SAP Cloud Platform Integration Security Guide
Content

1 Introduction .......................................................... 3
2 Technical Landscape ............................................. 4
3 Security Aspects of Processes ............................... 9
4 Security Aspects of Data, Data Flow .................... 10
5 Identity and Access Management .......................... 15
6 Data Storage Security ........................................... 17
7 Data Protection and Privacy ................................. 18
  7.1 Specific Data Assets ........................................... 19
8 Security-Relevant Logging and Tracing .................. 23
9 Other Security-Related Information ...................... 24
1 Introduction

Using a cloud-based integration platform imposes dedicated security measures on the software vendor (SAP) that hosts the platform as well as on those (the customers) who use the platform. This section describes the security-related aspects of the integration platform and shows which measures you can take in order to protect customer data that is passed on through the platform during the execution of an integration scenario.

Customers who use SAP’s cloud-based integration platform agree that a significant part of their (and their customers’) sensitive data is processed by and stored within an infrastructure owned by SAP.

The core task of an integration platform is to serve as the transit place for messages that may contain sensitive customer data. Therefore, first and foremost these messages must be protected against eavesdropping and unauthorized access.

Therefore, the following main requirements need to be fulfilled by the integration platform:

- The integration infrastructure provided by SAP is already designed and built in such a way that it meets the highest security standards. In particular, it must be guaranteed that the technical system landscape, the communication of the components of the integration platform, as well as the storage locations of messages are secure.

- The processes related to the usage of the platform meet the highest security standards. This relates to the processes at SAP that are related to the development and upgrade of the platform, the processes that are related to the provisioning and operation of the customers’ virtual environment by SAP, and the customer onboarding process during which customers set up secure connections between their infrastructure and SAP’s integration platform.

- Customers have several options to configure how messages are exchanged within an integration scenario so that the involved data is protected at the highest level. In particular, when designing integration flows, customers can choose between several options to protect messages by establishing secure communication channels (transport level security) and by configuring digital encryption and digital signing of messages (message level security).

This documentation summarizes the measures that are taken by SAP in order to fulfill these requirements.
2 Technical Landscape

The technical infrastructure comprises a set of technical components that can communicate with each other and with remote components in a secure way based on certain protocols such as HTTPS or SFTP, for example. In addition, user access to the technical infrastructure is designed in such a way that only users with well-defined permissions can access the different segments.

The following figure shows the high-level technical infrastructure and the main access points and connections. Areas in blue indicate components owned by customers, areas in gray are components that are owned by SAP (in most cases).
Components and Communication Paths

In technical terms, the integration platform is designed as a cluster of virtual machines (nodes) that runs within the SAP cloud. Although all users that connect to the platform through the Internet share the same physical infrastructure, each customer gets access to only one or more dedicated parts of the platform: accounts or tenants.

On each tenant, a clustered, virtual integration runtime is installed (referred to as a tenant cluster). Tenants are strictly isolated from each other with regard to their resources (such as CPU and memory) and to the data that is processed on them. Strictly speaking, each tenant stores data in a separate database schema (this is referred to as tenant isolation).
At runtime, the integration platform processes data that is exchanged between the involved participants on a cluster of different virtual machines hosted in the SAP Cloud. A cluster associated with a specific tenant is referred to as a **tenant cluster**.

**Note**

A virtual machine (VM) is a software implementation of a machine that executes a program like a physical machine.

The integration platform is designed in such a way that the involved virtual machines are strictly separated from each other with regard to the related customers. In other words, separate resources (memory, CPU, and file system) of the cloud-based integration platform are allocated to each customer – although all customers might share the same hardware. In addition, each tenant uses a separate database schema, which guarantees that the data of the different customers is strictly separated. This separation is also referred to as **tenant isolation**.

The following figure illustrates this concept for two customers communicating with each other.

![Diagram of tenant cluster](image)

The constituents of a tenant cluster are tenant management nodes and runtime nodes.
A tenant management node accomplishes tasks related to the management of a tenant cluster. It takes requests from the dialog users (for example, when an integration developer deploys an integration flow using the Web user interface). The tenant management node also manages the runtime nodes.

A runtime node processes messages that are exchanged with external components. Therefore, the runtime node is connected to the external systems. In other words, runtime nodes process customer data that might be confidential and has to be protected.

