset with the company to which you are assigned. If you use a B2B scenario, you must also enter a valid identification type.
 - c. If a communication arrangement contains a service interface that supports code list mapping, the *Code List Mapping* field is displayed. In this field you can choose the relevant code list mapping group for the communication scenario that you are using.
 - d. Click *Next*.
4. In the *Define Technical Data* step, define the technical settings for inbound and outbound communication.
- a. Select the *Communication Method* you want to use for the communication arrangement. To communicate with your business partner, you can either establish a direct connection or you can use a collaboration service provider that provides services for B2B communication.
 - b. If you use inbound communication, select the *Application Protocol* and *Authentication Method* in the *Inbound Communication: Basic Settings* section.
 - c. In the *User ID* field, click *Edit Credentials*.
Depending on the chosen authentication method, you need to define the credentials of the communication user as described in the following table. The user ID of the communication user is created automatically.

Authentication Method	Settings
SSL client certificate	<p>If you use this authentication method, you need to upload the public key certificate that has been provided by your communication partner. If your communication partner cannot provide a certificate, you can create and download a PKCS#12 key pair file. The PKCS#12 key pair file is password encrypted and contains a public key certificate and a private key. You need to provide the PKCS#12 file to your communication partner.</p> <ol style="list-style-type: none"> 1. Choose <i>Certificate</i>. 2. Click <i>Upload Certificate</i> and choose the relevant certificate. 3. Click <i>OK</i>. <p>To create a PKCS#12 key pair file, perform the following steps:</p> <ol style="list-style-type: none"> 1. Choose <i>Certificate</i>. 2. Click <i>Create and Download Key Pair</i>. 3. Define a name for the PKCS#12 file and save it. 4. Define a password for the PKCS#12 file and click <i>OK</i>. 5. Click <i>OK</i>. <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>i Note</p> <ul style="list-style-type: none"> ○ You have to provide your communication partner with the PKCS#12 file and the corresponding password. ○ To import the PKCS#12 key pair file to a third party tool, see the SAP Cloud for Customer Administration Guide. </div>

Authentication Method	Settings
User ID and password	<p>If you use this authentication method, you need to define a password as follows:</p> <ol style="list-style-type: none"> 1. Choose Change Password. 2. Enter a password. Note that you have to provide your communication partner with the user ID and password. 3. Click OK.

- d. If you use outbound communication, select the [Application Protocol](#), [Authentication Method](#) and enter the [Host Name](#) in the [Outbound Communication: Basic Settings](#) section. Depending on the chosen authentication method, you need to define the relevant settings as defined in the following table.

Authentication Method	Authentication	Settings
SSL client certificate	SAP system key pair	<p>If you use this authentication, the relevant certificate must be known to the communication partner. Therefore, you need to download the certificate as follows:</p> <ol style="list-style-type: none"> 1. In the Authentication field, click Download. 2. Choose a location to save the certificate. 3. Provide your communication partner with the downloaded certificate.
	Trusted third party key pair	<p>If you use this authentication, you need to upload the PKCS#12 key pair file provided by your communication partner. The PKCS#12 file is password-encrypted and contains a public key certificate and a private key.</p> <ol style="list-style-type: none"> 1. In the Authentication field, click Edit Key Pair. 2. Click Upload Key Pair and choose the PKCS#12 file you want to upload. 3. Enter the required password and click OK.
User ID and password		<p>If you use this authentication method, you need to enter the user ID and password that is used by the communication partner for the same communication arrangement.</p> <ol style="list-style-type: none"> 1. In the User ID field, click Edit Credentials. 2. Enter the User ID and Password. 3. Click OK.

- e. If necessary, you can individually configure each service that is used in the configuration scenario in the advanced settings.

The service URLs for outbound communication are calculated from the protocol, port, host name, and path. If you use SAP NetWeaver XI or IDoc, you do not need to change anything in the advanced settings since the path is preset. However, if you use Web Services Reliable Messaging, you have to enter the path for each service in the advanced settings.

- To edit the advanced settings, click [Edit Advanced Settings](#). Select the service you want to configure.
- In the [Details](#) section, deselect the [Use Basic Settings](#) check box and change the relevant settings.
- Click [Next](#).

5. In the [Review](#) step, review the data you entered in the previous steps.

- a. To ensure that all data is correct, click [Check Completeness](#). You also see the service URLs for inbound and outbound communication. If you use an inbound scenario, you must provide your communication partner with the URLs for inbound communication since it is that address to which messages should be sent.
 - b. To create and activate your communication arrangement in the system, click [Finish](#). You can also save an inactive version of the communication arrangement by clicking [Save as Draft](#).
6. If you have created a communication arrangement for a B2B outbound scenario, you have to activate the outbound channel for the business document that is used in the scenario.

Results

The system now uses electronic data exchange for the configured communication scenario.

2.2.1.2 Create a Communication Arrangement for On-Premise Integration

Multiple communication arrangements can be created for an on-premise integration through a guided activity.

Context

Instead of repeating common information each time you create a communication arrangement, you can enter common information once and create communication arrangements in bulk.

You can access this from the [Administrator](#) > [Create Communication Arrangement for On-Premise Integration](#) common task.

Note

This functionality is only valid for on-premise integrations.

Procedure

1. To open the [New Communication Arrangement](#) guided activity in the [Communication Arrangements](#) view, click [New](#).
2. In the [Select Communication System](#) step, enter business data.
 - a. Under [Integration Details](#) select the system you want to [Integrate with](#) and the relevant [Integration Middleware](#) you want to use.

i Note

If *PI* is selected as the middleware, fill in the system details in the field *PI Business System*.

- b. Under *Communication System* enter the *System Instance ID* of the communication system with which you want to set up a communication arrangement.

i Note

Before you create a communication arrangement, you need to create a communication system. See the SAP Cloud for Customer Administrator Guide for more detail.

With this action, the *Communication System*, *User ID (Inbound Communication Credentials)* and *Host Name* are automatically populated.

If a communication arrangement contains a service interface that supports code list mapping, the *Code List Mapping* field is displayed. In this field you can choose the relevant code list mapping group for the communication scenario that you are using.

- a. If you use inbound communication, select the *Authentication Method* in the *Inbound Communication Credentials* section. Depending on the chosen authentication method, you need to define the credentials of the communication user as described in the following table. The user ID is created automatically.

Authentication Method	Settings
SSL client certificate	<p>If you use this authentication method, you need to upload the public key certificate that has been provided by your communication partner. If your communication partner cannot provide a certificate, you can create and download a PKCS#12 key pair file. The PKCS#12 file is password encrypted and contains a public key certificate and private key. You need to provide the PKCS#12 file to your communication partner.</p> <ol style="list-style-type: none">1. Choose <i>Certificate</i>.2. Click <i>Upload Certificate</i> and choose the relevant certificate.3. Click <i>OK</i>. <p>To create a PKCS#12 key pair file, perform the following steps:</p> <ol style="list-style-type: none">1. Choose <i>Certificate</i>.2. Click <i>Create and Download Key Pair</i>.3. Define a name for the PKCS#12 file and save it.4. Define a password for the PKCS#12 file and click <i>OK</i>.5. Click <i>OK</i>. <p>Note that you have to provide your communication partner with the PKCS#12 file and the corresponding password.</p>
User ID and password	<p>If you use this authentication method, you need to define a password as follows:</p> <ol style="list-style-type: none">1. Choose <i>Change Password</i>.2. Enter a password. Note that you have to provide your communication partner with the user ID and password.3. Click <i>OK</i>.

If you use outbound communication, select the [Authentication Method](#). Depending on the chosen authentication method, you need to define the relevant settings as described in the following table:

Authentication Method	Authentication	Settings
SSL client certificate	SAP system key pair	<p>If you use this authentication, the relevant certificate must be known to the communication partner. Therefore, you need to download the certificate as follows:</p> <ol style="list-style-type: none"> In the Authentication field, click Download. Choose a location to save the certificate. Provide your communication partner with the downloaded certificate.
	Trusted third-party key pair	<p>If you use this authentication, you need to upload the PKCS#12 key pair file provided by your communication partner. The PKCS#12 file is password encrypted and contains a public key certificate and private key.</p> <ol style="list-style-type: none"> In the Authentication field, click Edit Key Pair. Click Upload Key Pair and choose the PKCS#12 file you want to upload. Enter the required password and click OK.
User ID and password		<p>If you use this authentication method, you need to enter the user ID and password that is used by the communication partner for the same communication arrangement.</p> <ol style="list-style-type: none"> In the User ID field, click Edit Credentials. Enter the User ID and Password. Click OK.

- In the [Communication Arrangements](#) step, select one or more [Communication Scenarios](#).

Status	Interpretation
Create	This status indicates that you have selected a communication scenario to be created for the relevant communication arrangement.
Not Created	This status indicates that the communication scenario has not yet been created and the check box is unchecked.
Already Exists	This status indicates that a communication scenario has been created already and the check box will be disabled.

- The [Inbound](#) and [Outbound](#) tabs are displayed, depending on the selected [Communication Scenario](#). For example, if a communication arrangement has only an inbound service interface, then the [Inbound](#) tab is displayed.
- Perform the following actions under the [Inbound](#) tab as necessary:

Enabled	The check box can be unchecked if it is not necessary.
Service	If the service is mandatory the check box is disabled.
Application Protocol	Choose a protocol from the drop-down list.
Service URL	Displays the URL of the service.

To check the information on the inbound service, click [Check Service](#). Perform the following functions on the [Outbound](#) tab as necessary.

Enabled	The check box can be unchecked if not required.
Service	If the service is mandatory the check box is disabled.
Application Protocol	Choose a protocol from the drop-down list.
Host Name	This field displays the host name of the system and is not editable.
Port	Enter the port or path for the outbound service.
Service URL	Displays the URL of the service.

6. To ensure that all data is correct, click [Check Completeness](#).
7. To create and activate your communication arrangement in the system, click [Finish](#).

Results

A success message is shown once the communication arrangement has been created successfully.

2.2.1.3 Edit a Communication Arrangement

Procedure

1. To open the [Edit Communication Arrangement](#) quick activity in the [Communication Arrangements](#) view, select the relevant communication arrangement and click [Edit](#).

i Note

You cannot edit predefined communication arrangements.

2. Change the relevant settings.
3. To save your changes and return to the work list, click [Save and Reactivate](#).
4. In the worklist, you can click [Check Completeness](#) to see if your changes have been updated in the system. It may take about a minute for the system to update the information.

2.2.1.4 Edit the Communication Credentials for a Predefined Communication Arrangement

This task is only relevant for predefined communication arrangements with inbound communication.

Procedure

1. In the *Communication Arrangements* view, select the relevant communication arrangement. Predefined communication arrangements are indicated by the selected *Predefined* check box.
2. Click *Edit Credentials*.
3. Depending on the authentication method that you have agreed upon with your communication partner, you need to define the credentials of the communication user as described in the following table. The user ID of the communication user is created automatically.

Authentication Method	Settings
SSL client certificate	<p>If you use this authentication method, you need to upload the public key certificate that has been provided by your communication partner. If your communication partner cannot provide a certificate, you can create and download a PKCS#12 key pair file. The PKCS#12 key file is password encrypted and contains a public key certificate and a private key. You need to provide the PKCS#12 file to your communication partner.</p> <p>To upload a public key certificate, perform the following steps:</p> <ol style="list-style-type: none">1. Choose <i>Certificate</i>.2. Click <i>Create and Download Key Pair</i>.3. Define a name for the PKCS#12 file and save it.4. Define a password for the PKCS#12 file and click <i>OK</i>.
	<p>Note</p> <ul style="list-style-type: none">○ You have to provide your communication partner with the PKCS#12 file and the corresponding password.○ To import the PKCS#12 key pair file to a third party tool, see Create a Communication Arrangement [page 10] in the Related Links section.
User ID and password	<p>If you use this authentication method, you need to define a password. The user ID is automatically predefined. Perform the following steps:</p> <ol style="list-style-type: none">1. Choose <i>Change Password</i>.2. Enter a password. Note that you have to provide your communication partner with the user ID and password.

4. Click *OK*.

Related Information

[Create a Communication Arrangement \[page 10\]](#)

2.2.1.5 Delete a Communication Arrangement

Procedure

1. In the *Communication Arrangements* view, select the relevant communications arrangement.
2. Click *Delete*.
3. In the dialog box that opens, click *Delete* to confirm the deletion.

Note

Predefined communication arrangements cannot be deleted.

2.3 E-Mail

SAP Cloud solutions enable you to encrypt outgoing e-mails and check the signature of incoming e-mails by using the Secure/Multipurpose Internet Mail Extensions (S/MIME) standard.

You can use this function for e-mail communication between your system and your employees, in e-mail scenarios provided by SAP (for example, self-service or approval scenarios). You can specify which e-mail scenarios you want to use in Business Configuration.

Caution

We strongly recommend that you only send encrypted mails and accept only signed e-mails.

The system uses the same certificate for signature check and e-mail encryption, which means that the same private key is used for signing and decrypting an e-mail to or from an employee.

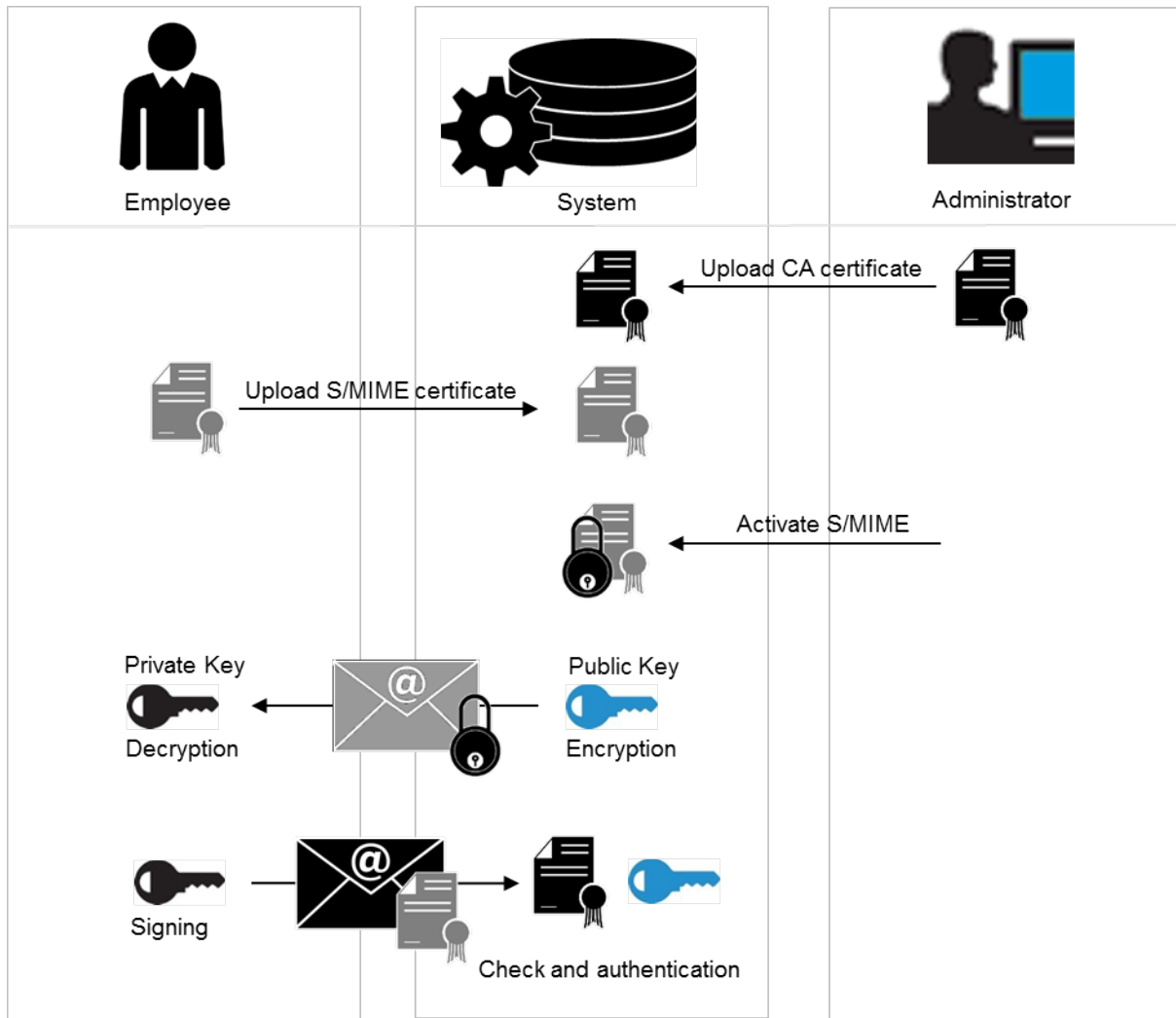
The following MIME types are supported for e-mail communication with the system:

- .gif
- .jpg/.jpeg
- .pdf
- .tif/.tiff
- .png

⚠ Caution

When you use S/MIME, ensure that the data is encrypted. Please note that e-mail header data, for example, the subject line, is not encrypted. The sensitivity setting for password e-mails is set by default to private.

