



Security Guide | PUBLIC
2022-07-28

Security Guide for SAP Business ByDesign

Content

- 1 Document History. 4**
- 2 Introduction. 5**
 - 2.1 About this Document. 5
 - 2.2 Necessity of Security. 5
 - 2.3 Document Structure. 5
- 3 Technical System Landscape. 7**
- 4 Security Aspects of Data, Data Flow, and Processes. 9**
 - 4.1 Communication Channels. 9
 - 4.2 Business-To-Business Communication and Application Integration. 10
 - 4.3 Communication Arrangement. 11
 - Create a Communication Arrangement. 12
 - Delete a Communication Arrangement. 13
 - 4.4 E-Mail. 14
 - MIME Type Configuration. 17
- 5 User Administration and Authentication. 18**
 - 5.1 User Management. 18
 - 5.2 User Types. 20
 - 5.3 Authentication Mechanisms. 21
 - Logon Using SAML 2.0 Assertion for Front-End Single Sign-On (SSO). 21
 - Logon Using Client Certificate (X.509). 23
 - Logon Using User ID and Password. 25
 - 5.4 Security Policy. 26
- 6 Authorizations. 27**
 - 6.1 Authorizations Assignment. 27
 - 6.2 Access Restriction. 27
 - 6.3 Segregation of Duties. 28
- 7 Mobile Applications. 31**
 - 7.1 General Information. 31
 - 7.2 Mobile Apps. 31
 - 7.3 Authorizations. 32
 - 7.4 Secure System Access and Authentication. 32
 - 7.5 Password Change and Password Reset. 32
 - 7.6 Special Considerations. 32

7.7	Data Storage.	33
	Password Retention.	33
	Cache Files.	33
8	Front-End Security.	34
8.1	HTML5.	34
9	Security of Data Storage and Data Centers.	35
9.1	Asset Protection and Data Integrity.	35
9.2	Power Backup and Redundancy.	35
9.3	Restricted Physical Access.	35
9.4	Communication Security.	36
9.5	Network Security.	36
10	Security for Additional Applications.	37
10.1	Confirm The Signature.	37
10.2	Saving Logon Data.	37
10.3	Intelligent Robotic Process Automation (IRPA).	37
11	Other Security-Relevant Information.	39
11.1	Service Composition Security.	39
	URL Mashup Integration.	39
	HTML Mashup Integration.	40
	Map Mashup Integration.	40
	Data Mashups.	41
11.2	Internal and External Audits.	42
	Security Management and Continual Improvement of Security.	42
12	Security-Relevant Logging and Tracing.	44
12.1	Information Lifecycle Management for Data Privacy.	45
12.2	Security-Relevant Reports.	46
13	Best Practices.	47

1 Document History

Version	Date	Change
1.0	2013-11-20	Initial version for SAP Business ByDesign, SAP Cloud for Customer and SAP Cloud for Travel and Expense November 2013
1.1	2013-11-28	The following chapters have been updated: <ul style="list-style-type: none">• Business-to-Business Communication and Application Integration• Logon Using Client Certificate (X.509)
1.2	2014-09-05	Miscellaneous typographical errors corrected. No technical updates made to the content
1.3	2016-11-06	Removed references for other cloud products and SSL protocol
1.4	2018-02-04	Data Protection and Privacy and Best Practices sections have been updated
1.5	2022-05-05	The following chapters have been updated: <ul style="list-style-type: none">• Communication Channels• Logon Using Client Certificate (X.509)• Mobile Applications• Front-End Security• Security of Data Storage and Data Centers
1.6	2022-07-28	General Information on Mobile Applications has been updated

2 Introduction

2.1 About this Document

The Security Guide provides an overview of the security-relevant information that applies to SAP Business ByDesign.

2.2 Necessity of Security

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 Business ByDesign 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 solution.
- **Security Aspects of Data, Data Flow, and Processes**
This section contains security information about the data flow such as B2B communication and e-mail.
- **User Administration and Authentication**
This section describes the user administration tools, and the system access and authentication concept that applies to the solution.
- **Authorizations**
This section describes the authorization concept of the solution.
- **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 solution, and the security mechanisms that apply.
- **Security for Additional Applications**
This section contains security information about additional software components that are associated with the solution.
- **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 Business ByDesign is hosted in SAP's own data center located either in China, Germany, the United States of America or Australia.

Customers can choose in which data center their solution shall run. The solution provides optional integration with a full Enterprise Resource Planning (ERP) suite, including the associated server landscape and system maintenance.

Since the SAP Business ByDesign solution deals with business data from your core business processes, SAP adheres to the highest security and quality requirements, as follows:

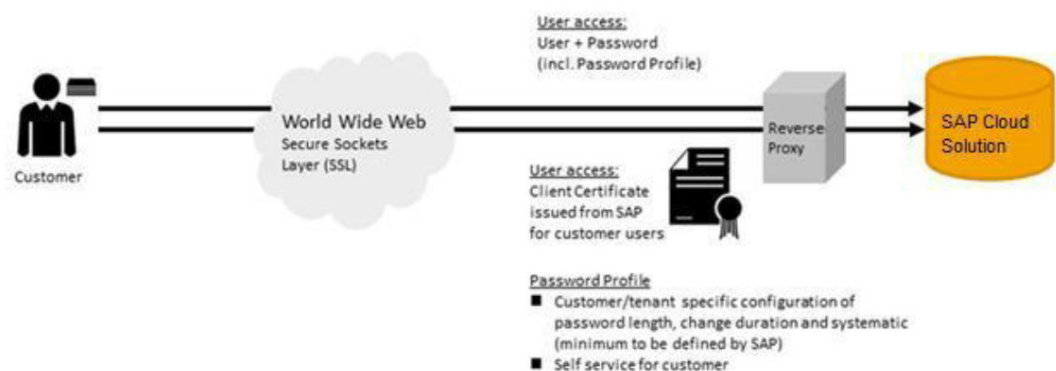
- The business data is stored securely in SAP data centers.
- Customers share physical hardware, but their data is separated into tenants.
- Users who require access to the business data must authenticate themselves, and their identity must be verified by user and access management.
- Customer data always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

You can access your SAP Business ByDesign 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 (Access via a Web browser on a mobile phone or tablet is neither supported nor recommended.)

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 Business ByDesign solution in the SAP data center.

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



To access SAP Business ByDesign solution, you must enter a unique, customer-specific URL.

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

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

The communication channels that require mutual authentication are secured by using standard Transport Layer Security (TLS) protocol. For more information about connectivity, see Technical Connectivity Guide for SAP Cloud Applications.

The server certificate used by the reverse proxy must be trusted by the SAP Cloud system.

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

Ensure that you also read the following relevant subsections:

- [Using Firewall Systems for Access Control](#) > [Application-Level Gateways Provided by SAP](#) > [Web Dispatcher](#)
- [Using Multiple Network Zones](#)

You can upload attachment files to the SAP Business ByDesign 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 you also use antivirus software. Uploaded files are blocked based on their filename extensions, that can be manipulated.

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

4 Security Aspects of Data, Data Flow, and Processes

4.1 Communication Channels

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

Communication Path	Protocol Used	Technology Used	Type of Data Transferred	Data Requiring Specific Protection
Web browser acting as front-end client to access the hosted SAP Business ByDesign system.	HTTPS	REST services	Application data	User IDs, passwords
Mobile Applications	HTTPS	REST services	Application data	User IDs, passwords, application data
E-mail	SMTP	SMTP server	Application data	Confidential data
Business-to-business communication and application integration	HTTPS	Web services	Application data	Application data

Cryptographic Protocols

Inbound Communications

For all inbound communications, TLS 1.2 or higher is required. The following cipher suites are supported:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

i Note

SAP Business ByDesign solution uses port 443 for HTTPS connectivity.

⚠ Caution

We strongly recommend that you use secure protocols such as Transport Layer Security (TLS) 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.

SAP Business ByDesign 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 SAP Business ByDesign. 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 and user names plus passwords for access from mobile devices. Please ensure that the passwords used are strong enough.

4.3 Communication Arrangement

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 communication arrangements can be created in the solution from the *Communication Arrangements* view. The *Communication 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 *Application and User Management* work center.

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 SAP Hybris Cloud for Customer Administration Guide on the [Help Portal](#).

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.

4.3.1 Create a Communication Arrangement

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](#).

i Note

Based on the communication scenario you selected, the system presets the fields in the next steps with default values. You can change the values where ever possible if in case it is 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.
 1. 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.

i Note

Before you set up a communication arrangement, you must create a communication system.

2. 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 that you are assigned to. If you use a B2B scenario, you must also enter a valid identification type.
3. 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.
4. Click [Next](#).
4. In the [Define Technical Data](#) step, define the technical settings for inbound and outbound communication.
 1. 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.
 2. If you use inbound communication, select the [Application Protocol](#) and [Authentication Method](#) in the [Inbound Communication: Basic Settings](#) section.
 3. In the [User ID](#) field, click [Edit Credentials](#).
Depending on the chosen authentication method, you need to define the credentials of the communication user as described in the following table. The user ID of the communication user is created automatically.

Authentication Method

Settings

SSL client certificate

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.

1. Choose [Certificate](#).
2. Click [Upload Certificate](#) and choose the relevant certificate.
3. Click [OK](#).

To create a PKCS#12 key pair file, perform the following steps:

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](#).

i Note

- 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 **Importing Key Pair file to a Third Party Tool**.

User ID and password

If you use this authentication method, you need to define a password as follows:

- Choose [Change Password](#).
- Enter a password.
Note that you have to provide your communication partner with the user ID and password
- Click [OK](#).

4.3.2 Delete a Communication Arrangement

1. In the [Communication Arrangements](#) view, select the relevant communication arrangement.
2. Click [Delete](#).
3. In the dialog box that opens, click [Delete](#) to confirm the deletion.

i Note

Predefined communication arrangements cannot be deleted.

4.4 E-Mail

SAP Business ByDesign enables 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.

