ERICSSON

ENM System Security Configuration Programmers Guide

User Instructions

1/19817-CNA 403 3065 Uen AA

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.

Contents

1	**ENM System Security Configuration Programmers Guide**	**1**
2	**Curl Examples Information**	**2**
3	**General Settings Interface**	**3**
3.1	Get General Settings	3
3.2	Update General Settings	4
4	**Password Settings Interface**	**5**
4.1	Get Password Settings	6
4.2	Update Password Settings	9
4.3	Get Password Aging Settings	13
4.4	Get Account Lockout Settings	13
4.5	Update Password Complexity	14
4.6	Update Password Aging	18
4.7	Update Account Lockout	19
4.8	Password Complexity Rules	21
4.9	Get Password Complexity Settings	23
5	**System Security Session Settings**	**26**
5.1	Get Session Settings	26
5.2	Update Session Settings	27
6	**User Profile Settings Interface**	**29**
6.1	Get User Profile Settings	29
6.2	Enable and Disable User to Modify Own Personals or Email	30
7	**External Identity Provider Settings and Monitoring Interface**	**31**
7.1	External Identity Provider Configuration Interface	31
7.2	Check Communication against External Identity Provider	36
7.3	Troubleshooting Cases	39
8	**Federated Identity Management Interface**	**45**
8.1	Get Federated Identity Synchronization State	53
8.2	Set Federated Identity Synchronization State	54
8.3	Get Federated Identity Synchronization Period	56
8.4	Set Federated Identity Synchronization Period	57

8.5 Import Federated Identity Synchronization Advanced Settings Configuration 58
8.6 Export Federated Identity Synchronization Advanced Settings Configuration 61
8.7 Test Federated Identity Synchronization 63
8.8 Federated Identity Synchronization Forced Delete 65
8.9 Federated Identity Synchronization Forced Sync 66
8.10 Federated Identity Synchronization Restore to Defaults 67
8.11 Get Federated Identity Last Synchronization Report 68
8.12 Error Code Responses - Federated Identity Management 72

Reference List **75**

1 ENM System Security Configuration Programmers Guide

This document describes how to interact with the RESTful system security configuration APIs.

It contains detailed information about:

— Available use cases.

— Who can perform the use cases.

— REST requests and responses with examples.

— URL and JSON templates.

Target Groups

This document is intended for users developing their own interface to ENM.

2 Curl Examples Information

The table describes the objects used in the Curl examples.

Parameters	Description of Objects Occurring in Examples
certificate.pem	ENM certificate file: `<file_path>/<file_name>`. PEM file which contains ENM certificate. Client is able to connect to ENM over TLS/SSL with the certificate. The user is provided with the certificate file by Security Administrator. To retrieve certificate by Security Administrator, see the section *Export ENM PKI Root CA Certificate* in ENM Public Key Infrastructure System Administrator Guide, Reference [1].
cookie.txt	Session cookie file: `<file_path>/<file_name>`. The cookie file is created during establishing the session of the credentials of the security administrator.
<hostName>	Fully Qualified Domain Name (FQDN) of the ENM.

Note: When NBI is used, the session cookie must be stored in a secure location (for example, in user home directory). To improve security even more, cookie must have permissions set to 600.

3 General Settings Interface

> This interface is provided for Security Administrators to configure general settings through REST API.

The table describes the parameters for the general settings management:

Parameter	Description
displaySuccessfulLoginScreen	Boolean - indicates if Login Successful Screen is displayed after successful logon.

3.1 Get General Settings

> This REST endpoint retrieves general settings.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Get General Settings	GET	/oss/idm/config/generalsettings

HTTP Response Code: 200

```
{
    "displaySuccessfulLoginScreen": true
}
```

Example 1

```
curl --cacert certificate.pem --cookie cookie.txt "https://<hostname>/oss/idm/co →
nfig/generalsettings"
```

Result

```
{"displaySuccessfulLoginScreen":true}
```

3.2 Update General Settings

> This REST endpoint updates general settings.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Update General Settings	PUT	/oss/idm/config/generalsettings

JSON Query

```
{
    "displaySuccessfulLoginScreen": false
}
```

Available Field

— displaySuccessfulLoginScreen [mandatory]

HTTP Response Code: 200

```
{
    "displaySuccessfulLoginScreen": false
}
```

Example 2

```
curl --cacert certificate.pem --cookie cookie.txt -X PUT -H "Content-Type: Appli →
cation/json" -d '{"displaySuccessfulLoginScreen":false}' "https://<hostname>/oss →
/idm/config/generalsettings"
```

Result:

```
{"displaySuccessfulLoginScreen":false}
```

4 Password Settings Interface

> This interface is provided for Security Administrators to configure password settings through REST API.

Password settings consist of Password Complexity, Password Aging, and Account Lockout settings.

Password Settings Parameter	Description
id	String - password settings identifier, supported values: enmuser.
passwordComplexity	List of password complexity rules. For details, see Password Complexity Rules on page 21.
passwordAgeing	Password Aging settings.
accountLocked	Account Lockout settings.

Password Aging Parameter	Description
enabled	Boolean - indicates if password aging is enabled in the system. Default vale: true.
pwdMaxAge	Integer - contains the value of maximum period the password is valid, specified in days. Mandatory when enabled is true, irrelevant when enabled is false. The value must be in range 1—180 days. Default value: 90 days.
pwdExpireWarning	Integer - contains the value of period to display information about the upcoming password expiration time, specified in days. Mandatory when enabled is true, irrelevant when enabled is false. The value must be less than pwdMaxAge value and must be in range 1—14 days. Default value: 7 days.
graceLoginCount	Integer - contains the value of logon attempts to allow the user to choose a new password. It is not configurable, must be set to 0 when enabled is true, irrelevant when enabled is false.

Account Lockout Parameter	Description
enabled	Boolean - indicates if account can be locked because of too many logon failures. Default value: true.
loginMaxFailedAttempts	Integer - indicates number of logon failures after which account is locked. Mandatory when enabled is true, irrelevant when enabled is false. The value must be in range 1—10. Default value: 3.
loginLockoutExpiration	Boolean - indicates if account lockout expires after some time. Mandatory when enabled is true, irrelevant when enabled is false. Default value: true.
loginLockoutExpirationTime	Integer - indicates number of minutes after which account is unlocked again. Mandatory when loginLockoutExpiration is true, irrelevant when enabled or loginLockoutExpiration is false. The value must be in range 1—60 minutes. Default value: 3 minutes.

