

# **Audit Data Dictionary**

Identity as a Service

Exported on 09/23/2024

# Table of Contents

- 1 Entity Types ..... 7
- 2 Authentication Events..... 10
- 3 Audit Details ..... 12
  - 3.1 SamlAuthenticationSuccessEvent..... 12
  - 3.2 OidcAuthenticationSuccessEvent..... 12

The audit event structure is:

| Event Attribute | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Example                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| id              | Unique ID for the event.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 313b43e7-098a-4cc9-a6fd-a1ac1c703e53                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| eventTime       | When the event happened in UTC time. The format is YYYY-MM-DDThh:mm:ssZ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2016-08-21T14:27:55Z                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| eventCategory   | The event category. Valid values are: AUTHENTICATION or MANAGEMENT                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | AUTHENTICATION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| eventType       | <p>Identifies the source of the event.</p> <p>Valid AUTHENTICATION values are listed under "Authentication Events" below.</p> <p>For MANAGEMENT actions, event types are built from the entity and action performed using this format: "&lt;EntityType&gt;&lt;EntityAction&gt;Event" where EntityType and EntityAction have the first letter capitalized. For instance, the events for the USERS entity type are the following:</p> <ul style="list-style-type: none"> <li>• UsersAddEvent</li> <li>• UsersEditEvent</li> <li>• UsersRemoveEvent</li> </ul> | <p>Some AUTHENTICATION examples:</p> <ul style="list-style-type: none"> <li>• AuthenticationDeniedEvent</li> <li>• AuthenticationOtpSuccessEvent</li> <li>• AuthenticationTokenSuccessEvent</li> <li>• AuthenticationTokenPushSuccessEvent</li> <li>• AuthenticationOtpEmailSentEvent</li> <li>• AuthenticationOtpSmsSentEvent</li> </ul> <p>Some MANAGEMENT examples:</p> <ul style="list-style-type: none"> <li>• UsersAddEvent</li> <li>• ContextrulesEditEvent</li> <li>• ApplicationsRemoveEvent</li> </ul> |
| accountId       | The account UUID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | a6cb609f-c6ea-48ad-ab61-433b4054a1f8                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Event Attribute | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Example                                                                                                      |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| subjectId       | <p>The user authenticating (in an AUTHENTICATION event) or administrator performing a management action—contains the internal UUID.</p> <p><b>Note:</b> For Azure AD conditional access authentication audits where a mapping to an IDaaS users is not found or the request fails validation, the subjectId value is a random UUID value.</p>                                                                                                                                                                                                                                                  | 72fd8717-fffe-462f-83c6-131c12539af7                                                                         |
| subjectName     | <p>The userId value of the user authenticating (in an AUTHENTICATION event) or administrator performing a MANAGEMENT action.</p> <p>Note: For Azure AD conditional access authentication audits where a mapping to an IDaaS users is not found or the request fails validation, the subjectName is the Azure AD provided user value (e.g., Azure AD user upn value).</p>                                                                                                                                                                                                                       | lp1415@brawlers.es                                                                                           |
| subjectType     | <p>The type of the subject. Valid values are:</p> <ul style="list-style-type: none"> <li>• USER - The subject is an end user or administrator user. The subjectName is the userId of that user.</li> <li>• ADMIN_API - The subject is an admin API application. The subjectName is the name of the application</li> <li>• SERVICE_PROVIDER - The subject is a service provider. The subjectName is hard-coded to "Service Provider". The subjectId is a random value.</li> <li>• AGENT - The subject is an Enterprise Service Gateway (ESG) agent. The subjectName is the ESG name.</li> </ul> | USERS                                                                                                        |
| eventOutcome    | The event outcome. Valid values are: SUCCESS or FAIL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | SUCCESS                                                                                                      |
| message         | <p>A message key for indicating what the event did. Note that the eventType and the message identify the same action. For management actions, the message key is built from the entity and action performed. For instance, for users, there are these message keys:</p> <ul style="list-style-type: none"> <li>• users.add</li> <li>• users.remove</li> <li>• users.edit</li> </ul>                                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>• service_authentication.otp_sms_send</li> <li>• users.add</li> </ul> |
| resourceId      | The resource identifier (for example, the application's UUID)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | a6cb609f-c6ea-48ad-ab61-433b4054a1f8                                                                         |