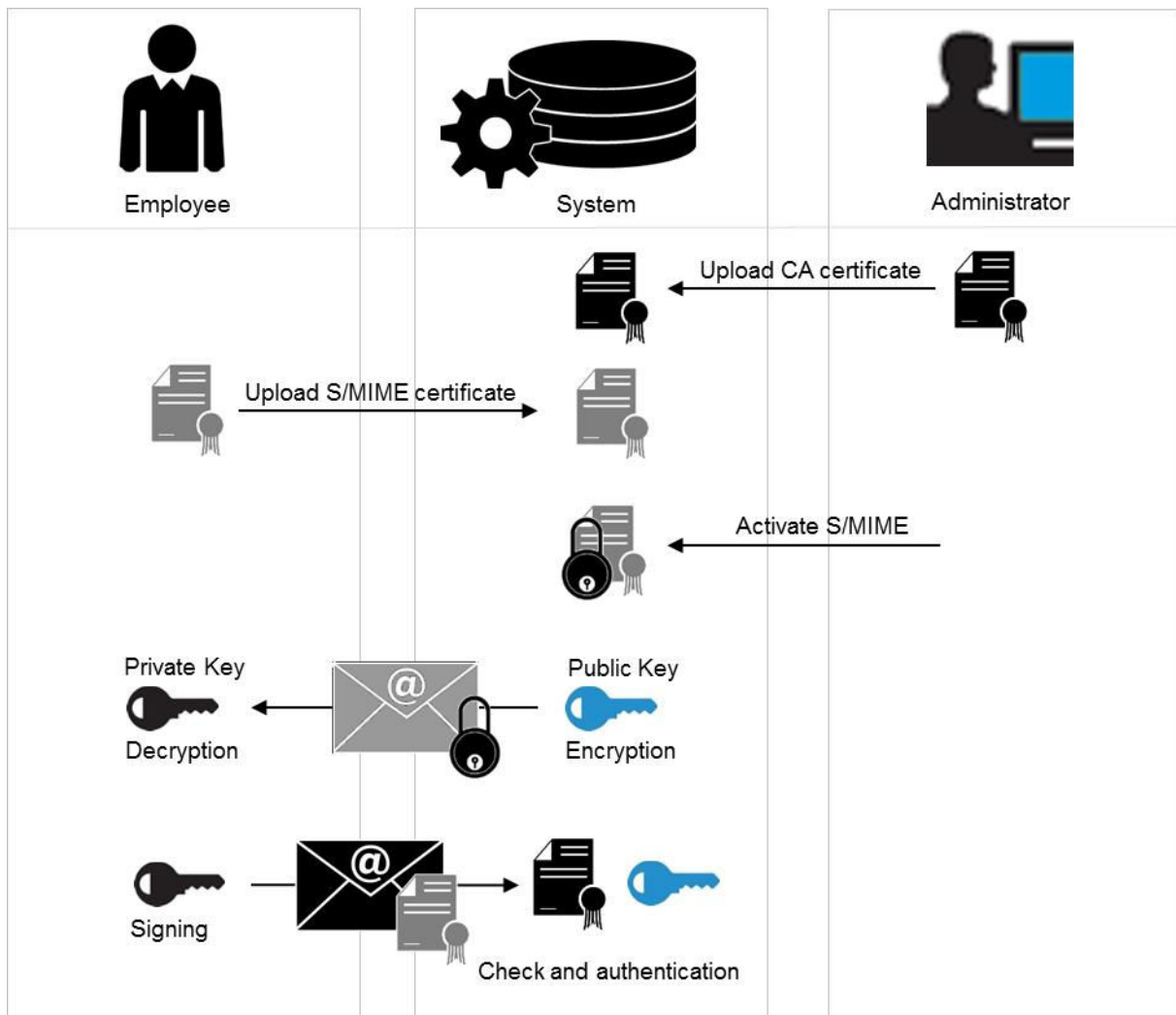
The following MIME types are supported for e-mail communication with the system:

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

⚠ Caution

When you use S/MIME, ensure that the data is encrypted. 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:



Enabling S/MIME Security

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

Procedure

1. Add e-mail security to your project scope.
2. Implement e-mail security for your solution.
 1. Choose [Business Configuration](#), select your project from the list, and click [Open Activity List](#).
 2. Click [Fine-Tune](#).
 3. Open [E-Mail Encryption and Signature Check](#).
 4. 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.

5. 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*.
6. Save your settings.
3. Activate your settings.
 1. Choose *AdministratorCommon TasksConfigure S/MIME*.
 2. Click *Activate S/MIME*.
 3. 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* gets enabled if you activate them. If you do not activate your settings, your system does not have security enabled.
4. Save your settings.

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.

Note

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 SAP Hybris Cloud for Customer Administrator Guide on [Help Portal](#).

Procedure

1. Choose *Configure S/MIME* in the *Business Configuration* 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:
 1. Click on *Link to SAP CA* and open the site *SAP Trust Center ServiceRoot Certificates*.
 2. Click on *SAP Passport CA Certificate*. A pop-up opens.
 3. Click *Install Certificate* and follow the wizard by clicking *Next*.
 4. Select *Place all certificates* in the following store and click *Browse*.
 5. 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:
 1. Check *Signature of Incoming E-Mails*
 2. *Encrypt Outgoing E-Mails* (optional)
 3. *Signing Outgoing E-Mails*

Note

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.

4.4.1 MIME Type Configuration

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

MIME type configuration controls the files you can add to SAP Business ByDesign. 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:

1. Go to *Business Configuration* work center, select your *Implementation Project* and click *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.

Caution

When checking documents, the system assigns unknown MIME types to the application/octet-stream MIME type. If you define the application/octet-stream MIME type as allowed, all documents whose MIME types are not specified in the MIME type list can be uploaded. This MIME type is available for fallback purposes. Therefore, we recommend that you not define the application/octet-stream MIME type as allowed until emergency. During Emergency, carefully scan the documents before uploading them.

