



PUBLIC

Document Version: 4.77.0 – 2022-04-18

Security

SAP IoT services for SAP BTP

Content

1	Security	3
2	Technical System Landscape	4
3	Security Recommendations	6
4	User Identity Management	7
4.1	User Roles	7
5	Secure Device Onboarding	9
6	Certificate Revocation	10
6.1	Process of Revocation	10
6.2	Access the Existing Certificates of a Physical Device	10
6.3	Revoke a Certificate	11
6.4	Access Revoked Device Certificates	12
7	Certificate Renewal	14
7.1	Check the Expiration Date of Your Certificate to Renew	14
7.2	Renew a Device or Gateway Certificate	15
8	Certificate Signing Request Procedure	17
8.1	Additional Information	22
9	Network and Communication Security	24
10	Data Protection and Privacy	25
10.1	Which Personal Data is Collected?	25
10.2	View Personal Data	25
10.3	Deletion of Personal Data	26
10.4	Deletion of Service Data	26
10.5	Export of Service Data	26
11	Auditing and Logging	27
11.1	Auditing and Logging Information	27
12	Related Information	84
12.1	Certificates	84
12.2	REST APIs	84
12.3	Message Queue	84



1 Security

The Security section of this documentation provides an overview of the security-relevant information that applies to the SAP IoT services for SAP BTP for the Cloud Foundry environment.

The Internet of Things Service is a service on the SAP BTP for the Cloud Foundry environment. Therefore, we highly recommend that you consult the SAP BTP Security section for your corresponding software version. You should also refer, as needed, to Security guides and other relevant documents such as Development guides and Installation guides for the related software systems.

Additional Information

For more information about security topics, consider the following resources.

Content	Link
SAP Security, Data Protection, and Privacy	https://www.sap.com/corporate/en/company/security.html 
SAP Cloud Trust Center	Security
OWASP (The Open Web Application Security Project) - OWASP Top 10	https://github.com/OWASP/Top10/raw/master/2017/OWASP Top 10-2017 (en).pdf
NIST (National Institute of Standards and Technology) - Recommendation for Key Management	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf 

Related Information

[Technical System Landscape \[page 4\]](#)
[Security Recommendations \[page 6\]](#)
[User Identity Management \[page 7\]](#)
[Secure Device Onboarding \[page 9\]](#)
[Certificate Revocation \[page 10\]](#)
[Certificate Renewal \[page 14\]](#)
[Network and Communication Security \[page 24\]](#)
[Data Protection and Privacy \[page 25\]](#)
[Related Information \[page 84\]](#)

2 Technical System Landscape

The following simplified representation of the solution components and their communication channels is used below to provide security-relevant information.

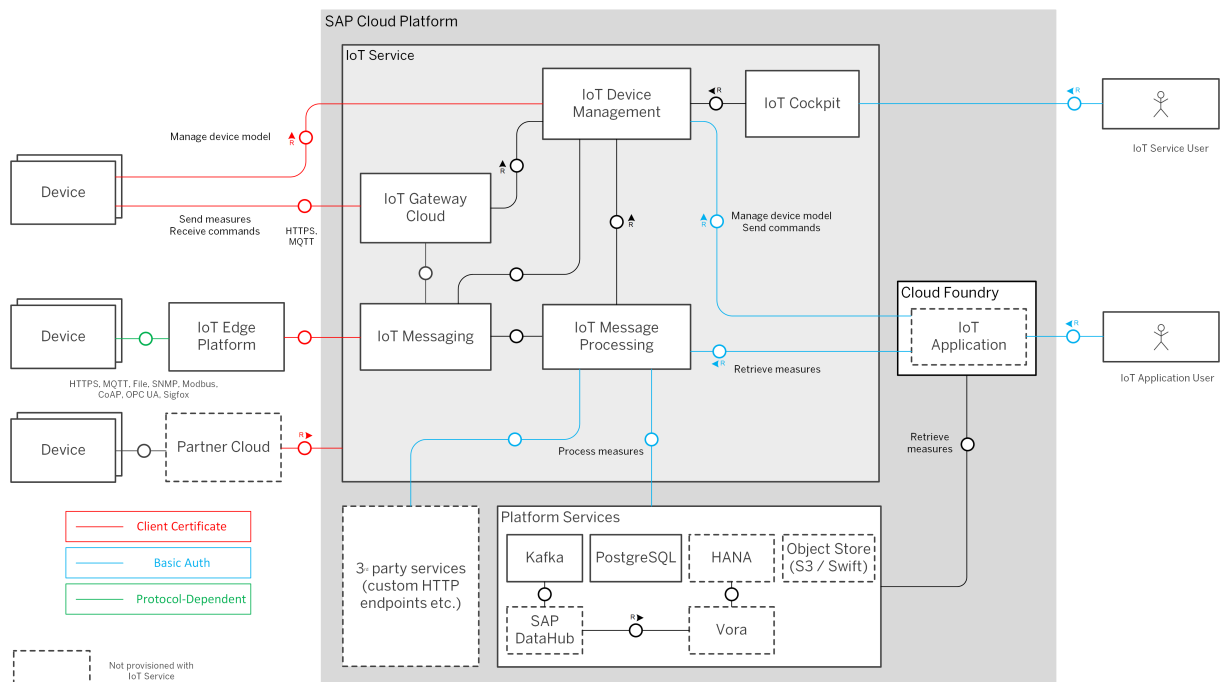
Customer Zone

This zone comprises the software running on the device, which has direct access to the device data and controls operations including communication on the device. This zone also includes the device certificate including its private key for the specific device, which should be stored securely on the device. Since bidirectional communication between the core services and the device may take place, this zone also includes the secure processing of messages received from the core services on the device.

Cloud Zone

The core functions provided by the Internet of Things Service are offered by the components hosted in an SAP-controlled cloud environment, the SAP BTP for the Cloud Foundry environment.

All components and their security-relevant information flows are shown in the figure below. For more information, please refer to sections [Secure Device Onboarding \[page 9\]](#) and [Network and Communication Security \[page 24\]](#). For a detailed description of the different entities please refer to the architecture in the section for the SAP IoT services for SAP BTP for the Cloud Foundry environment.



3 Security Recommendations

The SAP IoT services for SAP BTP for the Cloud Foundry environment currently comes with an initial set of security features. Please also consider the following points:

Recommendations

⚠ Caution

All Internet of Things Service APIs use Transport Layer Security (TLS) to secure the communication between the client and the server. Ensure that clients check the server certificate as part of the TLS handshake regarding to the correct host name and the trustworthiness of the Certificate Authority (CA). All server certificates are issued by well-known and generally trusted certificate authorities, for example DigiCert. Please be aware that CA certificates might be updated over time. Such updates are announced in the section [What's New](#) for SAP BTP. Clients need to implement a life-cycle management process for trusted certificates. Typically, this is done by relying on the default system trust store or by being extensible with respect to the list of trusted CAs.

