

SAP Hybris Cloud for Customer
Document Version: 1611 – 2016-04-11

Security Guide

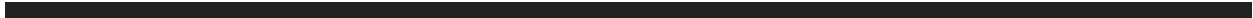
SAP Hybris Cloud for Customer



Content

1	Document History.	5
2	Introduction.	6
2.1	About this Document.	6
2.2	Why is Security Necessary?.	6
2.3	Document Structure.	7
3	Technical System Landscape.	8
4	Security Aspects of Data, Data Flow, and Processes.	10
4.1	Communication Channels.	10
4.2	Business-To-Business Communication and Application Integration.	11
	Communication Arrangements Quick Guide.	12
4.3	E-Mail.	21
	Enabling S/MIME Security.	22
	Configuring S/MIME Security.	23
4.4	MIME Type Configuration.	24
5	User Administration and Authentication.	26
5.1	User Management.	26
	VIDEO: Assigning User Access Rights by Roles.	27
	Restricting Access Roles.	28
5.2	User Types.	29
5.3	Authentication Mechanisms.	29
	Logon Using SAML 2.0 Assertion for Front-End Single Sign-On (SSO).	30
	Logon Using Client Certificate (X.509).	32
	Logon Using User ID and Password.	35
	Creating a Security Certificate for HTTPS-Enabled Computer Telephony Integration (CTI).	35
5.4	Security Policy Quick Guide.	36
	Business Background.	37
	Create a Security Policy.	37
	Edit an Existing Security Policy.	37
	Assign Security Policies.	38
	Define the Default Security Policy.	38
	Delete an Existing Security Policy.	39
6	Authorizations.	40
6.1	Authorization Assignment.	40

6.2	Access Restriction.	40
	Sales: Setting up User Access Rights and Restrictions.	41
	Service: Setting up User Access Rights and Restrictions.	46
	Restricting Access for Local Administrators.	47
6.3	Segregation of Duties.	48
7	Mobile Devices.	49
7.1	General Information.	49
7.2	Mobile Apps.	50
7.3	SAML2 Based SSO.	50
7.4	Authorizations.	51
7.5	Secure System Access and Authentication.	51
7.6	Password Change and Password Reset.	51
7.7	Special Considerations.	51
7.8	Data Storage.	52
	Password Retention.	53
	Support Log Files.	53
	Cache Files.	53
	Local Application Data Storage.	54
7.9	Offline Mode.	54
8	Front-End Security.	55
8.1	Microsoft® Silverlight™.	55
8.2	HTML5.	56
9	Security of Data Storage and Data Centers.	57
9.1	Asset Protection and Data Integrity.	57
9.2	Power Backup and Redundancy.	57
9.3	Restricted Physical Access.	57
9.4	Communication Security.	58
9.5	Network Security.	58
10	Security for Additional Applications.	59
11	Other Security-Relevant Information.	60
11.1	Security for End User Devices.	60
11.2	Service Composition Security.	60
	URL Mashup Integration.	61
	HTML Mashup Integration.	61
	Map Mashup Integration.	62
	Data Mashups.	62
11.3	Internal and External Audits.	63
	Security Management and Continual Improvement of Security.	64



- 12 Security-Relevant Logging and Tracing.65**
 - 12.1 Data Privacy.65
 - Prerequisites.66
 - Features.66
 - 12.2 Change Logs.67
 - 12.3 Security-Relevant Reports.67
 - 12.4 Connectivity Errors - Troubleshooting.68

1 Document History

This topic contains a table with the revision history of the SAP Hybris Cloud for Customer Security Guide.

Table 1: SAP Hybris Cloud for Customer Security Guide Document History

Version	Date	Change
1.0	2016-22-07	Initial version for SAP Hybris Cloud for Customer

2 Introduction

i Note

This guide does not replace the administration, operation, or integration guides that are available for productive operations, though it does contain a subset of specific security-related administration procedures.

[About this Document \[page 6\]](#)

[Why is Security Necessary? \[page 6\]](#)

With the increasing use of distributed systems and the Internet for managing business data, demands on security are also on the rise.

[Document Structure \[page 7\]](#)

The Security Guide contains the following sections:

2.1 About this Document

This Security Guide provides an overview of the security-relevant information that applies to SAP Hybris Cloud for Customer.

i Note

All technical documentation to set up, configure, integrate, secure, and operate your solution is published in English only. To ensure that you are reading the latest technical content, download it from SAP Service Marketplace.

2.2 Why is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, demands on security are also on the rise.

When using a distributed system, you must ensure that your business processes do not permit unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system should not result in loss of information or processing time. These security requirements apply equally to SAP Cloud solutions.

To assist you in ensuring the security of your SAP Cloud solution, we provide this Security Guide.