Account Lockout Parameter	Description
loginFailureExpiration	Boolean - indicates if logon failures expire after some time. Mandatory when enabled is true, irrelevant when enabled is false. Default value: true.
loginFailureExpirationTime	Integer - indicates number of minutes after which failure logon expires. Mandatory when loginFailureExpiration is true, irrelevant when enabled or loginFailureExpiration is false. The value must be in range 1–60 minutes. Default value: 5 minutes.

4.1 Get Password Settings

> This REST endpoint retrieves password settings.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
GET Password Settings	GET	/oss/idm/config/passwordsettings/{id}

Available Field

— id [mandatory] - password settings identifier

HTTP Response Code: 200


```
{
       "passwordComplexity": [
           {
               "name":"maximumLength",
               "value":32,
               "enabled":true,
               "valueConfigurable":false,
               "enablingConfigurable":false,
               "minimumValue":0,
               "maximumValue":32,
               "ruleCategory":"EAGER"
           },
           {
               "name":"minimumLength",
               "value":8,
               "enabled":true,
               "valueConfigurable":true,
               "enablingConfigurable":false,
               "minimumValue":8,
               "maximumValue":32,
               "ruleCategory":"EAGER"
           },
           {
               "name":"minimumLowerCase",
               "value":1,
               "enabled":true,
               "valueConfigurable":true,
               "enablingConfigurable":true,
               "minimumValue":1,
```

```
                "maximumValue":32,
                "ruleCategory":"EAGER"
            },
            {
                "name":"maximumUpperCase",
                "value":1,
                "enabled":true,
                "valueConfigurable":true,
                "enablingConfigurable":true,
                "minimumValue":1,
                "maximumValue":32,
                "ruleCategory":"EAGER"
            },
            {
                "name":"minimumDigits",
                "value":1,
                "enabled":true,
                "valueConfigurable":true,
                "enablingConfigurable":true,
                "minimumValue":1,
                "maximumValue":32,
                "ruleCategory":"EAGER"
            },
            {
                "name":"minimumSpecialChars",
                "value":1,
                "enabled":false,
                "valueConfigurable":true,
                "enablingConfigurable":true,
                "minimumValue":1,
                "maximumValue":32,
                "ruleCategory":"EAGER"
            },
            {
                "name":"maximumRepeatingChars",
                "value":4,
                "enabled":false,
                "valueConfigurable":true,
                "enablingConfigurable":true,
                "minimumValue":1,
                "maximumValue":32,
                "ruleCategory":"EAGER"
            },
            {
                "name":"maximumConsecutiveChars",
                "value":4,
                "enabled":false,
                "valueConfigurable":true,
                "enablingConfigurable":true,
                "minimumValue":1,
                "maximumValue":32,
                "ruleCategory":"EAGER"
            },
            {
                "name":"mustNotContainUserId",
                "value":0,
                "enabled":false,
                "valueConfigurable":false,
                "enablingConfigurable":true,
                "minimumValue":0,
                "maximumValue":0,
                "ruleCategory":"EAGER"
            },
            {
                "name":"mustNotContainDictionaryWords",
                "value":0,
                "enabled":false,
                "valueConfigurable":false,
                "enablingConfigurable":true,
                "minimumValue":0,
                "maximumValue":0,
                "ruleCategory":"EAGER"
            },
            {
                "name":"mustNotBeOldPassword",
                "value":1,
                "enabled":false,
                "valueConfigurable":true,
                "enablingConfigurable":true,
                "minimumValue":1,
```

```
                "maximumValue":12,
                "ruleCategory":"LAZY
            }
        ],
        "passwordAgeing" : {
            "enabled":true,
            "pwdMaxAge":90,
            "pwdExpireWarning":7,
            "graceLoginCount":0
        },
        "accountLockout" : {
            "enabled": true,
            "loginLockoutExpiration": true,
            "loginFailureExpiration": true,
          "loginMaxFailedAttempts": 3,
          "loginLockoutExpirationTime": 3,
          "loginFailureExpirationTime": 5
        },
}
```

Example 3

```
curl --cacert certificate.pem --cookie cookie.txt "https://<host name>/oss/idm/config/passwordsettings/enmuser"
```

Result

```
{"passwordComplexity":[{"name":"maximumLength","value":32,"enabled":true,"valueConfigurable":false,"enablingConfigurable":false,
"minimumValue":0,"maximumValue":32,"ruleCategory":"EAGER"},{"name":"minimumLength","value":8,"enabled":true,"valueConfigurable":true,
"enablingConfigurable":false,"minimumValue":8,"maximumValue":32,"ruleCategory":"EAGER"},{"name":"minimumLowerCase",
"value":1,"enabled":true,"valueConfigurable":true,"enablingConfigurable":true,"minimumValue":1,
"maximumValue":32,"ruleCategory":"EAGER"},{"name":"minimumUpperCase","value":1,"enabled":true,
"valueConfigurable":true,"enablingConfigurable":true,"minimumValue":1,"maximumValue":32,
"ruleCategory":"EAGER"},{"name":"minimumDigits","value":1,"enabled":true,"valueConfigurable":true,
"enablingConfigurable":true,"minimumValue":1,"maximumValue":32,"ruleCategory":"EAGER"},
{"name":"minimumSpecialChars","value":1,"enabled":false,"valueConfigurable":true,
"enablingConfigurable":true,"minimumValue":1,"maximumValue":32,"ruleCategory":"EAGER"},
{"name":"maximumRepeatingChars","value":4,"enabled":false,"valueConfigurable":true,
"enablingConfigurable":true,"minimumValue":1,"maximumValue":32,"ruleCategory":"EAGER"},
{"name":"maximumConsecutiveChars","value":4,"enabled":false,"valueConfigurable":true,
"enablingConfigurable":true,"minimumValue":1,"maximumValue":32,"ruleCategory":"EAGER"},
{"name":"mustNotContainUserId","value":0,"enabled":false,"valueConfigurable":false,
"enablingConfigurable":true,"minimumValue":0,"maximumValue":0,"ruleCategory":"EAGER"},
{"name":"mustNotContainDictionaryWords","value":0,"enabled":false,"valueConfigurable":false,
"enablingConfigurable":true,"minimumValue":0,"maximumValue":0,"ruleCategory":"EAGER"},
{"name":"mustNotBeOldPassword","value":1,"enabled":false,"valueConfigurable":true,
"enablingConfigurable":true,"minimumValue":1,"maximumValue":12,"ruleCategory":"LAZY"}],
"passwordAgeing":{"enabled":true,"pwdMaxAge":90,"pwdExpireWarning":7,"graceLoginCount":0},
"accountLockout":{"enabled":true,"loginLockoutExpiration":true,"loginFailureExpiration":true,
```

```
"loginMaxFailedAttempts":3,"loginLockoutExpirationTime":3,"loginFailureExpiratio →
nTime":5}}
```


