

Audit - Reading audit information

This article shows how to connect CzechIdM to automated security monitoring system (SIEM). This form of integration is necessary in many organizations. IdM, being the central point where identities and their roles are managed, is just another piece of the security monitoring mosaic.



Starting CzechIdM 11.2.0, we discourage reading audit information using REST as is explained on this page.

Please, use specialized [audit logging functionality](#).

Important events to monitor

For the basics, we recommend to monitor following events:

- Successful login.
- Unsuccessful login.
- New identity created.
- Identity deleted.
- Identity enabled.
- Identity disabled.
- Identity password changed.
- Privilege/role assigned to identity.
- Privilege/role revoked from identity.
- Role request approved.
- Role request rejected.
- New role created.
- Role modified.
- Role deleted.

For each event, we recommend to monitor (at least):

- Who performed the change / initiated the event.
- Which object was changed.
- When was the action performed.

Reading audits programmatically

In essence, everyone can read audit events using RESTapi. The user must be authenticated and authorized. In our examples, we will read audits using `curl`. When using automated tool, use some reasonable time period (say 15 minutes) between reading new audit events. You can specify the time range of audit events in the REST query. CzechIdM provides its response in JSON format. In the examples below, the response is redacted (and commented) for clarity.

Successful login



This example explains some of the response fields and overall structure of the response. Those comments and fields may be omitted or redacted in the rest of examples. Please read through this example carefully.

Request

```
GET /idm/api/v1/audits/search/quick
?size=99999
&page=0
&sort=timestamp,desc
&face=BETWEEN
&from=2019-08-12T09%3A50%3A00.000Z
&till=2019-08-12T10%3A00%3A00.000Z
&type=eu.bcvolutions.idm.core.model.entity.IdmPassword
&changedAttributesList=lastSuccessfulLogin
```

Response

```
"audits": [{
  // unique audit id
  "id": 3104,
  "entityId": "ff261f34-8133-4ae3-8244-30dd6371f0a3",
  // timestamp of the event
  "timestamp": 1565179463761,
  ... redacted ...
  // who performed the change
  "modifierId": "644f4790-607e-4933-b6bc-397d9da34544",
  "modifier": "admin",
  ... redacted ...
  // owner of the "password" object = the user who logged himself in
  "ownerId": "644f4790-607e-4933-b6bc-397d9da34544",
  "ownerCode": "admin",
  ... redacted ...
}, {
  ... redacted ...
}]
```

Unsuccessful login

Request

```
GET /idm/api/v1/audits/search/quick
?size=99999
&page=0
&sort=timestamp,desc
```

```
&face=BETWEEN
&from=2019-08-12T09%3A50%3A00.000Z
&till=2019-08-12T10%3A00%3A00.000Z
&type=eu.bcvolutions.idm.core.model.entity.IdmPassword
&changedAttributesList=unsuccessfulAttempts
```

Response

```
{
  "id" : 305,
  "timestamp" : 1565603696834,
  "modifier" : "[GUEST]",
  "ownerCode" : "admin",
  ... redacted ...
  "_embedded" : {
    ... redacted ...
    ,
    "ownerId" : {
      ... redacted ...
      // username of the unsuccessful logon
      "username" : "admin",
    }
  }
}
```

New identity created

Request

```
GET /idm/api/v1/audits/search/quick
?size=99999
&page=0
&sort=timestamp,desc
&face=BETWEEN
&from=2019-08-12T10%3A00%3A00.000Z
&till=2019-08-12T10%3A10%3A00.000Z
&type=eu.bcvolutions.idm.core.model.entity.IdmIdentity
&modification=ADD
```

Response

```
{
  "id" : 316,
  "timestamp" : 1565604153572,
  // who created
  "modifierId" : "3eb704d3-c177-4ffa-b889-34926c8e05c2",
  "modifier" : "admin",
  // login of created identity
  "ownerId" : "a72d5188-8e1b-47dc-b6af-7e44d8ba92c9",
```

```
"ownerCode" : "john_doe",  
... redacted ...  
}
```