| Event Attribute         | Description                                                                                                                                                                       | Example                              |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| resourceName            | The resource name (for example, the application name)                                                                                                                             | "Salesforce"                         |
| sourceIp                | The request IP address or IP address provided for authentication API applications.                                                                                                | 1.23.47.122                          |
| eventVersion            | Reserved for future use. Now it contains always "v1".                                                                                                                             | v1                                   |
| token                   | Depending at what stage the event is generated, it can contain nothing, the type of authentication the user is trying to use (OTP, TOKEN, TOKENPUSH), or the token serial number. | 1234-5678                            |
| requiredPermission      | The permission required to access a management entity. The permission is a duple <entityType:entityAction> in lowercase.                                                          | users:add                            |
| subscriberRoleId        | The role UUID used to access the Admin Portal management application.                                                                                                             | 775419bf-ffff-467a-8743-e77930cc7ed9 |
| subscriberRoleName      | The subscriber role name                                                                                                                                                          | "Super Administrator"                |
| serviceProviderRoleId   | The role UUID used to access the Service Provider management application.                                                                                                         | a6cb609f-c6ea-48ad-ab61-433b4054a1f8 |
| serviceProviderRoleName | The service provider role name                                                                                                                                                    | Auditor                              |
| entityType              | Identifies the business entity type. Valid values are listed under "Entity Types" below.                                                                                          | USERS                                |
| entityAction            | Identifies the action invoked on the entity. Valid values are: ADD, EDIT, REMOVE, VIEW. Note that there a few non-standard actions that are used at times (for example, ACTIVATE) | ADD                                  |

| Event Attribute | Description                                                                                                                                                                                                                                                                                                                                                                                                                         | Example                                                                                                                                                                                                                                                                                                                                                             |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| entityId        | The entity UUID identifier                                                                                                                                                                                                                                                                                                                                                                                                          | a6cb609f-c6ea-48ad-ab61-433b4054a1f8                                                                                                                                                                                                                                                                                                                                |
| entityName      | The entity name (for example, role name, group name, user ID)                                                                                                                                                                                                                                                                                                                                                                       | "Auditor", "Contractors", "jdoe"                                                                                                                                                                                                                                                                                                                                    |
| auditDetails    | <p>Additional audit details: a JSON document with these possible attributes:</p> <ul style="list-style-type: none"> <li>messageTokens: reserved for future uses</li> <li>modifiedEntityAttributes: [{name: "...", oldValue: "...", newValue: "..."}, {...}]</li> <li>entityAttributes: [{name: "...", value: "..."}, {...}]</li> </ul> <p>The attribute values are specific to the event type and are currently not documented.</p> | <pre>{   entityAttributes: [     {name: "Identity Provider",       value: "SP::twoco"},     {name: "Type", value:       "SP"},     {name: "Issuer", value:       "https://       entrust.us.dev.trustedauthd       ev.com/api/oidc"},     {name: "Role", value:       "Super Administrator"}   ],   messageTokens: null,   modifiedEntityAttributes:   null }</pre> |

# 1 Entity Types

SUBSCRIBERS  
USERS  
APPLICATIONS  
TOKENS  
ROLES  
SPROLES  
CONTEXTRULES  
AUTHORIZATIONGROUPS  
USERATTRIBUTES  
USERATTRIBUTEVALUES  
AGENTS  
GROUPS  
SETTINGS  
DIRECTORIES  
DIRECTORYSYNC  
DIRECTORYCONNECTIONS  
TEMPLATES  
USERSITEROLES  
REPORTS  
BULKUSERS  
BULKGROUPS  
USERPASSWORDS  
SERVICEPROVIDERS  
SERVICEPROVIDERACCOUNTS  
USERMACHINES  
CAS  
BULKHARDWARETOKENS  
BULKSMARTCARDS  
DIGITALIDCONFIGS  
DIGITALIDCONFIGVARIABLES  
DIGITALIDCONFIGCERTTEMPS  
DIGITALIDCONFIGSANS  
SCDEFNS  
SCDEFNPIVAPPLETCONFIGS  
SCDEFNVARIABLES  
SMARTCREDENTIALS  
SMARTCREDENTIALSSIGNATURE  
USERSPROLES  
EXPECTEDLOCATIONS  
USERLOCATIONS  
USERRBASETTINGS  
SPCLIENTCREDENTIALS  
SPMANAGEMENTPLATFORM  
ENTITLEMENTS  
QUESTIONS  
USERQUESTIONS  
USERQUESTIONANSWERS  
USERKBACHALLENGES

WORDSYNONYMS  
GATEWAYS  
GATEWAYCSRS  
SPUSERMGMT  
BULKIDENTITYGUARD  
TEMPACCESSCODES  
TEMPACCESSCODECONTENTS  
GRIDS  
GRIDCONTENTS  
FIDOTOKENS  
EXPORTREPORTS  
CUSTOMIZATIONVARIABLES  
BLACKLISTEDPASSWORDS  
SPENTITLEMENTS  
CREATETENANT  
TENANTS  
ARCHIVES  
CERTIFICATES  
INTELLITRUSTDESKTOPS  
ACTIVESYNC  
PRINTERS  
ISSUANCE  
IDPROOFING  
IDPROOFINGLICENSE  
OTPS  
AD\_CONNECTOR\_DIRECTORIES  
AZURE\_DIRECTORIES  
SCHEDULEDTASKS  
CREDENTIALDESIGNS  
ENROLLMENTS  
BULKENROLLMENTS  
EMAILTEMPLATES  
EMAILVARIABLES  
SENDEMAIL  
SENDSCIM  
SENDAZUREAD  
DIRECTORYPASSWORD  
TRANSACTIONITEMS  
TRANSACTIONRULES  
ENROLLMENTDESIGNS  
HIGH\_AVAILABILITY\_GROUPS  
PKIAASCREDENTIALS  
DIGITALIDCERTIFICATES  
PIVCONTENTSIGNER  
RESOURCESERVERAPIS  
RESOURCESERVERSCOPES  
USEROAUTHTOKENS  
GROUPPOLICIES  
OAUTHROLES  
IDENTITYPROVIDERS  
SMARTCARDS  
IPLISTS  
DOMAINCONTROLLERCERTS