Deactivation of MIME type Check

In case you would like to deactivate MIME type check, follow these steps:

1. Go to *Business Configuration* work center, select your *Implementation Project* and click *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, un select your project relevant MIME types.

Caution

MIME type checks provide additional protection in terms of security of the documents processed. We strongly recommend not to deactivate these checks.

5 User Administration and Authentication

5.1 User Management

User management for SAP Business ByDesign is located in the [Application and User Management](#) work center.

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

View	Subview	Activity	Documentation in the Help Center
Application and User Management	Business Users	Lock and unlock users	Business Users Quick Guide
		Change user password	
		Edit the validity of a user	
		Assign security policies to users	
Application and User Management	Support and Technical Users	Assign access rights to users for work centers and work center views	Business Roles Quick Guide
		Restrict read and write access for users to specific data	
		Assign business roles to users	
Application and User Management	Communication Arrangements	View all support and technical users available in the system	Business Roles Quick Guide
	Communication Certificates	Define access rights in business roles	
Application and User Management	Communication Arrangements	Create technical users for electronic data exchange	Business Roles Quick Guide
	Communication Certificates	Manage certificates that you use for electronic data exchange	

View	Subview	Activity	Documentation in the Help Center
Common Tasks	Edit Security Policies	Specify security policies for user passwords	Security Policies Quick Guide
	Configure Single Sign On	Download service proIDP metadata, and activate SSO	Configure your Solution for
	Configure S/MIME	Configure and activate e-mail communication with S/MIME	Email Security Configuration: Load Certificates and Activate Signing and Encryption for E-Mails
	Edit Certificate Trust List	Edit trust list of certificates used for communication arrangements	Communication Arrangements Quick Guide

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.

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

Business Roles

A business role is a set of access rights that you can assign to multiple business users who perform similar business tasks. You can also make employee assignments to define who is responsible for changing a business role, for example, managers who need to change business roles that are relevant for their business areas.

You can access the [Business Roles](#) view from the [Application and User Management](#) work center.

When creating and editing a business role, you can assign work centers and work center views, and define access restrictions for each view. You can also define a main, or default, business role when associating that business role with a relationship.

Procedure

1. From the [Application and User Management](#) work center, go to [Business Roles](#) view.
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:
 1. No Access (Only available as a restriction for write access) - The user has no write access.
 2. Unrestricted - The user has access to all business data related to the view.
 3. 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.
 4. 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.
 5. 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.
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 [Save](#) to save the edits you have made to the business role and the users.

5.2 User Types

SAP Business ByDesign provides the following user types:

User Type	Description
Business User	<p>A user type for normal interactive users resulting from hiring an employee or creating a service agent. Business users always have to change their initial password during the first logon. The properties of the passwords are determined by the assigned security policy.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin-top: 10px;"> <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>

User Type	Description
Technical User	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.
Support User	A user type for interactive support users used by SAP Cloud Services to access the system as part of incident processing.

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 Business ByDesign for regular browser-based front-end access, as well as for electronic data exchange, such as Business-to-Business communication. SAP Business ByDesign does not support anonymous access.

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

To log on the 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 Front-End Single Sign-On document and the SAP Identity Provider document in [Help Portal](#).

Configure Your Solution for Single Sign-On

This section 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).

You can configure SSO in your system using the [Configure Single Sign-On](#) common task that can be found in the [Application and User Management](#) work center.

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.

i 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 the URL that 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:
 1. 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.
 2. 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.
 3. 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*, that 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 need to get a suitable client certificate from a trusted Certificate Authority, then they can map the client certificate to their user ID.

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 certificate authorities for client certificates:

Trusted Certificate Authorities

Country	Organization	Organizational Unit	Common Name
BE	GlobalSign nv-sa	Root CA	GlobalSign Root CA
BM	QuoVadis Limited		QuoVadis Root CA 2 G3
BM	QuoVadis Limited		QuoVadis Root CA 2
CH	SwissSign AG		SwissSign Gold CA - G2
CH	SwissSign AG		SwissSign Platinum CA - G2
CH	SwissSign AG		SwissSign Silver CA - G2
DE	SAP SE		SAP Cloud Root CA
DE	SAP AG		SAP Global Root CA
DE	SAP IoT Trust Community II		SAP Internet of Things CA
DE	T-Systems Enterprise Services GmbH	T-Systems Trust Center	T-TeleSec GlobalRoot Class 2
DE	Atos		Atos TrustedRoot 2011
GB	COMODO CA Limited		COMODO RSA Certification Authority