Identity deleted

Request

```
GET /idm/api/v1/audits/search/quick  
?size=99999  
&page=0  
&sort=timestamp,desc  
&face=BETWEEN  
&from=2019-08-12T10%3A30%3A00.000Z  
&till=2019-08-12T10%3A40%3A00.000Z  
&type=eu.bcvolutions.idm.core.model.entity.IdmIdentity  
&modification=DEL
```

Response

```
{  
  "id" : 328,  
  "timestamp" : 1565606265372,  
  "modifier" : "admin",  
  "ownerCode" : "john_doe",  
  ... redacted ...  
}
```

Identity enabled

Request

```
GET /idm/api/v1/audits/search/quick  
?size=99999  
&page=0  
&sort=timestamp,desc  
&type=eu.bcvolutions.idm.core.model.entity.IdmIdentity  
&changedAttributesList=disabled  
&changedAttributesList=state  
&withVersion=true  
&modification=MOD
```

Response

```
{  
  "id" : 330,  
  "timestamp" : 1565606400341,  
  "modifier" : "admin",  
  ... redacted ...  
}
```

```
"ownerCode" : "john_doe",
... redacted ...
"entity" : {
  "lastName" : "Doe",
  "modifier" : "admin",
  "firstName" : "John",
  // current state of identity
  "disabled" : false,
  "state" : "VALID",
  "email" : "john.doe@czechidm.eu",
  "originalModifierId" : "3eb704d3-c177-4ffa-b889-34926c8e05c2",
  "username" : "john_doe"
},
"_embedded" : {
  "entityId" : {
    "modifier" : "admin",
    "username" : "john_doe",
    "firstName" : "John",
    "lastName" : "Doe",
    "email" : "john.doe@czechidm.eu",
    "phone" : null,
    "titleBefore" : null,
    "titleAfter" : null,
    "description" : null,
    // previous state
    "disabled" : true,
    "state" : "DISABLED_MANUALLY",
    ... redacted ...
  }
}
}
```

Identity disabled

Request

```
GET /idm/api/v1/audits/search/quick
?size=99999
&page=0
&sort=timestamp,desc
&type=eu.bcvolutions.idm.core.model.entity.IdmIdentity
&changedAttributesList=disabled
&changedAttributesList=state
&withVersion=true
&modification=MOD
```

Response

```
{
```

```
"id" : 330,
"timestamp" : 1565606400341,
"modifier" : "admin",
"ownerCode" : "john_doe",
... redacted ...
"entity" : {
  "lastName" : "Doe",
  "modifier" : "admin",
  "firstName" : "John",
  // current state of identity
  "disabled" : true,
  "state" : "DISABLED_MANUALLY",
  "email" : "john.doe@czechidm.eu",
  "originalModifierId" : "3eb704d3-c177-4ffa-b889-34926c8e05c2",
  "username" : "john_doe"
},
"_embedded" : {
  "entityId" : {
    "modifier" : "admin",
    "username" : "john_doe",
    "firstName" : "John",
    "lastName" : "Doe",
    "email" : "john.doe@czechidm.eu",
    "phone" : null,
    "titleBefore" : null,
    "titleAfter" : null,
    "description" : null,
    // previous state
    "disabled" : false,
    "state" : "VALID",
    ... redacted ...
  }
}
}
```

Identity password changed

Request

```
GET /idm/api/v1/password-histories/search/quick
?size=99999
&page=0
&sort=created,desc
&changedAttributesList=validFrom
&face=BETWEEN
&from=2019-08-12T12%3A00%3A00.000Z
&till=2019-08-12T12%3A20%3A00.000Z
```

Response

```
{
  "created" : "2019-08-12T12:09:41.260Z",
  "creator" : "john_doe",
  ... redacted ...
  "_embedded" : {
    "identity" : {
      "username" : "john_doe",
      "email" : "john.doe@czechidm.eu",
      ... redacted ...
    }
  }
}
```