- Do not delete or change applications and other security settings that are installed by the Internet of Things Service.
- Protect the devices and their stored device certificates including their private keys all times against unauthorized access. If possible, use an encryption method to store the private key on the device. Remove the old device certificate including its private key when installing a new device certificate on the device.
- Protect the system hosting the Internet of Things Edge Platform against unauthorized access as well.
- For both devices and the Internet of Things Edge Platform regularly check for security-relevant patches on OS/ firmware level.
- Quickly apply the provided Internet of Things Edge Platform security patches.
- If the device receives messages from the cloud, allow for secure processing of these messages to avoid unintended actions being triggered on the device.
- Use the existing logging capabilities to check the platform, monitor the system, and regularly check for any exceptional behavior.
- It is recommended to mark sensitive header as sensitive while creating HTTP configuration. Please refer .
- If you want to use Internet of Things Service to process sensitive data (including personal data), use your own database to store these sensitive data. You can setup your SQL processing service from .
- Consult a security expert or carefully read the information provided in the following sections to be aware of your current protection level.

4 User Identity Management

User identity management and resource access policies in the Internet of Things Service are provided through a series of APIs and the Internet of Things Service Cockpit.

The Internet of Things Service relies on mutual authentication to secure communication with users, where a user is any software, individual, or legal entity that is registered in the identity management component of the Internet of Things Service and consumes the available services.

To provide secure user identity management, users are assigned a unique digital identity across all system components. Moreover, users can be assigned user roles.

4.1 User Roles

User roles can be either tenant-specific or non-tenant-specific. The assignment of tenant-specific user roles is only valid for one specific tenant, while the non-tenant-specific user roles are global and valid across different tenants. Users can therefore have different tenant-specific roles within each tenant.

For more information, please refer to the section in the Internet of Things Service Cockpit documentation.

Depending on this role, a user either can or cannot access specific APIs or features of the Internet of Things Service. There, roles form a hierarchy, for example, the **Instance Owner** role includes the **Administrator** role, which in turn includes the **User** role.

The following table provides an overview of the different roles:

Roles	Type	Description
Instance Owner	Global	Users with the Instance Owner role are primarily allowed to manage users and tenants. It is also possible to support other users with tenant-specific interactions.
Administrator	Tenant specific	Users can get assigned to tenants with the Administrator role. Inside a tenant, users with this role gain all permissions from the User role. Additionally, they are allowed to create and manage devices as well as the Internet of Things Edge Platform.
User	Tenant specific	Users can get assigned to tenants with the User role. Inside a tenant, users with this role can access and review the

Roles	Type	Description
		device model and monitor the availability of existing devices and gateways.

5 Secure Device Onboarding

Obtaining a device certificate is a two-step process. In the first step the physical device (in this context the term applies to both gateways and devices) must obtain a registration certificate. Using this certificate, the physical device can create a device model entity in the Internet of Things Service data model. Once this device entity exists, the physical device can request its device-specific certificate.

Registration certificates are only valid in a specific context. For gateways, this context is a specific tenant. For devices, it is a single gateway. This means that a device can register itself for the correct gateway corresponding to the registration certificate. The registration certificate can be used by multiple physical devices to execute the onboarding procedure. It allows producers of physical devices to retrieve the registration certificate during device production and add it to the software running on the physical device. Once the physical device is delivered to a customer, the device can continue the onboarding procedure automatically.

The Internet of Things Service offers a set of APIs to retrieve the onboarding certificate. For details about this procedure, please refer to section in the *Internet of Things Gateway* documentation.

Physical devices can request their own device certificate in several ways. First, they can obtain the certificate in PEM or p12 format depending on their specific requirements. Second, there are two different approaches for generating PEM certificates: using a certificate signing request (CSR) generated and provided by the device or without a CSR. For security reasons, we recommend that you use the approach which includes sending a CSR. This way, the system does not transmit the private key over the internet, and the private key never leaves the physical device.

Once the onboarding process is complete and the physical device has its own specific certificate, we recommend for security reasons that you delete any registration certificate on the physical device.

6 Certificate Revocation

The Internet of Things Service uses certificates for mutual authentication and for secure device onboarding. For more information, please refer to section [Secure Device Onboarding \[page 9\]](#) and [Network and Communication Security \[page 24\]](#) respectively. In exceptional cases, it might be necessary to revoke a certificate for a physical device, for example, to render it invalid and unusable for the control path. The term physical device in this section refers to gateway and device registration certificates which are associated to a tenant and a gateway, as well as to gateway and device-specific certificates belonging to individual gateways and devices. So, all four types of certificates are covered. Reasons for revoking a certificate of a physical device could be: the private key is compromised, a certificate is not issued properly, or a malicious activity of a physical device is detected. Although such occurrences should be rare, the Internet of Things Service can be used to revoke a certificate for such reasons.

6.1 Process of Revocation

Revoking a certificate is usually a two-step process. In the first step, the fingerprint of the corresponding certificate must be obtained if not already known. The fingerprint can be obtained by having the Internet of Things Service list all existing certificates for a physical device.

i Note

The algorithm of the fingerprint/thumbprint is unrelated to the encryption algorithm of the certificate. We use the SHA-256 algorithm to compute the digest of the entire certificate. This results in a 256 bit / 64-byte string unique to the certificate in question.

Another way to acquire the fingerprint of a certificate to revoke is to use a cryptography tool. For example, if you use the well-known OpenSSL tool, the following command would output the fingerprint in the required format for a certificate with the name `certificate-file.crt` in the same directory.

```
openssl x509 -noout -fingerprint -sha256 -inform pem -in [certificate-file.crt]
```

6.2 Access the Existing Certificates of a Physical Device

The Internet of Things Service offers a set of APIs to retrieve all existing certificates for a specific physical device. Each API call returns a list consisting of the fingerprint and the end validity date of each certificate belonging to the physical device. These API endpoints are protected by instance owner credentials using BASIC authentication. For more information, please refer to section [User Roles \[page 7\]](#).

The following table lists the endpoints for accessing the certificate information depending on the type of the certificate.

HTTP Attribute	Description	Path using base path: /iot/core/api/v1
GET	Shows the gateway registration certificate fingerprints	/tenants/{tenantId}/gatewayRegistrations/clientCertificate
GET	Shows the device registration certificate fingerprints	/tenant/{tenantId}/gateways/{gatewayId}/deviceRegistrations/clientCertificate
GET	Shows the gateway certificate fingerprints	/tenant/{tenantId}/gateways/{gatewayId}/authentications/clientCertificate
GET	Shows the device certificate fingerprints	/tenant/{tenantId}/devices/{deviceId}/authentications/clientCertificate

6.3 Revoke a Certificate

When the fingerprint for a certificate to be revoked has been determined, the corresponding API endpoint for the physical device can be called and must be supplied with the fingerprint of the certificate.

i Note

For security reasons, we strongly recommend that you always revoke all existing certificates for a specific physical device if this device shows suspicious activity.

i Note

It is recommended that revocation certificate should be used only to revoke a certificate that is potentially dangerous, or if you are not able to retrieve your previous certificate. Please avoid revoking the certificates frequently. This will avoid creating large number of revoked certificates which can affect the performance of the Internet of Things Service platform.