The following diagram provides an overview of how e-mail encryption and signature is set up:



E-Mail Security with S/MIME

2.3.1 Enabling S/MIME Security

To add encryption security to e-mail channels, you can enable S/MIME to your solution.

Procedure

1. Add e-mail security to your project scope.

2. Implement e-mail security for your solution.
 - a. Choose *Business Configuration*, select your project from the list, and click *Open Activity List*.
 - b. Click *Fine-Tune*.
 - c. Open *E-Mail Encryption and Signature Check*.
 - d. In the list of incoming e-mails, set the *Signature* for *SAP Cloud for Service: E-Mail Security, B2B Scenario* and *SAP Cloud for Service: E-Mail, B2C Scenario*. Choose *Check (and Reject if Untrusted)* if you require a high level of security or *Do Not Check* if you do not have security requirements.
 - e. In the list of outgoing e-mails, set the *Encryption* and *Signature* for *SAP Cloud for Service: E-Mail Security, B2B Scenario* and *SAP Cloud for Service: E-Mail Security, B2C Scenario*. The suggested settings are *Encrypt if possible* for *Encryption* and *Sign* for *Signature*.
 - f. Save your settings.
3. Activate your settings.
 - a. Choose ► *Administrator* ► *Common Tasks* ► *Configure S/MIME* ►.
 - b. Click *Activate S/MIME*.
 - c. Select *Check signature of Incoming E-Mails* to encrypt incoming e-mails. Select *Encrypt Outgoing E-Mails* to encrypt outgoing e-mails. Select *Signing Outgoing E-Mails* for your solution to provide a signature to other systems.

The settings you selected in *Fine-Tuning* will only be enabled if you activate them. If you do not activate your settings, your system will not have security enabled.
4. Save your settings.

2.3.2 Configuring S/MIME Security

To enable e-mail notifications, you must also upload the CA certificates in this area for the generic business task management e-mail address for all involved employees and managers.

Procedure

1. Choose *Configure S/MIME* in the *Administrator* work center under *Common Tasks*.
2. On the *Incoming E-Mail* tab, upload the CA certificates from all involved employees for the generic incoming e-mail addresses *Business Task Management E-Mail Notifications*.
3. On the *Outgoing E-Mail* tab, install the system CA certificate in the e-mail client of the involved employee as follows:
 - a. Click on *Link to SAP CA* and open the site ► *SAP Trust Center Service* ► *Root Certificates* ►.
 - b. Click on *SAP Passport CA Certificate*. A pop-up opens.
 - c. Click *Install Certificate* and follow the wizard by clicking *Next*.
 - d. Select *Place all certificates in the following store* and click *Browse*.
 - e. Select *Trusted Root Certification Authorities* and click *OK* and then *Next*. Now the CA from the system is installed locally.
4. Now activate the S/MIME. On the *Activate S/MIME* tab, select the options:
 - a. *Check Signature of Incoming E-Mails*

- b. [Encrypt Outgoing E-Mails](#) (optional)
- c. [Signing Outgoing E-Mails](#)

Results

- **E-Mail Notifications:** Ensure that the involved employees are business users and have valid e-mail addresses, and that the CA certificates from the employees are uploaded to the system for outgoing e-mails.
- **E-Mail Notifications:** Each involved employee must subscribe to the e-mail notifications by opening the [Notifications](#) view and choosing [Subscribe to E-Mail](#).
- **E-Mail Notifications:** **Check that the e-mail clients of the involved employees have enabled the receipt of encrypted e-mails.**

2.3.3 Security Measures for E-Mail Domains

For outbound e-mail, SAP offers Sender Policy Framework (SPF) as a security measure and supports Domain Keys Identified Mail (DKIM) keys by request.

SPF is an e-mail authentication technique that is used to prevent spammers from sending messages on behalf of your domain. SAP creates an SPF record for all SAP Cloud for Customer tenants using the CISCO mail device.

i Note

SAP enables SPF automatically for outbound e-mail. SPF records are updated on the technical from/Mail From/Envelop-From address, which is one of the following:

- dsn@myXXXXXX.mail.crm.ondemand.com
- dsn@myXXXXXX.mail.c4c.saphybriscloud.cn

Sample SPF record for either domain: `v=spf1 include:_spf.cmail.ondemand.com ~all`

DKIM is an e-mail authentication technique involving a digital signature that allows the receiver to check that an e-mail was sent and authorized by the owner of that domain. The DKIM signature is a header that is added to the message and is secured with encryption. SAP recommends that sender domains used in your SAP solution are DKIM signed. Administrators must explicitly request a unique DKIM key from SAP.

You can use external tools to check the SPF record or check the DKIM key for a sender domain.

Users send business e-mail when they work with tickets, accounts, appointments, visits, sales quotes, workflow notifications, or similar objects in the SAP solution.

Business e-mail is:

- Relayed from the CISCO mail device on the SAP Network.
- Sent through these IP ranges:
 - 155.56.208.100/30
 - 157.133.97.216/30

- 169.145.66.70/31
- 169.145.66.72/31

If you have any throttling process or whitelisting of IPs for receiving mails in your network, update your network environment IP addresses and add `include:_spf.cmail.ondemand.com` in your SPF domain only if required.

- Sent with a DKIM key signed, provided that you've requested the DKIM key from SAP and activated this feature.

Related Information

[Request DKIM Key for Sender Domains \[page 22\]](#)

2.3.3.1 Request DKIM Key for Sender Domains

For outbound e-mail, SAP provides certain e-mail security measures automatically, such as the Sender Policy Framework (SPF). To add Domain Keys Identified Mail (DKIM) authentication, administrators must request a DKIM key.

Context

Use this procedure to request a DKIM key for outbound business e-mail, such as e-mail messages used as part of tickets, accounts, appointments, visits, workflows, and so on.

i Note

For scenarios that generate mass e-mails, such as marketing or campaign execution, follow the procedure to activate mass e-mail instead.

Procedure

1. Create an incident to request a DKIM key. Include your complete list of domains for outbound e-mail.

DKIM keys can't be generated for the following domains:

- gmail.com
- hotmail.com
- outlook.com
- sap.com
- your tenant domain (myxxxxxx.mail.crm.ondemand.com)

2. SAP responds to the incident with your public DKIM key and selector details.

3. Use the public DKIM key and selector details to maintain a DKIM TXT record in your DNS server.
4. You respond to the incident to confirm that you've added the DKIM key in your DNS server.
5. SAP activates the DKIM key for your solution and closes the incident.

Results

The DKIM key can be used in both test and productive tenants.

2.4 File and Attachment Processing

Define the allowed file types for attachments and discover how to handle temporary files.

2.4.1 Configure Upload Controls

This section describes the steps to specify the allowed file types.

Context

The Multipurpose Internet Mail Extensions (MIME) type configuration controls the files you can add to the SAP Cloud for Customer system. These file types include attachment uploads as well as files sent via e-mail attachments.

You can upload attachment files to your SAP Cloud solution in several application scenarios, for example in billing, in data migration, or image files of your travel expense receipts. Regularly updated anti-virus software checks the uploaded files for viruses and other types of malicious software.

→ Recommendation

In addition to this anti-virus software, we recommend that our customers also use anti-virus software.

In Business Configuration, you can define which file types can be uploaded to your solution. Note that file-name extensions can be changed to disguise the actual file format of the file.

We recommend that you start with a minimal MIME list, as you've the option of adding more later. Choose from the list of allowed MIME types for uploading documents that are specific for your project.

Follow these steps to select MIME types from the provided list:

Procedure

1. Navigate to ► [Business Configuration](#) ► [Implementation Projects](#) ► [Open Activity List](#) ► and open the [Allowed MIME Types for Document Upload](#) fine-tuning activity.
2. In the new screen, select your project relevant MIME types.

2.4.2 Temporary Files

Your browser saves temporary files as you work. Use your browser tools to delete cached information.

On PCs and laptops, the IndexedDB of the browser is used to cache information, such as:

- Recent history
- Basic search (recent search entries)
- Value help (recent search entries)
- Home page (title information and data)

→ Recommendation

SAP Cloud for Customer doesn't delete these types of temporary entries. To remove cached data, we recommend using the appropriate features of your browser.

2.5 Tax Numbers in SAP Cloud for Customer

Your SAP ERP or SAP S/4HANA system can contain various identification numbers, such as tax ID numbers or social security numbers. Some of these identification numbers can be sensitive information and special data protection policies could apply to them. To safeguard such information, you must filter out this information so that these numbers aren't replicated to SAP Cloud for Customer.

! Restriction

While data encryption is addressed in SAP Cloud for Customer in secure communication channels and at rest, there's no specific masking or additional encryption. Therefore, you must filter out sensitive information, such as personal identification numbers, before replicating.

To learn how to set up these filters for SAP ERP, see [Business Partner Tax Code](#).

For instructions on how to set up these filters for SAP S/4HANA, see [Restricting Sensitive Tax Number](#).

For instructions on how to set up these filters for SAP S/4HANA Cloud, see the section on **Restricting Sensitive Tax Number** in the document: [Setting Up Opportunity-to-Order with SAP Cloud for Customer \(1VP\)](#).

2.6 Cookies

A list of cookies and their functions in SAP Cloud for Customer.

SAP Cloud for Customer uses the following cookies to exchange information between the client and server. This information may include session IDs, load-balancing information, or performance indicators, for example.

To protect the information contained in the cookies, SAP Cloud for Customer requires secure communication channels (HTTPS) and sets the `Secure` and `HttpOnly` flags for all cookies.

Cookie	Purpose	When Set
<code>Sap-client</code>	Three-digit tenant number	Created as a browser session cookie whenever a new user visits the logon screen for SAP Cloud for Customer.
<code>Sap-ssolist</code>	Supports Single-Sign-On administration	Created as a browser session cookie
<code>Sap-usercontext</code>	Language and client number	Created as a browser session cookie whenever a new user successfully logs on to SAP Cloud for Customer.
<code>Sap_c4c_logon_record</code>	GUID to link requests that belong to one logon session (for performance analysis)	Created as a browser session cookie whenever a new user successfully logs on to SAP Cloud for Customer.
<code>SAP_SESSIONID_<systemname>_<tenant></code>	Session ID	Created as a browser session cookie whenever a new user successfully logs on to SAP Cloud for Customer.
<code>Sap1b<systemname></code>	Load balancing, system name, tenant number	Created as a browser session cookie whenever a new user successfully logs on to SAP Cloud for Customer.

3 User Administration and Authentication

User management for SAP Cloud for Customer is located in the Administrator work center.

[User Management \[page 26\]](#)

The solution allows you to limit administrative authorizations to users who perform the administrative functions.

[User Types \[page 30\]](#)

Learn about the different user types available in the solution.

[Authentication Mechanisms \[page 31\]](#)

Every user type must authenticate itself to SAP Cloud solutions for regular browser-based front-end access, as well as for electronic data exchange, such as Business-to-Business communication. SAP Cloud solutions don't support anonymous access.

[Security Policy Quick Guide \[page 39\]](#)

As an administrator, you can increase the security level, if desired, by editing and enhancing the security policy, for example, by changing the complexity and validity for all passwords, in accordance with your company's security requirements.

[Security Settings \[page 42\]](#)

As an administrator, you can define security settings that are applicable for all users, or a selected business role.

3.1 User Management

The solution allows you to limit administrative authorizations to users who perform the administrative functions.

There must be a clear definition of roles and duties within the administrator user group itself. For example: you have dedicated administrators for screen adoptions, but these team members can't change authorizations. Use the available standard reports to regularly monitor users with administration rights, and also track the changes made to the user access rights.

For access rights, you must maintain necessary authorizations.

i Note

Personalizing any part of the UI doesn't change or add any security settings, because personalization is part of extensibility, which allows you to display/hide fields based on user/business roles, screen adaptations and so on. For example: even if you remove the edit button from the UI, the edit option is still available via OData APIs.

→ Recommendation

We recommend using SSO for basic security. To protect accounts further, configure the identity provider (IdP) of the SSO solution to provide enhanced security, such as multifactor authentication (MFA), geofencing, and other additional security features.

The following table provides an overview of all activities related to user administration that you can perform as an administrator:

User Administration Activities

View	Subview	Activity	Documentation in the Help Center
<i>Administrator</i>	Business Users	Lock and unlock users	<i>Business Users Quick Guide</i>
		Change user password	
		Edit the validity of a user	
		Assign security policies to users	
		Assign access rights to users for work centers and work center views	
		Restrict read and write access for users to specific data	
	Support and Technical Users	View all support and technical users available in the system	
	Business Roles	Define access rights in business roles	<i>Business Roles Quick Guide</i>
<i>Administrator</i>	Communication Arrangements	Create technical users for electronic data exchange	<i>Business Roles Quick Guide</i>
	Communication Certificates	Manage certificates that you use for electronic data exchange	<i>Personalize my Settings</i>
▶ Administrator ▶ Common Tasks ▶	Edit Security Policies	Specify security policies for user passwords	<i>Security Policies Quick Guide</i>
	Configure Single Sign On	Download service provider metadata, upload IdP metadata, and activate SSO	<i>Configure your Solution for Single Sign-On</i>
	Configure S/MIME	Configure and activate e-mail communication with S/MIME	<i>E-Mail Security</i> <i>Configuration: Load Certificates and Activate Signing and Encryption for E-Mails</i>

View	Subview	Activity	Documentation in the Help Center
	Edit Certificate Trust List	Edit trust list of certificates used for communication arrangements	<i>Communication Arrangements Quick Guide</i>

i Note

The list of trusted certification authorities is available on the Web dispatcher. Certificates with which users logon must be issued by one of these certification authorities.

3.1.1 VIDEO: Assigning User Access Rights by Roles

Use this video to discover how to create roles that you can assign to users for easier maintenance of user access rights.

3.1.2 Restricting Access Roles

You use business roles to assign access rights to multiple business users who carry out the same activities. You can also define access restrictions for a business role.

Procedure

1. From the *Administrator* work center, click on *Business Roles*.
2. If you want to edit the read and write access for users to whom any of the business roles are assigned, click on any of the business roles listed and then click *Edit*. Next, click the *Access Restrictions* tab.
3. Select the view for which you want to restrict access rights and choose the corresponding access restriction in the *Read Access* and *Write Access* column. You can choose between the following settings for access restrictions:
 - *No Access* (Only available as a restriction for write access)
The user has no write access.
 - *Unrestricted*
The user has access to all business data related to the view.

- *Restricted*

The user only has access to specific business data, depending on the access context. If you select *Restricted*, you can restrict read and write access on the basis of predefined restriction rules that you can choose from the *Restriction Rule* drop-down list.

If you choose the *Define Specific Restrictions* restriction rule, another list appears in which you can restrict access to specific data, which is defined by the access group. For example, if a view has the Site access context, you can restrict write access in this view for business documents that belong to a specific site.

To do so, choose *Detailed Restrictions* and select or deselect the corresponding check box in the *Read Access* or *Write Access* column.

4. If you want to grant the user access to data that is no longer in use, choose *Historic Restrictions*. Select or deselect the corresponding check box in the *Read Access* or *Write Access* column.
5. To check whether the access rights are consistent, click *Actions* and choose *Access Rights Consistency*. Each view contains specific activities that can be carried out by a user with the necessary access rights for the view. Note that some activities can be carried out in multiple views. Therefore, when you grant access rights, you should be aware that if there is a conflict, unrestricted access rights override any restrictions you have defined.

→ Tip

View A and view B both contain activity C. For view A, a user has unrestricted read and write access, but for view B, the same user has read-only access. Because unrestricted access rights override restricted access rights, the user will actually have both read and write access to both views. Checking consistency will help you to identify these views and activities.

6. If there are activities displayed on the *Check Access Rights Consistency* screen, the access rights are inconsistent. Check whether you need to redefine the access rights.
7. When finished, click on ► *Assigned Users* ► *Activate User* ► to save the edits you have made to the business role and the users.

3.2 User Types

Learn about the different user types available in the solution.

SAP Cloud solutions provide the following user types:

User Type	Description
Business User	<p>A user type for normal interactive users resulting from hiring an employee or creating a service agent. Business users always have to change their initial password during the first logon. The properties of the passwords are determined by the assigned security policy.</p> <div data-bbox="821 779 1396 1070"><p>i Note</p><p>Service agents are used for external users, for example, partners or partner contacts. Apply specific security policies and use specific roles to keep internal and external employees separated. We also recommend that you lock external users as soon as they are no longer needed.</p></div>
Technical User	<p>A user type for non-interactive usage, either predefined by SAP for technical operations or resulting from the creation of communication arrangements. Technical users either do not have passwords or have password but do not have to change them.</p>
Support User	<p>A user type for interactive support users used by SAP Cloud Services to access the system as part of incident processing.</p> <div data-bbox="821 1384 1396 1848"><p>i Note</p><p>If support users receive a ticket and realize that they have to access the customer system in order to analyze the problem (for example, if they were not able to replicate and solve the issue in the internal test or development systems), they use the Cloud Access Manager (CAM) tool to generate temporary access to the corresponding customer system. Support users are not allowed to share these details. The CAM tool keeps a log of which user generated which support user at what date and time. So it is always possible to link a generic support user back to the real person.</p><p>Support users follow the pattern SAP_*.</p></div>

It is often necessary to specify different security policies for different users. For example, your policy may mandate that individual users who perform tasks interactively change their passwords on a regular basis.