Privilege/role assigned to identity

Request

```
GET /idm/api/v1/audits/search/quick
?size=99999
&page=0
&sort=timestamp,desc
&type=eu.bcvolutions.idm.core.model.entity.IdmIdentityRole
&face=BETWEEN
&from=2019-08-09T09%3A10%3A00.000Z
&till=2019-08-09T09%3A12%3A00.000Z
&changedAttributesList=role
&changedAttributesList=%20identityContract
&modification=ADD
```

Response

```
{
  "id" : 450,
  "timestamp" : 1565709288850,
  "modifier" : "admin",
  "ownerCode" : "john_doe",
  "subOwnerCode" : "manager",
  ... redacted ...
  "_embedded" : {
    "entityId" : {
      ... redacted ...
    },
    "identityContract" : {
      ... redacted ...
    },
    "role" : {
      "created" : "2019-08-09T09:10:37.264Z",
      "creator" : "[SYSTEM]",
      // name of the role
    }
  }
}
```

```
        "code" : "manager",
        ... redacted ...
    },
    "_eav" : [ ]
},
// identity the role was assigned to
"ownerId" : {
    "creator" : "admin",
    "username" : "john_doe",
    "firstName" : "John",
    "lastName" : "Doe",
    "email" : "john.doe@czechidm.eu",
    ... redacted ...
}
}
```

Privilege/role revoked from identity

Request

```
GET /idm/api/v1/audits/search/quick
?size=99999
&page=0
&sort=timestamp,desc
&face=BETWEEN
&from=2019-08-12T12%3A25%3A00.000Z
&till=2019-08-12T12%3A32%3A00.000Z
&type=eu.bcvolutions.idm.core.model.entity.IdmIdentityRole
&modification=DEL
&changedAttributesList=role&changedAttributesList=identityContract
```

Response

```
{
    "id" : 402,
    "timestamp" : 1565612905714,
    "modifier" : "admin",
    "ownerCode" : "john",
    "subOwnerCode" : "manager",
    ... redacted ...
    "_embedded" : {
        "subOwnerId" : {
            "code" : "manager",
            "baseCode" : "manager",
            // name of the role
            "name" : "manager",
            "roleType" : "TECHNICAL",
            ... redacted ...
        }
    }
}
```



```
    },  
    // user the role was removed from  
    "ownerId" : {  
      "firstName" : "John",  
      "lastName" : "Doe",  
      "email" : "john.doe@bcvsolutions.eu",  
      ... redacted ...  
    }  
  }  
} ]  
}
```

Role request approved

Request

```
GET /idm/api/v1/audits/search/quick  
?size=99999  
&page=0  
&sort=timestamp,desc  
&type=eu.bcvolutions.idm.core.model.entity.IdmIdentityRole  
&modification=ADD  
&changedAttributesList=role  
&changedAttributesList=identityContract  
&face=TODAY  
&from=2019-08-13T22%3A00%3A00.000Z  
&till=2019-08-14T21%3A59%3A59.999Z
```

Response

```
{  
  "id" : 540,  
  "timestamp" : 1565770422521,  
  "modifier" : "admin",  
  "ownerCode" : "jane",  
  "subOwnerCode" : "test|development",  
  ... redacted ...  
  "_embedded" : {  
    "entityId" : {  
      ... redacted ...  
      "_embedded" : {  
        ... redacted ...  
        "identityContract" : {  
          "_embedded" : {  
            "identity" : {  
              "username" : "jane",  
              "firstName" : "Jane",  
              "lastName" : "Doe",  
              "email" : "jane.doe@bcvsolutions.eu",  
            }  
          }  
        }  
      }  
    }  
  }  
}
```

```
        ... redacted ...
      },
    },
    "_eav" : [ ]
  },
  "role" : {
    "creator" : "admin",
    "code" : "test|development",
    "baseCode" : "test",
    "environment" : "development",
    "name" : "test",
    "roleType" : "TECHNICAL",
    ... redacted ...
  }
},
"_eav" : [ ]
} ]
}
```