The following table specifies the respective API depending on the physical device. This API is also protected by instance owner credentials using BASIC authentication.

HTTP Attribute	Description	Path using base path: /iot/core/api/v1
DELETE	Revokes a gateway registration certificate	/tenants/{tenantId}/gatewayRegistrations/clientCertificate/{fingerprint}
DELETE	Revokes a device registration certificate	/tenant/{tenantId}/gateways/{gatewayId}/deviceRegistrations/clientCertificate/{fingerprint}
DELETE	Revokes a gateway certificate	/tenant/{tenantId}/gateways/{gatewayId}/authentications/clientCertificate/{fingerprint}
DELETE	Revokes a device certificate	/tenant/{tenantId}/devices/{deviceId}/authentications/clientCertificate/{fingerprint}

6.4 Access Revoked Device Certificates

The Internet of Things Service offers an API to retrieve the revoked certificates which are not expired for a specific physical device. Each API call returns a list consisting of the fingerprint, the end validity date and the revoked timestamp of each certificate belonging to the physical device. By default, the API is paginated with 100 records per page. The API endpoint is protected by instance owner or tenant admin credentials using BASIC authentication. For more information, please refer to section [User Roles \[page 7\]](#).

The following table lists the endpoint for accessing the revoked certificate information.

HTTP Attribute	Description	Path using base path: /iot/ core/api/v1
GET	Shows the revoked device certificate fingerprints	/tenant/{tenantId}/ devices/{deviceId}/ authentications/ clientCertificate/ listRevoked

7 Certificate Renewal

The Internet of Things Service uses certificates for mutual authentication and for secure device onboarding. For more information, please refer to section [Secure Device Onboarding \[page 9\]](#) and [Network and Communication Security \[page 24\]](#) respectively.

The provided certificates are only valid for a certain time period. Currently, this period is one year. Therefore, to ensure continued operation of gateways and devices, it might be necessary to renew the certificates. For gateways, devices and their associated device-specific certificates, the Internet of Things Service provides a way to renew these certificates without manual intervention. Gateways and devices can use their current device-specific certificate, which must still be valid, to call the corresponding API endpoints and retrieve a renewed certificate.

i Note

In case the usual way of renewing gateway or device certificates is no longer possible, you can use your credentials to retrieve a renewed certificate manually. These renewed certificates are then downloaded in the browser or by the API and must be assigned to the corresponding gateway or device.

7.1 Check the Expiration Date of Your Certificate to Renew

The Internet of Things Service offers a set of APIs to retrieve all existing certificates for a specific gateway or device. Each API call returns a list consisting of the fingerprint and the expiration date of each certificate belonging to the specific device. By default, the API is not paginated and will return all the certificates for the device. Hence it is advised to use pagination with the top and skip values to avoid performance issues on the Internet of Things Service instance, especially if the device has a lot of certificates. These API endpoints are protected by instance owner credentials using BASIC authentication. For more information, please refer to section [User Roles \[page 7\]](#).

The following table lists the endpoints for accessing the certificate information depending on the type of the certificate.

HTTP Attribute	Description	Path using base path: /iot/core/api/v1
GET	Shows the gateway certificate expiration dates	/tenant/{tenantId}/gateways/{gatewayId}/authentications/clientCertificate

HTTP Attribute	Description	Path using base path: /iot/ core/api/v1
GET	Shows the device certificate expiration dates	/tenant/{tenantId}/ devices/{deviceId}/ authentications/ clientCertificate

Another way to retrieve the expiration date of a certificate to renew is to use a cryptography tool. For example, if you use OpenSSL, the following command would return the expiration date for a certificate with the name `certificate-file.pem` in the same directory.

Sample Code

```
openssl x509 -enddate -noout -inform pem -in [certificate-file.pem]
```

Of course, you can also provide a solution by writing your own code in Java as in the following code example. In this sample a periodic task is executed, which checks if the certificate expiration date is within a specific threshold. If this is the case, the certificate renewal is triggered.

Sample Code

```
Timer timer = new Timer();
MyTask myTask = new MyTask();
// This task is scheduled to run once every week
timer.scheduleAtFixedRate(myTask, 0, 604800000);
```

The following task checks, if the expiration date of the specific certificate is more than one month in the future.

Sample Code

```
X509Certificate certificate =
loadDeviceCertificate();
Date inOneMonth = new
Date((System.currentTimeMillis() + 2592000000L));
if (certificate.getNotAfter().before(inOneMonth))
{
    renewDeviceCertificate(certificate);
}
```

7.2 Renew a Device or Gateway Certificate

The renewal of certificates for devices or gateways works exactly as described in section in the *Internet of Things Gateway* documentation. The only difference here is that the device or gateway can call these API endpoints with their own valid device-specific certificate and do not need a registration certificate.

For reference, the corresponding API endpoints are listed here again. They can be called with a valid device-specific certificate as the client certificate.

HTTP Attribute	Description	Path using base path: /iot/core/api/v1
GET	Downloads device p12 file	/tenant/{tenantId}/ devices/{deviceId}/ authentications/ clientCertificate/p12
GET	Downloads a device private key and certificate in PEM format	/tenant/{tenantId}/ devices/{deviceId}/ authentications/ clientCertificate/pem
POST	Creates a device certificate in PEM format	/tenant/{tenantId}/ devices/{deviceId}/ authentications/ clientCertificate/pem
POST	Creates a gateway certificate in PEM format	/tenant/{tenantId}/ gateways/{gatewayId}/ authentications/ clientCertificate/pem

i Note

For security reasons, we strongly recommend that you generate the private key on the physical device itself. Furthermore, to renew a certificate in this way, we recommend that you renew the private key on the device as well.

i Note

It is not recommended to create large number of certificates for the same device. Certificates should be generated only on nearing expiry of the previous certificate, or if the previous certificate is potentially dangerous or if you are not able to retrieve your previous certificate. In all other cases, please use the existing certificate. This will avoid any latency or service interruptions in the Internet of Things Service platform due to generation of large number of certificates on a single device.

i Note

The Internet of Things Edge Platform is now capable of performing the renewal of the X.509 certificate, which it uses to communicate with the Internet of Things Service components in the cloud. A periodic task checks the certificate expiry date and, if it is closer than a specified time threshold, triggers the retrieval of a new certificate via the Device Management API.

8 Certificate Signing Request Procedure

This procedure describes how to generate public key or private key pairs and store them in a Java KeyStore. Follow these steps in order to generate a keypair and a Certificate Signing Request (CSR) which will be sent to the Internet of Things Service to get a signed certificate for devices.

Prerequisites

This procedure requires an existing Internet of Things Service instance with an already created tenant and a device for cloud gateways.

Information required from Internet of Things Service for next steps include:

- `deviceAlternateId`
- `gatewayId`
- `tenantId`
- `instanceId`
- `basic authentication token`

Java and the Java Keytool command line utility must be available in your environment.

The Java Keytool is a command line tool which can generate public key or private key pairs and store them in a Java KeyStore.

The Keytool executable is distributed with the Java SDK or JRE; so you will also have the Keytool executable if you have an SDK or JRE installed.