4.2 Update Password Settings

> This REST endpoint updates password settings.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Update Password Settings	PUT	/oss/idm/config/passwordsettings/{id}

JSON Query

```
{
    "passwordComplexity" : [
        {
            "name": "minimumLength",
            "value": 8
        },
        {
            "name": "minimumLowerCase",
            "value": 1,
            "enabled": true
        },
        {
            "name": "minimumUpperCase",
            "value": 1,
            "enabled": true
        },
        {
            "name": "minimumDigits",
            "value": 1,
            "enabled": true
        },
        {
            "name": "minimumSpecialChars",
            "value": 1,
            "enabled": false
        },
        {
            "name": "maximumRepeatingChars",
            "value": 4,
            "enabled": false
        },
        {
            "name": "maximumConsecutiveChars",
            "value": 4,
            "enabled": false
        },
        {
            "name": "mustNotContainUserId",
            "enabled": false
        },
        {
            "name": "mustNotContainDictionaryWords",
            "enabled": false
        },
        {
            "name": "mustNotBeOldPassword",
```

```
            "enabled": true,
            "value": 6
        }
       ],
       "passwordAgeing": {
                "enabled" : "true",
                "pwdMaxAge" : 100,
                "pwdExpireWarning" : 8,
                "graceLoginCount" : 0
       },
       accountLockout" : {
                "enabled" : true,
                "loginMaxFailedAttempts" : 5,
                "loginLockoutExpiration" : true,
                "loginLockoutExpirationTime" : 10,
                "loginFailureExpiration" : true,
                 "loginFailureExpirationTime" : 10
    }
}
```

Available Fields

— id [mandatory] - password settings identifier.

— passwordComplexity [mandatory] - list of password complexity rules.

— passwordAgeing [mandatory] - password aging settings.

— accountLockout [optional] - account lockout settings.

HTTP Response Code: 200

```
{
        "passwordComplexity": [
            {
                "name":"maximumLength",
                "value":32,
                "enabled":true,
                "valueConfigurable":false,
                "enablingConfigurable":false,
                "minimumValue":0,
                "maximumValue":32,
                "ruleCategory":"EAGER"
            },
            {
                "name":"minimumLength",
                "value":8,
                "enabled":true,
                "valueConfigurable":true,
                "enablingConfigurable":false,
                "minimumValue":8,
                "maximumValue":32,
                "ruleCategory":"EAGER"
            },
            {
                "name":"minimumLowerCase",
                "value":1,
                "enabled":true,
                "valueConfigurable":true,
                "enablingConfigurable":true,
                "minimumValue":1,
                "maximumValue":32,
                "ruleCategory":"EAGER"
            },
            {
                "name":"maximumUpperCase",
                "value":1,
                "enabled":true,
                "valueConfigurable":true,
                "enablingConfigurable":true,
```

```
                "minimumValue":1,
                "maximumValue":32,
                "ruleCategory":"EAGER"
            },
            {
                "name":"minimumDigits",
                "value":1,
                "enabled":true,
                "valueConfigurable":true,
                "enablingConfigurable":true,
                "minimumValue":1,
                "maximumValue":32,
                "ruleCategory":"EAGER"
            },
            {
                "name":"minimumSpecialChars",
                "value":1,
                "enabled":false,
                "valueConfigurable":true,
                "enablingConfigurable":true,
                "minimumValue":1,
                "maximumValue":32,
                "ruleCategory":"EAGER"
            },
            {
                "name":"maximumRepeatingChars",
                "value":4,
                "enabled":false,
                "valueConfigurable":true,
                "enablingConfigurable":true,
                "minimumValue":1,
                "maximumValue":32,
                "ruleCategory":"EAGER"
            },
            {
                "name":"maximumConsecutiveChars",
                "value":4,
                "enabled":false,
                "valueConfigurable":true,
                "enablingConfigurable":true,
                "minimumValue":1,
                "maximumValue":32,
                "ruleCategory":"EAGER"
            },
            {
                "name":"mustNotContainUserId",
                "value":0,
                "enabled":false,
                "valueConfigurable":false,
                "enablingConfigurable":true,
                "minimumValue":0,
                "maximumValue":0,
                "ruleCategory":"EAGER"
            },
            {
                "name":"mustNotContainDictionaryWords",
                "value":0,
                "enabled":false,
                "valueConfigurable":false,
                "enablingConfigurable":true,
                "minimumValue":0,
                "maximumValue":0,
                "ruleCategory":"EAGER"
            },
            {
                "name":"mustNotBeOldPassword",
                "value":1,
                "enabled":false,
                "valueConfigurable":true,
                "enablingConfigurable":true,
                "minimumValue":1,
                "maximumValue":12,
                "ruleCategory":"LAZY
            }
        ],
        "passwordAgeing" : {
            "enabled":true,
            "pwdMaxAge":90,
            "pwdExpireWarning":7,
            "graceLoginCount":0
```

```
        },
        "accountLockout" : {
            "enabled": true,
            "loginLockoutExpiration": true,
            "loginFailureExpiration": true,
          "loginMaxFailedAttempts": 3,
          "loginLockoutExpirationTime": 3,
          "loginFailureExpirationTime": 5
        },
}
```

Example 4

```
curl --cacert certificate.pem --cookie cookie.txt -X PUT -H "Con →
tent-Type: Application/json" -d '{"passwordComplexity":[{"name": →
"minimumLength","value":8},{"name":"minimumLowerCase","value":1, →
"enabled":true},{"name":"minimumUpperCase","value":1,"enabled":t →
rue},{"name":"minimumDigits","value":1,"enabled":true},{"name":" →
minimumSpecialChars","value":1,"enabled":false},{"name":"maximum →
RepeatingChars","value":4,"enabled":false},{"name":"maximumConse →
cutiveChars","value":4,"enabled":false},{"name":"mustNotContainU →
serId","enabled":false},{"name":"mustNotContainDictionaryWords", →
"enabled":false},{"name":"mustNotBeOldPassword","value":6,"enabl →
ed":true}],"passwordAgeing":{"enabled":true,"pwdMaxAge":100,"pwd →
ExpireWarning":8,"graceLoginCount":0,,"accountLockout":{"enabled →
":true,"loginLockoutExpiration":true,"loginFailureExpiration":tr →
ue,"loginMaxFailedAttempts":5,"loginLockoutExpirationTime":10,"l →
oginFailureExpirationTime":10}}' "https://<hostname>/oss/idm/con →
fig/passwordsettings/enmuser"
```