You can only specify security policies for the Business User.

3.3 Authentication Mechanisms

Every user type must authenticate itself to SAP Cloud solutions for regular browser-based front-end access, as well as for electronic data exchange, such as Business-to-Business communication. SAP Cloud solutions don't support anonymous access.

When a new user is created in your SAP Cloud solution, for example, during the hiring process of a new employee, a user ID is created.

To log on your SAP Cloud solution, the following authentication mechanisms are supported:

- Logon using SAML 2.0 assertion for front-end Single Sign-On (SSO)
- Logon using client certificate (X.509) as logon certificate
- Logon using user ID and password

→ Recommendation

We recommend using SSO for basic security. To protect accounts further, configure the identity provider (IdP) of the SSO solution to provide enhanced security, such as multifactor authentication (MFA), geofencing, and other additional security features.

As an additional security mechanism, we recommend that you enable multi-factor-authentication for users who are assigned to one or more of the workcenters in the following table. These users are power users and have access to admin-type features.

Work Center	Work Center ID
Administrator	SEODADMINWCF
Application and User Management	ITS_APPLICATIONUSERMANAGEMENT
Business Configuration	BC_BUSINESSCONFIGURATION
Business Analytics	ANA_BUSINESSANALYTICS
Data Workbench	COD_DATALOADER_WCF
Data Cleansing	COD_DATACLEANSING_WCF
Data Integration	DATA_INTEGRATION
Data Protection and Privacy	DATAPRIVACY
Developer Tools	OFFLINE_DEV_TOOLS_WOC
E-Mail Integration	GROUPWARE_INTEGRATION_WCF
Partner Access – Multi-Customer Solution	PARTNER DEVELOPMENT FOR MCS
Partner Development	PDI_PARTNER_DEVELOPMENT

Work Center	Work Center ID
Service Control Center	CI_CUSTOMER_CONTROL_CENTER
Organizational Management	MOM_ORGANIZATIONALMANAGEMENT

The MFA feature is provided by most of the Identity Providers such as SAP's Identity Access Service (IAS) as an optional feature and must be enabled. For more information about enabling MFA when using SAP's IAS, see [Configure SAP Authentication 365 in Administration Console](#)

3.3.1 Log on Using SAML 2.0 Assertion for Front-End Single Sign-On (SSO)

Your solution supports SSO based on Security Assertion Markup Language 2.0 (SAML 2.0). To use this function, your system landscape requires the following components:

- An SAML 2.0 enabled identity provider (IdP)
- At least one local service provider, for example, your solution or a Web-based 3rd-party product
- A browser client

The use of an SAML 2.0. enabled identity provider is mandatory. If you have no identity provider, it is recommended that you use **SAP Cloud Platform Identity Authentication - IAS** (former Cloud Identity).

When a user connects to the service provider by using the corresponding URL, the browser redirects the authentication request to the IdP. If the user is not yet logged on, they are prompted to log on to the IdP. After that the browser redirects the connection back to the original URL and the user is automatically logged on to the service provider. This process flow is always the same for all server providers.

The mutual trust between service provider and IdP is established by the exchange of certificates and additional metadata.

It is recommended you disable username and password based access for users who use SSO to log in. As the users would use SSO, they wouldn't be aware if their passwords get changed. IdPs could also provide extra security features such as two-factor authentication, which would not be effective in case the username and password option is still available.

For more information, see the *Front-End Single Sign-On* document in the Help Center and the SAP Identity Provider documentation on SAP Help Portal at <http://help.sap.com/netweaver> ► [SAP NetWeaver Identity Management](#) ► [<release>](#) ► [Application Help](#) ►.

3.3.1.1 Configure Your Solution for Single Sign-On

This topic describes how to set up your solution to use front end single sign-on (SSO).

Prerequisites

You've downloaded the XML file of the metadata of your identity provider (IdP).

Context

You can configure SSO in your system using the `Configure Single Sign-On` common task, which is available under `► Administrator ► Common Tasks ►`.

Procedure

1. Choose *My System*.
2. Under `► General ► Download Metadata ►`, depending on the type of metadata acceptable to your identity provider, choose either of the following: *SP Metadata* (Service Provider Metadata) or *STS Metadata* (Security Token Service Metadata).
3. Save the XML file for upload into the IdP.

Note

Some IdPs can upload all information from the metadata XML file. Others require manual entry of the information contained in the file.

4. Specify whether the employee can manually choose between logging on with a user ID and password or SSO by using the *Manual Identity Provider Selection* toggle button.
5. In the *Single Sign-On URL Handling* section, specify which URL employees must use to log on to the system. In the *URL Sent to Employee* drop-down list you can choose from the following options:
 - a. *Non-SSO URL*: The system sends only the normal system URL to the employee. The employee can't log on using SSO and must use a password or a certificate instead.
 - a. *SSO URL*: The system sends only the SSO URL to the employee. The employee can log on using SSO. The authentication request is redirected through the IdP.
 - a. *Automatic Selection*: If SSO isn't active, the system sends the normal system URL to the employee. If SSO is active, the system checks whether the employee has a password. If the password is available, both SSO URL and non-SSO URL are sent to the employee. However, if the employee has no password, only the SSO URL is sent to the employee.
6. Choose *Identity Provider*.

7. Click [New Identity Provider](#) and select the metadata XML file that you've downloaded from your IdP. By importing the metadata, the system automatically uploads the required signature certificate and encryption certificate.
 8. If you have multiple identity providers configured and you haven't selected the [Manual Identity Provider Selection](#) check box in the previous step, you must select the default IdP, which is automatically selected when logging on to the system. To do so, select the corresponding IdP and click [Actions](#), then choose [Set to Default](#).
 9. If necessary, you can specify the [Alias](#), which defines the displayed name of the IdP that appears on the logon screen.
 10. If your IdP requires the element `Assertion Consumer Service URL` in the SAML request, select the [Include Assertion Consumer Service URL](#) check box.
 11. The name ID format gives you two ways to map the IdP configuration to your SAP solution. Define the name ID format that you want to use as the default:
 - Unspecified
Maps the `NameID` attribute from the IdP configuration with the alias (username for logon) in the SAP solution.
 - E-Mail Address
Maps the `NameID` attribute from the IdP configuration with the e-mail address of the user in the SAP solution.
- i Note**

This option requires that an e-mail address is only associated with **one user** in the SAP solution. The SAP solution traces the e-mail address to one employee defined in the SAP solution, and then to the corresponding user.
12. Once you've configured your IdP, activate SSO in your cloud solution. To do so, click [Activate Single Sign-On](#).
 13. Save your changes.

3.3.2 Logon Using Client Certificate (X.509)

Users can also log on with a client certificate to complete authentication. To do so, users can choose between the following options:

- If users already possess a suitable client certificate from a trusted Certification Authority, then they can map the client certificate to their user ID.
- If no suitable client certificate is available, then users can request a client certificate from within the SAP Cloud solution. In response, an SAP Certification Authority will provide the requested certificate. This request can be repeated on any other device you use to access SAP Cloud solutions. You cannot use the same certificate to log on with multiple users.

We strongly recommend that you never store the X.509 client certificate in an unprotected keystore. The download also contains the corresponding private key. Therefore, the downloaded file should be protected with a sufficiently strong passphrase of the user's choice.

The following table contains the trusted certification authorities for client certificates:

Trusted Certification Authorities

Country	Organization	Organizational Unit	Common Name	Common Name E-Mail
DE	Deutsche Telekom AG	T-TeleSec Trust Center	Deutsche Telekom Root CA 1	
DE	SAP Trust Community		SAP Passport CA	
DE	TC TrustCenter GmbH	TC TrustCenter Class 2 CA	TC TrustCenter Class 2 CA II	
DE	TC TrustCenter GmbH	TC TrustCenter Universal CA	TC TrustCenter Universal CA I	
DE	TC TrustCenter for Security in Data Networks GmbH	TC TrustCenter Class 1 CA		certificate@trustcenter.de
IE	Baltimore	CyberTrust	Baltimore CyberTrust Root	
US	Entrust.net	www.entrust.net/ CPS incorp. by ref. (limits liab.), (c) 1999 Entrust.net Limited	Entrust.net Secure Server Certification Authority	
US	Entrust.net	www.entrust.net/ Client_CA_Info/C PS incorp. by ref. limits liab., (c) 1999 Entrust.net Limited	Entrust.net Client Certification Authority	
US	Equifax	Equifax Secure Certificate Au- thority		
US	GoDaddy.com, Inc.	http://certifi- cates.god- addy.com/reposi- tory	Go Daddy Secure Cer- tification Authority	
US	The Go Daddy Group, Inc.	Go Daddy Class 2 Certification Au- thority		
US	VeriSign, Inc.	Class 1 Public Pri- mary Certification Authority		
US	VeriSign, Inc.	Class 1 Public Pri- mary Certification Authority - G2, (c) 1998 VeriSign, Inc. - For authorized use only, VeriSign Trust Network		
US	VeriSign, Inc.	Class 2 Public Pri- mary Certification Authority		

Country	Organization	Organizational Unit	Common Name	Common Name E-Mail
US	VeriSign, Inc.	Class 1 Public Primary Certification Authority		
US	VeriSign, Inc.	Class 1 Public Primary Certification Authority - G2, (c) 1998 VeriSign, Inc. - For authorized use only, VeriSign Trust Network		
US	VeriSign, Inc.	Class 2 Public Primary Certification Authority		
US	VeriSign, Inc.	Class 2 Public Primary Certification Authority - G2, (c) 1998 VeriSign, Inc. - For authorized use only, VeriSign Trust Network		
US	VeriSign, Inc.	Class 3 Public Primary Certification Authority		
US	VeriSign, Inc.	Class 3 Public Primary Certification Authority - G2, (c) 1998 VeriSign, Inc. - For authorized use only, VeriSign Trust Network		
US	VeriSign, Inc.	Class 4 Public Primary Certification Authority - G2, (c) 1998 VeriSign, Inc. - For authorized use only, VeriSign Trust Network		
US	VeriSign, Inc.	VeriSign Trust Network, (c) 1999 VeriSign, Inc. - For authorized use only	VeriSign Class 1 Public Primary Certification Authority	
US	VeriSign, Inc.	VeriSign Trust Network, (c) 1999 VeriSign, Inc. - For authorized use only	VeriSign Class 2 Public Primary Certification Authority - G3	

Country	Organization	Organizational Unit	Common Name	Common Name E-Mail
US	VeriSign, Inc.	VeriSign Trust Network, (c) 1999 VeriSign, Inc. - For authorized use only	VeriSign Class 3 Public Primary Certification Authority - G3	
US	VeriSign, Inc.	VeriSign Trust Network, (c) 1999 VeriSign, Inc. - For authorized use only	VeriSign Class 4 Public Primary Certification Authority - G3	
US	VeriSign, Inc.	VeriSign Trust Network, (c) 2006 VeriSign, Inc. - For authorized use only	VeriSign Class 3 Public Primary Certification Authority - G5	
ZA	Thawte Consulting cc	Certification Services Division	Thawte Premium Server CA	premium-server@thawte.com
ZA	Thawte Consulting cc	Certification Services Division	Thawte Server CA	server-certs@thawte.com

For more information about trust configuration, see SAP Help Portal at <http://help.sap.com/netweaver> ► *SAP NetWeaver Platform* ► *<release>* ► *Application Help* ► *Function-Oriented View* ► *<language>* ► *Security* ► *User Authentication and Single Sign-On* ► *Integration in Single Sign-On (SSO) Environments* ► *Single Sign-On for Web-Based Access* ► *Using X.509 Client Certificates* ► *Using X.509 Client Certificates on the AS ABAP* ► *Configuring the System to Use the SAP Trust Center Service* ►.

3.3.3 Log On Using User ID and Password

Users log on to SAP Cloud solutions with their assigned user ID and password.

By default, a strong security policy for passwords is preconfigured in your solution, based on SAP's product security standard. You as an administrator can set an initial password and edit and create security policies according to the security requirements of your company.

For more information, see [Security Policy Quick Guide \[page 39\]](#).

If a user has forgotten the password, that person can request a new one by using the password self-service on the logon screen. A dialog box is displayed where the user has to enter the workplace e-mail address. Provided this workplace e-mail address has already been entered for corresponding employee or service agent in your solution, an e-mail containing a security code is sent to this e-mail address.

The system then displays a dialog box where the user can enter this security code. Note that the security code is only valid in this dialog box. If the security code has been entered correctly, the system generates a new temporary password with which the user can log on to the system. The system immediately displays another dialog box requiring the user to change this temporary password.

Password Security

We recommend that you implement some security parameters for password protection:

- Enforce strict password rules.
- Increase minimum requirement for password length, and encourage introduction of complexity.
- Validate password use and history to prevent repetition and reuse of same password.
- For administrative users, passwords should be at least 12 characters long.
- To reduce the risk of brute force attacks, keep the number of failed password attempts to less than five.

3.3.4 Creating a Security Certificate for HTTPS-Enabled Computer Telephony Integration (CTI)

You can enable HTTPS security for outbound phone calls made from your cloud solution. To fully enable this feature, you need to create a security certificate using the command line.

Prerequisites

To make outbound calls, you must have a CTI provider such as SAP Contact Center or an equivalent third-party product.

Context

After you complete this process, end-users will be able to call customers directly from the cloud solution without having to navigate another system.

Procedure

1. Enter the following into a command line prompt:

```
makecert -n "CN=CODCTI Authority" -cy authority -a t sha1 -sv "CODCTI_authority.pvk" -r "CODCTI_authority.cer" -sr localmachine -ss ROOT
```

Replace CODCTI with your company name.
2. Enter the following into a command line prompt:

```
makecert -n "CN=localhost" -ic "CODCTI_authority.cer" -iv "CODCTI_authority.pvk" -a sha1 -sky exchange -pe -sr localmachine -ss MY "codcti_adapter.cer"
```
3. Enter the following into a command line prompt:

```
netsh http add sslcert ipport=0.0.0.0:36731 certhash=0291c80612387afaee33f3589b4ab176c8d5336eappid={7346cd40-39c6-4813-b414-019ad22e55b2}
```

Results

In the step examples, *Certhash* is the thumbprint of the `codcti_adapter.cer`. You can look this up in the certificate. `Appid` is the appid of the CTI client adapter.

3.4 Security Policy Quick Guide

As an administrator, you can increase the security level, if desired, by editing and enhancing the security policy, for example, by changing the complexity and validity for all passwords, in accordance with your company's security requirements.

You can access the `Edit Security Policies` common task under **► Administrator ► Common Tasks ►**.

You can also define the length of time after which mobile users must reenter the app password to log on to the system from a mobile device and the maximum number of times in succession a user can enter an incorrect password before mobile app data is deleted from the mobile device as well as other properties regarding the complexity of the password.

You have the option of choosing a flag to enforce password change requested by the administrator. Navigate to **► Administrator ► Common Tasks ► Edit Security Policies ►**, and set the *Password Logon Enabled* toggle button to **Yes**. In the *Admin Password Change Enforcement* dropdown, you can choose *Enforce* or *Ignore*.

For more information about the app password, see [Secure System Access and Authentication \[page 54\]](#).

3.4.1 Business Background

A security policy is a set of rules that defines password complexity, such as including numerical digits and password validity, like requiring a password change after a certain period of time.

You can define multiple security policies because work areas or departments of a company may have different password security requirements.

3.4.2 Create a Security Policy

Procedure

1. To create a new security policy, click `Add Row`.
The system creates a new security policy and generates the associated policy ID.

i Note

To create a new security policy similar to an existing one, select an existing security policy and click `Copy`.

2. If necessary, change the `Policy ID`.
3. Enter a `Policy Name` and `Description` for the new security policy.
4. Save your changes.

3.4.3 Edit an Existing Security Policy

Use this procedure to edit an existing security policy.

Procedure

1. Choose the security policy you need to edit.

→ Remember

You cannot change policies that begin with `s_`. These are default security policies delivered by SAP.

2. Change the complexity and validity rules for passwords assigned to the security policy.
3. Save your changes.

→ Remember

If a user's password does not comply with the changed password rules, the user is prompted to change the password with the next system logon.

3.4.4 Assign Security Policies

You can assign a security policy to multiple business users at one time.

Procedure

1. In the Business User subview, click `Actions` and select `Assign Security Policy`.
2. Select one or more users that you need to assign a security policy to.
3. Click `Assign Business Role` and select the security policy that you would like to assign to the selected business users.
4. Click `OK` to save the assignment.