2.3 Document Structure

The Security Guide contains the following sections:

- **Technical System Landscape**
This section describes the technical components and communication paths that are used in the solutions.
- **User Administration and Authentication**
This section describes the user administration tools, and the system access and authentication concept that applies to the solutions.
- **Security Aspects of Data, Data Flow, and Processes**
This section describes the data flows and communications channels and the security characteristics of those channels.
- **Authorizations**
This section describes the authorization concept of the solutions.
- **Mobile Applications**
This section describes mobile applications.
- **Front-End Security**
This section describes the security mechanisms that apply to the front end.
- **Security of Data Storage and Data Centers**
This section describes critical data that is used by the solutions, and the security mechanisms that apply.
- **Security for Additional Applications**
This section contains security information about additional software components that are associated with the solutions.
- **Other Security-Relevant Information**
This section contains information about service composition security, and internal and external audits.
- **Security-Relevant Logging and Tracing**
This section describes trace and log files that contain security-relevant information, allowing you to reproduce activities if a security breach occurs.

3 Technical System Landscape

SAP Cloud solutions are hosted in SAP's own data center located either in Australia, Germany, or the United States. Customers can choose in which data center their solution shall run.

The solutions provide optional integration with 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:

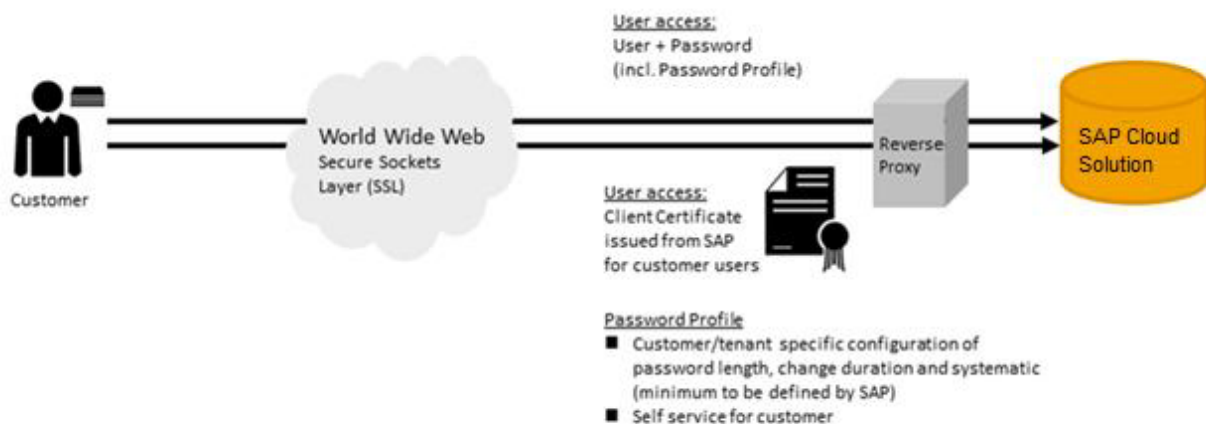
- The business data is stored securely in SAP data centers.
- Customers share physical hardware, but their data is separated into tenants.
- Users who require access to the business data must authenticate themselves, and their identity must be verified by user and access management.
- Customer data always 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 Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. For more information about connectivity, see the

Technical Connectivity Guide for SAP Cloud Applications, which you can find on SAP Service Marketplace:
<http://service.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.

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 antivirus software checks the uploaded files for viruses and other types of malicious software.

➔ Recommendation

In addition to this antivirus software, we recommend that our customers also use antivirus software.

In Business Configuration, you can define which file types can be uploaded to your solution. You should note that filename extensions can be changed to disguise the actual file format of the file.

4 Security Aspects of Data, Data Flow, and Processes

[Communication Channels \[page 10\]](#)

[Business-To-Business Communication and Application Integration \[page 11\]](#)

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 \[page 21\]](#)

[MIME Type Configuration \[page 24\]](#)

This section describes steps to select appropriate MIME types from the available list, that are specific to your project.

4.1 Communication Channels

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

Table 2:

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 Hybris Cloud solution system	HTTPS	REST services	Application data	User IDs, passwords
Apple® iPad® application, Apple® iPhone®, BlackBerry® player, Android™ (SAP Hybris 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 1.0 or higher is required. The following cipher suites are supported:

- TLS_RSA_WITH_AES128_CBC_SHA
- TLS_RSA_WITH_AES256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Note

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

Caution

We strongly recommend that you use secure protocols such as Secure Socket Layer (SSL) or Secure Network Communication (SNC).

4.2 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, in the *Communication Arrangements* work center view in the *Application and User Management* work center.

You can find the list of trusted certification authorities for server certificates in the *Application and User Management* work center under [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 *Application and User Management* work center under

► [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.

4.2.1 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](#) ► and/or from the [Application and User Management](#) work center.

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. For more information, see the SAP Hybris Cloud for Customer Administration Guide on the SAP Service Marketplace at <http://service.sap.com>. An SAP Service Marketplace Open ID is required to access this information. If you, as an administrator, do not have a user ID, then visit the SAP Service Marketplace at <http://service.sap.com/request-user> to request an ID.

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.

4.2.1.1 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. See the SAP Hybris Cloud for Customer Administration Guide for more details on the SAP Service Marketplace at <http://service.sap.com>.
 - 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. For more information, refer to the relevant integration guide on the SAP Service Marketplace at <http://service.sap.com>.
 - 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.