Country	Organization	Organizational Unit	Common Name
GB	COMODO CA Limited		COMODO Certification Authority
GB	COMODO CA Limited		COMODO ECC Certification Authority
IE	Baltimore	CyberTrust	Baltimore CyberTrust Root
PL	Unizeto Sp. z o.o.		Certum CA
RO	certSIGN	certSIGN ROOT CA	
US	Starfield Technologies, Inc.	Starfield Class 2 Certification Authority	
US	Starfield Technologies, Inc.		Starfield Services Root Certificate Authority - G2
US	DigiCert Inc	www.digicert.com	DigiCert Assured ID Root CA
US	DigiCert Inc	www.digicert.com	DigiCert Global Root CA
US	DigiCert Inc	www.digicert.com	DigiCert Global Root G2
US	DigiCert Inc	www.digicert.com	DigiCert High Assurance EV Root CA
US	DigiCert Inc	www.digicert.com	DigiCert Assured ID Root G2
US	DigiCert Inc	www.digicert.com	DigiCert Assured ID Root G3
US	DigiCert Inc	www.digicert.com	DigiCert Global Root G3
US	Entrust, Inc.	(c) 2009 Entrust, Inc. - for authorized use only, See www.entrust.net/legal-terms	Entrust Root Certification Authority - G2
US	Entrust, Inc.	(c) 2006 Entrust, Inc., www.entrust.net/CPS is incorporated by reference	Entrust Root Certification Authority
US	The Go Daddy Group, Inc.	Go Daddy Class 2 Certification Authority	
US	GoDaddy.com, Inc.		Go Daddy Root Certificate Authority - G2
US	The USERTRUST Network		USERTrust RSA Certification Authority

Country	Organization	Organizational Unit	Common Name
US	Amazon		Amazon Root CA 1
US	Internet Security Research Group		ISRG Root X1
US	Internet Security Research Group		ISRG Root X2
US	Google Trust Services LLC		GTS Root R1
US	Google Trust Services LLC		GTS Root R2
US	Google Trust Services LLC		GTS Root R3
US	Google Trust Services LLC		GTS Root R4
	Entrust.net	(c) 1999 Entrust.net Limited, www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)	Entrust.net Certification Authority (2048)
	GlobalSign	GlobalSign Root CA - R3	GlobalSign
	GlobalSign	GlobalSign ECC Root CA - R4	GlobalSign

For more information about trust configuration, see [Configuring the System to Use the SAP Trust Center Service on Help Portal](#).

5.3.3 Logon Using User ID and Password

Users log on to the solution 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 \[page 26\]](#).

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.

5.4 Security Policy

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 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 the *Edit Security Policies* under *Common Tasks* of *Application and User Management* work center. 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 \[page 32\]](#).

6 Authorizations

6.1 Authorizations 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 Customer OnDemand, 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 user has read or write access to data in a work center view.

You can only assign business roles that determine the authorization. The solution provides the user with access to all the business documents and Business Task Management items in that work center view.

You can restrict access to specific data based on 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 gets an 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 gets both the 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.

6.3 Segregation of Duties

If the user has been assigned to multiple work centers, the 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.

Users can define their own conflicts in addition to the ones delivered by SAP. The conflicts defined by SAP can be overridden or disabled.

Segregation of Duties Conflicts

Segregation of duties is designed to minimize the risk of fraud and errors, and protect company assets such as data or inventories. This is done through the appropriate assignment of access rights by distributing

responsibility for business processes and procedures amongst several users. For example, the requirement to have two employees responsible for the payment process. One employee creates a check and second employee signs it, ensuring that the responsibility for spending company finances is shared between two users.

The segregation of duties check in the *User and Access Management* view of the *Application and User Management* work center enables key users to assign access rights which are free of conflicts. Based on this information key users can alert business process owners to existing conflicts, so that they can implement process controls to mitigate the conflicts.

When you assign access rights in form of work center views to a user, the system checks if there is a segregation of duties conflict in the view assignment. A segregation of duties conflict occurs when a user has access to a set of work center views that could enable him to make an error or commit fraud, thereby damaging company assets. If there is a conflict, it is indicated by a red light and details of the conflict display under Conflict Description. Depending on the assignment, the system displays a list of conflicting work center views and a possible solution, for example, assign the two work center views to different users.

If it is not possible to separate duties, management should ensure there are mitigating controls in place outside the system, to prevent errors from being easily concealed and ensure that financial irregularities do not occur. There are other non-preventive control mechanisms that can help to mitigate segregation of duties conflicts including audit trails, reports, logs, and reviews by a supervisor.

Segregation of Duties Rules

The system provides you with a series of rules to assist you in protecting your company's assets and prevent irregularities. As different business scenarios might have different kinds of segregation of duty needs, in SAP Business ByDesign, we also provide a way to define the segregation of duty as required and demanded for your business. This includes:

- Changing the description of the standard conflict information provided
- Creating the additional segregation of duty conflicts
 - Between standard views
 - Between partner created views
 - Between standard and partner created views
- Deactivating the standard segregation of duty conflicts
- Converting standard / customer defined conflicts to technical conflicts, ensuring that the 2 views that are conflicting are not assigned to the users together
- Defining new technical conflicts between views where you would like to ensure the authorizations are assigned together

In case of a rule violation, the system provides details of the segregation of duties conflict, infringement details, possible solution, and proposals for mitigating controls.

- The system does not check the separation of maintaining master data and transactional data for all work centers.
- Even if you ensure that each rule is implemented, this does not guarantee that your system is completely compliant.

Conflict Type

There could be two types of conflict between two work center views in the system:

- Segregation of Duty Conflict
- Technical Conflict - workcenter views which can't be assigned together to any user

Configure Work Center View Conflicts

To customize and configure the conflicts as suited to your business, you need to follow the steps below:

- Scope in the functionality through scoping the business option *Do you want to define new or configure the SAP delivered work center view conflicts?*. This option can be found in *Built-in Services and Support* element within *System Management* under *User and Access Management*.
- After the scoping changes, new work center view *IAM_VIEW_CONFLICT* starts appearing in *Edit Access Right* screen for assignment.
- Assign this work center view to all the users who should be authorized for this functionality.
- Once authorized, user can find the *Work Center View Conflicts* view in the *Application and User Management* work center.