3.4.5 Define the Default Security Policy

When a business user is created, the system automatically assigns the default security policy to the business user.

Context

To define the default security policy, perform the following steps:

Procedure

1. In the `Default` column, set the check box for the security policy for the security policy you want to define as the default security policy.
2. Save your changes.

i Note

You can change the security policy assignment in the `Business Users` view. .

3.4.6 Delete an Existing Security Policy

Procedure

1. Choose the security policy you need to delete.

i Note

- If you have selected a security policy beginning with `S_`, the `Remove` button is deactivated, as the deletion of a default security policy delivered by SAP is not permitted.
- You cannot delete a security policy that is currently assigned to users.

2. Click `Remove`.
3. Save your changes.

3.5 Security Settings

As an administrator, you can define security settings that are applicable for all users, or a selected business role.

Auto Sign Out

For security reasons, users are automatically logged off of the system if they've been inactive in the system for a certain period of time. If you leave this option empty, inactive users will be logged off of the system after 1 hour.

You can set the auto logoff time for all users in your company. To do so, proceed as follows:

1. Navigate to the user menu, and click ► [Settings](#) ► [Company](#) ▾
2. Under *Define Settings* for, select one the following:
 - *Company*: To apply settings for all users
 - *Role*: To apply settings for a selected role.
3. In the *Auto sign out* tab, open the dropdown list, and select the preferred time duration when inactive users will be automatically logged off of the system.
4. Click *Save*.

i Note

This is currently only supported in browsers.

Certificate Pinning

Enabling the certificate pinning feature allows secure communication between the app. and the SAP Cloud for Customer server. Your administrator would have to enable the feature.

Enabling of IP/Username in performance logs

Allowing export of data sources/reports via APIs

Enabling Read access log

4 Authorizations

i Note

For access rights, you must maintain necessary authorizations.

i Note

Personalizing any part of the UI does not change/add any security settings, as this is part of extensibility which allows you to display/hide fields based on user/business roles, screen adaptations and so on. For Example: even if you remove the edit button from the UI, the edit option is still available via OData API's.

[Authorization Assignment \[page 43\]](#)

You can assign authorizations to each employee who has a user ID in your solution.

[Access Restriction \[page 44\]](#)

You can define whether a particular user has read or write access to data in a work center view.

[Segregation of Duties \[page 51\]](#)

If the user has been assigned to multiple work centers, your SAP Cloud solution checks whether the assigned views conflict with the segregation of duties.

4.1 Authorization Assignment

You can assign authorizations to each employee who has a user ID in your solution.

Employees are assigned to org units within organizational management. The assigned org unit determines the functions that the employee can use.

Based on these functions, work centers and work center views are proposed for the users. Some business processes require that a work center view can only be assigned together with one or more other work center views. If you as an administrator assign such a work center view to a user, then your solution automatically assigns these additional views to the user.

In SAP Cloud for Customer, you can enable partner contacts to access your SAP system by creating a user ID separate from employees in your solution. Partner contacts are service agents, being used to give external employees system access. Partner contacts should be assigned with their own business roles to maintain limited access to your SAP system.

⚠ Caution

Creating user IDs for your business partners will allow outside access to your system.

4.2 Access Restriction

You can define whether a particular user has read or write access to data in a work center view.

Your SAP Cloud solution provides the user with access to all of the business documents and Business Task Management items in that work center view.

You can restrict access to specific data on the basis of the access context assigned to the work center view in which the data appears.

⚠ Caution

It is important to be aware of the following dependencies when you assign work centers and views directly to users:

- Each work center view contains specific activities that can be carried out by a user with the necessary access rights for the view. When you assign a view or work center directly to a user, rather than assigning these through a business role, by default the user will have unrestricted read and write access to all the functions associated with the work center view.
- Additionally, in some cases the same activities can be carried out in multiple views. When you grant access rights, you should be aware that if there is a conflict, unrestricted access rights override any restrictions you have defined. For example, view A and view B both contain activity C. For view A, a user has unrestricted read and write access but for view B, the same user has read-only access. Because unrestricted access rights override restricted access rights, the user will actually have both read and write access to both views.

→ Recommendation

We recommend that you handle access rights by assigning business roles to users rather than by assigning work centers views directly to users. The advantages of assigning access rights through business roles are considerable:

- It eliminates the risk of a user accidentally having authorizations to read or edit data to which he or she should not have unrestricted access.
- There is much less maintenance effort involved when you have to edit access rights, for example, after an upgrade. You only have to edit the access rights associated with the business role and not the individual user's access rights.

4.2.1 Sales: Setting up User Access Rights and Restrictions

In SAP Cloud for Sales, the ability to grant and restrict authorizations is supported for most work center views, such as [Accounts](#), [Employees](#), [Products](#), [Activities](#), or [Opportunities](#).

Views are assigned through a work center to business roles. Authorizations for certain views can be restricted either to employees or territories associated to the specific item within a view, or through an assignment of the employee to an organizational unit.

Access Contexts and Restriction Rules

Access contexts bundle context-specific restriction rules that are assigned to various work center views and you as administrator can choose a business role level which restriction rule will be used for which view.

You will find a could of applicable restriction rules when you set at least the *Write Access* to *Restricted*.

For example:

- 1015: Employee or territory:
 - 1: Assigned territories or and employees (for managers)
This rule implies that data can be accessed through direct employee assignment independent of the employee role or through territory assignment. In case the rule applies to a manager, data is accessible through employee and territorial hierarchy.
 - 2: Assigned territories and employee of user
This rule implies that data can only be accessed through direct employee assignment independent of the employee role or through territory assignment.
 - 3: Assigned territories
This rule implies that data can only be accessed through territory assignment.
 - 99: Define specific restrictions
This rule should apply only if the above rules do not satisfy the access needs. Note that the restriction rule 99 likely requires the set up of different business roles.
- 2001: Business object product:
 - 1: Sales organization of user
This rule implies that data can be accessed through the organizational assignment of the employee.
 - 99: Define specific restrictions
This rule should only apply if the above rules do not satisfy the access needs. Note that the restriction rule 99 likely requires the set up of different business roles.

Access Context ID

Access context IDs are only appearing in the context of access rights on the business user level and you can find the IDs of employees, business users, org units, territories, and sales channels. The following objects and access context IDs are available:

- Employee: Employee ID
- Territories: Territory ID
- Org center: Org center ID
- Sales chain: Org center ID plus distribution channel

4.2.1.1 Sales: Setting up Business Roles and Users

Procedure

1. In the *Administrator* work center, choose **General Settings > Users > Business Roles** and create a business role. The business role defines a set of work centers and its associated views, including its restriction rules.
2. Assign work centers and views under *Work Center and View Assignments*. Select views applicable for the business role.

3. Under *Access Restrictions* restrict the access for the work center views as appropriate by setting at least the *Write Access* to *Restricted* or *No Access*. In case a view offers specific rules, you can select it from the *Restriction Rule* drop-down box.
If you like to have different rules for write and read access for the same view, you need to create two business roles with the same view assignment. One business role should get specific read access and write restriction to *No Access* and the second business role should get the same view with both read and write access.
4. Under *Fields & Actions* you can restrict the access for all extension fields and selected business fields and actions.
5. Save your work and choose **► Actions > Activate ►** to activate your role.
6. In the Administrator work center, choose **► Users > Employees ►** and create an employee. Note that you can create an employee only when you do not use external integration with, for example, SAP ERP.
7. Choose **► Users > Business Users ►** and open the created employee as a business user and choose **► Edit > Access Rights ►**.
8. Under *Business Role Assignment*, assign the created business role to the user.
Under *Access Restrictions* you can restrict the access on a user-level only if you haven't assigned a business role. For this, change at least the *Write Access* to *Restricted*. Now the restrictions on the *Detailed Restrictions* tab are changeable and you can change the access on the *Access Group ID* level. We recommend to restrict through the business role assignment only.
9. Save the changes.

Results

The authorization is set up for the corresponding business user.

4.2.1.2 Sales: Restricting Authorizations by Fields and Actions

Note that the value *Unrestricted* is only relevant if the a user is assigned to more than one business role.

If a business field occurs in one of the business roles with access restriction *Unrestricted*, then the user has no restriction even if there is another business role restricting the business field. If the business field does not occur in a business role, but is restricted in another business role, then the user is restricted accordingly.

4.2.1.3 Sales: Restricting Authorizations by Employees

By editing the access group ID *Employees*, you, as an administrator, can grant authorizations to employees to see items of their own, or of other employees.

Employees who have been granted the appropriate authorizations can see or update each item, as follows:

- Provided that they belong to the account team or territory team, meaning that they are directly or indirectly associated with an account by means of any role (including a customer-derived one). Authorized employees can view or updated accounts.
- Provided that they belong to the account team of an account that is associated with a contact, authorized employees can view or update contacts.
- Provided that they are assigned as an involved party or sales team in a document such as activity, lead, sales quote, or opportunity, authorized employees can view or update them.

i Note

Items for which no employee or territory has been assigned to can be accessed by all employees.

Within *User Management*, employees can be displayed either in simple list format or in the corresponding organizational hierarchy, which indicates the employees responsible for each organizational unit. You, as an administrator, can therefore choose to modify either the authorizations of the employee or of the employees who are assigned to the relevant organizational unit.

If you choose to modify authorizations in relation to a particular organizational unit, then the authorization changes will be applied to all employees who belong to that organizational unit, or to any subordinate unit. At a later date, you can also modify the authorizations of individual employees on this organizational unit, if desired.

4.2.1.4 Sales: Restricting Authorizations by Territories

Authorizations for employees, fields, and actions can also be restricted on the basis of the territory that it is automatically determined or maintained for that item.

i Note

Several territories can be assigned to an account at a given time.

By editing the access group ID *Territories*, you, as an administrator, can grant authorizations to the business users that are associated with the territories. If you modify the authorization of a business user in relation to a territory, then that user can view or update the items that are assigned to that territory, or to any corresponding territory.

For example, if you assign authorization to an employee to view or update items that are related to a certain territory, for example, the United States, then that employee can also view or update items that are related to subordinate territories, such as California or Florida.

4.2.1.5 Sales: Recommended Rules for Authorization Restrictions

To reduce the effort for the maintenance of authorizations, administrators should avoid using the specific restriction 99 within a particular access context.

The other access restrictions rules are binding for the overall master data, meaning that you do not need to need to change user restrictions seperately, or create new business roles. Rather, you, as an administrator, can

specify a restriction rule within a business role, and then assign that business role to multiple users. With this approach, authorizations are automatically derived from the existing master data.

i Note

If employee's organizational or territory assignment changes occur after the initial assignment of a restriction to a business role, then you, as a business administrator, must update your business users, to ensure that these changes are considered:

- Choose ► [Administrator](#) ► [Business Roles](#) ►.
- Find the relevant business role.
- Choose ► [Actions](#) ► [Update Business Users](#) ►.

Whenever you, as an administrator, maintain the authorizations of business users, we recommend you assign business roles to these users in concert with restriction rules.

Example: Using Restriction Rules in Access Context 1015

Access context 1015 ([Employee](#) or [Territory](#)) can be applied accounts, contacts, leads, sales leads, opportunities, and sales quotes. Two restriction rules, described below, are delivered for this access context:

- [Assigned Territories and Employees \(for Managers\)](#):
This restriction rule grants authorization for:
 - The employee him- or herself
 - All employees within the line of organization of the employee, if the employee is a manager
 - All territories to which the employee is assigned, and all territories beneath the employee
- [Assigned Territories and Employees of User](#)
This restriction rule grants authorization for:
 - The employee him- or herself
 - All territories to which the employee is assigned, and all subterritories beneath the employee

4.2.1.6 Sales: User Authorization Troubleshooting

This section describes authorization issues that you, as an administrator, may encounter, and how you can resolve them.

Authorization for a certain user has been restricted for a particular item, but the user can still view or edit the item.

This issue commonly occurs for the following reasons:

- No employee or territory is assigned to an account, lead, opportunity, activity, or sales quote.
- No sales organization is assigned to the product.
- Employee is not assigned to a sales org unit.
- The restricted item appears in two work center views, but you did not restrict the user's authorization in the same way in each view.

For example, if opportunities are not restricted under ► [Analysis](#) ► [Pipeline](#) ► and ► [Analysis](#) ► [Forecast](#) ► in the same way, then users who are restricted from seeing opportunities in the sales pipeline may nonetheless see opportunities in the forecast opportunity list, and vice versa.

The organizational or territory assignment of an employee or manager has changed, but the user cannot access the items that relate to the new assignment.

If master data changes occur, then you, as the administrator, must update your business users as follows:

1. Choose ► [Administrator](#) ► [Business Roles](#) ►.
2. Find the relevant business role.
3. Choose ► [Actions](#) ► [Update Business Users](#) ►.

This action is especially important if you change, for example, the managerial responsibility for organizational centers within the organizational hierarchy, or if you modify the assignment of employees to territories.

4.2.2 Service: Setting up User Access Rights and Restrictions

Allowing employees to edit tickets gives an employee the ability to engage with customers.

In SAP Cloud for Service, you can limit the employee access to tickets to ensure that only qualified employees engage with customers. You can limit the access of a single employee or group of employees. You can also limit access for partners and partner contacts.

It is recommended that you use roles to enable access restriction. Assigning access using roles allows you to create one set of access definitions that can be copied to multiple users.

4.2.2.1 Service: Defining User Access for a Group

Procedure

1. Create the organization that will contain the employees that you assign to this group.
2. After you have created the organization, create routing rules to define which tickets are assigned to the organization.
3. Create a role. A role contains permissions that are inherited by each employee assigned to the role.
 - a. In the [Access Restrictions](#) tab, restrict read and write access for [Tickets](#) and [Queue](#) in the [Assigned Work Center Views](#) list. Assign access rights to users according to your business needs.
 - b. To restrict employee access to the employee's organization, open the [Detailed Restrictions](#) list and ensure that the check boxes for [Read Access](#) and [Write Access](#) are checked only for the employee's organization.
 - c. To allow employees to read tickets in other organizations, open the [Detailed Restrictions](#) list and ensure that the [Read Access](#) and [Write Access](#) check boxes list are checked for the employee's organization. Select [Read Access](#) to allow the employee to read the tickets of the selected organization.
4. Assign the role to all applicable employees.

4.2.3 Restricting Access for Local Administrators

In a company with a global workforce, it is important to have administrators for global work tasks as well as local administrators that cover subsidiary tasks. Therefore, the company should have a few global administrators with expansive rights and many more local administrators with more restrictive rights.


Context

Additionally, these global and local administrators can edit access rights for business users by assigning business roles with local scope to the users.

→ Tip

Your company's headquarters are located in Paris and you have subsidiaries in Chicago, Tokyo, and New Delhi. If issues happen in the subsidiaries the workforce there can't wait until the administrators in Paris are working again because they are in different time zones. So it would be better if you can create roles for local administrators that are enabled to manage the local issues but without access to other data outside their local organization.

Procedure

1. As global administrator you need to generally restrict access of your local administrators for views they will be able to access and to assign them to the users of their sales organization. For this, select [▶ Administrator > General Settings > Users > Work Center View Restrictions for Local Administrators](#) . The views must either be *Allowed* or *Partially Allowed*. We recommend that you un-restrict at least the *Employees* and *Business Users* views.
2. Create a business role for the local administrators. The role for the local administrators should have all *Allowed* and *Partially Allowed* views that you defined in [Work Center View Restrictions for Local Administrators](#), and especially *Employees* and *Business Users*. Take care that the access for the *Employees* and *Business Users* views are restricted to the sales organization of the users.
Only business roles with the scope *Local* can be assigned to business users by local administrators. A business user is *Global*, if at least one view is either *Not Allowed* or *Partially Allowed*, but not restricted with a restriction rule (besides restriction rule 99).
3. Now you can create business roles for local administrators with the allowed and partially allowed views you defined in [Work Center View Restrictions for Local Administrators](#).
 - You can only create local roles for views that you defined in [Work Center View Restrictions for Local Administrators](#) view as *Partially Allowed* or *Allowed*. In case one view is marked as *Not Allowed*, the role isn't visible for the local administrator.
 - Local administrators are disabled to assign global roles to local business users.
 - If you un-restrict a view in [Access Restrictions](#) that is set as *Partially Allowed* in [Work Center View Restrictions for Local Administrators](#), the entire role switches to *Global* and disappears for the local administrator.
 - Local administrators can only use roles with scope *Local*.

4. On the *Fields & Actions* tab of your local administrator role, under *Business Restrictions*, you can also restrict that the local administrator can be the only one to edit access rights or attributes of other users.

4.3 Segregation of Duties

If the user has been assigned to multiple work centers, your SAP Cloud solution checks whether the assigned views conflict with the segregation of duties.

Segregation of duties is designed to minimize the risk of errors and fraud, and to protect company assets, such as data or inventories.

The appropriate assignment of access rights distributes the responsibility for business processes and procedures among several users.