The Keytool executable is called 'keytool' and is located in the `JAVA_HOME_DIRECTORY>/jre/bin` path.

To get a signed device certificate, the CSR must specify a Common Name (CN) according to the following structure:

```
deviceAlternateId:<DEVICE_ALTERNATE_ID>|gatewayId:<GATEWAY_ID>|  
tenantId:<TENANT_ID>|instanceId:<INSTANCE_ID>
```

Procedure

1. Go to the directory where you would like to store your certificate.
2. Generate a keypair entry.
 - a. Execute the command:
 - `keytool -genkeypair -alias <ALIAS> -keypass <PASSWORD> -keyalg RSA -sigalg SHA256withRSA -keysize 2048 -keystore <KEYSTORE_NAME>.jks -storepass <PASSWORD>`
where `< ALIAS >`, `< PASSWORD>` and `<KEYSTORE_NAME>` is of your choice.

Example:

Sample Code

```
keytool -genkeypair -alias testAlias -keypass testPsw123 -keyalg RSA  
-sigalg SHA256withRSA -keysize 2048 -keystore my_keystore.jks -  
storepass testPsw123
```

- b. Enter the resulting CN from the above structure for the full name (first and last name):

- deviceAlternateId:<DEVICE_ALTERNATE_ID>|gatewayId:<GATEWAY_ID>|
tenantId:<TENANT_ID>|instanceId:<INSTANCE_ID>

Example:

Sample Code

```
deviceAlternateId:device_1|gatewayId:3|tenantId:732185401|  
instanceId:test_instance
```

- c. Enter **IoT Services** when asked for *Organizational Unit*.
- d. Press Enter to skip all other fields.
- e. When asked for a final confirmation, type **yes** and press Enter. It is possible to ignore the warning about PKCS12 migration.
- f. A jks file is generated with the chosen <KEYSTORE_NAME>.
3. Generate the Certificate Signing Request.
- a. Execute the command:

- keytool -certreq -alias <ALIAS> -keystore <KEYSTORE_NAME>.jks -file
<CRS_NAME>.csr

Example:

Sample Code

```
keytool -certreq -alias testAlias -keystore my_keystore.jks -file  
my_csr.csr
```

- b. When asked, enter the store <PASSWORD>
- c. When asked, enter the key <PASSWORD>
- d. A file named <CRS_NAME>.csr is generated.
4. Encode the content of the resulting CSR file <CRS_NAME>.csr with base64 encoding.
- **Example 1**
 - For linux/macOS terminal, execute the following command:
base64 <CRS_NAME>.csr.
 - **Example 2**
 - Copy all the content from the file <CRS_NAME>.csr by opening it with a text editor and encode it with any free online encoder like <https://base64.guru/converter/encode>.

The resulting encoded string will be used as value for <CSR_B64_ENCODED_VALUE>.

5. Do a POST call by sending the CSR to the Internet of Things Service endpoint to get the signed certificate.
- a. Generate <BASIC_AUTH_TOKEN> by concatenating the username and password with : character and encoding it with base64.

- **Example:**

≡ Sample Code

```
base64 <username>:<password>
```

- b. Do the POST call.

```
curl -X POST "https://<INSTANCE_URL>/<INSTANCE_ID>/iot/core/api/v1/tenant/<TENANT_ID>/devices/<DEVICE_ID>/authentications/clientCertificate/pem" -H "accept: */*" -H "authorization: Basic <BASIC_AUTH_TOKEN>" -H "Content-Type: application/json" -d "{ \"csr\": \"<CSR_B64_ENCODED_VALUE>\", \"type\": \"clientCertificate\"}"
```

You will get back a signed certificate as JSON content from the API:

```
{
  "type": "clientCertificate",
  "pem": "-----BEGIN CERTIFICATE-----\n<CERTIFICATE CONTENT>-----END CERTIFICATE-----\n"
}
```

Example:

≡ Sample Code

```
curl -X POST "https://test_instance/test_instance/ /iot/core/api/v1/tenant/732185401/devices/64585c35-9467-494f-92d2-e1cb1c10bfc2/authentications/clientCertificate/pem" -H "accept: */*" -H "authorization: Basic c2FyYTpTYXJhMTIz" -H "Content-Type: application/json" -d "{ \"csr\": \"LS0tLS1CRUdJTiB0RVcgcQ0VSVELGSUNBVEUgUkVRVUVTVVC0tLS0tCk1JSURPVENDQWlFQ0FRQXdnY014RURBT0JnTlZCQVlUQjFWdWEyNXZkMjR4RURBT0JnTlZCQWdUQjFWdWEyNXYNcmQyNHhFREFPQmdOVkJBb1RCMVZlYTI1dmQyNHhFREFPQmdOVkJBb1RCMVZlYTI1dmQyNHhGVEFUQmdOVkJBb1QNCkRFbHJWQ0JlUWlhKMMFXTmxjekZpTUDBR0ExVUVBd3haWkdWMmFXTmxRV3gwWlhKdVlUmxTV1E2WjJGdFpWOXQNC1lXTm9hVzVsWHpGOFOyRjBaWGRoZVVsa09qTjhhR1Z1WVc1MFNlXUJ0ek15TVRnMU5EQXhmR2x1YzNSaGJtTmwNC1NXUTZibWxUUhSc2VTMXpjSEpwYmljd2dnRWlNQTBlHQ1Nxr1NjYjNEUUVUQVVFVQUE0SUJEd0F3Z2dFS0FvSUIncFRFRFZpTX1VSHdMTlaT3o5N1krNXNUdnovKzgyYVJWVm5Db0ZQR1NsdVl4K2RncUNHQxSQldpY3MzZ3JtZEoNCkhLVFBIZ2NxdVZaXpEWC8wTjRQMwJXZmM4aFI5SnRVQWo4eXA3NWJJSUXZpWC9TNEJ3VnlwSDA2dmRyEVo4Q1MNCncvQU9qMGhtV2F4UHRTNnJjdVhmUHJxM3krZlCa3RjZU5nSTh0NUTwajg4eUdXeEF6Q0RkMC9GbmhzOCTiY3MNCk12SDNvOTc4OHJnN1ZzT1RtYlJhck12MnRaZG82dDBZby9NdnJSMWR1RUNDMjZvSmpLRStWcmJBVFPJbG1FNUQNCm1MNkQ1dm1YNDBTV0E2a1A3Sk42K3RUeGM5WEsvak95MlFDUmtFQ1M2UWxQTW9RekgxeC9jcmkxZFJQZ20reVUNCjhWNUpKeG0zVklHUEdPVTNHwGY3TUhlLdkFnTUJBQUdnTURBdUJna3Foa21HOXcwQkNRNHhJVEFmTUIwR0ExVWQNCkRnUVdCQlFwTUF3QUlIRnY0bm9KNlRNZHDxYzAvUkxHanpBTkna3Foa21HOXcwQkFRc0ZBQU9DQVFFQXU3dSsNCnNBWE4wOHNGeWxtVX10VnV0dHNxV3UUrUk1OT3pram5Ga2MrVGM5bmJtN2pCTDZ6V2RYbGFwYTdqWkp0ZVkyYnINCisxZ05ockdrTGI0anM4VUw1SVprdFJ3SkhvMX1CbE9tOEh5RHgxMmc5N05HczFKenBmY3AwMWNqSWJzeEE3M24NCi9OVkU1TEdrV3M4S1NHSjdEZVRjNUFOcjF1R2RsaDZwd1RLUzBLR1Z5MEFCRXVQRzZ0THpra0Mxei85NXF0dnINCktGeWVJbn1lZ1R2N2dNWTA2UVBCFR4N0pnZFRic05WTG8yb3M1RnRvWG9hVjVOMXVEZE10OVR1M3NzdTZpOWUNC1RDeUpNSysyUHc0SHVTa2tTb2pLaHhtMDBTaEhMTGR0djhvZnRITW1sS2hBNmkt2NEVzVtTXVWVjJHNWNkK3INC1RhYmtEdmdCZGpNdUlKZFFiQT09Ci0tLS0tRU5EIE5FVjYBRVJUSUZJQ0FURSBRSRVFVRVNUlS0tLS0K\", \"type\": \"clientCertificate\"}"
```