Typically, one tenant management node has one or more runtime nodes assigned to it. However, in order to support failover scenarios, more than one tenant management node can be operated in a tenant cluster.

As a consequence of this cluster design, the following main communication paths are active during the operation of an integration scenario:

- Communication of tenant cluster and remote components
  
  You can use both cloud systems and on-premise systems (such as on-premise SAP systems) as remote components. Remote receiver systems are directly connected to the runtime node through a protocol, which depends on the type of the designed receiver adapter. If the integration platform communicates with an on-premise receiver system, you can interconnect the SAP Cloud Connector. This component runs as on premise agent in a secured network and acts as a reverse invoke proxy between the on premise network and SAP Cloud Platform Integration. Due to its reverse invoke support, you don’t need to configure the on premise firewall to allow external access from the cloud to internal systems.
  
  For communication in the opposite direction, a load balancer is interconnected between remote sender systems and the involved SAP Cloud Platform components. The load balancer terminates incoming Transport Layer Security (TLS) requests and establishes new ones.

- Communication within a tenant cluster: Within a tenant cluster, the tenant management nodes and runtime nodes communicate with each other through a messaging service.
  
  The internal network only allows specific communication (HTTPS) from one virtual machine to another, and this only by taking the loop to the load balancer (not depicted in the figure).

Various secure technical protocols can be used for these communication paths. Depending on the adapter type, the following protocols are available:

- Hyper Text Transfer Protocol (HTTP) over Transport Layer Security (TLS), which is referred to as HTTPS
- SSH File Transfer Protocol (SFTP) for the exchange of data with an SFTP server
- Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP)3, and Internet Message Access Protocol (IMAP) for the exchange of data with mail servers

**User Access**

In addition to the above mentioned components that interact with each other when messages are being processed and exchanged between the involved systems, additional components come into play when a dialog user accesses the infrastructure (for example, when an administrator accesses monitoring data or when an integration developer deploys an integration artifact).

People with different roles can access the infrastructure – both on the SAP side (as the provider of the integration infrastructure) and on the customer side. Human access points (for dialog users) are:

- Dedicated experts at SAP access the infrastructure to provide a tenant cluster for the customer.
- Experts on the customer side access the infrastructure to design and deploy integration content and to monitor an integration scenario at runtime (integration developers and tenant administrators).
Data Storage

Although the main focus of an integration platform is to receive, process, and forward messages, data can also be stored in dedicated steps during message processing (data at-rest).

The following kinds of data can be stored during the execution of an integration scenario:

- **Message content**
  The runtime node persists message content data in dedicated steps of an integration flow. This data is stored encrypted. The runtime node can also read message content data if the integration flow is designed in such a way that certain steps depend on this data (for example, in content-based routing scenarios).

- **Monitoring data**
  During message processing, the runtime node also persists monitoring data. Monitoring data records the executed processing steps. An administrator (with dedicated permissions) can access this data (for example, using the Web user interface).

Related Information

Data Storage Security [page 17]
3 Security Aspects of Processes

Processes that are related to the provisioning, update, and usage of the cloud-based integration platform meet the highest security standards.

Cloud Integration is compliant with various SAP-internal technical policies, procedures, directives, guidelines, and product standards.

In addition, employees and operators are bound to the SAP code of business conduct and other behavioral security standards such as clean desk and communication.

For example, SAP software is developed in compliance with the SAP Secure Development Lifecycle (SDLC), which helps to implement measures such as test-driven development and threat modeling.

4 Security Aspects of Data, Data Flow

All data in transit, either exchanged with remote components or internal, can be protected by methods such as encryption.

Data in transit can be protected at two levels:

During a scenario, the connected remote systems exchange data with each other based on the configured transport protocol. These protocols support different options to protect the exchanged data against unauthorized access. In addition to security at transport level, the content of the exchanged messages can also be protected by means of digital encryption and signature.

Transport Level Security

Each adapter allows you to set up a specific security level.