For example, suppose that your company requires that two employees be responsible for the payment process. This requirement ensures that the responsibility for managing company finances is shared by two employees.

A segregation of duties conflict occurs when a user has access to a set of work center views that could enable him or her to make an error or commit fraud, thereby damaging company assets. If the application detects a conflict, it indicates that conflict in the user interface and proposes possible solutions.

Based on this information, you can alert business process owners to existing conflicts, so that they can implement process controls to mitigate them.

5 Mobile Devices

With the SAP Cloud mobile solutions, you can access many of the functions that have been tailored to business on-the-run.

Changes made on mobile apps are automatically updated in the system over the internet, online, and in real time. Mobile solutions connect to the SAP Cloud solution in the same way as personal computers do.

The following table provides information about the mobile devices on which you can run SAP Cloud solutions:

Supported Mobile devices:

Device/Operating System	Supported
iPhone/iPad	X
Android	X
Windows Tablet	X
Windows Phone	X

Offline Support

SAP Cloud Solution	iPad/iPhone	Android Tablet/Phone	Windows Tablet
Offline Support	X	X	X

[SAML2 Based SSO \[page 53\]](#)

List of SAML2 based SSO supported mobile devices.

[SSO Recommendation \[page 53\]](#)

The following is our recommendation for the users.

[Authorizations \[page 53\]](#)

When you use SAP Cloud mobile solutions, you use the same URL address and logon credentials as for desktop applications.

[Secure System Access and Authentication \[page 54\]](#)

Access from mobile devices is enabled by connecting to the back-end system using HTTPS and the same user and password authentication used for connection from a personal computer.

[Special Considerations \[page 55\]](#)

Unlike stationary personal computers, mobile devices are at greater risk of being lost or stolen. Therefore, we recommend that you use the security features provided by your mobile device platform.

[Data Storage \[page 55\]](#)

This section describes the types of data stored on the mobile device.

[Offline Mode \[page 59\]](#)

For working offline, data is stored on the device and encrypted.

5.1 SAML2 Based SSO

List of SAML2 based SSO supported mobile devices.

The following devices support the SAP Cloud for Customer hybrid apps with SAML2 based SSO:

Hybrid Apps

- SAP Cloud for Customer, extended edition for Android
- SAP Cloud for Customer, extended edition for iOS
- SAP Cloud for Customer, extended edition for Windows

Supported Devices

- Apple (iPhone and iPad)
- Android (Phone and Tablet)
- Microsoft Windows (Phone and Tablet)

→ Recommendation

For set up information, refer to [Log on Using SAML 2.0 Assertion for Front-End Single Sign-On \(SSO\) \[page 32\]](#).

5.2 SSO Recommendation

The following is our recommendation for the users.

For the Single Sign On (SSO) option we recommend disabling the username and password access. However, ensure that you maintain updated and accurate e-mail addresses for the users, as this is required in case of a problem with the Single Sign On. The username and password options could be used as a fallback. Administrators might have to send out initial passwords or users would have to reset password via self-service. Both options require updated, correct e-mail addresses.

5.3 Authorizations

When you use SAP Cloud mobile solutions, you use the same URL address and logon credentials as for desktop applications.

Ensure that for each mobile work center view to be accessed on a mobile device, the user of the mobile device is assigned the related desktop work center view.

5.4 Secure System Access and Authentication

Access from mobile devices is enabled by connecting to the back-end system using HTTPS and the same user and password authentication used for connection from a personal computer.

i Note

SAP Cloud for Customer solution now supports certificate pinning in the extended edition for the following apps:

- iOS apps
- Android apps

5.4.1 SAP Cloud for Customer for Android

Android Credential Storage requires maintaining secure settings on the screen lock feature.

For SAP Cloud for Customer, extended edition for Android, it is mandatory for the user to have a screen lock to be able to use the application. The application uses the Android Credential Storage to securely store sensitive information and this requires the user to enable the screen lock.

Administrators can enforce this policy if the device is managed under *MDM*, otherwise, they have to inform the users that a screen lock is mandatory. Earlier, it was possible for a user to create a logon profile, login and work normally with the app. With 1811 the app can be installed but no logon profile can be created if the screen lock is not enabled.

⚠ Caution

Removing the screen lock will result in data loss (logon profiles will have to be re-created; unsynced offline data will be lost).

5.4.2 Certificate Pinning

Enabling the certificate pinning feature allows secure communication between the app. and the SAP Cloud for Customer server. Your administrator would have to enable the feature.

Go to ► *Administrator* ► *General Settings* ► *Mobile Settings* ► and in the *Certificate Pinning* field, select *Activate*.

With the feature enabled, users cannot communicate with our server with a false or forged certificate. However, the feature is disabled by default, but customers have the option to enable it via mobile configuration. When you enable the feature, the mobile application performs the check.

i Note

For our forthcoming releases, we will enable the certificate pinning feature by default.

5.5 Special Considerations

Unlike stationary personal computers, mobile devices are at greater risk of being lost or stolen. Therefore, we recommend that you use the security features provided by your mobile device platform.

For example:

- Use an additional, sufficiently long, PIN (personal identification number) to lock the device.
- Enable remote management software that allows you to lock the device remotely, or wipe data from it.

Stored data may contain potentially sensitive information. Ensure adequate protection for your business data by using a strong password for device access. As an additional security measure, the stored data is also encrypted with a Passcode.

The Passcode has a minimum length of 8 characters, with a longer length making for a stronger password.

The Passcode feature is available only for Mobile apps.

Caution

Currently, when you edit the security policy for the extended apps, the *Mobile App Password Complexity* settings are not considered. The mobile app password, known as passcode has to comply to a fixed complexity rule defined by the extended app .

For information on how to operate your mobile device, refer to the device manufacturer's documentation.

5.6 Data Storage




This section describes the types of data stored on the mobile device.

The mobile apps for SAP Cloud solutions store three types of data on the mobile device, as outlined below.

User Name

On providing the login information, the user name will be masked to ensure the user's security. Refer to the screen shots below:



●●○○○ Verizon  1:53 PM    

System URL	User Name	Language
https://my300900.crm.ondemand.com	a*****h	EN
https://vf4-cust233.dev.sapbydesign.com	m*****y	EN
https://vf4-cust233.dev.sapbydesign.com	f***** **1	EN
https://a6p-cust220.dev.sapbydesign.com	c****s	EN
https://my306164.crm.ondemand.com	c*****a	EN
https://qxl-cust233.dev.sapbydesign.com	j*****l	EN



SAP Hybris Cloud for Customer

https://qxl-cust233.dev.sapbydesign.com | j***** | EN

●●●●●●●●

Logon

Manage Logon Profiles

Change Passcode

[Forgot your Passcode?](#)

Passcode

The passcode feature applies to the extended apps only, and is turned on by default. It is possible to enable Touch ID as an alternative option for passcode if the device supports iOS and Android apps. However, the administrator has the ability to disable the passcode for the user. The administrator can make this change in the administration settings area of the solution. Refer to the *Administrator Guide* for more details on how to do this.

i Note

SAP recommends having a device passcode in place for security reasons. The administrator has the ability to make this feature optional for users.

Encryption

We recommend you keep the devices and apps as secure as possible by encrypting all data. However, if the customer wants to increase the usability they need to be aware of the risk and must ensure there are other protections (for example: strong device lock) in place.

All extended apps use *AES 256* encryption to protect the offline data storage. The only exception are the Android devices, where the device pin has to be enabled to enable encryption.

[Support Log Files \[page 58\]](#)

To obtain support for a technical error within the mobile app, you may be requested to activate the app's error-logging functionality. When error logging is active and the technical error is reproduced, files containing technical data are created. These files enable SAP Cloud Support representatives to resolve the error. Delete the log files once they are no longer required.

[Cache Files \[page 59\]](#)

To improve the mobile app's performance, metadata is stored on your mobile device. The cached information contains technical data that describes the user interface. The cache files can be deleted.

[Local Application Data Storage \[page 59\]](#)

SAP Cloud for Customer supports local application data storage.

5.6.1 Support Log Files

To obtain support for a technical error within the mobile app, you may be requested to activate the app's error-logging functionality. When error logging is active and the technical error is reproduced, files containing technical data are created. These files enable SAP Cloud Support representatives to resolve the error. Delete the log files once they are no longer required.

5.6.2 Cache Files

To improve the mobile app's performance, metadata is stored on your mobile device. The cached information contains technical data that describes the user interface. The cache files can be deleted.

For device-specific instructions on how to set the password expiration, enable logging, or delete logs and cache files, refer to the mobile app's documentation.

It is sometimes possible to upload pictures and other files from the mobile device to the SAP Cloud solution, for example, pictures captured on a mobile phone's camera. Such files are not managed through the SAP mobile app. When files are uploaded to the solution, they are not deleted from the mobile device. To protect any sensitive or confidential data that such files may contain, we recommend that you take extra precautions appropriate for the specific mobile device in use. For more information, see the device manufacturer's documentation.

For device-specific instructions on how to set the password expiration, enable logging, or delete logs and cache files, refer to the mobile app's documentation.

You can upload pictures and other files from the mobile device to the SAP Cloud solution, for example, pictures captured on a mobile phone's camera. Such files are not managed through the SAP mobile app. When files are uploaded to the solution, they are not deleted from the mobile device. To protect any sensitive or confidential data that such files may contain, we recommend that you take extra precautions appropriate for the specific mobile device in use. For information on how such files are secured and stored on your mobile device, refer to the device manufacturer's documentation.

5.6.3 Local Application Data Storage

SAP Cloud for Customer supports local application data storage.

To enable this, start the app and setup passcode, and enter system URL, username and password. During the setup, the user has to enter a passcode that is different from the system password. The local application data has been encrypted with a key derived from the app password. Authentication is required to switch between online and offline mode

5.7 Offline Mode

For working offline, data is stored on the device and encrypted.

For mobile apps, once the device is online, data is sent to the back-end system and synchronized from the mobile device.

When you set up a passcode for container apps for storing data in the offline mode, remember the following points:

- The passcode should be at least eight characters long.
- There must be at least one numeral and one uppercase alphabet.
- You are allowed upto a maximum of eight failed attempts to logon. After which, you will need to reset the passcode that will delete all information from the database.

i Note

If you disable the device pin on an Android device, then the offline encryption is also disabled.

6 Front-End Security

The SAP Cloud solutions front ends consist of Web application user interfaces that support the following features:

- X-Frame-options response header to avoid clickjacking attacks
- Cross-site request forgery (CSRF) protection
- Cross-site scripting (XSS) output encoding during SAP UI5 rendering
- UI and domain protection against URL mashups and content mashups in iFrames
- Secure socket layer (SSL) transport layer encryption using HTTPS
- Access to business data only after authentication and with sufficient authorizations using identity management and Role-Based Access Management (RBAM)
- Cross-site-scripting counter measures

7 Security of Data Storage and Data Centers

The data centers that support SAP Cloud solutions incorporate multiple safeguards for physical data security and integrity. They also provide high availability of your business data, using redundant networks and power systems.

7.1 Asset Protection and Data Integrity

SAP follows operating best practices for data centers by deploying computation and storage parts of the solution over separated fire-safe areas to support disaster recovery in the event of a fire.

For data backup and recovery purposes, a redundant hardware storage system performs regular backups. To provide enhanced data integrity, your SAP Cloud solution uses an advanced database management solution to store customer data and securely isolate each customer's business information in its own database instance.

7.2 Communication Security

SAP relies on encryption technology that uses HTTPS to prevent unauthorized parties from intercepting network traffic. The encryption is based on the Transport Layer Security (TLS) protocol. The required encryption software is a standard component of up-to-date client operating systems and Web browsers.

7.3 Data Storage

All storage devices use *AES 256* encryption to protect data at rest. Current and backup data is covered by encryption.

7.4 Network Security

The network for your SAP Cloud solution employs a number of security technologies. The multilayered, partitioned, proprietary network architecture permits only authorized access to the data centers that support your SAP Cloud solution, with features that include:

- A Web dispatcher farm that hides the network topology from the outside world
- Multiple Internet connections to minimize the impact of distributed denial-of-service (DDoS) attacks
- An advanced intrusion detection system that continuously monitors solution traffic for possible attacks
- Multiple firewalls that divide the network into protected segments and shield the internal network from unauthorized Internet traffic
- Third-party audits performed throughout the year to support early detection of any newly introduced security issues

7.5 Power Backup and Redundancy

SAP data centers maintain multiple connections to several power companies, making a complete power outage highly unlikely. Even if the local power grid were to fail, the data centers supporting your SAP Cloud solution have an uninterruptible power supply for short-term outages, and a diesel generator backup power supply for longer-term outages. Therefore, power interruptions or outages are unlikely to affect customer data or solution access.

7.6 Restricted Physical Access

SAP data centers, located in the United States of America and Germany, are logically separated and staffed around the clock, 365 days a year. A biometrics security system permits access only to authorized personnel, and the data centers are partitioned such that authorized personnel can access only their designated areas. Moreover, no direct network connection exists between individual SAP data centers; each SAP data center is fully autonomous.

8 Security for Additional Applications

SAP offers a set of additional software components that you can install, on desktop computers, for printing and additional functionality.

Confirm the Signature

All additional applications of SAP Cloud solutions that are delivered for download are digitally signed. To confirm the signature, proceed as follows:

1. Right-click on the file you have downloaded, then choose *Properties*.
2. In the dialog box, choose the *Digital Signatures* tab.
3. Confirm that the indicated *Name of signer* is SAP AG.

When you execute the installation of a file, a popup appears, indicating the *Verified publisher*. In this case, SAP AG is indicated as well.

Saving Logon Data

SAP front-end components never share an existing authentication session on SAP Cloud solutions, for example, within a Web browser or with another front-end component. Dedicated authentication is always required to build a confidential communication channel, secured via the Secure Sockets Layer (SSL) protocol, to your SAP Cloud solution.

If you log on to the system from a desktop computer with a user ID and password, you are asked whether you want to store the password locally for subsequent authentication purposes. The password is encrypted, and not stored as plain text. It is stored using the available protection mechanisms of the operating system, and can be reused only by the operating system user who is currently logged on. If you do elect to use this function, then you should activate it on your device only, and never on public computers.

9 Other Security-Relevant Information

[Security for End-User Devices \[page 65\]](#)

Security recommendations for end-user devices such as PCs, and laptops for windows and apple products.

[Service Composition Security \[page 66\]](#)

This section describes security considerations that apply to the built-in mashups integration and web services composition capabilities of SAP Cloud Solutions.

[Security Management and Continual Improvement of Security \[page 68\]](#)

Security Management at SAP Cloud for Customer aims towards the continual improvement of the information security framework.

9.1 Security for End-User Devices

Security recommendations for end-user devices such as PCs, and laptops for windows and apple products.

Since you can download data to your local devices, it's important that you follow strict security protocols to protect your data from getting compromised.

SAP Cloud for Customer offers many data-extraction features such as Data Workbench, OData APIs, Microsoft Excel downloads, and so on.

Caution

We strongly recommend that you use secure protocols to prevent security breaches of confidential data.

We recommend:

- Protect user accounts with strong passwords.
- Enable and activate whole disk encryption to protect the data in case your machine gets lost/stolen.
- Keep operating system software, virus checkers, browsers, and other applications current, and ensure available security patches are deployed.

Related Information

[File and Attachment Processing \[page 23\]](#)

9.2 Service Composition Security

This section describes security considerations that apply to the built-in mashups integration and web services composition capabilities of SAP Cloud Solutions.

Mashups and service composition entail cross-domain communication between various internet domains.

Content from different domains – especially active content, such as JavaScript – is always domain-separated in the Web browser.

A same origin security policy common in Web browsers, prohibiting access to content across domain separations, is activated, if necessary.

9.2.1 URL Mashup Integration

Both partners and administrators can create URL mashups to perform the following tasks:

- Open a Web page.
- Open a resource, for example, a Microsoft® Office or Adobe® PDF document, an Adobe® Flash® or multimedia video file, and so on.
- Open a custom URL of a front-end application, for example, Microsoft® Outlook®, Apple iTunes®, and so on.

You can open these items from an SAP Cloud solution screen by configuring the URL with dynamic parameters that are derived from the screen out-port interface of your SAP Cloud solution.

⚠ Caution

Some URLs may pass your business data to an external application provided by a third-party organization, for example, account data passed to a search engine when performing a reverse lookup in an online address book. Therefore, before you use the URL mashup, we recommend that you confirm that it conforms with your company's security and data privacy policies.

Some Web browser settings, for example, popup blockers, may prevent the new browser window from appearing in the URL mashup. We therefore recommend that you review your browser settings to determine whether popups are allowed.

9.2.2 HTML Mashup Integration

Both partners and administrators can create HTML mashups to embed an HTML-based Web page or a resource that can be rendered in a Web browser – for example, a Microsoft Office or Adobe PDF document, or an Adobe Flash or multimedia video file – into an SAP Cloud solution screen by configuring the URL with dynamic parameters that are derived from the SAP Cloud solution screen out-port interface.

