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 .................... 13
6. Data Storage Security .................................. 17
7. Data Protection and Privacy .......................... 18
   7.1 Types of Stored Data ............................... 20
   7.2 Specific Data Assets ............................... 21
   7.3 Security-Relevant Logging and Tracing .......... 23
8. Other Security-Related Information ................. 25
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 to protect customer data that is passed 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, which may contain sensitive customer data. First and foremost, these messages must be protected against eavesdropping and unauthorized access.

Therefore, the integration platform must fulfill the following main requirements:

- 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 between the components of the integration platform, and 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 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 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 (even though 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**.

**Note**

All editions of SAP Cloud Platform Integration for process services include the usage of the SAP ASE Platform Edition with a disk space limit of 32 GB.

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 an 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 the 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 based on the underlying transport protocol.

### Transport-Level Security Options

<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>This protocol is supported by the SFTP sender and receiver adapter.</td>
</tr>
<tr>
<td></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.</td>
</tr>
<tr>
<td></td>
<td>Default length of asymmetric keys provided by SAP is 2048 bits.</td>
</tr>
<tr>
<td></td>
<td>Supported authentication methods:</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>Supported versions:</td>
</tr>
<tr>
<td></td>
<td>● SSH File Transfer Protocol (SFTP) version 3 or higher</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>This protocol is supported by all adapters that allow communication over HTTPS (for example, the IDoc adapter, the SOAP adapters, and the HTTP adapter). 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). Default length of asymmetric keys provided by SAP is 2048 bits.</td>
</tr>
<tr>
<td></td>
<td><strong>i Note</strong></td>
</tr>
<tr>
<td></td>
<td>SAP Cloud Platform Integration supports TLS 1.1, and 1.2 for inbound and outbound communication for all HTTP(S)-based channels.</td>
</tr>
<tr>
<td></td>
<td><strong>i Note</strong></td>
</tr>
<tr>
<td></td>
<td>The HTTP receiver adapter also allows you to use HTTP URLs. However, we do not recommend using this option when transferring confidential data (including the password for basic authentication). Also, if the network is not entirely trusted, there is no way to verify whether the result of an HTTP request originates from a trustworthy source. Therefore, we do not recommend using this option for productive scenarios over the Internet.</td>
</tr>
<tr>
<td></td>
<td><strong>Supported authentication methods:</strong></td>
</tr>
<tr>
<td></td>
<td>• Basic authentication</td>
</tr>
<tr>
<td></td>
<td>The client authenticates itself to the server based on a user and password.</td>
</tr>
<tr>
<td></td>
<td>• Client certificate authentication based on SSL certificates (X.509)</td>
</tr>
<tr>
<td></td>
<td>The client authenticates itself to the server based on a certificate, which is signed by a trusted certification authority.</td>
</tr>
<tr>
<td></td>
<td>• For specific scenarios, SAML Bearer Ticket-based authentication is also supported for inbound traffic.</td>
</tr>
<tr>
<td></td>
<td>Receiver adapters also support principal propagation via SAP Cloud Platform Connector.</td>
</tr>
<tr>
<td>SMTP (Simple Mail Transfer Protocol)</td>
<td>These protocols are supported for the exchange of e-mails (in combination with the Mail adapter).</td>
</tr>
<tr>
<td></td>
<td><strong>i Note</strong></td>
</tr>
<tr>
<td></td>
<td>The (optional) password-based authentication only applies to communication between the Cloud Integration system and the mail server. Communication between mail servers is usually not authenticated. Therefore, you must not assume that data received by mail comes from a trustworthy source, unless other security measures (such as digital signatures at message level) are applied.</td>
</tr>
<tr>
<td>POP3 (Post Office Protocol)</td>
<td>Transport encryption is supported via the STARTTLS extended operation.</td>
</tr>
<tr>
<td>IMAP (Internet Message Access Protocol)</td>
<td>To authenticate against the e-mail server, you can send user name and password in plain text or encrypted (the latter only in case the e-mail server supports this option).</td>
</tr>
</tbody>
</table>
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 types).

The following standards and algorithms are supported:

<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></td>
<td>Signing/verification of payload</td>
</tr>
<tr>
<td>PKCS#7/CMS Enveloped and Signed Data</td>
<td>Encryption/decryption and signing/verification of 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/verification of message</td>
</tr>
<tr>
<td>XML Signature</td>
<td>Signing/verification of payload</td>
</tr>
<tr>
<td>WS-Security</td>
<td>Signing/verification of SOAP body</td>
</tr>
</tbody>
</table>
5 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. SAP Identity Service (ID Service) is used by default. 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. If the client sends a client certificate, the authentication is done by the load balancer. The load balancer terminates the TLS connection; therefore, 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. A number of authorization groups are available to manage the authorizations of dialog users. An authorization group is based on a persona and defines a set of dedicated permissions relating to the tasks that come into play during the lifecycle of an integration project.