Table 3:

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 Certificate. 2. Click Upload Certificate and choose the relevant certificate. 3. Click OK. <p>To create a PKCS#12 key pair file, perform the following steps:</p> <ol style="list-style-type: none"> 1. Choose Certificate. 2. Click Create and Download Key Pair. 3. Define a name for the PKCS#12 file and save it. 4. Define a password for the PKCS#12 file and click OK. 5. Click OK. <div> <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 the SAP Hybris Cloud for Customer Administration Guide. </div>
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.

Table 4:

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

4.2.1.2 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.

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.

Note

Before you create a communication arrangement, you need to create a communication system. See the SAP Hybris 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. For more information, refer to the relevant integration guide on the SAP Service Marketplace at <http://service.sap.com> .

- 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.

Table 5:

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 Certificate.2. Click Upload Certificate and choose the relevant certificate.3. Click OK. <p>To create a PKCS#12 key pair file, perform the following steps:</p> <ol style="list-style-type: none">1. Choose Certificate.2. Click Create and Download Key Pair.3. Define a name for the PKCS#12 file and save it.4. Define a password for the PKCS#12 file and click OK.5. Click OK. <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 Change Password.2. Enter a password. Note that you have to provide your communication partner with the user ID and password.3. Click OK.

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:

Table 6:

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.

Authentication Method	Authentication	Settings
	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"> 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.

3. 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.

4. 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.
5. 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.

4.2.1.3 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](#).

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.

4.2.1.4 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 Certificate. 2. Click Create and Download Key Pair. 3. Define a name for the PKCS#12 file and save it. 4. Define a password for the PKCS#12 file and click OK. <div> <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 Create a Communication Arrangement [page 13] in the Related Links section. </div>
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 Change Password. 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 \[page 13\]](#)

4.2.1.5 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.

4.3 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:

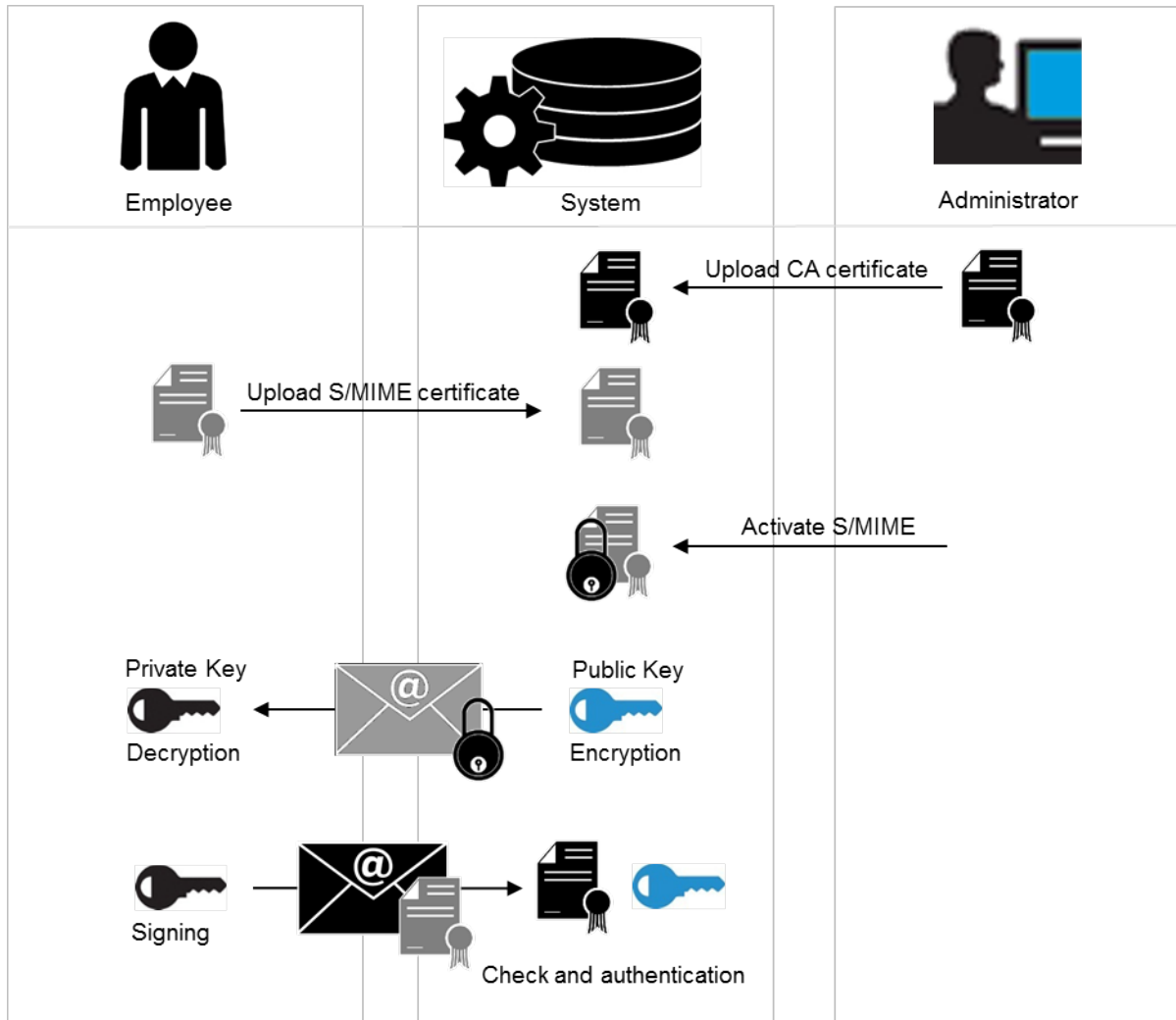


Figure 1: E-Mail Security with S/MIME

4.3.1 Enabling S/MIME Security

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

Context

To set up your SAP Hybris Cloud for Customer solution system to include e-mail as a communication channel for creating and responding to customer service tickets, see the Administrator Guide found on the SAP Service Marketplace at <http://service.sap.com>. An SAP Service Marketplace Open ID is required to access this information. If you, as an administrator, do not have a user ID, then visit the SAP Service Marketplace at <http://service.sap.com/request-user> to request an ID.

Procedure

1. Add e-mail security to your project scope. For more information, see the Administrator Guide.
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.

4.3.2 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.

Context

To set up your SAP Hybris Cloud for Customer solution system to include e-mail as a communication channel for creating and responding to customer service tickets, see the Administrator Guide found on the SAP Service Marketplace at <http://service.sap.com>. An SAP Service Marketplace Open ID is required to access this information. If you, as an administrator, do not have a user ID, then visit the SAP Service Marketplace at <http://service.sap.com/request-user> to request an ID.

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.

4.4 MIME Type Configuration

This section describes steps to select appropriate MIME types from the available list, that are specific to your project.

Context

MIME type configuration controls the files you can add to the SAP Hybris Cloud for Customer system. This includes attachment upload as well as files sent via email attachments.

We recommend that you start with a minimal MIME list, as you have 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* ► Select the *All* tab and search for *Allowed MIME Types for Document Upload*.
2. In the *ALLOWED MIME TYPES FOR DOCUMENT UPLOAD* screen, select your project relevant MIME types.

5 User Administration and Authentication

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

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

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

[User Types \[page 29\]](#)

[Authentication Mechanisms \[page 29\]](#)

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 do not support anonymous access.

[Security Policy Quick Guide \[page 36\]](#)

You as an administrator 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.

5.1 User Management

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

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

Table 7: User Administration Activities

View	Subview	Activity	Documentation in the Help Center
<i>Administrator</i> (SAP Hybris Cloud for Customer)	Business Users	Lock and unlock users 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 Assign business roles to users	<i>Business Users Quick Guide</i>

View	Subview	Activity	Documentation in the Help Center
	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>
Administrator (SAP Hybris Cloud for Customer)	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>
Business Configuration (SAP Hybris Cloud for Customer)	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>
	Edit Certificate Trust List	Edit trust list of certificates used for communication arrangements <div> <i>i</i> Note The list of trusted certification authorities is available on the Web dispatcher. Certificates with which users log on must be issued by one of these certification authorities. </div>	<i>Communication Arrangements Quick Guide</i>

For more information about how to perform these activities, see the documentation of the corresponding work center view.

5.1.1 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.

5.1.2 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.

5.2 User Types

SAP Cloud solutions provide the following user types:

Table 8:

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><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>

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 user type.

5.3 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 do not 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

5.3.1 Logon 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 Identity Provider.

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, he or she is prompted to logon 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.

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* ►.

5.3.1.1 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 have 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 started from ► [Application and User Management](#) ► [Common Tasks](#) ►.

For more information, see the administrator guide for your cloud product at help.sap.com.

Procedure

1. Choose [My System](#).
2. Under [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 selecting the [Manual Identity Provider Selection](#) check box.
5. In the [SSO URL](#) section, specify which URL should be used by the employee 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 cannot 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 is not 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 have 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 have not selected the [Manual Identity Provider Selection](#) check box in the previous step, you must select the default IdP, which is automatically selected when logging onto the system. To do so, select the corresponding IdP and click [Actions](#), then choose [Set to Default](#).
9. If required, you can specify the [Alias](#), which defines the displayed name of the IdP that appears on the log on 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. Once you have configured your IdP, activate SSO in your cloud solution. To do so, click [Activate Single Sign-On](#).

12. Save your changes.

5.3.2 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:

Table 9: 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/CPS incorp. by ref. limits liab., (c) 1999 Entrust.net Limited	Entrust.net Client Certification Authority	

Country	Organization	Organizational Unit	Common Name	Common Name E-Mail
US	Equifax	Equifax Secure Certificate Authority		
US	GoDaddy.com, Inc.	http://certificates.godaddy.com/repository	Go Daddy Secure Certification Authority	
US	The Go Daddy Group, Inc.	Go Daddy Class 2 Certification Authority		
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 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		

Country	Organization	Organizational Unit	Common Name	Common Name E-Mail
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	
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](#) >.

5.3.3 Logon 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 pre-configured 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 \[page 36\]](#).

If a user has forgotten the password, he or she 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.

5.3.4 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.

5.4 Security Policy Quick Guide

You as an administrator 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 in the `Administrator/Application and User Management` work center.