The following table lists the supported protocols.
<table>
<thead>
<tr>
<th>Transport Protocol</th>
<th>Transport Level Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFTP (Secure Shell File Transfer Protocol)</td>
<td>Secure Shell (SSH) is used to securely transfer files in an open network.</td>
</tr>
<tr>
<td></td>
<td>SSH uses a symmetric key length with at least 128 bits to protect FTP communication. The asymmetric key length used in SSH is typically 2048 bits, but at least 1024 bits.</td>
</tr>
<tr>
<td></td>
<td>The following authentication methods are supported:</td>
</tr>
<tr>
<td></td>
<td>• User name/password authentication (where the SFTP server authenticates the calling component based on the user name and password)</td>
</tr>
<tr>
<td></td>
<td>• Public key authentication (where the SFTP server authenticates the calling component based on a public key)</td>
</tr>
<tr>
<td></td>
<td>Secure data transfer with SFTP is based on a combination of symmetric and asymmetric keys. Symmetric (session) keys are used to encrypt and decrypt data within a session. Asymmetric key pairs are used to encrypt and decrypt the session keys.</td>
</tr>
<tr>
<td></td>
<td>When asymmetric key pairs are used, SFTP also ensures that only authorized public keys are used by the involved participants.</td>
</tr>
<tr>
<td></td>
<td>The following versions are supported:</td>
</tr>
<tr>
<td></td>
<td>• SSH version 2 (as specified at <a href="http://tools.ietf.org/html/rfc4251">http://tools.ietf.org/html/rfc4251</a>)</td>
</tr>
<tr>
<td></td>
<td>• SSH File Transfer Protocol (SFTP) version 3 or higher</td>
</tr>
<tr>
<td></td>
<td>This protocol is supported by the SFTP sender and receiver adapter.</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>Transport Level Security</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>HTTP(S) (Hypertext Transfer Protocol Secure)</td>
<td>You can protect communication using Transport Layer Security (TLS). In this case, a symmetric key length of at least 128 bits is used (which is technically enforced). The asymmetric key length used in TLS is typically 2048 bits, but at least 1024 bits.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>SAP Cloud Platform Integration supports TLS 1.0, 1.1 and 1.2 for inbound and outbound communication for all HTTP(S)-based channels.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The HTTP receiver adapter also allows to use HTTP URLs. However, SAP does not recommend to use this options when transferring confidential data (including the password for basic authentication).</td>
</tr>
<tr>
<td></td>
<td>It also cannot be verified if the result of an HTTP request originates from a trustworthy source in case the network is not entirely trusted. Therefore, SAP does not recommend to use this option for productive scenarios over the Internet.</td>
</tr>
<tr>
<td></td>
<td>Authentication based on SSL certificates (X.509)</td>
</tr>
<tr>
<td></td>
<td>- Basic authentication</td>
</tr>
<tr>
<td></td>
<td>The client authenticates itself to the server based on user and password.</td>
</tr>
<tr>
<td></td>
<td>- Certificate-based authentication</td>
</tr>
<tr>
<td></td>
<td>The client authenticates itself to the server based on a certificate, which is signed by a trusted authority (certification authority, or CA for short).</td>
</tr>
<tr>
<td></td>
<td>- For specific scenarios also SAML Bearer Ticket-based authentication is supported for inbound traffic.</td>
</tr>
<tr>
<td></td>
<td>For HTTP-based receiver adapters, also principal propagation via SAP Cloud Platform Connector is supported.</td>
</tr>
<tr>
<td></td>
<td>This protocol is supported by all adapters that allow communication over HTTPS (for example, the IDoc adapter, the SOAP adapters, and the HTTP adapter).</td>
</tr>
<tr>
<td>SMTP (Simple Mail Transfer Protocol)</td>
<td>These protocols are supported for the exchange of emails (in combination with the Mail adapter).</td>
</tr>
<tr>
<td>POP3 (Post Office Protocol)</td>
<td></td>
</tr>
</tbody>
</table>
Transport Protocol

IMAP (Internet Message Access Protocol)

Transport Level Security

Transport encryption is supported via the STARTTLS extended operation.

Authentication using plain user/password or CRAM-MD5 (Challenge-Response Authentication Mechanism, Message Digest 5) to avoid transmitting passwords in clear text.

Note

The (optional available) password-based authentication only applies for the communication between the Cloud Integration system and the mail server. The communication between mail servers is usually not authenticated. Therefore, data received by mail must not be considered as coming from a trustworthy source, unless other security measures (such like digital signatures on message level) are applied.