Result

```
{"passwordComplexity":[{"name":"maximumLength","value":32,"enabled":true,"valueC →
onfigurable":false,"enablingConfigurable":false,
"minimumValue":0,"maximumValue":32,"ruleCategory":"EAGER"},{"name":"minimumLengt →
h","value":8,"enabled":true,"valueConfigurable":true,
"enablingConfigurable":false,"minimumValue":8,"maximumValue":32,"ruleCategory":" →
EAGER"},{"name":"minimumLowerCase","value":1,"enabled":true,
"valueConfigurable":true,"enablingConfigurable":true,"minimumValue":1,"maximumVa →
lue":32,"ruleCategory":"EAGER"},{"name":"minimumUpperCase",
"value":1,"enabled":true,"valueConfigurable":true,"enablingConfigurable":true,"m →
inimumValue":1,"maximumValue":32,"ruleCategory":"EAGER"},
{"name":"minimumDigits","value":1,"enabled":true,"valueConfigurable":true,"enabl →
ingConfigurable":true,"minimumValue":1,"maximumValue":32,
"ruleCategory":"EAGER"},{"name":"minimumSpecialChars","value":1,"enabled":false, →
"valueConfigurable":true,"enablingConfigurable":true,
"minimumValue":1,"maximumValue":32,"ruleCategory":"EAGER"},{"name":"maximumRepea →
tingChars","value":4,"enabled":false,"valueConfigurable":true,
"enablingConfigurable":true,"minimumValue":1,"maximumValue":32,"ruleCategory":"E →
AGER"},{"name":"mustNotContainUserId","value":0,"enabled":false,
"valueConfigurable":false,"enablingConfigurable":true,"minimumValue":0,"maximumV →
alue":0,"ruleCategory":"EAGER"},{"name":"mustNotContainDictionaryWords",
"value":0,"enabled":false,"valueConfigurable":false,"enablingConfigurable":true, →
"minimumValue":0,"maximumValue":0,"ruleCategory":"EAGER"},
{"name":"mustNotBeOldPassword","value":6,"enabled":true,"valueConfigurable":true →
,"enablingConfigurable":true,"minimumValue":1,"maximumValue":12,
"ruleCategory":"LAZY"}],"passwordAgeing":{"enabled":true,"pwdMaxAge":60,"pwdExpi →
reWarning":5,"graceLoginCount":0},"accountLockout":{"enabled":true,
"loginLockoutExpiration":true,"loginFailureExpiration":true,"loginMaxFailedAttem →
pts":3,"loginLockoutExpirationTime":3,"loginFailureExpirationTime":5}}
```

4.3 Get Password Aging Settings

> This REST endpoint retrieves password aging settings.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
GET Password Ageing Settings	`GET`	`/oss/idm/config/passwordsettings/{id}/passwordageing`

Available Field

— id [mandatory] - password settings identifier

HTTP Response Code: 200

```
{
    "enabled":"true"
    "pwdMaxAge":40
    "pwdExpireWarring":8
    "graceLoginCount":0
}
```

Example 5

```
curl --cacert certificate.pem --cookie cookie.txt "https://<hostname>/oss/idm/co
nfig/passwordsettings/enmuser/passwordageing"
```

Result

```
{"enabled":true,"pwdMaxAge":100,"pwdExpireWarning":8,"graceLoginCount":0}
```

4.4 Get Account Lockout Settings

> This REST endpoint retrieves account lockout settings.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
GET Account Lockout Settings	GET	/oss/idm/config/passwordsettings/{id}/accountlockout

Available Fields

— id [mandatory] - password settings identifier

HTTP Response Code: 200

```
{
    "enabled":true,
    "loginMaxFailedAttempts":3,
    "loginLockoutExpiration":true,
    "loginLockoutExpirationTime":3,
    "loginFailureExpiration":true,
    "loginFailureExpirationTime": 5
}
```

Example 6

```
curl --cacert certificate.pem --cookie cookie.txt "https://<hostname>/oss/idm/co →
nfig/passwordsettings/enmuser/accountlockout"
```

Result

```
{"enabled":true,"loginLockoutExpiration":true,"loginFailureExpiration":true,"log →
inMaxFailedAttempts":3,"loginLockoutExpirationTime":3,"loginFailureExpirationTim →
e":5}
```

4.5 Update Password Complexity

> This REST endpoint updates password complexity.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Update Password Complexity	PUT	/oss/idm/config/passwordsettings/{id}/passwordcomplexity

JSON Query

```
[
    {
```

```
        "name":  "minimumLength",
        "value":  8
    },
    {
        "name":  "minimumLowerCase",
        "value":  1,
        "enabled":  true
    },
    {
        "name":  "minimumUpperCase",
        "value":  1,
        "enabled":  true
    },
    {
        "name":  "minimumDigits",
        "value":  1,
        "enabled":  true
    },
    {
        "name":  "minimumSpecialChars",
        "value":  1,
        "enabled":  true
    },
    {
        "name":  "maximumRepeatingChars",
        "value":  4,
        "enabled":  true
    },
    {
        "name":  "maximumConsecutiveChars",
        "value":  4,
        "enabled":  true
    },
    {
        "name":  "mustNotContainUserId",
        "enabled":  true
    },
    {
        "name":  "mustNotContainDictionaryWords",
        "enabled":  true
    },
    {
        "name" : "mustNotBeOldPassword",
        "enabled" : true,
        "value" : 3
]
```


Available Fields

— id [mandatory] - password settings identifier

— Password Complexity Rules on page 21 [mandatory]