i Note

You must be careful to select the POST api when post is done using Internet of Things Device Management API documentation.

- c. Unescape the value from the pem field obtained in step b.

```
"-----BEGIN CERTIFICATE-----\n<...>-----END CERTIFICATE-----\n".
```

Result will remove all the '\n' elements.

You can use any free online tool like <https://www.freeformatter.com/javascript-escape.html>, copy the content in the text area and unescape it.

Save the resulting unescaped content in a file named <CERTIFICATE>.crt.

6. Save the trusted Certification Authorities (CAs).

- a. Do a GET call to get the trusted Certification Authorities (CAs) from the dedicated Internet of Things Service endpoint.

```
curl -X GET "https://<INSTANCE_URL>/<INSTANCE_ID>/iot/core/api/v1/tenants/  
<TENANT_ID>/trustedCACertificates" -H "accept: */*" -H "authorization:  
Basic <BASIC_AUTH_TOKEN>"
```

- **Example**

≡ Sample Code

```
curl -X GET "https://test_instance/test_instance /iot/core/api/v1/  
tenants/732185401/trustedCACertificates" -H "accept: */*" -H  
"authorization: Basic c2FyYTpTYXJhMTIz"
```

The result is a list of CAs as JSON content:

```
[  
  {  
    "pem": "-----BEGIN CERTIFICATE-----\n<...>-----END  
CERTIFICATE-----"},  
  {  
    "pem": "-----BEGIN CERTIFICATE-----\n<...>-----END  
CERTIFICATE-----"},  
  {  
    "pem": "-----BEGIN CERTIFICATE-----\n<...>-----END  
CERTIFICATE-----"}  
]
```

- b. Unescape the value from the pem field for each one in the result for step a.

```
"-----BEGIN CERTIFICATE-----\n<...>-----END CERTIFICATE-----\n".
```

It will remove all the '\n' elements.

You can use any free online tool as mentioned in step 5c.

Escape the single value alone, not the whole result content.

Save the output for each unescaped content into a file named ca1.crt, ca2.crt ... caN.crt.

- c. Import the CA entries into the generated keystore <KEYSTORE_NAME>.jks by executing the command for each entry.

≡ Sample Code

```
keytool -import -trustcacerts -alias <FILENAME> -keystore  
<KEYSTORE_NAME>.jks -file <FILENAME>.crt
```

- When asked, type **yes** to trust the CA and press Enter.

Example:

Sample Code

```
keytool -import -trustcacerts -alias ca1 -keystore my_keystore.jks -file ca1.crt
```

Sample Code

```
keytool -import -trustcacerts -alias ca2 -keystore my_keystore.jks -file ca2.crt
```

7. Import the signed certificate entry by using the file named <CERTIFICATE>.crt, generated in step 5c by using the command:

- `keytool -import -alias <ALIAS> -keystore <KEYSTORE_NAME>.jks -file <CERTIFICATE>.crt`

Example:

Sample Code

```
keytool -import -alias testAlias -keystore my_keystore.jks -file my_certificate.crt
```

You will get the message:

Certificate reply was installed in keystore

Now it is possible to:

8. Use the JKS file <KEYSTORE_NAME>.jks as the device certificate keystore, for example with the Paho MQTT client.
9. Translate the JKS file <KEYSTORE_NAME>.jks into a P12 based keystore according to your needs.
 - For example, you can use the following command to translate it into P12 format:

Sample Code

```
keytool -importkeystore -srckeystore <KEYSTORE_NAME>.jks -destkeystore <KEYSTORE_P12_NAME>.p12 -srcstoretype JKS -deststoretype PKCS12 -deststorepass <PASSWORD> -destkeypass <PASSWORD>
```

Example:

Sample Code

```
keytool -importkeystore -srckeystore my_keystore.jks -destkeystore my_keystore.p12 -srcstoretype JKS -deststoretype PKCS12 -deststorepass testPassword -destkeypass testPassword
```

10. (Optional) Translate the JKS file <KEYSTORE_NAME>.jks into a PEM based keystore according to your needs.
 - a. OpenSSL is required for this step execution; please refer to documentation .
 - b. Execute the following:

- Translate it into P12 format as mentioned in step 2.
- Run the command:
`openssl pkcs12 -in <KEYSTORE_P12_NAME>.p12 -out <KEYSTORE_PEM_NAME>.pem`
 When asked *Enter Import Password*, enter the `< PASSWORD >`
 When asked *Enter PEM pass phrase*, enter a `< PASSPHRASE >` of your choice.

Example:

≡ Sample Code

```
openssl pkcs12 -in my_keystore.p12 -out my_keystore.pem
```

Related Information

[Additional Information \[page 22\]](#)

8.1 Additional Information

1. When connecting against a Cloud Gateway, you must use, as the truststore, the one which comes from your local machine certificate truststore. For example:

≡ Sample Code

```
<JAVA_HOME_DIRECTORY>/jre/lib/security/cacerts;
```

2. When connecting against an Edge Gateway (Internet of Things Edge Platform), you can use the same jks generated in step 2 `<KEYSTORE_NAME>` as the truststore.
3. Send data for REST with curl and P12.

```
curl -v -k --cert-type P12 -E <KEYSTORE_P12_NAME>.p12: < PASSPHRASE > -H "Content-Type:application/json" -d "<ENCODED_JSON_MESSAGE>" <REST_ENDPOINT>
```

Example:

≡ Sample Code

```
curl -v -k --cert-type P12 -E my_keystore.p12:pippo -H "Content-Type:application/json" -d "{ \"capabilityAlternateId\": \"1\", \"sensorAlternateId\": \"game_machine_sensor_1\", \"measures\": [[25,1]] }" https://test_instance/iot/gateway/rest/measures/game_machine_1
```

4. Send data for REST with curl and PEM.

```
curl -v -k -E <KEYSTORE_PEM_NAME>.pem: < PASSPHRASE > -H "Content-Type:application/json" -d "<ENCODED_JSON_MESSAGE>" <REST_ENDPOINT>
```