⚠ Caution

Certain URLs may pass your business data to an external application provided by a third-party organization, for example, account or contact data passed to a social media Web site when displaying the

related profile. Therefore, before you use the map mashup, we recommend that you confirm that it conforms with your company's security and data privacy policies.

Bing Maps Web service communication takes place directly between the user's Web browser and the service provider via the Secure Sockets Layer (SSL), with the dedicated API key applied for each SAP Cloud solution. Bear in mind that the Bing Map Web service provider may monitor the Bing Maps Web service API usage in accordance with the terms of licensing. Therefore, before you use the map mashup, we recommend that you review the API usage and licensing details with the Bing Maps Web service provider.

9.2.3 Map Mashup Integration

SAP Cloud solutions use Microsoft® Bing Maps™ as a built-in map service provider. Both administrators and end users can configure the map mashup usage on an SAP Cloud solution screen to display the visual location or route information on a map. Before Bing Maps mashups can be used, you as an administrator must activate them by entering the Application Programming Interface (API) key for Bing Maps usage under ► [Administrator Mashup Authoring](#) ▾. For more information about the Bing Maps Web service partner, and to apply for an API key, visit the SAP Cloud solutions communities.

⚠ Caution

Bear in mind that the map mashup may convey business data of yours to the Bing Maps Web service provider. For example, ship-to and bill-to addresses are transferred to the Bing Maps Web service provider when displaying the related visual location on the map. Therefore, before you use the map mashup, we recommend that you confirm that it conforms with your company's security and data privacy policies.

Bing Maps Web service communication takes place directly between the user's Web browser and the service provider via the Secure Sockets Layer (SSL), with the dedicated API key applied for each SAP Cloud solution. Bear in mind that the Bing Map Web service provider may monitor the Bing Maps Web service API usage in accordance with the terms of licensing. Therefore, before you use the map mashup, we recommend that you review the API usage and licensing details with the Bing Maps Web service provider.

9.2.4 Data Mashups

Both partners and administrators can create data mashups for composing Web services (provided by third-party Web service providers) with business data derived from the SAP Cloud solutions. You can use the integrated authoring tool, the Data Mashup Builder, to transform or merge external Web services with internal business data, using industry-standard Web service protocols, for example, RSS/Atom, REST or SOAP Web services.

Create Web services in your SAP Cloud solution before creating the Web service composition in the Data Mashup Builder. API keys can be specified for the Web service security by means of industry-standard or Web service specific authentication methods, for example, basic authentication, REST body credentials, or SOAP service parameter credentials. The API keys entered by partners and administrators are stored in an isolated secure storage of the your SAP Cloud solution back end, which is never exposed to end users.

⚠ Caution

Certain Web services may transfer business data of yours to an external Web service provider from a third-party organization. For example, account or address data is transferred to a data quality Web service provider when data quality cleansing operations in Cloud applications are performed. Therefore, before you use the mashup, we recommend that you confirm that the Web service conforms to your company's security and data privacy policies.

Web service communication in data mashups does not take place directly between the user's Web browser and the Web service provider. Rather, as a result of the cross-domain access policy restriction, it is tunneled using the SAP Cloud solution system back-end Web service proxy. Only the Web service endpoints that have been confirmed with acknowledgement by partners and administrators can be accessed by the SAP Cloud solution system back-end Web service proxy by all end users of a customer. Therefore, before you confirm that a Web service is added to your SAP Cloud solution, we recommend that you ensure that it conforms to your company's and country's security policies.

9.3 Security Management and Continual Improvement of Security

Security Management at SAP Cloud for Customer aims towards the continual improvement of the information security framework.

Compliance

SAP conducts several external audits every year for various certificates and attestations such as ISO, C5, SOC, and so on.

You can find the current list of certifications in [SAP Trust Center](#) under the *Compliance* tab. Filter with **SAP Cloud for Customer** to find the right compliance documents for your business needs including certifications, attestations, and SOC reports.

Penetration Tests and Vulnerability Scans

SAP conducts external penetration tests for product and infrastructure at least once a year. In addition, a number of internal tests and security validations are performed by dedicated teams throughout the year.

Vulnerability scans with internal and external scope are performed on an ongoing basis.

You can find more details about scope and frequencies in the SOC2/C5 reports.

Code Scans

The complete code base is covered with static code scans. For the non-ABAP code base, SAP carries out additional checks to look for open source vulnerabilities and ensures license compliance. Used open source components are monitored for newly disclosed vulnerabilities.

10 Data Protection and Privacy

Use the [Data Protection and Privacy](#) work center to manage personal and sensitive personal data of employees, individual customers, and contacts. As an employee responsible for data protection and privacy regulation compliance in an organization, you can use the work center to disclose as well as remove data on request.

Data processing systems store master data or transactional data used to perform business processes and to document them. In many cases, it involves the personal data of employees, individual customers, and contacts. In many countries, the storage, disclosure, and removal of such personal data from data storage systems must be in accordance with statutory data protection laws. One requirement in many countries is that the personal data can only be stored if a clear business reason for this data retention exists. Most data protection legislation proscribes fixed retention periods, defining how long data can be stored in data systems, after which it must be deleted. In addition, legislation in many countries stipulates that the data protection officer must disclose the personal data of individuals, when they expressly request it.

The [Data Protection and Privacy](#) work center allows those responsible for data protection functions in an organization to respond to requests to fulfill the following requirements:

- Disclose personal data for all employees, individual customers, and contacts.
- Remove personal data once the retention period for all relevant data is expired.
- Monitor and manage background data removal processes using an application log.
- Display log data detailing each access made to the [Personal Data Disclosure](#) and [Personal Data Removal](#) overview screens containing personal data.

i Note

In this document, employees, individual customers, and contacts are collectively referred to as business partners.

Features

There are a number of key features of Data Protection and Privacy in SAP Cloud for Customer. These are outlined as follows:

Data Disclosure — Obligation to Disclose

A key principle in data protection and privacy is the Obligation to Disclose. This is an obligation set in legislation in many countries where data protection regulation has been adopted. As an administrator responsible for data protection regulation compliance, you can disclose personal data of employees, individual customers, and contacts. You can display a summary of all data associated with these business partners stored in the SAP Cloud for Customer system. You can also access the detailed records.

Data Removal — Deletion on Request

This second data protection and privacy principle refers to the requirement of organizations to delete personal data held on its business partners that is kept in an identifiable form, and retain this data for no longer than necessary. Where specified, organizations must delete all such personal data after the relevant data retention period has elapsed.

Read Access Logging

Certain categories of personal data are considered sensitive due to their criticality and importance. You can activate tracking of read access to such personal data. You have to carefully review the groups of such personal data available and activate read access logging for those groups which are processed by your organization. In the SAP Cloud for Customer, you can also add custom fields and mark them for read access logging.

Change Log for Personal Data

A log is created whenever there is a change in personal data. You can view the change records for a specific business object in the respective *Changes* tab.

If you are an administrator, you can restrict access to the change logs by removing access to the *Changes* tab for regular users. You can then create a new layout that includes the *Changes* tab and assign this layout to authorized users.

The change logs are not available via regular APIs. They can only be exported using a specific API accessible to users with data protection and privacy related authorizations.

A change log is removed only when an object is completely depersonalized. This means that a log remains unchanged even if personal data is removed from an active object.

Data Protection Roles

In large organizations, employees with the designated role (Data Protection Officer, for example) are responsible for ensuring that data protection and privacy principles are followed, and that the organization complies with all data protection and privacy legislation in force within the country (or countries) it operates. However, these tasks can be delegated to other authorized employees, for example, designated Human Resources administrators.

Authorization

The *Data Protection and Privacy* work center is only available to authorized employees or Data Privacy officers in your organization. It is therefore strongly recommended this work center assignment is only given to those employees directly responsible for data protection and privacy regulation compliance in your organization.

Usage Block

This is the point in time for a data set when the processing of personal data is no longer required for the primary business purpose. After the End of Purpose has been reached, the data is blocked and can only be accessed by users with special authorization, for example, tax auditors. In SAP Cloud for Customer, we have the following solution:

- You can set a business process to end-of-purpose via an API call, which helps support integration. It prevents the business process from displaying value helps, so you cannot use it to create new transactions. There is however no standard access restriction. Any user can still search for the business process and open it.
- You can delete or depersonalize data. If the data is still required for later audits, you can export it using the OData APIs.

i Note

Employees, such as Data Protection officers with responsibility for data protection have full access rights for the *Data Protection and Privacy* work center. These access rights allow an authorized user to access personal data for the selected business partner in all SAP Cloud for Customer work centers where such data exists. Because of the ability for an individual user to access large volumes of personal employee data across many work centers, the access log is provided to allow transparency and traceability of user access

to personal data. The log does not contain detailed personal data, but rather a summary of the types of data accessed, when, and by whom it was accessed.

10.1 Disclose Personal Data

Disclose personal data of employees, individual customers, and contacts in the [Data Protection and Privacy](#) work center.

As an administrator responsible for data protection regulation compliance, you can disclose personal data of employees, individual customers, and contact. You can display a summary of all data associated with these business partners stored in the SAP Cloud for Customer system. You can also access the detailed records.

i Note

In this document, employees, individual customers, and contacts are collectively referred to as business partners.

Procedure

1. In the [Data Protection and Privacy](#) work center, open the [Personal Data Disclosure](#) view.
2. To display the disclosure-relevant data for employees, individual customers, and contacts, select the relevant option from the dropdown. For example: If you want to disclose an employee's data, select [All Employees](#).
3. Select the desired business partner from the list and click [Disclose Data](#). A new overview screen opens that displays all the disclosed data for the selected business partner.

i Note

Before the overview screen is loaded, a dialog box appears informing you that your access to this screen is logged. Confirm this message to proceed.

4. Click [Expand all](#) to view all individual records that are to be disclosed. Click the expand and collapse triangle icons to view individual data record summaries for the selected entity.
5. Click the links for the individual records, for example, [General Data](#) or transactional data, such as [Leads](#) or [Opportunities](#), to navigate to the actual data record held in the SAP Cloud for Customer system.

i Note

The figure shown in the [Records](#) column represents the number of discreet data records (for example, Sales Orders) of the selected type assigned to the employee in the SAP Cloud for Customer system. A zero indicates that no records of this type exist for the selected employee.

6. Click [Close](#) to return to the [Personal Data Disclosure](#) view.

You have successfully extracted a summary of all personal data required for disclosure to an individual who requests it.

i Note

In addition to the above, you can use the following methods for data disclosure:

- **Data workbench:** If you want to disclose more personal details, you can use the data workbench to export full datasets for employees and contacts of individual customers. The data workbench export functions allows you to specify one or more persons to be processed. It also allows you to select the fields you would like to export, for example, ignore technical IDs, don't export business addresses. For more information, see
- **OData APIs:** You can use APIs to build custom processes to export exactly what you need for your use cases, including all the personal data of the business partner, linked transactions, and other related data. The APIs can be called using custom logic, from excel spreadsheets, and so on. For more details, see [SAP Cloud for Customer OData API v2 Reference](#)

10.2 Remove Personal Data

Delete personal data of employees, individual customers, and contacts on their request in the [Data Protection and Privacy](#) work center.

Once the end of purpose has been reached for personal data (e.g. business partners, transactions), it has to be removed. SAP Cloud for Customer offers business partner driven removal (this will delete the person and all the related data/transactions), or transaction driven removal (this targets individual transactions that are no longer needed).

It is now possible for you, as an administrator responsible for data protection regulation compliance, to delete personal data of employees, individual customers, and contacts on their request, at a time in the [Personal Data Removal](#) view of the [Data Protection and Privacy](#) work center.

i Note

In this document, employees, individual customers, and contacts are collectively referred to as business partners.

Prerequisite

You have defined the retention periods relevant for your country/region in your system configuration. Navigate to [Business Configuration](#) > [Overview](#) and search for the following fine-tuning activities:

- [Data Retention Rule for Employees](#)
If you configure this activity, the system runs a query for the employee validity dates. It then checks these validity dates against the retention period configuration, which is similar to private accounts, sales orders and quotes that raise vetoes. It also checks if any sales order or sales quote exists against the retention period configuration, and then proceeds with the data removal process.
- [Data Retention Rule for Private Accounts](#)

If you configure this activity, the system checks if any sales order or sales quote exists against the retention period configuration. If yes, the system uses the validity period end date for sales quotes and the last change date for sales orders to check the data retention period.

Additionally, you can also delete private accounts if sales orders and sales quotes are depersonalized.

Note that even if there is no retention period setup for contacts, they can only be removed if linked sales quotes or sales orders are in status **Complete**.

i Note

Users with authorization to access the [Data Protection and Privacy](#) work center can perform all data protection and privacy functions within this work center, including the disclosure and deletion of personal data. Access to this work center is granted in the [Administrator](#) work center. Ensure that only employees with authorization to disclose or delete personal data are granted access to the [Data Protection and Privacy](#) work center.

Procedure

1. In the [Data Protection and Privacy](#) work center, open the [Personal Data Removal](#) view.
2. To display data for removal of employees, individual customers, and contacts, select the relevant option from the drop-down. For example: If you want to remove an employee's data, select [All Employees](#). If you want to delete the data for multiple employees, click the **Show Advanced Filter** icon. In the [Employee ID](#) field, click the **More Options** icon. In the [Employee ID](#) dialog box that opens, enter the employee IDs or employee names in the [Value](#) field and click [Go](#).

⚠ Caution

If there is a legal requirement to keep a business partner information in the system, click [Block Removal](#) to block the entity from being depersonalized. Click [Unblock Removal](#) once the blocking need no longer exists.

When a business partner is blocked for removal, it is not possible to trigger a personal data removal run from the [Data Protection and Privacy](#) work center. During scoping, you can prevent the deletion of transactions that are assigned to a blocked business partner. To enable this option, navigate to

▮ [Business Configuration](#) > [Implementation Projects](#) ▮. Select your project and navigate to ▮ [Edit Project Scope](#) > [Questions](#) > [Built-in Services and Support](#) > [System Management](#) > [Security](#) > [Data Privacy](#) ▮ and select the related option.

3. Select the desired business partner from the list and click [Remove Data](#). A new overview screen opens that displays all the data that can be deleted.
4. To delete personal data of individual customers, and contacts, click [Delete](#).
To delete employee data, follow these steps:
 1. Select the [Marked for Deletion](#) checkbox for each work agreement (and associated documents) and availability calendars you wish to set for later removal from the system
 2. Click [Delete](#) to trigger the removal of all work agreements, availability calendars, and associated application data marked for deletion from your system.
 3. Confirm that you still wish to continue with this irreversible deletion of the selected records. If you are removing the last remaining work agreement held for an employee, the system warns you that continuing with this process removes the employee record from the SAP Cloud for Customer system.

4. Confirm that you wish to continue with the removal or cancel it.
After clicking *Delete* for all records marked for deletion, the *Marked for Deletion* checkbox is disabled, while the remainder of the removal process is performed by the system in the background. After the deletion process is successfully completed, for the affected work agreements, the *Marked for Deletion* checkbox is disabled and *Retention Period Completion* status changes to *No* or *No available data*. The start dates for these records also change .
5. Click *Close* to return to the *Personal Data Removal* screen.

i Note

- The data removal process is local in Cloud for Customer and is not replicated to any external system such as SAP CRM, SAP S/4HANA, or SAP ERP. In an integrated landscape we presume that the back end systems are the leading system which governs the life cycle of the customer record because the back end solution ideally has financial documents such as invoices.
As an alternative you can mark the customer record as obsolete and let the automated removal run take care of triggering the removal. Once you mark the records as obsolete, the change is replicated to the connected systems where each of these systems handle the customer records locally.
- If an individual account is deleted, all appearances in any party role for this instance in transactional documents are depersonalized unless it is blocked for deletion.
- In addition, removal of employees and contact persons lead to different results for different transactions. For example, activities might be deleted completely, but other transactions have their descriptions removed or scrambled, or attachments deleted. During scoping, you can choose to retain the transactional data that are assigned to contacts and employees. To enable this option, navigate to [▶ Business Configuration ▶ Implementation Projects ▶](#). Select your project and navigate to [▶ Edit Project Scope ▶ Questions ▶ Built-in Services and Support ▶ System Management ▶ Security ▶ Data Privacy ▶](#) and select the following question: *During personal data removal, do you want to retain the transactional data and remove only the personal data of contacts and employees?*

Result

You have successfully removed all work agreements (and associated application data) and availability calendars from the system for the selected unblocked entities. You can verify this removal by starting the *Administer Data Removal Runs* common task, and selecting *Successful Removal Runs* in the *Show* field.