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 ► Edit Security Policies ►](#), and choose the *Password Logon Enabled* flag. 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 \[page 51\]](#).

5.4.1 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.

5.4.2 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.

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.

5.4.3 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 login.

5.4.4 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.

5.4.5 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.

Note

You can change the security policy assignment in the **Business Users** view. For more information, see the Administrator Guide for your cloud product on the on the SAP Service Marketplace at <http://service.sap.com>. An SAP Service Marketplace Open ID is required to access this information. If you, as an administrator, do not have a user ID, then visit the SAP Service Marketplace at <http://service.sap.com/request-user> to request an ID.

5.4.6 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.

6 Authorizations

[Authorization Assignment \[page 40\]](#)

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

[Access Restriction \[page 40\]](#)

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

[Segregation of Duties \[page 48\]](#)

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.

6.1 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 Hybris 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.

6.2 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.

6.2.1 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

6.2.1.1 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.

6.2.1.2 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.

6.2.1.3 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.

6.2.1.4 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.

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.







6.2.1.5 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 separately, 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.

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

6.2.1.6 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.

6.2.2 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.

6.2.2.1 Service: Defining User Access for a Group

Procedure

1. Create the organization that will contain the employees that you assign to this group. For more information, see the administration guide for your cloud product on the SAP Service Marketplace at <http://service.sap.com>.
2. After you have created the organization, create routing rules to define which tickets are assigned to the organization. For more information, see the administration guide for your cloud product on the SAP Service Marketplace at <http://service.sap.com>.
3. Create a role. A role contains permissions that are inherited by each employee assigned to the role. For more information, see the administration guide for your cloud product on the SAP Service Marketplace at <http://service.sap.com>.
 - 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.

6.2.3 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:
 - a. You un-restrict at least the views [Employees](#) and [Business Users](#).
 - b. You set the [General Settings](#) view and the [Application and User Management](#) work center to [Not Allowed](#).
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.

6.3 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.

7 Mobile Devices

[General Information \[page 49\]](#)

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

[Mobile Apps \[page 50\]](#)

You can download the mobile apps for SAP Cloud solutions from the respective stores as follows:

[SAML2 Based SSO \[page 50\]](#)

List of SAML2 based SSO supported mobile devices.

[Authorizations \[page 51\]](#)

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 \[page 51\]](#)

[Password Change and Password Reset \[page 51\]](#)

On the application level, you can either change or reset your app password.

[Special Considerations \[page 51\]](#)

[Data Storage \[page 52\]](#)

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

[Offline Mode \[page 54\]](#)

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

7.1 General Information

With the SAP Hybris 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 Hybris 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 Hybris Cloud solutions:

Table 10:

SAP Cloud Solution	Device/Operating System		
		Android	Windows Tablet
	iPhone/iPad		

SAP Cloud Solution	Device/Operating System		
SAP Hybris Cloud for Customer	X	X	X

Table 11: Offline Support

SAP Cloud Solution	iPad	Android Tablet	Windows Tablet
Offline Support	X	X	X

7.2 Mobile Apps

You can download the mobile apps for SAP Cloud solutions from the respective stores as follows:

- Download the app for your SAP Cloud solution for the Apple® iPhone® or iPad® from the iTunes Store®. A notification will be displayed on-device when a new version of the app is available for download.
- Install the app for your SAP Cloud solution for Android® smartphones and tablets from the Google Play Store™. A notification will be displayed on-device when a new version of the app is available for download.
- Install the app for your SAP Cloud solution for Windows® after downloading it from the windows store.

7.3 SAML2 Based SSO

List of SAML2 based SSO supported mobile devices.

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

Native Apps

- SAP Customer Insight for iPad
- SAP Hybris Cloud for Customer for iPad
- SAP Hybris Cloud for Customer for iPhone
- SAP Hybris Cloud for Customer for Android phone

Hybrid Apps

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

➔ Recommendation

For set up information, refer to [Logon Using SAML 2.0 Assertion for Front-End Single Sign-On \(SSO\) \[page 30\]](#).

7.4 Authorizations

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

In the *Application and User Management* work center, 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. For more information, see the *Business Users Quick Guide* in the Help Center from any work center.

7.5 Secure System Access and Authentication

Access from mobile devices via the mobile apps or the device browser (HTML5) 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. To allow users to use their mobile devices in offline mode, you must enable the use of an app or offline password and define additional security settings for those passwords.

Note

Connect directly to SAP Hybris Cloud for Customer system as the native iOS app now supports certificate pinning. Hence the proxy server will not work.

7.6 Password Change and Password Reset

On the application level, you can either change or reset your app password.

To change your app password, you must first enter your current app password. If you forgot your app password, you must reset it. Please note that in this case, your data (logon credentials and not synchronized changes) are deleted.

On the server level, you can reset your password by entering your e-mail address. Please note that your data is not deleted.

7.7 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 an **offline** password.

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

The offline password feature is available both for mobile and for HTML5 UI clients.

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

7.8 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 (not relevant for HTML5 offline).

Passcode

The passcode feature applies to the extended apps only, and is turned on by default. 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.

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.