Example:

Sample Code

```
curl -v -k -E my_keystore.pem:test123Phrase -H "Content-Type:application/json" -d "{ \"capabilityAlternateId\": \"1\", \"sensorAlternateId\": \"game_machine_sensor_1\", \"measures\": [[25,1]] }" https://test_instance/iot/gateway/rest/measures/game_machine_1
```

5. For other examples for sending data, please refer to:

-
-

9 Network and Communication Security

The platform uses standard mechanisms to establish secure links among its components:

- Applications can consume data from the Internet of Things Message Processing where a BASIC authentication over TLS. The REST API endpoints of core are accessible via BASIC authentication.
- The Internet of Things Edge Platform components connect to the Internet of Things Messaging through an encrypted connection, where mutual authentication based on X.509 certificates is in place. For more information, please refer to section [Secure Device Onboarding \[page 9\]](#).
- Devices can connect to the Internet of Things Gateway Cloud (MQTT or REST) through a secure TLS, where client certificate authentication is in place. Here we enforce the current version of Transport Layer Security, version 1.2.
- Security between devices and the Internet of Things Edge Platform depends on the protocol implemented by the devices. The specific Internet of Things Edge Platform implementation is in charge of leveraging the protocol security mechanism to guarantee end-to-end security from devices up to applications connecting to the Internet of Things Service for the Cloud Foundry environment.

10 Data Protection and Privacy

This Data Protection and Privacy Statement applies to the Internet of Things Service for the Cloud Foundry environment.

We have created this Privacy Statement to demonstrate our firm commitment to the individual's right to privacy. This Privacy Statement outlines our handling practices regarding such information that can be used to directly or indirectly identify an individual (personal data).

Some SAP group entities, offerings, programs, or websites may have their own, possibly different privacy statements. We therefore encourage you to read the privacy statements of each of the SAP websites, offerings, or programs you visit or review.

i Note

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, considering 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.

Except for the data described below, the Internet of Things Service does not collect any personal data by itself. DPP features are not provided in the Internet of Things Service. Therefore, if you use our service to process or store other personal data, you are responsible for all legal and data privacy regulations.

You can use your own database to store your personal data; please check the documentation .

10.1 Which Personal Data is Collected?

The following personal data will be collected:

- User name

10.2 View Personal Data

If you want to see your personal data associated with the SAP Cloud Identity Authentication service that is stored by SAP, please contact us. For more information, please refer to section .

10.3 Deletion of Personal Data

SAP will not retain your personal data longer than is necessary to fulfill the purposes for which it was collected or than is required by applicable laws or regulations. In particular, and if no such contradicting statutory obligation exists, SAP will delete your personal data once you inform SAP that you do not want SAP to further process your personal data. Please contact us as described in the section .

Please note that in this case the use of certain services or offerings may either be limited or not possible any longer. In case there is a contradicting statutory obligation for SAP to retain your personal data, SAP will block it against further processing, and then delete the relevant personal data as soon as the requirement to retain it ends.

10.4 Deletion of Service Data

In addition to personal data, SAP will also delete data specific to the Internet of Things Service. This includes application and account settings as well as device meta data such as:

- Capabilities
- Sensor Types
- Devices
- Sensors

Please note that the Internet of Things Service ingests messages into user-controlled systems. Thus, SAP may not have access to these systems and therefore be unable to delete messages sent by devices. In addition, the Internet of Things Service provides a data retention feature that can be set by the customer. For more information, please refer to section .

10.5 Export of Service Data

During your term of subscription, you may export your data. To retrieve metadata, you may use the Device Management API. For more information, please refer to the [Internet of Things Service API](#) documentation. This API offers a complete collection of your metadata in JSON format.

Note that messages sent by the device cannot be obtained using the Device Management API. The data export process for device messages depends on the respective processing service. For more information, please refer to section in the Internet of Things Message Processing documentation.

11 Auditing and Logging

This section describes how to access and configure security-related logs for each of the services in SAP IoT services for SAP BTP.

11.1 Auditing and Logging Information

Here you can find a list of the security events that are logged by SAP IoT services for SAP BTP.

Security events written in audit logs

Event grouping	What events are logged	How to identify related log events	Additional information
Device Management Events	Login Success	Successful login userId: <userId> - The unique ID of the user instanceId: <instanceId> - The unique identifier of the customer instance tenantId: <tenantId> - The identifier of the consumer account for the current application context requestTime: <requestTime> - Date and time when the event occurs	

Event grouping	What events are logged	How to identify related log events	Additional information
	Login Failed	<p>Failed login</p> <p><code>userId: <userId></code> - The unique ID of the user</p> <p><code>instanceId: <instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId: <tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime: <requestTime></code> - Date and time when the event occurs</p>	
	Logout Success	<p>Successful logout</p> <p><code>userId: <userId></code> - The unique ID of the user</p> <p><code>instanceId: <instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId: <tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime: <requestTime></code> - Date and time when the event occurs</p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Certificate Login	<p>Successful certificate login</p> <p><code>fingerprint:</code> <code><fingerprint></code> - The unique identifier of the certificate</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Certificate Login Failure	<p>Certificate login failure</p> <p><code>fingerprint:</code> <code><fingerprint></code> - The unique identifier of the certificate</p> <p><code>commonName:</code> <code><commonName></code> - Set of metadata that represents the entity</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Certificate Creation	<p>Certificate creation</p> <p><code>fingerprint:</code> <code><fingerprint></code> - The unique identifier of the certificate</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p>	
	Certificate Revocation	<p>Revocation of certificate</p> <p><code>fingerprint:</code> <code><fingerprint></code> - The unique identifier of the certificate</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p>	

Event grouping	What events are logged	How to identify related log events	Additional information
Device Management Events	User Locked	<p>User locked</p> <p><code>userId: <userId></code> - The unique ID of the user</p> <p><code>instanceId: <instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId: <tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime: <requestTime></code> - Date and time when the event occurs</p>	
	User Unlocked	<p>User unlocked</p> <p><code>userId: <userId></code> - The unique ID of the user</p> <p><code>instanceId: <instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId: <tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime: <requestTime></code> - Date and time when the event occurs</p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	User Password Changed	Password changed userId: <userId> - The unique ID of the user instanceId: <instanceId> - The unique identifier of the customer instance tenantId: <tenantId> - The identifier of the consumer account for the current application context requestTime: <requestTime> - Date and time when the event occurs	
	User Authorization Failed	Authorization failed userId: <userId> - The unique ID of the user instanceId: <instanceId> - The unique identifier of the customer instance tenantId: <tenantId> - The identifier of the consumer account for the current application context requestTime: <requestTime> - Date and time when the event occurs	