Your access to the data removal overview has been logged.

i Note

In addition to the above, you can use the following methods for data removal:

- **Data workbench:** If you want to remove more personal details, you can use the data workbench to export full datasets for employees and contacts of individual customers. The data workbench export functions allows you to specify one or more persons to be processed. It also allows you to select the fields you would like to export, for example, ignore technical IDs, don't export business addresses. For more information, see
- **OData APIs:** You can use APIs to build custom processes to export exactly what you need for your use cases, including all the personal data of the business partner, linked transactions, and other related data. The APIs can be called using custom logic, from excel spreadsheets, and so on. For more details, see [SAP Cloud for Customer OData API v2 Reference](#)

Related Information

[Data Retention \[page 78\]](#)

10.3 Depersonalize Transactional Data


Delete or depersonalize data from all transactional documents.

The processing of personal data is subject to applicable laws related to the deletion of this data when the specified, explicit, and legitimate purpose for processing this personal data has expired. If there is no longer a legitimate purpose that requires the use of personal data, it must be removed. When removing data in a data set, all referenced objects related to that data set must be removed as well.

As an administrator with responsibility for data protection functions, you have the ownership to decide when a document loses its business purpose. In the SAP Cloud for Customer system, you can delete or depersonalize a document based on the following conditions:

- **Delete:** Documents that do not provide any value after personal data is removed, are deleted. They are no longer available in the system.
- **Depersonalize:** Documents that have business value, even if no personal data is available, are depersonalized. The system removes all the personal data, but retains the business data. The documents are still in the system and an authorized person can access them. However, these documents can no longer be changed.

Since depersonalization removes all personal information, the processed objects are no longer available with the **My <business object>** filter. Some data in a depersonalized document is replaced by XXXX, and others, such as, attachments, are deleted. The transaction itself remains, but the personal data is either removed completely, or replaced with XXXX.

You can trigger a deletion in the following ways: To delete or depersonalize a document, navigate to any object worklist (For example: appointment, lead, opportunity), select the object, and from the actions list , click [Delete](#), or [Depersonalize](#). If there are no blockers (either due to an involved Business Partner being blocked for deletion, or due to the object still being active), the selected objects are depersonalized.

If you are required to keep data without purpose longer due to conflicting laws or regulations, you must export it using archiving, data workbench or the corresponding OData API before you delete or depersonalize it from the system. For more information, see the reference in the **Related Information** section at the end of this document.

Blocked for Deletion

In the [Data Protection and Privacy](#) work center, under [Personal Data Removal](#), it is possible to block person based business partners from being deleted.

During the depersonalization run, the system checks to ensure that none of the involved business partners have been blocked from deletion. It continues with the depersonalization of the business partners only if they are not blocked for deletion. The same settings also prevents the deletion of transactions that are linked to a business partner who has the deletion block set.

When you mark a document for deletion or depersonalization, the system ignores any defined retention periods since the customer is in full control over what should be deleted or exported.

The following table gives an overview of all the objects that can either be deleted or depersonalized.

Business Objects	Delete	Depersonalize	More Information
Activity Lists	Yes		
Appointments	Yes		
Phone Calls	Yes		
Tasks	Yes		
Visits	Yes		
Chats	Yes		
Routes	Yes		
Plans	Yes		
Deal Registration		Yes	
Sales Lead		Yes	
Leads		Yes	
Opportunities		Yes	
Sales Forecast	Yes		
Sales Target Plan	Yes		
Sales Territories	Yes		
Promotions		Yes	
Invoice		Yes	
Payments		Yes	
Partner Application		Yes	
Contracts		Yes	
Customer Orders		Yes	
Customer Quotes		Yes	
Sales POD	Yes		
Installation Point		Yes	
Installed Base		Yes	

Business Objects	Delete	Depersonalize	More Information
Maintenance Plan		Yes	
Registered Product		Yes	
Tickets		Yes	
Time Entry		Yes	
Time Reports		Yes	

In addition to the objects in the table, there are some special objects that are handled differently:

- **Surveys:** Surveys are not intended to collect personal data and are therefore not deleted during a depersonalization run.
- **Routing Rules, Tours, and Routes:** Routing rules, tours, and routes are configuration settings and are not depersonalized. These objects are directly deleted if they are no longer needed.
- **Territory:** Territory is not part of document driven deletion. If necessary, Business Partners can be removed from it.
- **Sales Target Plan and Sales Forecast:** Sales target plan and forecast does not have an OData based export. It is possible to export planning data as an excel in the OWL
- **Sales Price Specifications:** Sales Price Specifications are replicated from ERP to Cloud for Customer. This data is read-only in SAP Cloud for Customer and cannot be changed. If this information must be removed, it must be deleted in the system that owns those records and then replicated into Cloud for Customer.

Related Information

[Data Retention \[page 78\]](#)

10.4 Data Retention

If the purpose for which you acquired data is not valid anymore, but you must retain it for audit purposes, you can export the data before deleting it from the system.

SAP Cloud for Customer supports this data retention requirement with the following options:

- **Archiving:** Data no longer needed can be removed from the SAP Cloud for Customer system and placed in an archive with limited access. This way, regular users can no longer access the data, but it would still be possible for auditors to review the data. For more information, see [Archiving](#)

i Note

Archiving removes data solely based on the retention periods defined per object. If you need more detailed retention criteria, we recommend that you use OData APIs to remove your data.

- **Data workbench:** You can use the data workbench to export full datasets for employees and contacts of individual customers. The data workbench export functions allows you to specify one or more persons to be processed. It also allows you to select the fields you would like to export, for example, ignore technical IDs, don't export business addresses. For more information, see
- **OData APIs:** You can use APIs to build custom processes to export exactly what you need for your use cases, including all the personal data of the business partner, linked transactions, and other related data. The APIs can be called using custom logic, from excel spreadsheets, and so on. For more details, see [SAP Cloud for Customer OData API v2 Reference](#)

10.5 Administer Data Removal Runs

Check the status of all data removal runs performed in the background.

Removal of personal data in the [Data Protection and Privacy](#) work center is performed automatically in a separate background process. The [Administer Data Removal Runs](#) common task provides you with an overview of planned, current and completed data removal runs, the ability to reschedule failed runs, mark runs as obsolete, and delete runs.

Data removal runs are triggered by users in the [Personal Data Removal](#) view and executed by the system in the background. Within the [Personal Data Removal](#) screen from which the process is started, the user receives no direct feedback on the status of the removal run that has been triggered. You check the outcome of all data removal runs in the system using the [Administer Data Removal Runs](#) common task.

Features

The [Administer Data Removal Runs](#) common task provides you with an entry point to check the status of all background data removal runs performed by the system.

Three key features of this common task are summarized below:

Schedule Job

Select an existing removal run and click [Schedule](#) on the initial [Administer Data Removal Runs](#) screen. Allows you to reschedule runs that have previously failed.

Set Run To Obsolete

Select an existing removal run and click [Actions](#) > [Set to Obsolete](#) . This is useful in situations when, for example, technical issues mean there is no point in retrying the run in question at this point in time.

Delete Run

Select an existing failed removal run with the status [Obsolete](#) and click [Delete](#) . The removal run is deleted from the system. You can also delete successfully completed removal runs.

i Note

Information about the removal run itself is stored by the system in the Removal Log if you are deleting a previously successful removal run. However, the deletion of failed removal runs is not logged.

You access this log in the *Common Tasks* section of the *Personal Data Removal* view.

You can also access the *Job Monitor* by selecting an existing removal run and clicking *View Jobs* on the initial *Administer Data Removal Runs* screen. The monitor displays the status for individual removal run jobs that have commenced in the system and can provide more information as to why a particular job has failed, the actual status of the job in the system (for example, Pending), or if there is an error in the job itself.

Application Log Detailed View

Accessed by clicking the *Application Log ID* for a given job in the *Details* section of the initial *Administer Data Removal Runs* screen. Each instance of the Application Log consists of three different tab sections that group the messages posted to the log itself:

- *Overview*
Displays an aggregation of the removal run data collected in *Results*.
- *Settings*
Contains information on the parameters and settings of the business objects in the system background: log parameters, selection criteria used to create the log data, and any relevant data derived from configuration settings.
- *Results*
Provides detailed information and status of the removal run, including any error messages generated during execution.

Example

As the Human Resources administrator, responsible for employee data protection and privacy in Akron Heating, Oliver Adams must remove personal data for an employee who has requested its removal. The statutory retention period for this data is completed, so Oliver can now remove this data from the system. Oliver triggers removal of the employee's data on the *Remove Employee* screen and receives a message that the data removal process for this employee has started in the background. Oliver now checks on the status of the removal run he has triggered as follows:

1. He opens the *Administer Data Removal Runs* common task and in the *Show* field, he selects *All Removal Runs*.
2. He sees from the *Removal Failed* column that the removal run he triggered was not successful.
3. He decides to reattempt this removal run, so clicks *Schedule* and opens the *Schedule Job* screen for his selected run and selects the *Start Immediately* radio button.
4. This removal run unfortunately fails for a second time. Oliver decides therefore to abandon this particular removal run and seek support from colleagues. He sets the run as obsolete and then clicks *Delete* to remove all data about this failed run from the system. As the run failed and no personal data was removed for the employee on this occasion, there is no entry made in the *Removal Log* by the system.

10.6 Automate Removal of Obsolete Business Partners

As a data protection officer, you can schedule automated deletion of obsolete business partners, such as, contacts, employees, and individual customers.

In the *Administer Obsolete Business Partner Removal Runs* view, you can create a batch job to schedule deletion runs. You can schedule the runs immediately, or set a recurrence to continuously purge obsolete business partners from the system. The system selects all the business partners that have been set as obsolete before a certain cut-off date. This is required to account for deletion vetoes if a business partner can't be deleted. Once the selection is done, the system creates one data removal run per business partner.

Prerequisite

The business partners are already marked as obsolete.

You can enable mass-setting of the obsolete status for Business Partners using one of the following:

- End-of-purpose APIs that have been provided for integration scenarios. For more information, see [Web Services for Business Partner End-of-Purpose \[page 82\]](#)
- Custom development using the SAP Cloud Applications Studio
- oData APIs or Data Workbench using the following steps:
 1. Export set of Business Partners based on selection criteria
 2. Run further checks if needed, and then update the status flag to **Obsolete**
 3. Import the Business Partners back into the system and update the records

Procedure

1. Navigate to ► *Data Protection and Privacy* ► *Common Tasks* ► and click *Administer Obsolete Business Partner Removal Runs*.
2. Click *New* to open the *Schedule Deletion Run* screen.
3. Enter a *Run ID* and description. The Run ID must be a unique ID with no spaces or special characters.
4. Enter the *Date Offset* period. This means that the business partners are removed from the system after the offset time is over, for example, 30 days after the business partners are set to obsolete.
5. Choose a *Business Partner Type*.
To include business partners that are mapped to other systems, select the *Include Business Partners with ID Mapping* checkbox.
If you do not select the checkbox, the system excludes the business partners that are replicated in other external systems such as SAP S/4HANA, and ERP, and only triggers removal for business partners available locally in the SAP Cloud for Customer system.
To further filter, and include only business partners that are not blocked for removal, select the *Only Business Partners marked as End of Purpose* checkbox.
6. Select the run option to either start the run immediately or schedule a recurring run.
7. Click *Save and Close*.

In the *Deletion Runs* overview screen, select your run to see the details in the table below. Click the *Application Log ID* hyperlink to open the screen with details of your run. In the *Results* tab, the system displays the status of all the individual removal runs for each business partner, and the corresponding Run ID, if already scheduled.

Note

- The green icon indicates that the removal run has been already scheduled. This does not mean that the removal is successful. To check the status of the obsolete business partner removal runs performed in the background, navigate to the *Administer Data Removal Runs* view and search by the Run ID.
- The red icon indicates that the system failed to trigger a removal run.

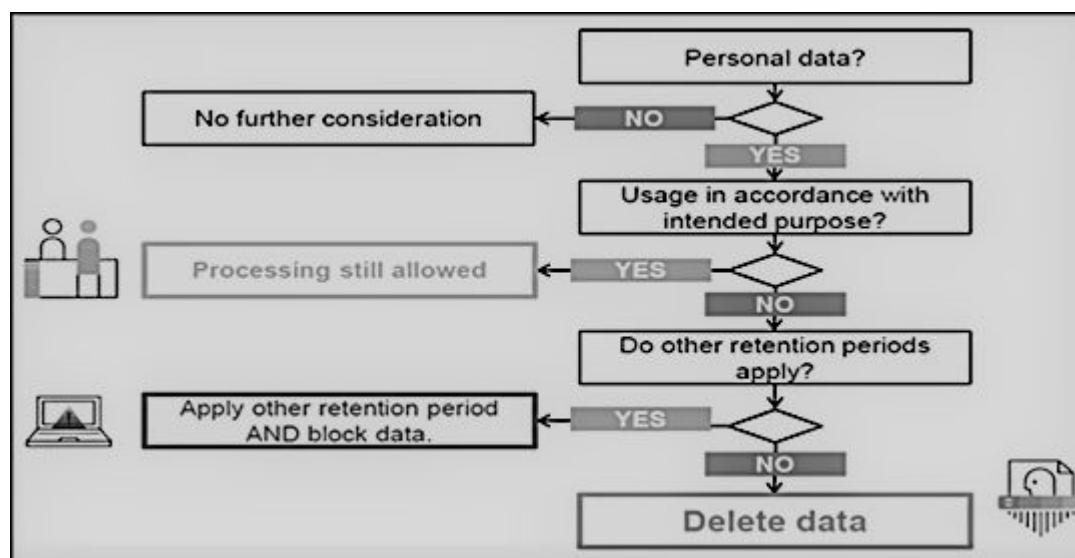
Related Information

[Web Services for Business Partner End-of-Purpose \[page 82\]](#)

10.6.1 Web Services for Business Partner End-of-Purpose

Determine if you need to retain business partner data in your system when that data has already been deleted from an integrated external system.

The following graphic describes process flow to determine the End-of-Purpose for your business partner data. You can use web services or manually block such business partners in your system using blocking reasons.



Web service interfaces and enhanced interfaces are enabled to support blocking of business partners. Use these services in scenarios where integrated external systems block or delete business partner data in their system landscape. These interfaces allow the external systems to query and maintain the End-of-Purpose for business partners. Since the definition of what constitutes the end-of-purpose for a business partner is subjective to the external system, these interfaces are empty CHECK interfaces to allow you to create custom queries.

For business partners blocked using the below mentioned interfaces, data cannot be retrieved in list views in work centers, value help in related fields, values selectors, analytics, duplicate checks and web service or oData queries in the application.

Web Services for Business Partner End-of-Purpose

Web Service	Description
II_BUPA_EOP_CHECK_IN	This interfaces uses enhancement spot ES_BUPA_EOP_CHECK to provide a business add-in hook in SAP Cloud Application Studio. Use this hook to create custom query for setting end-of-purpose information.
II_BUPA_EOP_MAINTAIN_IN	Use this interface to set the <i>End-of-Purpose</i> flag for business partners. If this flag is set, then the business partner data is hidden in corresponding work centers and value helps and is not visible to users. Note that the data can be viewed by administrators in the <i>Data Protection and Privacy</i> work center.
II_BUPA_ERP_EOP_CHECK_IN	This interface uses enhancement spot ES_BUPA_ERP_EOP_CHECK to provide a business add-in hook in SAP Cloud Application Studio. Use this hook to create custom query for setting end-of-purpose information.
II_BUPA_ERP_REPL_IN	New attribute has been added in element structure for the existing interface. Set the indicator for business completed / End-of-Purpose flag. If this flag is set, then the business partner data is hidden in corresponding work centers and value helps and is not visible to users. Note that the data can be viewed by administrators in the <i>Data Protection and Privacy</i> work center.

10.7 Enable Read Access Logging

Use Read Access Logging (RAL) to log and monitor read-access to sensitive personal data such as bank data. You can identify and track who has accessed critical information and when.

In the SAP Cloud for Customer system, you can monitor the access to sensitive personal data in the [Log Display](#) view under the *Data Protection and Privacy* work center.

Read access logging is enabled for the following channels:

- User Interface (UI)
- Attachments
- Web Services
- OData Services
- Data workbench
- Change Log

- Analytics
- Excel Download
- Output Management
- Business Task Management

Whenever sensitive personal data fields are viewed by a user, a Read Access Log (RAL) entry is created. These entries form different RAL field groups in the system.

If the field that you have marked as sensitive personal is part of a field group that is already active, the system takes one day to start reading the access log for the same. To start read access logging immediately, activate or deactivate the corresponding field group.

i Note

- You can add sensitive personal data fields only to Business Partner extensions.
- You can't add sensitive personal data fields to object worklists, value selections, enterprise search, or extension scenarios.
- You can't use sensitive personal data fields as placeholders in workflow rules.

Standard RAL Field Groups

The standard Read Access Logging enabled fields along with the corresponding Field Group are listed in the following table:

Business Objects	Field	Field Group
Business Partner – Banking extension	Bank Account Number (Bank account number for the liquid asset)	Business Partner Banking Data
Business Partner – Banking extension	Bank Account Number (Bank account number for the liability)	Business Partner Banking Data
Business Partner	Tax number and Type	Business Partner Tax Data
Business Partner	Place of Birth	Business Partner Origin

i Note

The Field Group configuration is shared between Business by Design and SAP Cloud for Customer. In SAP Cloud for Customer, the banking field group is not relevant. The corresponding functionality exists only in Business by Design.