Role request rejected

Request

```
GET /idm/api/v1/audits/search/quick
?size=99999
&page=0
&sort=timestamp,desc
&type=eu.bcvolutions.idm.core.model.entity.IdmConceptRoleRequest
&modification=MOD
&changedAttributesList=state
&face=BETWEEN
&from=2019-08-13T15%3A40%3A00.000Z
&till=2019-08-13T15%3A50%3A00.000Z
```

Response

```
{
  "id" : 522,
  "modifier" : "admin",
  ... redacted ...
  "_embedded" : {
    "entityId" : {
      "state" : "DISAPPROVED",
      ... redacted ...
    },
    "_embedded" : {
      ... redacted ...
    },
    "identity" : {
```

```
        "username" : "jane",
        "firstName" : "Jane",
        "lastName" : "Doe",
        "email" : "jane.doe@bcvsolutions.eu",
        ... redacted ...
    },
    "_eav" : [ ]
},
"role" : {
    "creator" : "admin",
    "code" : "test|development",
    "baseCode" : "test",
    "environment" : "development",
    "name" : "test",
    "roleType" : "TECHNICAL",
    ... redacted ...
}
},
"_eav" : [ ]
}
}
```

New role created

Request

```
GET /idm/api/v1/audits/search/quick
?size=99999
&page=0
&sort=timestamp,desc
&type=eu.bcvolutions.idm.core.model.entity.IdmRole
&face=BETWEEN
&from=2019-08-12T11%3A00%3A00.000Z
&till=2019-08-12T11%3A10%3A00.000Z
&modification=ADD
```

Response

```
{
    "id" : 528,
    "timestamp" : 1565769780568,
    // who created the role
    "modifier" : "admin",
    // role name in the form of NAME|environment
    "ownerCode" : "CT0|production",
    ... redacted ...
    "_embedded" : {
```

```
"entityId" : {
  "creator" : "admin",
  "code" : "CT0|production",
  // implementation name of the role
  "baseCode" : "CT0",
  // deployment environment the role is intended for
  "environment" : "production",
  // user friendly name of the role
  "name" : "CT0",
  "roleType" : "TECHNICAL",
  "priority" : 2,
  ... redacted ...
}
}
```

Role modified

Request

```
GET /idm/api/v1/audits/search/quick
?size=99999
&page=0
&sort=timestamp,desc
&type=eu.bcvolutions.idm.core.model.entity.IdmRole
&face=BETWEEN
&from=2019-08-12T11%3A00%3A00.000Z
&till=2019-08-12T11%3A10%3A00.000Z
&modification=MOD
```

Response

```
{
  "id" : 341,
  "entityId" : "2bc71f8f-3ba2-44d7-af90-c1155c1a1e35",
  "changedAttributes" : "name,code,baseCode",
  "modifier" : "admin",
  "ownerId" : null,
  "ownerCode" : "manager|test",
  ... redacted ...
}
```

Role deleted

Request

```
GET /idm/api/v1/audits/search/quick
?size=99999
```

```
&page=0
&sort=timestamp,desc
&type=eu.bcvolutions.idm.core.model.entity.IdmRole
&face=BETWEEN
&from=2019-08-12T11%3A10%3A00.000Z
&till=2019-08-12T11%3A20%3A00.000Z
&modification=DEL
```

Response

```
{
  "id" : 342,
  "timestamp" : 1565608213844,
  "modifier" : "admin",
  "ownerCode" : "manager|test",
  ... redacted ...
}
```

From:

<https://wiki.czechidm.com/> - CzechIdM Identity Manager

Permanent link:

https://wiki.czechidm.com/tutorial/adm/reading_audits

Last update: **2021/10/07 13:39**