OTPPROVIDERS  
PREFERREDOTPPROVIDERS  
SPIDENTITYPROVIDERS  
PUSHCREDENTIALS  
DIRECTORYSEARCHATTRIBUTES  
DIRECTORYATTRIBUTES  
RISKENGINES  
SCIMPROVISIONINGS  
RATELIMITING  
CLAIMS  
CONTACTVERIFICATION  
HOSTNAMESETTINGS  
MAGICLINKS  
MAGICLINKCONTENTS  
AUTHENTICATIONFLOWS  
FACE  
TOKENACTIVATIONCONTENTS  
POLICYOVERRIDE  
ORGANIZATIONS

## 2 Authentication Events

AuthenticationDeniedEvent  
VerificationDeniedEvent  
VerificationIdpSuccessEvent  
AuthenticationOtpUnavailableEvent  
AuthenticationExternalSuccessEvent";  
AuthenticationExternalSecondFactorBypassEvent  
AuthenticationOtpSentToAllEvent  
AuthenticationOtpEmailSentEvent  
AuthenticationOtpNoCreditEvent  
AuthenticationOtpSmsSentEvent  
AuthenticationOtpVoiceSentEvent  
AuthenticationOtpCreatedEvent  
AuthenticationLockedEvent  
UserPasswordChangeLockedEvent  
UserPasswordChangeFailedEvent  
UserStepUpAuthenticationSuccess  
SamlAuthenticationFailedEvent  
SamlAuthenticationSuccessEvent  
OidcAuthenticationFailedEvent  
OidcAuthenticationSuccessEvent  
MachineLockedEvent  
AuthenticationAdminApiSuccessEvent  
AuthenticationMagicLinkSuccessEvent  
AuthenticationPasswordSuccessEvent  
AuthenticationExternalSuccessEvent  
AuthenticationKbaSuccessEvent  
AuthenticationTempAccessCodeSuccessEvent  
AuthenticationOtpSuccessEvent  
AuthenticationOtpWithTempAccessCodeSuccessEvent  
AuthenticationGridSuccessEvent  
AuthenticationGridWithTempAccessCodeSuccessEvent  
AuthenticationTokenSuccessEvent  
AuthenticationTokenWithTempAccessCodeSuccessEvent  
AuthenticationTokenPushSuccessEvent  
AuthenticationFIDOSuccessEvent

AuthenticationPasskeySuccessEvent  
AuthenticationSmartCredentialPushSuccessEvent  
AuthenticationSmartLoginSuccessEvent  
AuthenticationUserCertificateSuccessEvent  
AuthenticationIdpSuccessEvent  
AuthenticationFaceSuccessEvent  
AuthenticationFirstFactorPasswordSuccessEvent  
AuthenticationFirstFactorExternalSuccessEvent  
AuthenticationFirstFactorIdpSuccessEvent  
AuthenticationSecondFactorKbaSuccessEvent  
AuthenticationSecondFactorTempAccessCodeSuccessEvent  
AuthenticationSecondFactorOtpSuccessEvent  
AuthenticationSecondFactorOtpWithTempAccessCodeSuccessEvent  
AuthenticationSecondFactorGridSuccessEvent  
AuthenticationSecondFactorGridWithTempAccessCodeSuccessEvent  
AuthenticationSecondFactorTokenSuccessEvent  
AuthenticationSecondFactorTokenWithTempAccessCodeSuccessEvent  
AuthenticationSecondFactorTokenPushSuccessEvent  
AuthenticationSecondFactorFIDOSuccessEvent  
AuthenticationSecondFactorUserCertificateSuccessEvent  
AuthenticationSecondFactorSmartCredentialPushSuccessEvent  
AuthenticationSecondFactorFaceSuccessEvent

## 3 Audit Details

### 3.1 SamlAuthenticationSuccessEvent

Application Name

SP/IDP Initiated (IDP or SP)

SP Issuer

Name ID

ACR URL

Organization ID

Organization Name

### 3.2 OidcAuthenticationSuccessEvent

Client ID

Application Name

Response Types

ID Token Subject

Redirect URI

ACR

AMR

Organization ID

Organization Name