HTTP Response Code: 200


```
[
    {
        "name":  "maximumLength",
        "value":  32,
        "enabled":  true,
        "valueConfigurable":  false,
        "enablingConfigurable":  false,
        "minimumValue":  0,
        "maximumValue":  32,
        "ruleCategory": "EAGER"
    },
    {
        "name":  "minimumLength",
        "value":  8,
        "enabled":  true,
        "valueConfigurable":  true,
        "enablingConfigurable":  false,
```

```
        "minimumValue":  8,
        "maximumValue":  32,
        "ruleCategory": "EAGER"
    },
    {
        "name":  "minimumLowerCase",
        "value":  1,
        "enabled":  true,
        "valueConfigurable":  true,
        "enablingConfigurable":  true,
        "minimumValue":  1,
        "maximumValue":  32,
        "ruleCategory": "EAGER"
    },
    {
        "name":  "minimumUpperCase",
        "value":  1,
        "enabled":  true,
        "valueConfigurable":  true,
        "enablingConfigurable":  true,
        "minimumValue":  1,
        "maximumValue":  32,
        "ruleCategory": "EAGER"
    },
    {
        "name":  "minimumDigits",
        "value":  1,
        "enabled":  true,
        "valueConfigurable":  true,
        "enablingConfigurable":  true,
        "minimumValue":  1,
        "maximumValue":  32,
        "ruleCategory": "EAGER"
    },
    {
        "name":  "minimumSpecialChars",
        "value":  1,
        "enabled":  true,
        "valueConfigurable":  true,
        "enablingConfigurable":  true,
        "minimumValue":  1,
        "maximumValue":  32,
        "ruleCategory": "EAGER"
    },
    {
        "name":  "maximumRepeatingChars",
        "value":  4,
        "enabled":  true,
        "valueConfigurable":  true,
        "enablingConfigurable":  true,
        "minimumValue":  1,
        "maximumValue":  32,
        "ruleCategory": "EAGER"
    },
    {
        "name":  "maximumConsecutiveChars",
        "value":  4,
        "enabled":  true,
        "valueConfigurable":  true,
        "enablingConfigurable":  true,
        "minimumValue":  1,
        "maximumValue":  32,
        "ruleCategory": "EAGER"
    },
    {
        "name":  "mustNotContainUserId",
        "value":  0,
        "enabled":  true,
        "valueConfigurable":  false,
        "enablingConfigurable":  true,
        "minimumValue":  0,
        "maximumValue":  0,
        "ruleCategory": "EAGER"
    },
    {
        "name":  "mustNotContainDictionaryWords",
        "value":  0,
        "enabled":  true,
        "valueConfigurable":  false,
        "enablingConfigurable":  true,
```

```
        "minimumValue":  0,
        "maximumValue":  0,
        "ruleCategory": "EAGER"
    },
    {
        "name":  "mustNotBeOldPassword",
        "value":  3,
        "enabled":  true,
        "valueConfigurable":  true,
        "enablingConfigurable":  true,
        "minimumValue":  1,
        "maximumValue":  12,
        "ruleCategory": "LAZY"
    }
]
```

Example 7

```
curl --cacert certificate.pem --cookie cookie.txt -X PUT -H "Content-Type: Appli →
cation/json" -d '[{"name":"minimumLength","value":8},{"name":"minimumLowerCase", →
"value":1,"enabled":true},{"name":"minimumUpperCase","value":1,"enabled":true}," →
name":"minimumDigits","value":1,"enabled":true},{"name":"minimumSpecialChars","v →
alue":1,"enabled":false},{"name":"maximumRepeatingChars","value":4,"enabled":fal →
se},{"name":"maximumConsecutiveChars","value":4,"enabled":false},{"name":"mustNo →
tContainUserId","enabled":false},{"name":"mustNotContainDictionaryWords","enable →
d":false,{"mustNotBeOldPassword","enabled":true,"value":3}]' "https://<hostname> →
/oss/idm/config/passwordsettings/enmuser/passwordcomplexity"
```

Result

```
list of password[{"name":"maximumLength","value":32,"enabled":true,"valueConfigu →
rable":false,"enablingConfigurable":false,"minimumValue":0,"maximumValue":32,"ru →
leCategory":"EAGER"},
{"name":"minimumLength","value":8,"enabled":true,"valueConfigurable":true,"enabl →
ingConfigurable":false,"minimumValue":8,"maximumValue":32,"ruleCategory":"EAGER" →
},{"name":"minimumLowerCase",
"value":1,"enabled":true,"valueConfigurable":true,"enablingConfigurable":true,"m →
inimumValue":1,"maximumValue":32,"ruleCategory":"EAGER"},{"name":"minimumUpperCa →
se","value":1,"enabled":true,
"valueConfigurable":true,"enablingConfigurable":true,"minimumValue":1,"maximumVa →
lue":32,"ruleCategory":"EAGER"},{"name":"minimumDigits","value":1,"enabled":true →
,"valueConfigurable":true,
"enablingConfigurable":true,"minimumValue":1,"maximumValue":32,"ruleCategory":"E →
AGER"},{"name":"minimumSpecialChars","value":1,"enabled":false,"valueConfigurabl →
e":true,"enablingConfigurable":true,
"minimumValue":1,"maximumValue":32,"ruleCategory":"EAGER"},{"name":"maximumRepea →
tingChars","value":4,"enabled":false,"valueConfigurable":true,"enablingConfigura →
ble":true,"minimumValue":1,
"maximumValue":32,"ruleCategory":"EAGER"},{"name":"maximumConsecutiveChars","val →
ue":4,"enabled":false,"valueConfigurable":true,"enablingConfigurable":true,"mini →
mumValue":1,"maximumValue":32,"ruleCategory":"EAGER"},
{"name":"mustNotContainUserId","value":0,"enabled":false,"valueConfigurable":fal →
se,"enablingConfigurable":true,"minimumValue":0,"maximumValue":0,"ruleCategory": →
"EAGER"},{"name":"mustNotContainDictionaryWords","value":0,"enabled":false,"valu →
eConfigurable":false,"enablingConfigurable":true,"minimumValue":0,"maximumValue" →
:0,"ruleCategory":"EAGER"},
{"name":"mustNotBeOldPassword","value":3,"enabled":true,"valueConfigurable":true →
,"enablingConfigurable":true,"minimumValue":1,"maximumValue":12,"ruleCategory":" →
LAZY"}]
```

4.6 Update Password Aging

This REST endpoint updates password aging settings.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Update Password Ageing	PUT	/oss/idm/config/passwordsettings/{id}/passwordageing

JSON Query

```
{
    "enabled":true,
    "pwdMaxAge":60,
    "pwdExpireWarning":5,
    "graceLoginCount":0}
```

Available Fields

— id [mandatory] - password settings identifier

— enabled [mandatory] - indicates if password aging is enabled.

  Set it to false to disable password aging.

— pwdMaxAge [optional] - the value of maximum period the password is valid, specified in days. Mandatory when enabled is true, irrelevant when enabled is false.

— pwdExpireWarning [optional] - the value of period to display information about the upcoming password expiration time, specified in days. Mandatory when enabled is true, irrelevant when enabled is false.