For offline data storage, we recommend the use of:

- AES 256 encryption for all extended apps.
- AES 128 encryption for native iPad apps.

[Password Retention \[page 53\]](#)

[Support Log Files \[page 53\]](#)

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 \[page 53\]](#)

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 \[page 54\]](#)

SAP Hybris Cloud for Customer supports local application data storage. To enable this, you first have to log on to the Cloud system, and enter user name, system password, and system URL. During the setup, the user has to enter an app password 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.

7.8.1 Password Retention

When logging on to the SAP Cloud solution from a mobile app, the user is required to provide the user ID and system password. The mobile app does not store this data by default, but the user can change this setting by defining an app password.

In this case, the user ID and system password are encrypted and stored on the mobile device, using the secure storage features provided by the operating system of that device. The app password itself, however, is not stored on the mobile device, but is used to retrieve the stored user ID and system password when connecting to the SAP Cloud solution from it.

As an administrator, you can specify the length of time after which the mobile user must reenter the app password to log on to the system. For more information, see Security Policy.

7.8.2 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.

7.8.3 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.

7.8.4 Local Application Data Storage

SAP Hybris Cloud for Customer supports local application data storage. To enable this, you first have to log on to the Cloud system, and enter user name, system password, and system URL. During the setup, the user has to enter an app password 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.

7.9 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, synchronized, and deleted from the mobile device.

Follow these steps to set up PIN for container apps for storing data in the offline mode:

- The PIN should be atleast eight characters long.
- Make sure you include one numeric and one uppercase alphabet.
- You are allowed upto a maximum of eight failed attempts to logon. After which, you will need to reset the PIN that will delete all information from the database.

8 Front-End Security

The SAP Cloud solutions front ends consist of Web application user interfaces based on Microsoft® Silverlight™ or HTML5 technology.

[Microsoft® Silverlight™ \[page 55\]](#)

Microsoft® Silverlight™ is a development platform for Web applications.

[HTML5 \[page 56\]](#)

HTML is a markup language for the Web. HTML allows you to format text, add graphics, create links, input forms, frames and tables, and save it all in a text file that any browser can read and display. HTML5 is the latest version. It offers enhanced multimedia capabilities.

8.1 Microsoft® Silverlight™

Microsoft® Silverlight™ is a development platform for Web applications.

You can run Microsoft® Silverlight™ applications in your Web browser and benefit directly from the browser's security mechanisms. Examples of browser security mechanisms are secure cookie handling and same-origin policy. The same-origin policy ensures that confidential data is exchanged only with the domain of origin and that it is not stored on the client after the current session ends.

Microsoft® Silverlight™ applications from different domains of origin run independently of one another. They do not share resources, such as business data. The applications have very limited access to the client's resources, such as the local file system.

The user interface of your SAP Cloud solution benefits from the following front-end security mechanisms and concepts:

- Microsoft® Silverlight™ application sandbox and resource isolation
- 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 countermeasures
- Microsoft's secure default configuration in the framework
- Secure Web Application Development Guide

For more information, see the security information for Microsoft® Silverlight™.

8.2 HTML5

HTML is a markup language for the Web. HTML allows you to format text, add graphics, create links, input forms, frames and tables, and save it all in a text file that any browser can read and display. HTML5 is the latest version. It offers enhanced multimedia capabilities.

Note

HTML5 has been released for SAP Hybris Cloud for Customer only.

In addition to the features that are also supported by Microsoft® Silverlight™, HTML5 supports 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

For more information, see the security information for HTML5.

9 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.

[Asset Protection and Data Integrity \[page 57\]](#)

[Power Backup and Redundancy \[page 57\]](#)

[Restricted Physical Access \[page 57\]](#)

[Communication Security \[page 58\]](#)

[Network Security \[page 58\]](#)

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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

10 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.

11 Other Security-Relevant Information

[Security for End User Devices \[page 60\]](#)

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

[Service Composition Security \[page 60\]](#)

[Internal and External Audits \[page 63\]](#)

11.1 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 is very important that you follow strict security protocols to protect your data from getting compromised.

SAP Hybris Cloud for Customer offers many data extraction features such as: mass data maintenance, excel downloads etc.

Caution

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

These are our recommendations:

- 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.

11.2 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.

11.2.1 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.

11.2.2 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.

11.2.3 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 in the *Mashup Authoring* work center view of the *Application and User Management* work center. 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.

11.2.4 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.

11.3 Internal and External Audits

SAP is committed to third-party validations, standards, and certifications of the policies and procedures we use to maintain our customers' security, privacy and data integrity. SAP maintains several certifications and accreditations to ensure that we provide the highest standards of service and reliability to our customers. SAP will continue efforts to obtain the strictest of industry certifications in order to verify its commitment to provide secure and reliable services.

For more information, see the security and standard accreditations on the Business Center for Cloud Solutions from SAP, at: www.sme.sap.com/irj/sme/solutions?rid=/webcontent/uuid/30f7e866-fe58-2c10-5780-f056f2d71ed2&language=en

The *Audit* work center helps external and internal auditors conduct an audit for a company. It provides you with read access to all information that is relevant for an audit, such as financial reports, master data, documents and document flow, as well as user and access rights. The system provides this information through a selection of reusable views from other areas. Unlike other work centers, the *Audit* work center permits read access only. You cannot perform any changes there.