Note

Basic authentication is recommended for test purposes only. For productive scenarios, we recommend that you use certificate-based authentication.

Message Level Security

On top of the transport level security options, you can also secure the communication at message level, where the content of the exchanged messages can also be protected by means of digital encryption and signatures. Various security standards are available to do this, as summarized in the table below.

To configure message level security options, you use dedicated integration flow steps (for example, the Encryptor and Signer step type).

The following standards and algorithms are supported.

Table 2: Message-Level Security Standards and Algorithms

<table>
<thead>
<tr>
<th>Standard</th>
<th>Security Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKCS#7/CMS Enveloped Data and Signed Data</td>
<td>Encryption/decryption of message content</td>
</tr>
<tr>
<td>PKCS#7/CMS Enveloped and Signed Data</td>
<td>Encryption/decryption and signing/verifying payload</td>
</tr>
<tr>
<td>Open Pretty Good Privacy (PGP)</td>
<td>Encryption/decryption of message content</td>
</tr>
<tr>
<td></td>
<td>Encryption/decryption and signing/verifying the message</td>
</tr>
<tr>
<td>Standard</td>
<td>Security Feature</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>XML Signature</td>
<td>Signing/verifying payload</td>
</tr>
<tr>
<td>WS-Security</td>
<td>Signing/verifying SOAP body</td>
</tr>
</tbody>
</table>
Identity and Access Management

Identity and access management features of SAP Cloud Platform are used during the lifecycle of an integration scenario.

Access Management

Dialog users who access the platform are authenticated against an identity provider. By default, SAP Identity Service (ID Service) is used. SAP ID Service is the central service for the process of managing identities and their lifecycles.

The authentication of inbound calls to the platform depends on the chosen authentication mode. In case the client sends a client certificate, the authentication is done by the load balancer. As the load balancer terminates the TLS connection, it checks the client certificate of the calling component against a list of trusted certification authorities (CAs). This certificate is mapped to a user. If basic authentication is configured, the calling entity is checked by the connected identity provider. Besides client certificate authentication, the platform supports basic authentication, OAuth and Security Assertion Markup Language (SAML).

User Management and Authorizations

Access to dedicated functions of the platform is controlled and protected by authorization checks. To manage the authorizations of dialog users, a number of authorization groups are available. An authorization group defines a set of dedicated permissions. Authorization groups are designed along the persona and tasks that come into play during the lifecycle of an integration project.

Note

Example:

If the logged-in user has to perform only tasks like designing and deploying integration flows, the user has to be assigned with the authorization group AuthGroup.IntegrationDeveloper.

Authentication and Authorization Options for Inbound Calls

For HTTPS-based (inbound) requests from a sender system that calls the integration platform, there are different ways for the calling sender to authenticate itself against the integration platform. The options are client certificate authentication, basic authentication, OAuth and SAML.

Detailed access to the resources of the integration platform is controlled by certain authorization options. Within sender channels that are based on transport protocol HTTP authorization options are User Role and
Client Certificate, whereas the usage of Client Certificate is deprecated. Instead of this, a certificate-to-user mapping should be maintained. When using this option, within user management a role has to be assigned to the user to grant access to the resource.

Note

- Authentication
  Verifies the identity of the calling entity.
- Authorization
  Checks what a user or other entity is authorized to do (for example, as defined by roles assigned to it).
  In other words, the authorization check evaluates the access rights of a user or other entity.

Authentication and authorization options can be combined in a specific way for inbound communication.
6 Data Storage Security

Customer data can be stored in dedicated steps during message processing.

Customer data stored at rest is strictly separated and isolated for each tenant. Although different tenants might share a common physical infrastructure, each tenant stores its data in a separate schema.

For certain use cases the customer can configure if the data at rest is encrypted.

Message content can be stored encrypted. If this security measure is configured, the encryption key that is generated automatically is unique for each tenant and is renewed periodically.

Data storage encryption uses AES and a key length of 256 bits. The encryption key is not stored in the same location as the encrypted data.

Kinds of Stored Data

The following kinds of data can be stored during the execution of an integration scenario:

- Message content
  The runtime node writes message content data to the in dedicated steps of an integration flow. There is the option to either store message content for a longer time period (the default is 30 days) or temporarily. Temporarily stored message content can be used for subsequent message processing steps. Such steps can then also read message content from the . There is the option to configure the retention period of the message content.

