Audit Data Dictionary

Identity as a Service

23 July, 2025

Table of Contents

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	Identifies the source of the event. Valid AUTHENTICATION values are listed under "Authentication Events" below. For MANAGEMENT actions, event types are built from the entity and action performed using this format: "<EntityType><EntityAction>Event" where EntityType and EntityAction have the first letter capitalized. For instance, the events for the USERS entity type are the following: • UsersAddEvent • UsersEditEvent • UsersRemoveEvent	Some AUTHENTICATION examples: • AuthenticationDeniedEvent • AuthenticationOtpSuccessEvent • AuthenticationTokenSuccessEvent • AuthenticationTokenPushSuccessEvent • AuthenticationOtpEmailSentEvent • AuthenticationOtpSmsSentEvent Some MANAGEMENT examples: • UsersAddEvent • ContextrulesEditEvent • ApplicationsRemoveEvent
accountId	The account UUID.	a6cb609f-c6ea-48ad-ab61-433b4054a1f8
subjectId	The user authenticating (in an AUTHENTICATION event) or administrator performing a management action—contains the internal UUID. **Note:** 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.	72fd8717-fffe-462f-83c6-131c12539af7

Event Attribute	Description	Example
subjectName	The userId value of the user authenticating (in an AUTHENTICATION event) or administrator performing a MANAGEMENT action. 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).	lp1415@brawlers.es
subjectType	The type of the subject. Valid values are: • USER - The subject is an end user or administrator user. The subjectName is the userId of that user. • ADMIN_API - The subject is an admin API application. The subjectName is the name of the application • SERVICE_PROVIDER - The subject is a service provider. The subjectName is hard-coded to "Service Provider". The subjectId is a random value. • AGENT - The subject is an Enterprise Service Gateway (ESG) agent. The subjectName is the ESG name.	USERS
eventOutcome	The event outcome. Valid values are: SUCCESS or FAIL	SUCCESS
message	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: • users.add • users.remove • users.edit	• service_authentication.otp_sms_send • users.add
resourceId	The resource identifier (for example, the application's UUID)	a6cb609f-c6ea-48ad-ab61-433b4054a1f8
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

Event Attribute	Description	Example
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-efff-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
entityId	The entity UUUID identifier	a6cb609f-c6ea-48ad-ab61-433b4054a1f8
entityName	The entity name (for example, role name, group name, user ID)	"Auditor", "Contractors", "jdoe"

Event Attribute	Description	Example

auditDetails	Additional audit details: a JSON document with these possible attributes:
	• messageTokens: reserved for future uses
	• modifiedEntityAttributes: [{name: "...", oldValue: "...", newValue: "..."}, {...}]
	• entityAttributes: [{name: "...", value: "..."}, {...}]
	The attribute values are specific to the event type and are currently not documented.
		{
		entityAttributes: [
		{name: "Identity Provider", value: "SP::twoco"},
		{name: "Type", value: "SP"},
		{name: "Issuer", value: "https://entrust.us.dev.trustedauthdev.com/api/oidc"},
		{name: "Role", value: "Super Administrator"}
		],
		messageTokens: null,
		modifiedEntityAttributes: null
		}

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

AuthenticationSecondFactorMagicLinkSuccessEvent

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