— graceLoginCount [optional] - the value of logon attempt to allow the user to choose a new password.

  It is not configurable, must be set to 0 when enabled is true, irrelevant when enabled is false.

HTTP Response Code: 200

```
{
    "enabled":true,
    "pwdMaxAge":60,
    "pwdExpireWarning":5,
```

```
    "graceLoginCount":0
}
```

Example 8

```
curl --cacert certificate.pem --cookie cookie.txt -X PUT -H "Content-Type: Appli
cation/json" -d '{"enabled":true,"pwdMaxAge":100,"pwdExpireWarning":8,"graceLogi
nCount":0}' "https://<hostname>/oss/idm/config/passwordsettings/enmuser/password
ageing"
```

Result

```
{"enabled":true,"pwdMaxAge":100,"pwdExpireWarning":8,"graceLoginCount":0}
```

4.7 Update Account Lockout

> This REST endpoint updates account lockout settings.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Update Account Lockout	PUT	/oss/idm/config/passwordsettings/{id}/accountlockout

JSON Query

```
{
    "enabled":"true",
    "loginMaxFailedAttempts":5,
    "loginLockoutExpiration":true,
    "loginLockoutExpirationTime":10,
    "loginFailureExpiration":true,
    "loginFailureExpirationTime": 10
}
```

Available Fields

— id [mandatory] - password settings identifier

— enabled [mandatory] - indicates if account must be locked because of too many logon failures.

— loginMaxFailedAttempts [mandatory if enabled is true] - indicates number of logon failures, after which account is locked. Mandatory when enabled is true, irrelevant when enabled is false.

— loginLockoutExpiration [mandatory if enabled is true] - indicates if account lockout expires after a period of time.

  Mandatory when enabled is true, irrelevant when enabled is false.

— loginLockoutExpirationTime [mandatory when loginLockoutExpiration is true] - indicates number of minutes after which account is unlocked again. Mandatory when loginLockoutExpiration is true, irrelevant when enabled or loginLockoutExpiration is false.

— loginFailureExpiration [mandatory when enabled is true] - indicates if logon failures expire after a period of time.

  Mandatory when enabled is true, irrelevant when enabled is false.

— loginFailureExpirationTime [mandatory when loginFailureExpiration is true] - indicates number of minutes after which failure logon expires. Mandatory when loginFailureExpiration is true, irrelevant when enabled or loginFailureExpiration is false.

HTTP Response Code: 200

```
{
    "enabled":true,
    "loginMaxFailedAttempts":3,
    "loginLockoutExpiration":true,
    "loginLockoutExpirationTime":3,
    "loginFailureExpiration":true,
    "loginFailureExpirationTime": 5
}
```

Example 9

```
curl --cacert certificate.pem --cookie cookie.txt -X PUT -H "Content-Type: Appli →
cation/json" -d '{"enabled":true,"loginLockoutExpiration":true,"loginFailureExpi →
ration":true,"loginMaxFailedAttempts":5,"loginLockoutExpirationTime":10,"loginFa →
ilureExpirationTime":10}' "https://<hostname>/oss/idm/config/passwordsettings/en →
muser/accountlockout"
```

Result

```
{"enabled":true,"loginLockoutExpiration":true,"loginFailureExpiration":true,"log →
inMaxFailedAttempts":5,"loginLockoutExpirationTime":10,"loginFailureExpirationTi →
me":10}
```

Account Unlock

An account can be unlocked by Security Admin by changing user password.

4.8 Password Complexity Rules

> The REST endpoints for receiving password complexity rules always return list of all rules.

Every rule contains all parameters.

Parameters	Description of Password Complexity Rule
`name`	String - name of password complexity rule.
`value`	Integer - current value of password complexity rule.
`enabled`	Boolean - indicates if password complexity rule is enabled in the system.
`valueConfigurable`	Boolean - indicates if value of password complexity rule can be changed.
`enablingConfigurable`	Boolean - indicates if password complexity rule can be changed to enabled or disabled.
`minimumValue`	Integer - minimum allowable value for password complexity rule. If parameter valueConfigurable is false, this parameter is insignificant.
`maximumValue`	Integer - maximum allowable value for password complexity rule. If parameter valueConfigurable is false, this parameter is insignificant.

In updating configuration, password complexity rules list can contain only rules which must be changed. The password complexity rules not specified in the list remain unchanged. Password complexity rules list must contain at least one rule.

In case of updating configuration, the number of parameters is limited. Every password complexity rule must contain the name of the rule. Rules which have configurable value must also contain value parameter and rules which have configurable enabling must contain enabled parameter.

Password Complexity Rule Description	Name	enablingConfigurable	valueConfigurable	Allowable Values Range	Default	Configuring Example
New password must not contain the Username, Name, Surname with which they are associated.	mustNotContainUserId	true	false	-	Disabled	`{ "name": "mustNotContainUserId", "enabled": false }`
Password must not contain any dictionary words.	mustNotContainDictionaryWords	true	false	-	Disabled	`{ "name": "mustNotContainDictionaryWords", "enabled": false }`
Enforce minimum password length.	minimumLength	false	true	8–32	Enabled, value 8	`{ "name": "minimum`

Password Complexity Rule Description	Name	enablingConfigurable	valueConfigurable	Allowable Values Range	Default	Configuring Example
						Length", "value": 10 }
Enforce maximum password length.	maximumLength	false	false	-	Enabled, value 32	Not configurable
Password must contain lowercase letters.	minimumLowerCase	true	true	1–32	Enabled, value 1	{ "name": "minimumLowerCase" "enabled": true, "value": 3 }
Password must contain uppercase letters.	minimumUpperCase	true	true	1–32	Enabled, value 1	{ "name": "minimumUpperCase" "enabled": true, "value": 3 }
Password must contain digits.	minimumDigits	true	true	1–32	Enabled, value 1	{ "name": "minimumDigits" "enabled": true, "value": 3 }
Password must contain special characters.	minimumSpecialChars	true	true	1–32	Disabled	{ "name": "minimumSpecialChars" "enabled": true, "value": 3 }
Restrict the number of repeating characters.	maximumRepeatingChars	true	true	1–32	Disabled	{ "name": "maximumRepeatingChars" "enabled": true, "value": 3 }
Restrict the number of consecutive repeating characters.	maximumConsecutiveChars	true	true	1–32	Disabled	{ "name": "" "enabled": true, "value": 3 }