Event grouping	What events are logged	How to identify related log events	Additional information
	Gateway Bundle Start	<p>Gateway bundle started</p> <p><code>gatewayId:</code> <code><gatewayId></code> - The unique ID of the gateway</p> <p><code>bundleId:</code> <code><bundleId></code> - The unique ID of the bundle</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Gateway Bundle Stop	<p>Gateway bundle stopped</p> <p>gatewayId: <gatewayId> - The unique ID of the gateway</p> <p>bundleId: <bundleId> - The unique ID of the bundle</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p>	
Device Management Events	DB Instance Creation	<p>DatabaselInstance creation</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	DB Instance Deletion	<p>Databaselnstance deletion</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p>	
	Messaging Instance Creation	<p>MessagingInstance creation</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Messaging Instance Deletion	<p>MessagingInstance deletion</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p>	
	Platform Tenant Creation	<p>PlatformTenant creation</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Platform Tenant Deletion	PlatformTenant deletion instanceId: <instanceId> - The unique identifier of the customer instance tenantId: <tenantId> - The identifier of the consumer account for the current application context requestTime: <requestTime> - Date and time when the event occurs	
	Vendor Creation	Vendor creation instanceId: <instanceId> - The unique identifier of the customer instance tenantId: <tenantId> - The identifier of the consumer account for the current application context requestTime: <requestTime> - Date and time when the event occurs	

Event grouping	What events are logged	How to identify related log events	Additional information
	Vendor Deletion	<p>Vendor deletion</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p>	
	Protocol Creation	<p>Protocol creation</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Protocol Deletion	<p>Protocol deletion</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p>	
	User Creation	<p>User creation</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	User Deletion	<p>User deletion</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p>	
	User Custom Properties Creation	<p>User update</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>name:</code> <code><customProperties></code> - custom property attributes</p> <p><code>old:</code> <code><n/a></code></p> <p><code>new:</code> <code><UserCustomProperty></code></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	User Custom Properties Update	<p>User update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <customProperties> - custom property attributes</p> <p>old: <old custom property></p> <p>new: <new custom property></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	User Custom Properties Deletion	<p>User update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <customProperties> - custom property attributes</p> <p>old: <old custom property></p> <p>new: <new custom property></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	User Role Creation	<p>User update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <roles> - roles attributes</p> <p>old: <n/a></p> <p>new: <UserRole></p>	
	User Role Deletion	<p>User update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <roles> - roles attributes</p> <p>old: <old role name></p> <p>new: <new role name></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Tenant Creation	<p>Tenant creation</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <name> - tenant attributes</p> <p>old: <n/a></p> <p>new: <new tenant name></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Add Tenant Custom Property	<p>Tenant update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <customProperties> - Custom property attributes</p> <p>old: <n/a></p> <p>new: <new custom property></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Tenant Custom Property Update	<p>Tenant update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <customProperties> - Custom property attributes</p> <p>old:<old custom property></p> <p>new:<new custom property></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Tenant Custom Property Delete	<p>Tenant update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <customProperties> - custom property attributes</p> <p>old:<old custom property></p> <p>new:<new custom property></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	User Tenant Assignment Creation	<p>Tenant update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <tenantUsers> - tenant user attributes</p> <p>old: <n/a></p> <p>new: <UserTenantAssignment></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	User Tenant Assignment Update	<p>Tenant update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <tenantUsers> - tenant user attributes</p> <p>old: <old user assignment></p> <p>new: <UserTenantAssignment></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	User Tenant Assignment Delete	<p>Tenant update</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>name: <tenantUsers></code> - tenant user attributes</p> <p><code>old: <old user assignment></code></p> <p><code>new:</code> <code><UserTenantAssignment></code></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Capability Creation	<p>Capability creation</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>name:</code> <code><name></code> - capability attributes</p> <p><code>old:</code> <code><n/a></code></p> <p><code>new:</code> <code><new capability></code></p>	
	Capability Update	<p>Capability update</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>name:</code> <code><name></code> - capability attributes</p> <p><code>old:</code> <code><old capability></code></p> <p><code>new:</code> <code><new capability></code></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Capability Deletion	<p>Capability deletion</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>name: <name></code> - capability attributes</p> <p><code>old: <old capability></code></p> <p><code>new: <new capability></code></p>	
	Sensor Type Creation	<p>SensorType creation</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>name: <name></code> - sensor type attributes</p> <p><code>old: <n/a></code></p> <p><code>new: <new sensor type></code></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Sensor Type Update	<p>SensorType update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <name> - sensor type attributes</p> <p>old:<old sensor type></p> <p>new:<new sensor type></p>	
	Sensor Type Delete	<p>SensorType deletion</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <name> - sensor type attributes</p> <p>old:<old sensor type></p> <p>new:<new sensor type></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Capability Assignment Creation	<p>SensorType update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <capabilityAssignments> - capability assignment attributes</p> <p>old: <n/a></p> <p>new: <CapabilityAssignment></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Capability Assignment Update	<p>SensorType update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <capabilityAssignments> - capability assignment attributes</p> <p>old:<old capability assignment></p> <p>new: <CapabilityAssignment></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Capability Assignment Deletion	<p>SensorType update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <capabilityAssignments> - capability assignment attributes</p> <p>old: <CapabilityAssignment></p> <p>new: <n/a></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Device Creation	<p>Device creation</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <alternateId> - Device attributes</p> <p>old: <n/a></p> <p>new: <alternateId></p>	
	Device Update	<p>Device update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <name> - Device attributes</p> <p>old: <old device></p> <p>new: <new device></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Device Deletion	<p>Device deletion</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>name:</code> <code><name></code> - Device attributes</p> <p><code>old:</code> <code><old device></code></p> <p><code>new:</code> <code><n/a></code></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Add Device Custom Property	<p>Device update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <customProperties> - Custom properties attributes</p> <p>old: <n/a></p> <p>new: <DeviceCustomProperty></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Device Custom Property Update	<p>Device update</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>name:</code> <code><customProperties></code> - Custom properties attributes</p> <p><code>old:</code> <code><DeviceCustomProperty></code></p> <p><code>new:</code> <code><DeviceCustomProperty></code></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Device Custom Property Deletion	<p>Device update</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>name:</code> <code><customProperties></code> - Custom properties attributes</p> <p><code>old:</code> <code><DeviceCustomProperty></code></p> <p><code>new:</code> <code><n/a></code></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Sensor Creation	<p>Sensor creation</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>name: <name></code> - Sensor attributes</p> <p><code>old: <n/a></code></p> <p><code>new: <sensor name></code></p>	
	Sensor Update	<p>Sensor update</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>name: <name></code> - Sensor attributes</p> <p><code>old: <sensor name></code></p> <p><code>new: <sensor name></code></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Sensor Deletion	<p>Sensor update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <name> - Sensor attributes</p> <p>old: <sensor name></p> <p>new: <n/a></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Add Sensor Type Custom Property	<p>Sensor update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <customProperties> - Custom property attributes</p> <p>old: <n/a></p> <p>new: <SensorCustomProperty></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Sensor Type Custom Property Update	<p>Sensor update</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>name:</code> <code><customProperties></code> - Custom property attributes</p> <p><code>old:</code> <code><SensorCustomProperty></code></p> <p><code>new:</code> <code><SensorCustomProperty></code></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Sensor Type Custom Property Delete	<p>Sensor update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <customProperties> - Custom property attributes</p> <p>old: <SensorCustomProperty></p> <p>new: <n/a></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Gateway Creation	<p>Gateway creation</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>name:</code> <code><name></code> - Gateway attributes</p> <p><code>old:</code> <code><n/a></code></p> <p><code>new:</code> <code><gateway name></code></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Gateway Bundle Upload	<p>Gateway update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <bundleDownloadAssignmentList> - Gateway bundle attributes</p> <p>old: <n/a></p> <p>new: <GatewayBundleDownloadAssignment></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Gateway Bundle Delete	<p>Gateway update</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>name:</code> <code><bundle></code> - Gateway bundle attributes</p> <p><code>old:</code> <code><GatewayBundle></code></p> <p><code>new:</code> <code><n/a></code></p>	
	Configuration Creation	<p>ConfigurationBean creation</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>name:</code> <code><name></code> - Configuration attributes</p> <p><code>old:</code> <code><n/a></code></p> <p><code>new:</code> <code><configuration name></code></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Configuration Update	<p>ConfigurationBean update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <properties> - Configuration attributes</p> <p>old: <property></p> <p>new: <property></p>	
	Configuration Deletion	<p>ConfigurationBean deletion</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <Entity> - Configuration attributes</p> <p>old: <entity id></p> <p>new: <n/a></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Retention Creation	<p>RetentionPolicy creation</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <name> - Retention Policy attributes</p> <p>old: <n/a></p> <p>new: <retention policy name></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Retention Update	<p>RetentionPolicy update</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <name> - Retention Policy attributes</p> <p>old: <retention policy name></p> <p>new: <retention policy name></p>	
	Retention Deletion	<p>RetentionPolicy deletion</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <Entity> - Retention Policy attributes</p> <p>old: <entity id></p> <p>new: <n/a></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
Message Processing Events	User Authorization Failure	<p>Authorization failed</p> <p>userId: <userId> - The unique ID of the user</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p>	
	Selector Creation	<p>Selector creation</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <name> - Selector attributes</p> <p>old: <n/a></p> <p>new: <selector name></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Selector Update	<p>Selector update</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>name:</code> <code><name></code> - Selector attributes</p> <p><code>old:</code> <code><selector name></code></p> <p><code>new:</code> <code><selector name></code></p>	
	Selector Deletion	<p>Selector deletion</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>name:</code> <code><Entity></code> - Selector attributes</p> <p><code>old:</code> <code><entity id></code></p> <p><code>new:</code> <code><n/a></code></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Mapping Creation	<p>MappingBean creation</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <name> - Mapping attributes</p> <p>old: <entity id></p> <p>new: <n/a></p>	
	Mapping Deletion	<p>MappingBean deletion</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p> <p>name: <Entity> - Mapping attributes</p> <p>old: <entity id></p> <p>new: <n/a></p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Read measures	<p>Read measures</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p> <p><code>id: <Capability Id></code> - The unique identifier for the capability</p>	