Restrictions on Configuring the Work Center View Conflicts

- Customer can't delete any conflict but they can disable SAP delivered SoD conflict and their own conflicts.
- SAP delivered Technical Conflicts can't be disabled.
- Self-conflicting view can't be defined as technical conflicts.
- A technical conflict can't be enabled in the system if the same combination of views is already assigned to any use
- Multiple entries are not allowed for the same combination of work center view.

7 Mobile Applications

7.1 General Information

The following table provides information about the mobile devices on which you can run SAP Business ByDesign.

SAP Cloud Solution	Device/Operating System	
	iPhone/iPad	Android
SAP Business ByDesign Mobile	X	X
SAP Time Recording		No longer supported
SAP Manager Approvals		No longer supported

With the SAP Business ByDesign 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 apps connect to the SAP Cloud solution in the same way as personal computers do.

The functionality of SAP Time Recording and SAP Manager Approvals applications are covered by the central SAP Business ByDesign Mobile application.

7.2 Mobile Apps

You can download the mobile apps for SAP Business ByDesign from the respective stores.

- Download the app for the Apple® iPhone® or iPad® from the iTunes Store®.
- Install the app for Android® smartphones from the Google Play Store™.

7.3 Authorizations

When you use the mobile solution, you use the same URL address and logon credentials as for the desktop application.

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 SAP Business ByDesign Library on the Help Portal.

7.4 Secure System Access and Authentication

Access from mobile devices via the native 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.

7.5 Password Change and Password Reset

When logging on to the SAP Business ByDesign 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. The encryption key is protected by 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 SAP Business ByDesign from it.

As an administrator, you can specify the length of time after which the mobile user must re-enter the app password to log on to the system.

7.6 Special Considerations

Unlike stationary personal computers, mobile devices are at greater risk of being lost or stolen.

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

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

7.7 Data Storage

The mobile apps store two types of data on the mobile device, as outlined in this section.

7.7.1 Password Retention

When logging on to the SAP Business ByDesign from a mobile app, the user is required to provide the user ID and system password.

The password can be stored on the device as described in the section [Password Change and Password Reset \[page 32\]](#).

7.7.2 Cache Files

To improve the mobile app's performance, metadata is stored on your mobile device.

The cached information contains technical data that describes the user interface.

You can upload pictures and other files from the mobile device to the 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.

8 Front-End Security

SAP Business ByDesign front end consists of Web application user interfaces based on HTML5 technology.

8.1 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.

The following are some of the features that HTML5 supports:

- 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

For more information, see the security information for HTML5.

9 Security of Data Storage and Data Centers

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

For more information about the data center security measures, visit <https://www.sap.com/about/trust-center/data-center.html>.

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, SAP Business ByDesign 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 the 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 SAP Business ByDesign employs a number of security technologies. The multilayered, partitioned, proprietary network architecture permits only authorized access to the data centers that support the 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

i Note

Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose. Furthermore, persons or organizations that collect and manage personal information must protect it from misuse and must respect certain rights of the data owners that are guaranteed by EU law.

Customers can opt for the European data centers, and they can geographically limit remote access to their data and installations to SAP support centers and subcontractors located in the European Union, European Economic Area, and Switzerland.

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.

10.1 Confirm The Signature

All additional applications of SAP Business ByDesign solution 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.

10.2 Saving Logon Data

SAP front-end components never share an existing authentication session on solution, 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 Transport Layer Security (TLS) protocol, to the 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.

10.3 Intelligent Robotic Process Automation (IRPA)

→ Remember

Some of the SAP Best Practices for Intelligent Automation for SAP Business ByDesign are using OData or SOAP services for the backend connection to SAP Business ByDesign. These services are using basic authentication (user name and password). For storing the users and passwords used for the bots (no

matter if the bot is using the front end or backend) we were designing our template bots to use the Windows® Credential Manager, but you may adapt the bot to use other similar secure storage systems. Also, regardless of whether the bot is design to use the front end UI or the back end services, we highly recommend that you create individual technical users (communication arrangement) for each “bot + business user / business scenario” pair in order to be able to distinguish whether the action was carried out by a physical business user or by a robot and to have full traceability on the bots and human actions individually. As per any other best practices, the user must not share their bot credentials with anyone else.

11 Other Security-Relevant Information

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 Business ByDesign offers many data extraction features such as: mass data maintenance, excel downloads etc.

⚠ Caution

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

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

- 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
- In case of mobile devices:
 - "Jail Broken" devices are not considered secure and are prone to security related issues than normal devices. So, it is recommended not to allow usage of the jail broken device with SAP Business ByDesign.
 - Enable remote management software that allows you to lock the device remotely, or wipe data from it

11.1 Service Composition Security

This section describes security considerations that apply to the built-in mashups integration and Web services composition capabilities of SAP Business ByDesign solution. 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.

11.1.1 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 Business ByDesign solution screen by configuring the URL with dynamic parameters that are derived from the screen out-port interface of the 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 to 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.