- Monitoring data
  During message processing, the runtime node also writes monitoring data to the . Monitoring data comprises the message processing log (MPL), which records the executed processing steps.

Physical Site

Customer data is stored in various regions worldwide. Here, highest security standards are met. To mention a few examples, redundant power supplies are used and physical access is restricted by means such as biometric access control mechanisms. All of these measures are regularly checked and audited.

More information: http://www.sapdatacenter.com
7 Data Protection and Privacy

Various types of customer data are processed by and stored on the integration platform at different times. This data gets the highest level of protection, and SAP takes dedicated measures to guarantee this security level.

Protected Types of Data and Protection Measures

The following types of sensitive data need to be protected during the operation of an integration scenario (examples):

- **Message content**
  Messages processed on a runtime node typically contain business data of an integration scenario and therefore can contain sensitive customer data such as addresses, names, or financial information. When this data is **at-rest**, it can be stored encrypted. Note however, that in some use cases the customer can configure that the data is not encrypted. When this data is **in-transit**, several measures can be taken, such as digital message signing or message content encryption.

- **Monitoring data**
  The message processing log records the processing steps of an integration flow. Only users assigned to this tenant and with dedicated permissions can access this data.

- **Other data, such as the content of log files**

**Note**

Personal data processed by and stored on the integration platform is handled according to the Data Processing Agreement, which you can find at [http://www.sap.com/about/agreements.html](http://www.sap.com/about/agreements.html) under SAP Cloud Services Customers.

Due to the tenant isolation concept, data from different customers (stored in different tenants) is strictly isolated from each other. Additionally, SAP has no access to data stored in customer tenants.

In exceptional cases, however, dedicated SAP employees can get restricted temporary permissions to execute specific tasks (for example, error analysis tasks in support cases). These permissions are granted by the customer to specific groups only (for example, to members of the SAP Operations team). Furthermore, these permissions are typically limited to the assignment of read permissions using authorization group AuthGroup.ReadOnly.

Also, the need-to-know principle (least privilege) is applied: Permissions are restricted/limited to the minimum set of privileges required to perform a specific task.

Every SAP employee who could have access to data stored within SAP Cloud Platform must successfully complete human resource security measures in accordance with applicable law.

For more information, see the document [SAP Cloud Platform Security: Trust Matters](#) under Data Governance and Legal Compliance.
Audit Logging and Tracing

Audit logs allow administrators at SAP to monitor events such as data read accesses or system configuration changes. This enables them to proactively take the necessary measures to prevent malicious usage of the system.

Related Information

Security-Relevant Logging and Tracing [page 23]
Data Storage Security [page 17]

7.1 Specific Data Assets

Different kinds of data are stored in the SAP Cloud Platform Integration infrastructure during the lifecycle of an integration project.

The following table lists the different kinds and attributes such like storage location and retention time, for example.