All planning, follow-up activities, reporting of audit results, and findings must be completed outside your SAP Cloud solution.

The *Audit* work center provides the following information:

- General Ledger
- Fixed Assets
- Cost and Revenue
- Inventory Valuation
- Receivables
- Payables
- Liquidity Management
- User and Access Management

For more information, see the documentation of the *Audit* work center.

11.3.1 Security Management and Continual Improvement of Security

Security Management at SAP Cloud Solutions aims towards the continual improvement of the information security framework. SAP conducts several external audits to make sure that these aims are reached.

Table 12:

Certificate/Report	Interval	Conducted by
ISO 27001 (SAP Cloud Operations)	Once a year	Accredited auditing company
ISO 27001 (SAP Data Center Operations)	Once a year	Accredited auditing company
External pentest	Every major release (SAP Hybris Cloud for Customer)	Third-party security company
Internal pentest	Minimum once a year (SAP Hybris Cloud for Customer)	SAP C.E.R.T.
Code Scan ABAP (SAP Hybris Cloud for Customer) Non-ABAP (SAP Hybris Cloud for Customer)	ABAP: Daily Non-ABAP: Minimum once per release	SAP Hybris Cloud for Customer
BS25999 (SAP Data Center Operations)	Once a year	Accredited auditing company

12 Security-Relevant Logging and Tracing

[Data Privacy \[page 65\]](#)

[Change Logs \[page 67\]](#)

Most business objects and every business partner object displays their detailed change logs in the [Changes](#) 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-Relevant Reports \[page 67\]](#)

[Connectivity Errors - Troubleshooting \[page 68\]](#)

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

12.1 Data Privacy

Data processing systems store master data or transactional data used to perform business processes and to document them. In many cases, this is personal data relating to employees or other private persons. In many countries, the storage, processing, disclosure, and deletion of such personal data from data processing systems must be in accordance with statutory data protection laws. One requirement in many countries is that such personal data can only be stored if a clear business reason exists for the retention of this data. Most data protection laws mandate that data is deleted after the business reason has expired. Alternatively, data can be anonymized rather than removed completely.

In addition, legislation in many countries stipulates that organizations must disclose the personal data stored on an individual, if the individual expressly requests it.

The Data Privacy Management work center allows those responsible for data protection matters within an organization to respond to and fulfill requests for the following in relation to the personal data of employees and customers:

- Disclose personal data relating to employees and private persons
- Remove employee personal data once the retention period for all relevant data has expired
- Monitor and manage automatic data removal processes using an application log
- Display log data detailing each access made to the Disclose Employee Data and Remove Employee Data overview screens

12.1.1 Prerequisites

The legally required retention periods relevant for your country have been maintained in your system configuration.

You can find the relevant configuration activities for *Data Retention Rules* in the *Business Configuration Implementation Projects* view. Here, you can set one retention period per country. For more information about system configuration for data privacy management, see the administration guide for your cloud product on the SAP Service Marketplace at <http://service.sap.com>.

Caution

Users with authorization to access the *Data Privacy Management* work center can perform all data privacy functions within this work center, including the disclosure and deletion of personal data belonging to employees and private persons. Access to this work center is granted in the *Application and User Management* work center. You must ensure that only employees with authorization to disclose/delete personal data are granted access to *Data Privacy Management*. If your corporate group consists of more than one company, you can set access to this work center at a company level. For example, you can assign one user with data privacy rights for the employees in one company and assign different a different user with these same rights for a separate company in your group.

To support auditing of data protection actions in the system, the system logs every access made to the *Disclose Employee Data* and *Remote Employee Data* overview screens of a selected employee.

12.1.2 Features

The *Data Privacy Management* work center helps your company to fulfill requests to disclose and/or delete personal data.

Personal Data Disclosure

The obligation to disclose personal data is set in legislation in many countries where data protection regulation has been adopted. An employee can request to view the personal data held by the employer and the employer must confirm that such personal data exists. The employee can then request a description of any such personal data, and in some legal jurisdictions, why the data is being stored or processed and who the recipients of this data are, or have been.

The *Personal Data Disclosure* view allows employees responsible for data protection to administer data disclosure of personal data upon request.

Personal Data Removal

An employee can request if personal data are held by the by the employing organization. If such data exists, the employee can request a description of this data, and request its deletion. You can delete a complete work agreement, which includes all dependent application-relevant data within an employee's work agreement.

In the *Personal Data Removal* view, you can delete personal data on request from the system, once the applicable required retention periods have expired.

Logging Access Information

To support auditing of data protection actions in the system, the system logs every access made to the [Disclose Employee Data](#) and [Remove Employee Data](#) overview screens of a selected employee.

Employees, such as Data Protection Officers with responsibility for data protection have full access for the [Data Privacy Management](#) work center. These access rights allow an authorized user to access personal data for the selected employee in all 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 by whom, and when.

12.2 Change Logs

Most business objects and every business partner object displays their detailed change logs in the [Changes](#) 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.