Field Groups for Attachments

The following table gives you a list of the objects that support RAL enabled custom document type attachments:

Business Objects	Field Group
Activity	Activity Attachment
Business partner	Business Partner Attachment
Contract	Contract Attachment
Lead	Lead Attachment
Opportunity	Opportunity Attachment
Promotion	Purpose
Sales Document	Sales Document Attachments
Service Request	Service Request Attachment

Other Field Groups

The following list provides an overview of other available field groups:

- **Data Workbench:** Access to files stored in the Data Workbench can be enabled for read access logging.
- **Key User Tools Extension Fields:** This field group contains all custom fields added via the adaptation mode and marked as sensitive personal data. This group is activated or deactivated after each change to the custom field classification
- **Output Management Data:** Data that leaves the system via the Output Management (for example printing) can be tracked via this group.
- **Web Service Message:** The Web service monitoring provides access to the payloads of the processed Web service calls. Due to its potentially sensitive nature, this feature is restricted to administrators.
- **SAP Cloud Applications Studio:** Sensitive personal data custom fields added via the SAP Cloud Applications Studio are controlled via field groups that correspond to their project name.

i Note

You are not allowed to debug or trace the SAP Cloud Applications Studio solution in the production system, if RAL is scoped and any RAL field group is active. However, if you want to debug the solution, your administrator must assign your user to the [Production Debugging Authorization](#) work center view. After the debugging is complete, it is recommended that the authorization is removed.

Prerequisites

- You have selected the scoping question *Do you want to switch on the Read Access Logging for sensitive personal data?* To find this question, navigate to ► [Business Configuration](#) ► [Implementation Project](#) ► [Edit Project Scope](#) ► [Questions](#) ► [Built-in Services and Support](#) ► [System Management](#) ► [Security](#) ►.
- You have defined customer document types for attachments using the following steps:
 1. Navigate to ► [Business Configuration](#) ► [Implementation Project](#) ► and click [Open Activity List](#).
 2. Search and select the *Customer-defined document types for attachments* activity.
 3. Under *Customer-Defined Document Types*, click [Add Row](#), and then define your document type.
 4. Select the relevant usage, and click [Save and Close](#).
If you select the applicable usage on both the documents, attachments are copied to a follow-up document.

Field Group Configuration

1. Navigate to ► [Data Protection and Privacy](#) ► [Field Group Configuration](#) ►.
The system displays a list of field groups that are available for the limited set of standard fields, as well as for any documents that support sensitive custom document types. There is also a specific field group to include all extension fields.
2. Select a field group from the available list and click [Activate](#). The data for this field group is now enabled for read access logging.
Click [Deactivate](#), if you do not want read access to that field group information to be included in the log.

To view changes to the field group, click [Changes](#) and enter the date range for which you want to see the changes.

Click ► [Actions](#) ► [Show Read Access Log](#) ► to go directly to the [Read Access Log](#) screen.

Click ► [Actions](#) ► [Generate Field Group Configurations](#) ► to add a new field group to the list of Field Groups whenever it is available in the system.

Download Log Data

To download log data manually, follow these steps:

1. Navigate to ► [Data Protection and Privacy](#) ► [Log Display](#) ►.
2. Click the **Advanced Search** icon and select your date range.
3. Select the desired record and click [Download](#).
The downloaded log entries are available in the XML format. The XML log lists the information about where the data has been accessed, who has viewed the data, when the data was accessed, and what has been accessed.

You can also download the RAL data via Web service [QueryReadAccessLogIn](#). To enable this service, navigate to ► [Administrator](#) ► [Integration](#) ►, and create a new Communication Scenario and a new Communication Arrangement.

i Note

- Read access logs are deleted automatically after 14 days.
- The data is stored in a safe place, which is accessible to only a few authorized people.

10.8 Prerequisites for Usage Block Integration

When a business partner is blocked in an SAP CRM, SAP S/4HANA, or ERP system, you must ensure that the usage block is retained when you integrate these systems with the SAP Cloud for Customer system. To do that, you must follow specific guidelines for each system.

Prerequisites for SAP CRM system

- Ensure that the CRM system is at least on SAP CRM EHP3 SP05.
- In the SAP Cloud for Customer system, ensure the following:
 - In the *Business Configuration* work center, navigate to your project and click *Edit Project Scope*. Under **► Questions ► Communication and Information Exchange ► Integration with External Applications and Solutions ► Integration of Master Data**, select the *Do you want to check and maintain end of purpose of a business partner from an external application?* business option.
 - In the *Administration* work center, navigate to **► General Settings ► Integration ► Communication Arrangement** and configure the *Business Partner End of Purpose Check from SAP Business Suite* communication scenario.
 - In the **SAP Cloud Applications Studio**, implement the `CheckBusinessPartnerEndOfPurpose` BAdI in the <http://sap.com/xi/AP/Common/Global> namespace. You can implement end of purpose checks in this BAdI and raise a VETO check .
- If you are using the SAP NetWeaver Process Integration (PI):
 - Download the following PI content versions:
 - CRMCOD01 IC 700 – SP25
 - SAP BYD 2.40 – SP26
 - CRMPCD01 700 – SP25
 - Configure the following operation mapping:
 - CRM_COD_BusinessPartnerEndOfPurposeCheck
 - CRM_COD_BusinessPartnerEndOfPurposeSet.
- If you are using the Cloud Platform Integration:
 - Download the 1805 version of SAP Cloud for Customer Integration with SAP CRM
 - Configure the following iFlows:
 - Check End of Purpose of Business Partners from SAP Business Suite
 - Maintain End of Purpose of Business Partners from SAP Business Suite
- To see how you can control the blocking and deletion of personal data in SAP CRM, refer to the SAP Help Portal for SAP CRM: <http://help.sap.com/crm>. Choose the relevant release, and navigate to **► Application**

Prerequisites for SAP S/4HANA system

- In the SAP Cloud for Customer system, ensure the following:
 - In the *Business Configuration* work center, navigate to your project and click *Edit Project Scope*. Under [Questions](#) > [Communication and Information Exchange](#) > [Integration with External Applications and Solutions](#) > [Integration of Master Data](#) >, select the *Do you want to check and maintain end of purpose of a business partner from an external application?* business option.
 - In the *Administration* work center, navigate to [General Settings](#) > [Integration](#) > [Communication Arrangement](#) > and configure the *Business Partner End of Purpose Check from SAP Business Suite* communication scenario
 - In the **SAP Cloud Applications Studio**, implement the `CheckBusinessPartnerEndOfPurpose` BAdI in the <http://sap.com/xi/AP/Common/Global> namespace. You can implement end of purpose checks in this BAdI and raise a VETO check .
- If you are using the SAP NetWeaver Process Integration (PI):
 - Download the following PI content versions:
 - C4CS4_IC 100 – SP08
 - SAP BYD 2.40 – SP26
 - Configure the following operation mapping:
 - S4_C4C_BusinessPartnerEndOfPurposeCheck
 - S4_C4C_BusinessPartnerEndOfPurposeSet
- If you are using the Cloud Platform Integration:
 - Download the 1805 version of SAP Cloud for Customer Integration with SAP S/4HANA
 - Configure the following iFlows:
 - Check End of Purpose of Business Partners from SAP Business Suite
 - Maintain End of Purpose of Business Partners from SAP Business Suite
- To see how you can control the blocking and deletion of personal data in SAP S/4HANA, refer to the SAP Help Portal for SAP S/4HANA: <http://help.sap.com/s4hana>. Choose the relevant release, and navigate to [Product Assistance](#) > [English](#) > [Cross Components](#) > [Data Protection](#) >.

Prerequisites for ERP system

- Ensure that the ERP system is at least on SAP ERP 6.0 EhP7 SP05.
- In the SAP Cloud for Customer system, ensure the following:
 - In the *Business Configuration* work center, navigate to your project and click *Edit Project Scope*. Under [Questions](#) > [Communication and Information Exchange](#) > [Integration with External Applications and Solutions](#) > [Integration with SAP ERP](#) >, select the *Do you want to integrate with the end of purpose check of SAP ERP?* business option.

- In the *Administration* work center, navigate to **General Settings > Integration > Communication Arrangement** and configure the *Business Partner End of Purpose Check from SAP ERP* communication scenario
- In the **SAP Cloud Applications Studio**, implement the `CheckBusinessPartnerERPEndOfPurpose` BAdI in the <http://sap.com/xi/AP/Common/Global> namespace. You can implement end of purpose checks in this BAdI and raise a VETO check .
- If you are using the SAP NetWeaver Process Integration (PI):
 - Download the following PI content versions:
 - COD_ERP_INT_IC 6.00 – SP25
 - SAP BYD 2.40 – SP26
 - COD_ERP_INT 6.00 – SP25
 - Configure the following operation mapping: `ERP_COD_BusinessPartnerEndOfPurposeCheck`
- If you are using the Cloud Platform Integration:
 - Download the 1805 version of SAP Cloud for Customer Integration with SAP ERP
 - Configure the following iFlows: *Business Partner End of Purpose Check from SAP ERP*
- Read note [2623441](#)
- To see how you can control the blocking and deletion of personal data in ERP, refer to the ILM document: [Data Protection](#)

11 Security-Relevant Logging and Tracing

[Change Logs \[page 90\]](#)

Most business objects and every business partner object displays their detailed change logs in the *Change Logs* tab. For example: Contacts, Individual Customer. If you are unable to see the tabs, then you have to enable it using personalization; or have your administrator enable it for you.

[Security Monitoring and Alerting \[page 90\]](#)

Monitoring and alerting is a shared responsibility in which SAP focuses on infrastructure level events and customers focus on the application level events.

[Connectivity Errors - Troubleshooting \[page 93\]](#)

The following table provides an overview of the error codes for outbound errors and recommendations on how to solve the errors.

11.1 Change Logs

Most business objects and every business partner object displays their detailed change logs in the *Change Logs* tab. For example: Contacts, Individual Customer. If you are unable to see the tabs, then you have to enable it using personalization; or have your administrator enable it for you.

The *Business Partners* work center provides access to changes for all business partners such as: accounts, employees, contacts, or individual customers. Different users can filter on their role to view and check on the changes applicable to their activities. The *Business Partner Changes* tab, makes the change logs available to a business partner. Access to the change log for the *Business Partners* tab should be restricted to users who require it.

Go to ► *Administrator* ► *Flexibility Change Log* ► to view the custom changes applied to the system.

You can restrict access to the *Change Logs* tab using adaptation, based on the user role. This helps control access to private information for all users.

11.2 Security Monitoring and Alerting

Monitoring and alerting is a shared responsibility in which SAP focuses on infrastructure level events and customers focus on the application level events.

11.2.1 Security-Relevant Reports

The solution offers a set of reports that provide insight into the system's behavior. Depending on your authorizations, not all of these reports may be accessible.

The following reports have security-relevant information and are available under ► [Business Analytics](#) ► [Design Reports](#) ►:

- **Access Rights Change Log**
This report displays a list of all users in the system and their assigned access rights. It also lists when and how the access rights were changed, and by whom. This information is relevant for compliance reasons, enabling you to monitor the system to prevent fraud, or to trace who made system changes, if fraud has been committed.
- **All Current Access Rights**
This report displays a list of all users in the system, and the access rights currently assigned to them. This information is relevant for compliance reasons, enabling you to monitor the system to prevent fraud.
- **All Current Users**
This report displays a list of all users in the system. This information is relevant for compliance reasons, enabling you to monitor the system to prevent fraud.
- **User Activation and Deactivation Log**
This report displays a list of all users in the system, and when they were activated or deactivated. This information is also relevant for compliance reasons, enabling you to monitor the system to prevent fraud.

Also under [Administration](#), you can find a list of IT control processes that allows you to monitor service provider access to your solution. IT control processes are IT-related changes made in your system, such as software updates or processes involving incident analysis.

11.2.2 Security-Relevant Data Sources

Security-relevant information is captured in data sources. As an administrator you can use reports that are based on these data sources.

These data sources can also be accessed via the OData API to enable the extraction of security-relevant information. You can extract the following data sources with the relevant OData APIs under ► [Business Analytics](#) ► [Design Data Sources](#) ► [Build OData Queries](#) ►:

- **User - Current Status Details**
Provides data about the current status of users, including assigned work center, work center views, validity dates, and whether the user is inactive.
- **User - Activation Change Documents**
Provides data about the activation change documents for users, including technical ID, whether the user is a technical user or locked, and validity dates.
- **User - Access Rights Change Documents**
Provides data about the access rights change documents for users, including changes to the assignment of work centers, work center views, and access rights.
- **Identity**
Provides all the attributes of an user.
- **User Logon Details**

Shows all the logon information for an user.

- User Logon Activity
Provides logon/logoff timestamps, current logon status.

Use Case	Data source	Sample Events
Suspicious user creation or change	User - Current Status Details	<p>Several users are getting created (creation timestamps)</p> <p>Formally invalid users have their validity period changed to be valid again.</p> <p>Mass change to invalidate users</p>
Suspicious logon times	User Logon Details	A user is logging on during non-business hours
Logon via suspicious client types and/or device type	User Logon Details	User connects via an Android device and Firefox despite company policy to only issue Apple devices, use Chrome
Suspicious user lock/unlock	User - Current Status Details	<p>Users are being locked/unlocked over a certain threshold</p> <p>Admin users are locked/unlocked</p>
Password brute force attempts	User Logon Details	<p>Number of failed logon attempts is spiking over several users, is spiking outside of business hours</p> <p>Several users show the same Date of Last Password Lock</p>
Password changes	User Logon Details	<p>Password change on weekends</p> <p>Password of technical user got changed</p> <p>Password change even though user should authenticate only via SSO</p>
Authorization changes	User - Access Rights Change Documents	Users getting access rights outside their area of responsibility (e.g. users belonging to lead qualification get access to sales orders and contracts)
Suspicious Security Policy used in logon	User Logon Details	<p>The security policy controls password complexity, if username/password authentication is allowed at all</p> <p>Administrator logs in using a security policy for low-privilege users</p>
Assignment of administrator rights	User - Access Rights Change Documents	<p>List of administration related work center is available under Authentication Mechanisms</p> <p>Non-Admin users get assigned to admin work centers</p>

11.2.3 Security-Relevant Log APIs

Use Read Access Logging (RAL) to log and monitor read-access to sensitive personal data such as bank data. You can identify and track who has accessed critical information and when.

To download log data manually, follow these steps:

1. Navigate to ► [Data Protection and Privacy](#) ► [Log Display](#) ►.
2. Click the **Advanced Search** icon and select your date range.
3. Select the desired record and click [Download](#).

The downloaded log entries are available in the XML format. The XML log lists the information about where the data has been accessed, who has viewed the data, when the data was accessed, and what has been accessed.

You can also download the RAL data via web service [QueryReadAccessLogIn](#). To enable this service, navigate to ► [Administrator](#) ► [Integration](#) ►, and create a new Communication Scenario and a new Communication Arrangement.

i Note

- Read access logs are deleted automatically after 14 days.
- Store the data in a safe place which is accessible to only few authorized people.

11.3 Connectivity Errors - Troubleshooting

The following table provides an overview of the error codes for outbound errors and recommendations on how to solve the errors.

Connectivity errors can occur on the client or on the server side. Errors that occur on the client side usually mean that it is not possible to establish the technical HTTP(S) connection to the server on the network level. Errors that occur on the server side are usually reported through an HTTP error code.



Error Code	Reasons and Recommended Actions
ICM_HTTP_SSL_ERROR	<p data-bbox="694 360 1396 416">SSL error. This error may occur for several reasons. Depending on the reason, proceed as follows:</p> <ul data-bbox="703 434 1396 857" style="list-style-type: none"><li data-bbox="703 434 1396 528">• Reason: The configured port exists but is not an SSL port. Action: Correct the port number in the Communication Arrangement view.<li data-bbox="703 539 1396 689">• Reason: The SSL server certificate is signed by a Certificate Authority (CA) that is unknown or not included on the trust list. Action: Carefully check the certificate. If it is signed by the correct CA, add the certificate from the CA to the trust list using the Edit Certificate Trust List common task in the Administrator work center.<li data-bbox="703 701 1396 857">• Reason: The server certificate is not part of the certificate chain or is sent in the wrong sequence, or the chain contains superfluous certificates. Action: Check that the certificate chain that the server sends complies with RFC5246.
ICM_HTTP_SSL_CERT_MISMATCH	<p data-bbox="694 887 1396 913">Invalid host name in SSL server certificate.</p> <p data-bbox="694 936 1396 992">Reason: The server name or the server name pattern contained in the server's certificate does not match the host name of the server.</p> <p data-bbox="694 1014 1396 1162">Action: Contact the person responsible for the server and ask for the server certificate setup to be checked and corrected if necessary. Note that if the server is set up correctly, this error may indicate a man-in-the-middle attack.</p>

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 a 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.

© 2021 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.