Table 3: Data Assets

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
<th>Logical Storage</th>
<th>Classification</th>
<th>Can Contain Personal Data</th>
<th>Retention Time</th>
<th>Backup Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message processing log</td>
<td>Structured information on the processing of a message</td>
<td>Log data</td>
<td>No</td>
<td></td>
<td>30 days</td>
<td>14 days</td>
</tr>
<tr>
<td>Message processing log attachments</td>
<td>Data attached to a message processing log during runtime</td>
<td>Message store</td>
<td>Log data</td>
<td>Business data</td>
<td>30 days</td>
<td>14 days</td>
</tr>
<tr>
<td>Audit log</td>
<td>Information on events such as data read accesses or system configuration changes</td>
<td>Log data</td>
<td>Yes</td>
<td></td>
<td>30 days</td>
<td>14 days</td>
</tr>
<tr>
<td>Data</td>
<td>Description</td>
<td>Logical Storage</td>
<td>Classification</td>
<td>Can Contain Personal Data</td>
<td>Retention Time</td>
<td>Backup Available</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>---------------------</td>
<td>---------------------------</td>
<td>----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Integration flow tracing data</td>
<td>Information on the message flow (including the message payload) and on errors that occurred during message processing</td>
<td>Trace store</td>
<td>Log data</td>
<td>Yes</td>
<td>60 minutes</td>
<td>14 days</td>
</tr>
<tr>
<td>Integration content (design time)</td>
<td>Integration flow models and value mappings created or edited by an integration developer</td>
<td>Workspace</td>
<td>Configuration data</td>
<td>Yes</td>
<td>Unlimited</td>
<td>14 days</td>
</tr>
<tr>
<td>Integration content (runtime)</td>
<td>Camel XML representation of integration flows and other design time entities (as deployed on a runtime node)</td>
<td>Configuration data</td>
<td>Yes</td>
<td>Unlimited</td>
<td>14 days</td>
<td></td>
</tr>
<tr>
<td>Data stored by Data Store operations step</td>
<td>Description</td>
<td>Logical Storage</td>
<td>Classification</td>
<td>Can Contain Personal Data</td>
<td>Retention Time</td>
<td>Backup Available</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-------------</td>
<td>----------------</td>
<td>----------------</td>
<td>---------------------------</td>
<td>----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Message content stored in dedicated steps in an integration flow (contains information such as message GUID, message processing log GUID, tenant ID, time stamp, and payload). Is used for further message processing in subsequent steps in an integration flow.</td>
<td>Data store</td>
<td>Business data</td>
<td>Yes</td>
<td>Can be defined by integration developer (default value: 90 days)</td>
<td>14 days</td>
<td></td>
</tr>
<tr>
<td>Message content stored in dedicated steps in an integration flow (contains information such as message GUID, message processing log GUID, tenant ID, time stamp, and payload) Can be accessed and analyzed after message processing.</td>
<td>Message store</td>
<td>Business data</td>
<td>Yes</td>
<td>90 days</td>
<td>14 days</td>
<td></td>
</tr>
<tr>
<td>Message content stored by JMS adapter</td>
<td>Message content stored in JMS message queues</td>
<td>JMS queue</td>
<td>Business data</td>
<td>Yes</td>
<td>Can be defined by integration developer (default value: 90 days)</td>
<td>Not supported</td>
</tr>
<tr>
<td>Data</td>
<td>Description</td>
<td>Logical Storage</td>
<td>Classification</td>
<td>Can Contain Personal Data</td>
<td>Retention Time</td>
<td>Backup Available</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------</td>
<td>----------------</td>
<td>----------------------------</td>
<td>----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Lock entries</td>
<td>Lock entries that are created (in the in-progress repository) to avoid the same message being processed several times in parallel (for example, by different runtime nodes)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>14 days</td>
</tr>
</tbody>
</table>
8 Security-Relevant Logging and Tracing

Audit logs allow administrators at SAP to monitor events such as data read accesses or system configuration changes. This enables administrators to take adequate measures to prevent malicious usage of the system.

Audit logs are generated for all virtual machines (nodes) of the customer’s tenant clusters as well as for the load balancer. These logs can cover events such as:

- Remote accesses to the system
- Changes to the setup of a tenant cluster (for example, if VM has been started or stopped)
- Changes to the configuration (for example, an integration flow has been deployed or undeployed)
- Changes of the tenant configuration

An audit log records the following type of information for each logged event:

- Type of the event
- Date and time of the event
- Initiator of the event
- Source of the event

A system from Splunk is used to provide audit logs. Audit logs related to different customers are separated from each other (according to the tenant isolation feature).

Audit logs are kept for 18 months.
9 Other Security-Related Information

User Interface Security

Cloud Integration provides user interfaces for designing and deploying message flows, and monitoring them at runtime.

A Web tool (Web UI) and Eclipse-based tools are available to accomplish these tasks. The Web UI is implemented using JavaScript and HTML (UI5).

These user interfaces are built to prevent vulnerabilities such as cross-site scripting (XSS) and cross-site request forgery (XSRF). The built-in security capabilities of these technologies are used together with secure design and coding principles.

Security Measures for Remote API

You can access certain functions of Cloud Integration through application programming interfaces (APIs).

The OData API is protected by basic authentication.

In order to protect the API against CSRF (cross-site request forgery) attacks, modifying operations (for example, POST, DELETE) should be used in conjunction with session-based authentication and client-side CSRF handling.
Important Disclaimers and Legal Information

Coding Samples

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

Accessibility

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

Gender-Neutral Language

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

Internet Hyperlinks

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