12.3 Security-Relevant Reports

The Application and User Management work center offers a set of reports that provide insight into the system's behavior. Depending on your authorizations, not all of those reports may be accessible.

The following reports are provided:

- **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.
- **Segregation of Duties (SOD) Conflicts Report**
This report displays the list of segregation of conflicts existing between assigned views of the business users. Segregation of duties is designed to minimize the risk of fraud and errors, and protect company assets such as data or inventories. This information is relevant for compliance reasons, enabling you to monitor the kind of authorizations you have for the users in your system and to make you aware of the kind of conflicting authorization assignments for any of the users.
- **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 in the User and Access Management work center, the IT Compliance view displays a list of IT control processes and 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.

12.4 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.

Table 13: Outbound Errors

Error Code	Reasons and Recommended Actions
ICM_HTTP_SSL_ERROR	<p>SSL error. This error may occur for several reasons. Depending on the reason, proceed as follows:</p> <ul style="list-style-type: none">• Reason: The configured port exists but is not an SSL port. Action: Correct the port number in the Communication Arrangement view.• 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 Application and User Management work center.• 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>Invalid host name in SSL server certificate.</p> <p>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>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

Coding Samples

Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP's gross negligence.

Accessibility

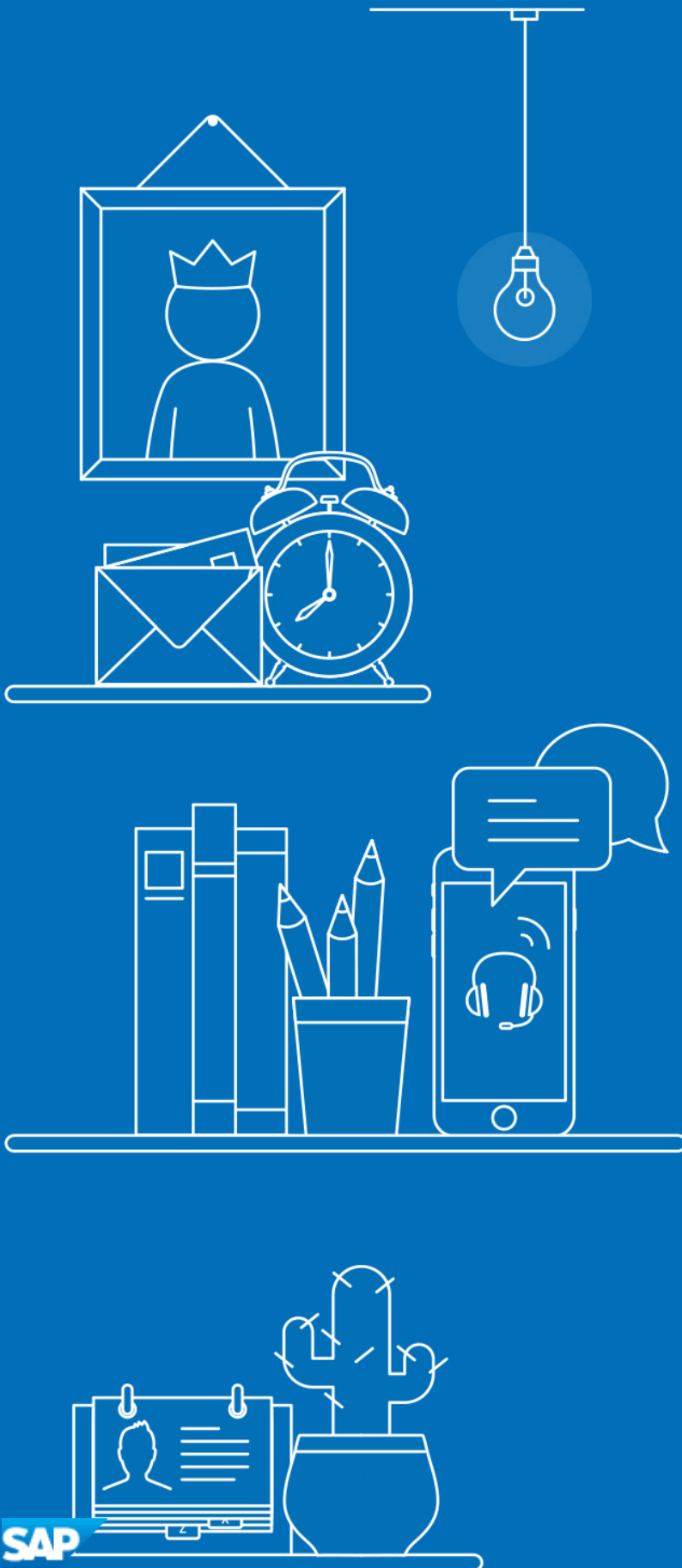
The information contained in the SAP documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of willful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP's gross negligence or willful misconduct. All links are categorized for transparency (see: <http://help.sap.com/disclaimer>).



**[go.sap.com/registration/
contact.html](https://go.sap.com/registration/contact.html)**

© 2016 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 <http://www.sap.com/corporate-en/legal/copyright/index.epx> for additional trademark information and notices.