Note

Example:

If the logged-in user has to perform tasks such as designing and deploying integration flows, the user must be assigned the authorization group AuthGroup.IntegrationDeveloper.

Authorization for the Integration Developer

The tasks of persons with integration developer permissions (short: integration developers) constitute a key part of the SAP Cloud Platform Integration lifecycle. Permissions for the integration developer (who is in charge of modeling integration flows) are contained in the authorization group AuthGroup.IntegrationDeveloper.

Note that the roles contained in this authorization group give an integration developer full control over message processing during runtime.
More information:

During integration flow modeling, the integration developer defines how messages are mapped, which credentials are used, and to which recipients messages are sent. The set of roles provides very powerful permissions and in some cases allows the integration developer to access sensitive data.

**i Note**

The integration developer can control which credentials are to be used in connections with basic authentication by deploying the associated **User Credentials** artifacts on the tenant. These artifacts contain user names and passwords. Note that, however, a password specified in a **User Credentials** is never displayed. Furthermore, passwords cannot be downloaded (by either using the user interface or the application programming interface). The integration developer, although having full control over the integration flow, does not have access to credentials of another tenant of the same customer.

Therefore, apply the following measures when designing integration flows for security-sensitive areas:

- Don’t give the integration developer access to productive systems.
- Consider applying a four-eyes principle and implement a review process before deploying integration flows to production.
- An integration developer has the option to develop integration flows on a separate development or test tenant. These integration flows can then be transported to the productive tenant by another person.
- Consider using client certificate-based authentication rather than basic authentication. When using client certificates, the private key remains in the sender system and no secret password is transmitted through the network.
- Don’t share the same secret credentials between tenants with different security levels (for example, between test tenant and productive tenant).
- If you suspect a security violation, check the audit log to find out which user deployed the integration flow in question.
- If read-only access is required to analyze issues in the productive system, use the authorization group **AuthGroup.ReadOnly**.

**Tip**

Hint: Instead of using the predefined authorization groups, you can tailor the permissions to your own requirements by applying elementary roles that are defined for individual tasks.

More information:

**Authentication and Authorization Options for Inbound Calls**

When a sender system calls the integration platform using HTTPS-based (inbound) requests, 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. In sender channels that are based on transport protocol HTTP, the authorization options are **User Role** and **Client Certificate**.
**Client Certificate** is now 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.

### Combinations of Authentication and Authorization (Inbound)

For inbound communication based on HTTPS, the authentication and authorization options can be combined in a specific way.

**Combination of Authentication/Authorization Options**

<table>
<thead>
<tr>
<th>Authentication Option ...</th>
<th>Can Be Used with the Following Authorization Option ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic authentication</td>
<td>Role-based authorization</td>
</tr>
<tr>
<td>The sender (client)</td>
<td>For this user, the authorizations are checked based on user-to-role assignments defined on the tenant.</td>
</tr>
<tr>
<td>authenticates itself</td>
<td></td>
</tr>
<tr>
<td>against the server</td>
<td></td>
</tr>
<tr>
<td>based on user</td>
<td></td>
</tr>
<tr>
<td>credentials (user name</td>
<td></td>
</tr>
<tr>
<td>and password). The</td>
<td></td>
</tr>
<tr>
<td>HTTP header of the</td>
<td></td>
</tr>
<tr>
<td>inbound message (from</td>
<td></td>
</tr>
<tr>
<td>the sender) contains</td>
<td></td>
</tr>
<tr>
<td>the user name and</td>
<td></td>
</tr>
<tr>
<td>password.</td>
<td></td>
</tr>
<tr>
<td>Client-certificate</td>
<td>Role-based authorization</td>
</tr>
<tr>
<td>authentication and</td>
<td>For the user derived from the certificate-to-user</td>
</tr>
<tr>
<td>certificate-to-user</td>
<td>mapping, the authorizations are checked based on user-</td>
</tr>
<tr>
<td>mapping</td>
<td>to-role assignments defined on the tenant.</td>
</tr>
<tr>
<td>The sender (client)</td>
<td></td>
</tr>
<tr>
<td>authenticates itself</td>
<td></td>
</tr>
<tr>
<td>against the server</td>
<td></td>
</tr>
<tr>
<td>based on a digital</td>
<td></td>
</tr>
<tr>
<td>client certificate.</td>
<td></td>
</tr>
<tr>
<td>Furthermore, this</td>
<td></td>
</tr>
<tr>
<td>certificate is mapped to</td>
<td></td>
</tr>
<tr>
<td>a user (based on the</td>
<td></td>
</tr>
<tr>
<td>information contained</td>
<td></td>
</tr>
<tr>
<td>in a Certificate-to-User</td>
<td></td>
</tr>
<tr>
<td>Mapping artifact deployed on the tenant).</td>
<td></td>
</tr>
</tbody>
</table>