11.1.2 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 the solution screen by configuring the URL with dynamic parameters that are derived from the 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 Transport Layer Security (TLS), 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.

11.1.3 Map Mashup Integration

SAP Business ByDesign solution use Microsoft® Bing Maps™ as a built-in map service provider. Both administrators and end users can configure the map mashup usage on the 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.

11.1.4 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 Business ByDesign solution. 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 Business ByDesign 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 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 the SAP Business ByDesign 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 Business ByDesign solution, we recommend that you ensure that it confirms to your company's security policies.

11.2 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 <http://help.sap.com/disclaimer?site=http://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

11.2.1 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.

Certificate/Report	Interval	Conducted by
ISAE-3402/SSAE-16 (SAP Business By-Design)	Twice a year	External accounting company
ISO 27001 (SAP Cloud Operations)	Once a year	Accredited auditing company

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

12 Security-Relevant Logging and Tracing

Data processing systems store master data and transactional data used to perform business processes and to document them. In many countries, the storage, disclosure, and deletion of personal data of natural persons from data storage systems must be in accordance with statutory data protection laws.

The Information Lifecycle Management (ILM) work center allows those responsible for data privacy in an organization to respond to requests to disclose personal information, to delete it and to track read access to special categories of data.

i Note

In this document, natural persons, for instance, employees, private accounts, contacts, and service agents are collectively referred to as business partners. Only data of natural persons (also called data subjects) is managed within the Information Lifecycle Management work center. Corporate business partners are not included.

Relevance

Applies if your organization wishes to disclose personal data or delete it if requested by natural persons. The ILM work center is also relevant if you want to monitor and log read access of sensitive information, for example bank data.

Prerequisites

- You have enabled Information Lifecycle Management in the scoping phase of *Business Configuration*:
▶ *Built-in Services and Support* ▶ *System Management* ▶ *Information Lifecycle Management* ▶
- The required statutory retention periods have been specified in the fine-tune phase of *Business Configuration*, in the *Business Document Deletion - Retention Periods for Business Documents* activity.

⚠ Caution

Users who are authorized to access the *Information Lifecycle Management* work center are entitled to perform **all** data privacy functions within this work center, including the disclosure and deletion of a business partner's personal data. Access to this work center is granted in the *Application and User Management* work center.

12.1 Information Lifecycle Management for Data Privacy

In the *Information Lifecycle Management* work center, you can:

- **Analyze Business Documents**

Analyze business documents, their relations to other documents as well as information specific to business partners, to identify deletable information and detect possible issues that may interfere with document deletion.
- **Disclose Personal Data**

Disclose personal data of business partners (employees, private accounts, service agents, and contacts) who request it.
- **Delete Personal Data**

Delete personal data of business partners once the end of the retention period has been reached.
- **Read Access Logging**

Certain categories of personal data are considered sensitive due to their criticality and importance. You can activate tracking of read access to such personal data. Carefully review the groups of such personal data available and activate read access logging for those groups that are processed by your organization. This is possible in the *Field Group Configuration* and *Log Display* views.

 - *Field Group Configuration*

In this view, you can select available field groups to activate or deactivate them for read access logging. You can select a field group and click *Activate*, if you want to see the access log for that field group data. You can deactivate a field group by clicking *Deactivate*, if you do not want that field group information access to be seen in the log.
 - *Log Display*

In this view, you can find the files containing the read access logs for the specific period. This view lists the read access logs generated on a periodic basis for download. You can select a specific entry to download the content. You can set the queries for *Start Date Time* and *End Date Time* and click *Go*. It will display the dates selected. You can also save the queries. You can track and download the access log by clicking *Download*. These log files are not intended to be stored in the SAP Business ByDesign system and will be deleted automatically after a few weeks. A web service is provided to permit automated downloads on a regular base.
- **Business Configuration**
 - Specify Retention Periods

You can determine retention periods on a company level in the fine-tune phase of the *Business Document Deletion - Retention Periods for Business Documents* activity.
 - Enable Read Access Logging in Business Configuration

You can enable read access logging using a business option in the *Business Configuration* work center. To find this business option, choose your *Implementation Project* in the *Business Configuration* work center and click *Edit Project Scope*. In the *Questions* step, navigate to ► *Built-in Services and Support* ► *System Management* ► and select *Security*. Within the business option group *Data Privacy*, confirm the question *Do you want to switch on the Read Access Logging for sensitive personal data?*.
 - Assign work center views

You can assign the *Field Group Configuration* and *Log Display* work center views to the person responsible for data protection and privacy from the *Application and User Management* work center.

12.2 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 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.