Password Complexity Rule Description	Name	enablingConfigurable	valueConfigurable	Allowable Values Range	Default	Configuring Example
New password must be different to previous ones with a 'window' with a width equal to the configured value. For example, if the value is equal 3, the new password must be different to the 3 previous ones already used.	mustNotBeOldPassword	true	true	1–12	Disabled, value=1	`{ "name": "mustNotBeOldPassword" "enabled": true, "value": 3 }`

4.9 Get Password Complexity Settings

> This REST endpoint retrieves password complexity settings.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
GET Password Complexity Settings	`GET`	`/oss/idm/config/passwordsettings/{id}/passwordcomplexity`

Available Field

— id [mandatory] - password settings identifier

HTTP Response Code: 200

Example 10

```
[ { "name":"maximumLength", "value":32, "enabled":true,
"valueConfigurable":false, "enablingConfigurable":false,
"minimumValue":0, "maximumValue":32, "ruleCategory":"EAGER" },
{ "name":"minimumLength", "value":8, "enabled":true,
"valueConfigurable":true, "enablingConfigurable":false,
"minimumValue":8, "maximumValue":32, "ruleCategory":"EAGER" },
{ "name":"minimumLowerCase", "value":1, "enabled":true,
"valueConfigurable":true, "enablingConfigurable":true,
"minimumValue":1, "maximumValue":32, "ruleCategory":"EAGER" },
{ "name":"minimumUpperCase", "value":1, "enabled":true,
```

"valueConfigurable":true, "enablingConfigurable":true,
"minimumValue":1, "maximumValue":32, "ruleCategory":"EAGER" },
{ "name":"minimumDigits", "value":1, "enabled":true,
"valueConfigurable":true, "enablingConfigurable":true,
"minimumValue":1, "maximumValue":32, "ruleCategory":"EAGER" },
{ "name":"minimumSpecialsChars", "value":1, "enabled":false,
"valueConfigurable":true, "enablingConfigurable":true,
"minimumValue":1, "maximumValue":32, "ruleCategory":"EAGER" },
{ "name":"maximumRepeatingChars", "value":4, "enabled":false,
"valueConfigurable":true, "enablingConfigurable":true,
"minimumValue":1, "maximumValue":32, "ruleCategory":"EAGER" },
{ "name":"maximumConsecutiveChars", "value":4, "enabled":false,
"valueConfigurable":true, "enablingConfigurable":true,
"minimumValue":1, "maximumValue":32, "ruleCategory":"EAGER" },
{ "name":"mustNotContainUserId", "value":0, "enabled":false,
"valueConfigurable":false, "enablingConfigurable":true,
"minimumValue":0, "maximumValue":0, "ruleCategory":"EAGER" },
{ "name":"mustNotContainDictionaryWords", "value":0,
"enabled":false, "valueConfigurable":false,
"enablingConfigurable":true, "minimumValue":0, "maximumValue":0,
"ruleCategory":"EAGER" }, { "name":"mustNotBeOldPassword",
"value"1, "enabled":false, "valueConfigurable":true,
"enablingConfigurable":true, "minimumValue":1, "maximumValue":12,
"ruleCategory":"LAZY"]

```
curl --cacert certificate.pem --cookie cookie.txt "https://<hostname>/oss/idm/co →
nfig/passwordsettings/enmuser/passwordcomplexity"
```

Result:

[[{"name":"maximumLength","value":32,"enabled":true,"valueConfigu
rable":false,"enablingConfigurable":false,"minimumValue":0,"maxim
umValue":32,"ruleCategory":"EAGER"},
{"name":"minimumLength","value":8,"enabled":true,"valueConfigurab
le":true,"enablingConfigurable":false,"minimumValue":8,"maximumVa
lue":32,"ruleCategory":"EAGER"},
{"name":"minimumLowerCase","value":1,"enabled":true,"valueConfigu
rable":true,"enablingConfigurable":true,"minimumValue":1,"maximum
Value":32,"ruleCategory":"EAGER"},
{"name":"minimumUpperCase","value":1,"enabled":true,"valueConfigu
rable":true,"enablingConfigurable":true,"minimumValue":1,"maximum
Value":32,"ruleCategory":"EAGER"},
{"name":"minimumDigits","value":1,"enabled":true,"valueConfigurab
le":true,"enablingConfigurable":true,"minimumValue":1,"maximumVal
ue":32,"ruleCategory":"EAGER"},{"name":"minimumSpecialChars",
"value":1,"enabled":false,"valueConfigurable":true,"enablingConfi
gurable":true,"minimumValue":1,"maximumValue":32,"ruleCategory":"
EAGER"},{"name":"maximumRepeatingChars","value":4,
"enabled":false,"valueConfigurable":true,"enablingConfigurable":t
rue,"minimumValue":1,"maximumValue":32,"ruleCategory":"EAGER"},

{"name":"maximumConsecutiveChars","value":4,"enabled":false,
"valueConfigurable":true,"enablingConfigurable":true,"minimumValu
e":1,"maximumValue":32,"ruleCategory":"EAGER"},
{"name":"mustNotContainUserId","value":0,
"enabled":false,"valueConfigurable":false,"enablingConfigurable":
true,"minimumValue":0,"maximumValue":0,"ruleCategory":"EAGER"},
{"name":"mustNotContainDictionaryWords","value":0,
"enabled":false,"valueConfigurable":false,"enablingConfigurable":
true,"minimumValue":0,"maximumValue":0,"ruleCategory":"EAGER"},
{"name":"mustNotBeOldPassword","value":1,"enabled":false,
"valueConfigurable":true,"enablingConfigurable":true,"minimumValu
e":1,"maximumValue":12,"ruleCategory":"LAZY"}]

5 System Security Session Settings

This section outlines REST request for the System Administrator to manage session settings.

The table describes the parameters for the session management:

Parameters	Description
`timestamp`	String - contains the time of last modification of session settings. This field is used to prevent overwriting configuration without checking actual values.
`session_timeout`	String - contains the value of maximum session duration, specified in minutes.
`idle_session_timeout`	String - contains the value of session idle time, specified in minutes.

Note: If `idle_session_timeout` value is less than the `session_timeout` value and the user inactivity time reaches the `idle_session_timeout` value, the current ENM user session is automatically closed, overriding the `session_timeout` value. A new authentication session is needed to log in.

For example, if `session_timeout` value is set to 10 hours and `idle_session_timeout` value is set to two hours, and the user inactivity time reaches two hours, the ENM user session is automatically closed though eight hours have to pass before the `session_timeout` value is reached. The user must open a new session authentication to log in and the `session_timeout` time becomes 10 hours again.