**Note**
You can map multiple certificates to the same user (n:1 certificate-to-user mappings possible).

<table>
<thead>
<tr>
<th>Certificate-to-User Mapping</th>
<th>Subject/Issuer DN authorization check of a certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>The sender (client)</td>
<td>In a subsequent authorization check, the permissions of the sender are checked on the tenant by evaluating the distinguished name (DN) of the client certificate of the sender.</td>
</tr>
<tr>
<td>Authentication Option ...</td>
<td>Can Be Used with the Following Authorization Option ...</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>OAuth</td>
<td>Role-based authorization</td>
</tr>
</tbody>
</table>

Grants access to resources of SAP Cloud Platform Integration without the need to share passwords with the client.

**Note**

This option is supported for the following sender adapter types: SOAP (SOAP 1.x), SOAP (SAP RM), HTTPS.
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 database 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 database. 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 database. 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](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.

General Information

Governments place legal requirements on industry to protect data and privacy. We provide features and functions to help you meet these requirements.

⚠️ Caution

SAP does not provide legal advice in any form. SAP software supports data protection compliance by providing security features and data protection-relevant functions, such as blocking and deletion of personal data. In many cases, compliance with applicable data protection and privacy laws is not covered by a product feature. Furthermore, this information should not be taken as advice or a recommendation regarding additional features that would be required in specific IT environments. Decisions related to data protection must be made on a case-by-case basis, taking into consideration the given system landscape and the applicable legal requirements. Definitions and other terms used in this documentation are not taken from a specific legal source.

⚠️ Caution

We assume that you have not maintained any data related to an individual in the tools provided by SAP Cloud Platform Integration (for example, when using the Web UI to design integration content).

We expect that sensitive personal data can only be included in message payloads. This responsibility lies exclusively with you as the operator of an integration scenario using SAP Cloud Platform Integration and remains your responsibility. If you include sensitive personal data within payloads or message attachments, SAP Cloud Platform Integration may store this information on your behalf. This applies also for data maintained in the tools provided by SAP Cloud Platform Integration, however, data within payloads can be protected by enabling encrypted storage.

The knowledge of sensitive personal data lies exclusively with you and remains your responsibility.

The tools of SAP Cloud Platform Integration only use technical users or data without any references to individuals.

User Consent

We assume that software operators, such as SAP customers, collect and store the consent of data subjects, before collecting their personal data. A data privacy specialist can later determine whether data subjects have granted, withdrawn, or denied consent.
Read Access Logging

Read Access Logging is used to monitor and log read access to sensitive data. Data may be categorized as sensitive by law, by external company policy, or by internal company policy. Read Access Logging enables you to answer questions about who accessed particular data within a specified time frame. Such questions could be:

- Who accessed the data of a given business entity, for example, a bank account?
- Who accessed personal information, such as health data?
- Who accessed personal data of accounts or business partners?

A tenant administrator can display audit logs for a tenant using the Monitoring application of the Web UI (under Manage Security in the Audit Log tile).

Additionally, within SAP, audit logs can be displayed for teams in charge of maintaining the virtual cloud environment and to analyze and resolve error situations. Audit logs related to different customers are separated from each other (according to the tenant isolation feature).

More information: Security-Relevant Logging and Tracing [page 23]

Information Report

An information report is a collection of data relating to a data subject. A data privacy specialist may be required to provide such a report or an application may offer a self-service. SAP Cloud Platform Integration assumes that software operators, such as SAP customers, can provide such information.

Erasure of Personal Data

When handling personal data, consider the legislation in the different countries where your organization operates. After the data has passed the end of purpose, regulations may require you to delete the data. However, additional regulations may require you to keep the data longer. During this period you must block access to the data by unauthorized persons until the end of the retention period, when the data is finally deleted.

Data stored on the SAP Cloud Platform Integration platform is only stored for a limited time period (referred to as retention time).

For more information on the retention times for the various kinds of data stored by SAP Cloud Platform Integration, see Specific Data Assets [page 21].

Related Information

Types of Stored Data [page 20]
Specific Data Assets [page 21]
7.1 Types of Stored Data

Different kinds of data, such as message content or monitoring data, can be stored during the operation of an integration scenario.