13 Best Practices

User Management and Authorizations

- User authorizations are critical, that decides what kind of activities the user can perform in the system. So, carefully review the kind of authorizations required for each user based on the roles they play and the business needs, grant only those authorizations to the users.
- Segregation of duties is designed to minimize the risk of errors and fraud, and to protect company assets, such as data or inventories. Therefore, carefully review all segregation of duty conflicts displayed in red. Go through the information or risk and mitigation, take necessary steps to ensure the risks are mitigated.
- Based on your company's business needs, you might have different sets of authorizations, that can lead to conflict of segregation of duties apart from the standard ones. You must, redefine the segregation of duties as and when required to add/suppress/change the description to reflect the details as applicable to your industry.
- If in case granting two views is critical than just optional, you can increase the severity from segregation of duty conflicts to *Technical Conflicts*, that prevents assigning of views together.
- Increasing severity to technical conflicts is possible only when all existing users assigned the two views together are adapted to ensure that they do not have both the views together. Review the authorizations to identify which of the two views are necessary for the user to perform the roles and then take decision for every user individually.
- Business role is the recommended way of assigning the authorizations to the users as it enables paternalizing and reusability.
- Lock the users when they are no longer required to access the system.
- Request the users for service agents only when they need access to the system and ensure they are locked when the end of purpose is reached.
- Security policy determines the strength of password and other aspects. Based on the criticality of role of employees, have different security policies emphasizing on the strong security needs based on critical business functions performed.
- Critical business functions like user management, data privacy management have high impact on the overall security of the system. Assign the authorizations to only those users who are designated to perform these tasks. Avoid assigning these authorizations to all business users in the system.
- Proposed work center views are to assist the authorization granting. Carefully review the authorizations along with the detailed restrictions proposed for the user before saving the authorizations.
- In some cases, the same activities can be performed in multiple views and these views are granted to the user with different restrictions, thus summing up the access rights required to perform the activity. Checking access rights consistency enables you to identify these views, and activities displayed on executing this screen indicate some access rights are inconsistent. Review the access rights consistency to adjust the authorizations of the user to avoid unexpected authorization behavior.
- When accessed from the *Audit* work center, the available views are normally read-only except when they are granted from the work centers in which these views are in write mode. Review the authorizations granted to the *Audit* work center along with other authorizations granted to the user.

Data Access and Environment

- Public and unprotected networks are vulnerable to easy security attacks. Therefore, it is recommended to access your business software in a protected network environment.
- Publicly available devices and the devices that are accessible to multiple people are potentially vulnerable to viruses and security issues. Therefore, it is recommended to access your business software from those devices that are protected and accessible to only a closed set of members within the network.
- “Jail Broken” devices are not considered secure and are prone to security related issues than normal devices. Therefore, it is advised to be cautious while allowing usage of the Jail Broken device with SAP Business ByDesign.
- Customer Specific Trust List will facilitate inclusion of additional list of CAs, that can be trusted for your business processes. You / your administrator needs to perform all mandatory processes / steps as per your company policy and as per the legal requirements of your country / country of business before adding the CA to your trusted CAs list.
- Checking MIME type for the documents to be uploaded into the business system provides additional possibility to identify issues with content. Therefore, it is recommended to have MIME type check activated in the system.
- Review the list of MIME types that are activated, to ensure only those types relevant and required for your business processes are allowed.
- When checking documents, the system assigns unknown MIME types to the **application/octet-stream** MIME type. If you define the application/octet-stream MIME type as allowed, all documents whose MIME types are not specified in the MIME type list can be uploaded. This MIME type is available for fallback purposes. Therefore, we recommend that you should not define the **application/octet-stream** MIME type as allowed until emergency. During Emergency, carefully scan the documents before uploading them.
- Mashups might be deals with third party solutions, that can transfer / store critical business data. Therefore, we recommend that you ensure that the mashups conform with your company's security and data privacy policies.

Data Privacy

- Personal data is critical information related to individual persons. Therefore, assign the *Information Lifecycle Management* work center and work center views which process personal data only to the people who access and process them.
- If the business needs to process personal data, several country and regional regulations might require a legal basis. One of the legal grounds is the consent of the individual for the processing of personal data. Different countries provide specific guidelines for the legal grounds to process the personal data like contract, legal obligation, protection of vital interest, public interest and legitimate interest. While processing the personal data, carefully review the need and required consent or other legal grounds to be fulfilled as per your country and regional regulations.
- Special case of personal data is sensitive due to the criticality and impact of people knowing it. Various country and regional regulations require special and restricted handling of such data. Therefore, it is recommended to restrict access to such data by authorizing only the designated users such as the data privacy officer or human resources officers to process this information.
- Review all partner created applications to ensure that they are processing and treating the personal and special case personal data in the right way.



- Contact your partner to check if the applications created by them deal with personal and special case personal data, to take necessary steps to cater to the data privacy needs.
- Verify with the partner to ensure that no personal data in the application is written into technical processes like *Application Logs*.
- It is recommended not to take automated business decisions based on personal and special case personal data such as religion, birth place, etc. Avoid using the personal and special case personal data attributes as part of processes such as workflow definitions and responsibility determination process.
- Users with authorization to access the *Information Lifecycle 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 designated employees of your organization, with authorization to disclose/delete personal data receive access rights.
- Free text fields and general attachment sources in the documents is not able to automatically detect personal data persisted in them. Therefore, avoid usage of personal data related information in these kinds of sources.
- Incidents created from the system gets processed by the people outside the organization. Carefully review the content in the incident such as incident description text, screenshots supported as part of incident creation process and attachment to avoid exposing of personal data.
- Incident data in the system gets erased on a regular basis, to ensure any kind of personal data persisted as part of the information and the context collection is removed.

Important Disclaimers and Legal Information

Hyperlinks

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

About the icons:

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

Videos Hosted on External Platforms

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

Beta and Other Experimental Features

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

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

Example Code

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

Bias-Free Language

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

© 2022 SAP SE or an SAP affiliate company. All rights reserved.

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

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

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

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

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