Event grouping	What events are logged	How to identify related log events	Additional information
MQTT Gateway	Connection Unauthorized	<p>Connection Unauthorized</p> <p><code>deviceId:</code> <code><deviceId></code> - The unique ID of the device</p> <p><code>alternateId:</code> <code><alternateId></code> - The alternateId is the unique and immutable identifier of an entity</p> <p><code>clientId:</code> <code><clientId></code> - The ID of the client connection</p> <p><code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance</p> <p><code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context</p> <p><code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs</p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Subscription Unauthorized	<p>Subscription Unauthorized</p> <p>deviceId: <deviceId> - The unique ID of the device</p> <p>alternateId: <alternateId> - The alternateId is the unique and immutable identifier of an entity</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Sending Unauthorized	<p>Sending Unauthorized</p> <p>deviceId: <deviceId> - The unique ID of the device</p> <p>alternateId: <alternateId> - The alternateId is the unique and immutable identifier of an entity</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p>	

Event grouping	What events are logged	How to identify related log events	Additional information
REST Gateway	Connection Unauthorized	<p>Connection Unauthorized</p> <p>deviceId: <deviceId> - The unique ID of the device</p> <p>alternateId: <alternateId> - The alternateId is the unique and immutable identifier of an entity</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p>	
Messaging	Connection Unauthorized	<p>Connection Unauthorized</p> <p>gatewayId: <gatewayId> - The unique ID of the Gateway</p> <p>instanceId: <instanceId> - The unique identifier of the customer instance</p> <p>tenantId: <tenantId> - The identifier of the consumer account for the current application context</p> <p>requestTime: <requestTime> - Date and time when the event occurs</p>	

Event grouping	What events are logged	How to identify related log events	Additional information
	Subscription Unauthorized	Subscription Unauthorized <code>clientId:</code> <code><clientId></code> - This value includes the ID of the Gateway <code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance <code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context <code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs	
	Sending Unauthorized	Sending Unauthorized <code>clientId:</code> <code><clientId></code> - This value includes the ID of the Gateway <code>instanceId:</code> <code><instanceId></code> - The unique identifier of the customer instance <code>tenantId:</code> <code><tenantId></code> - The identifier of the consumer account for the current application context <code>requestTime:</code> <code><requestTime></code> - Date and time when the event occurs	

The following information is described in the table columns:

- [Event grouping](#) - Events that are logged with a similar format or are related to the same entities.

- [*What events are logged*](#) - Description of the security or data protection and privacy related event that is logged.
- [*How to identify related log events*](#) - Search criteria or key words, that are specific for a log event that is created along with the logged event.
- [*Additional information*](#) - Any related information that can be helpful.

Related Information

[Audit Logging in the Cloud Foundry Environment](#)

12 Related Information

12.1 Certificates

In cryptography, X.509 is a standard that defines the format of public key certificates. X.509 certificates are used in many internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the Web. An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is usually signed by a certificate authority. When a certificate is signed by a certificate authority, someone holding that certificate can rely on the public key it contains to establish secure communications with another party.

12.2 REST APIs

The URL for the REST APIs has the following format:

```
https://<HOST_NAME>/<INSTANCE_ID>/iot/core/api/v1/<service>
```

As an example, the [Devices](#) APIs are available at URL:

```
https://<HOST_NAME>/<INSTANCE_ID>/iot/core/api/v1/devices
```

All REST endpoints require Basic Authentication, with username and password provided as follows:

- [user](#) must be in the form `<user_id>`
- [password](#) is the `<password>` assigned to the Internet of Things Service user

Additionally, you need to complete the HTTP request by setting a [Content-Type](#) header to `application/json`.

For more information, please refer to the [Internet of Things Service API](#) documentation.

12.3 Message Queue

The Internet of Things Messaging provides JMS queues that both enable the communication between Internet of Things Service components, and which is used by applications to consume device data and events.

A JMS client can connect to the Internet of Things Messaging leveraging a secure transport backed by the NIO protocol, where mutual authentication based on client certificate authentication over TLS/SSL is in place. For more information, please refer to section [Secure Device Onboarding \[page 9\]](#).

The client shall specify a connection string with the following format:



```
nio+ssl://<HOST_NAME>/<INSTANCE_ID><:61616
```

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.