Such data needs to be considered as sensitive data as it can contain personal information. The following list provides 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. Additionally, SAP has no access to data stored in customer tenants.

The customer can grant people outside its organization permissions to execute specific tasks on its cluster (for example, to SAP employees to execute error analysis tasks in support cases).

For more information, see the document SAP Cloud Platform Security: Trust Matters under Data Governance and Legal Compliance.

---

### Related Information

**Specific Data Assets** [page 21]
### 7.2 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 as storage location and retention time, for example.

<table>
<thead>
<tr>
<th>Data Assets</th>
<th>Description</th>
<th>Logical Storage</th>
<th>Classification</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>Message store</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>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></td>
<td>30 days</td>
<td>14 days</td>
</tr>
<tr>
<td>System log</td>
<td>Information about errors that occurred during HTTP inbound processing</td>
<td>Log data</td>
<td></td>
<td>7 days</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>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>Unlimited</td>
<td>14 days</td>
</tr>
<tr>
<td>Data Stored by</td>
<td>Description</td>
<td>Logical Storage</td>
<td>Classification</td>
<td>Retention Time</td>
<td>Backup Available</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>-----------------</td>
<td>----------------</td>
<td>----------------</td>
<td>------------------</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></td>
<td>Configuration data</td>
<td>Unlimited</td>
<td>14 days</td>
</tr>
<tr>
<td>Data Store operations step</td>
<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>Can be defined by integration developer (default value: 90 days)</td>
<td>14 days</td>
</tr>
<tr>
<td>Persist step</td>
<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>90 days</td>
<td>14 days</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>Can be defined by integration developer (default value: 90 days)</td>
<td>Not supported</td>
</tr>
</tbody>
</table>
Limited retention times make sure that data is stored in the system only for a limited time period.

### 7.3 Security-Relevant Logging and Tracing

Audit logs allow administrators at SAP or the tenant administrator 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.

A tenant administrator can display system access logs for his or her tenant using the Monitoring application of the Web UI (under Access Logs in the Audit Log and System Log Files tile).

The Audit Log section allows you to monitor changes to the configuration of the tenant cluster such as (examples):

- Access to the system (for example, read access to message content)
- Deletion of data from the message store
- Change in the content of a keystore

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 (user)
- Source of the event (IP address of the source that issued the action)

To view audit logs, the tenant administrator needs to have assigned the roles IntegrationOperationServer.read and AuditLog.Read.

The audit log data retention time in the database is 30 days.

The System Log Files section provides information related to errors that occurred during HTTP inbound processing and contains 2 different log types: the HTTP Access Logs and the Worker Nodes Default Traces.

- For both log types, the access is granted through personas or composite roles such as (IntegrationDeveloper, Administrator, BusinessExpert, ReadOnly, SystemDeveloper). They all can open the log files as the composite roles always contain the single role IntegrationOperationServer.read. You need this role to download logs.
Retention time for both logs is 7 days. After that period, the log files are deleted.

Stored information

The information stored depends on the log type.

For the **HTTP Access Logs**, the system stores information about the incoming HTTP request on the worker node, such as:

- The incoming time of the call
- The IP address of the sender client
- The User Id, if included in the request
- The HTTP method (HEAD, POST, PUT, GET, DELETE)
- The call path such as e.g. /cf/SOD/incoming
- The HTTP status code (e.g. 200, 401, 403, 500)
- The call size in bytes
- The duration of the call.

This information is stored to be able to identify authentication or authorization problems arising in an early message processing phase, since no Message Processing Log Entries are logged yet. It is used by integration developers or administrators for trouble-shooting and/or configuration purposes.

The **Default Trace** contains general information about system activities according to the log level you have set.

In case of the default settings, errors and stack traces are logged. The default trace format is:

- Log entry time stamp
- Log level (ERROR, INFO, WARNING, DEBUG,...)
- Class name of the logger
- Tenant
- Log text

This information is stored for trouble-shooting purposes, for example if an component monitor throws an error message during deployment of the corresponding integration flow and this error message does contain enough details. In this case the developer or the administrator might have a look into the **Worker Nodes Default Traces**.

---

**Note**

Audit logs managed by SAP

Audit logs are also generated SAP-internally and displayed for people with dedicated permissions. Such 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:

- Access to the system (for example, read access to message content)
- Change to the setup of a tenant cluster (for example, if VM has been started or stopped)
- Change to the configuration (for example, an integration flow has been deployed or undeployed)
- Change of the tenant configuration

Audit logs related to different customers are separated from each other (according to the tenant isolation feature).
8 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

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.

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.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.