5.1 Get Session Settings

This REST endpoint retrieves session settings.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Get Session Settings	GET	/oss/sso/utilities/config

HTTP Response Code: 200

```
{
    "timestamp": "1470020129662",
    "idle_session_timeout": "60",
    "session_timeout": "600"
}
```

Example 11

```
curl --cacert certificate.pem --cookie cookie.txt "https://<hostname>/oss/sso/ut
ilities/config"
```

Result

```
{"timestamp":"1479370848860","idle_session_timeout":"60","session_timeout":"120"
}
```

5.2 Update Session Settings

> This REST endpoint updates session settings.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Update Session Settings	PUT	/oss/sso/utilities/config

JSON Query

```
{
    "timestamp": "1470020129662",
    "idle_session_timeout": "70",
    "session_timeout": "700"
}
```

Available Fields

— timestamp [mandatory] - proper value is read with Get Session Settings interface

— session_timeout [mandatory]

— idle_session_timeout [mandatory]

HTTP Response Code: 200

```
{
    "timestamp": "1470045874541",
    "idle_session_timeout": "70",
    "session_timeout": "700"
}
```

Example 12

```
curl --cacert certificate.pem --cookie cookie.txt -X PUT -H "Content-Type: Appli →
cation/json" -d '{"timestamp":"1479370848860","idle_session_timeout":"70","sessi →
on_timeout":"150"}' "https://<hostname>/oss/sso/utilities/config"
```

Result:

```
{"timestamp":"1481211741312","idle_session_timeout":"70","session_timeout":"150" →
}
```

6 User Profile Settings Interface

> This interface allows Security Administrators to configure user profile settings through REST API.

The table describes the parameters for the user profile settings management:

Parameter	Description
`allowDataModification`	List of configuration properties responsible for allowing or denying user to modify specific user attribute.
`name`	String - name of users attribute. Supported values: personals, email.
`enabled`	Boolean - indicates if user is allowed to modify users attribute.

6.1 Get User Profile Settings

> This REST endpoint retrieves user profile settings.

Required Security Role

None

REST Endpoint

Description	Method	Path
Get User Profile Settings	`GET`	`/oss/idm/config/usersettings`

HTTP Response Code: 200

```
{
    "allowDataModification":[
        {
            "name":"personals",
            "enabled":false
        },
        {
            "name":"email",
            "enabled":true
        }
    ]
}
```

6.2 Enable and Disable User to Modify Own Personals or Email

> This REST endpoint updates user profile setting to allow or deny user to modify own personals or email.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Update User Profile Settings	PUT	/oss/idm/config/userprofilesettings

JSON Query

```
{"allowDataModification":[{"name":"personals", "enabled":false}, {"name":"email"
, "enabled":false}]}
```

Available Fields

— allowDataModification [mandatory] - list must contain at least one configuration parameter

— name [mandatory]

— enabled [mandatory]

HTTP Response Code: 200

```
{
    "allowDataModification":[
        {
            "name":"personals",
            "enabled":false
        },
        {
            "name":"email",
            "enabled":false
        }
    ]
}
```

7 External Identity Provider Settings and Monitoring Interface

For External Identity Provider two different use cases are provided:

— Configuration implementing read and update configuration purpose.

  Configuration interface gets or updates External Identity Provider configuration.

— Communication against External Identity Provider.

  Monitoring interface checks External Identity Provider connectivity at IP/TCP port level and External Identity Provider authentication providing BindDN, BindPassword, and ldapConnectionMode information.

  In case ldapConnectionMode=LDAPS, the secure connection is implemented with 'trustAll' setting.

Both these RESTs are allowed for Security Administrators.

External Identity Provider Configuration and Monitoring interfaces are designed to work both in IPv4 and IPv6 scenario.

Source IP addresses used by ENM applications to establish TCP connection to External Identity Provider can be found in the section *Connectivity to External Identity Provider* of ENM Network Integration Guideline, Reference [3].

7.1 External Identity Provider Configuration Interface

> This interface is provided to explore and configure External Identity Provider settings through REST API.

Two different RESTs are provided:

— GET REST to read configuration. This REST always provides the entire External Identity Provider configuration. No Body is required.

— PUT REST to update configuration. This REST can accept one, several, or all parameters to be configured in the External Identity Provider configuration. The Response body contains JSON with the following JSON objects:

  — isBindPasswordEmpty: reports if the BindPassword is empty or contains a value. This attribute has been introduced not to show the password as clear text but only to provide information that password has been set.

  — extIdpSettings: contains the External Identity Provider configuration as per the parameters reported in the table.

These RESTs share the parameters described in the following table:

Table 1

Parameter	Values	Description	REST
authType	LOCAL/REMOTEAUTHN	Authentication and authorization type supported by current ENM installation. LOCAL means that both authentication and authorization are made locally. REMOTEAUTHN means that authorization is made locally while authentication can be done by External IdP server, depending on the authMode attribute set per user basis on User Management application.	GET/PUT
primaryServerAddress	For IPv4: < IP server_address>:<port> For IPv6: [<IP server_address>]:<port>	IP address and port of primary External IdP server. In PUT REST, validation rule for IPv4 and IPv6 is present.	GET/PUT
secondaryServerAddress	For IPv4: < IP server_address>:<port> For IPv6: [<IP server_address>]:<port>	IP address and port of secondary External IdP server. In PUT REST, validation rule for IPv4 and IPv6 is present.	GET/PUT
ldapConnectionMode	LDAP/LDAPS	It is the LDAP connection mode type that can be secure (LDAPS) or unsecure (LDAP). This configuration is independent to <port> configuration in primaryServerAddress and secondaryServerAddress.	GET/PUT
bindDN	<Proxy_Account_DN>	It is the proxy account Distinguish Name. Empty value causes LDAP anonymous bind.	GET/PUT
bindPassword	<bindPassword>	It is the proxy account password. Empty value causes LDAP anonymous bind. In GET REST and PUT response, this field always provides an empty value. To check if a password has been set, refer to 'isBindPasswordEmpty'.	GET/PUT
RemoteAuthProfile	NOSEARCH/STANDARD	STANDARD for External IdP with search/bind operation. NOSEARCH for External IdP with only bind operation.	GET/PUT
baseDN	<attribute>=<value>{[,<attribute>=<value>]}	It is the distinguish name of the LDAP node root of the sub-tree spanned by search operations.	GET/PUT
userBindDNFormat	<attribute>=<value>{[,<attribute>=<value>]}	For External IdP with search/bind operation (remoteAuthProfile=STANDARD), it is the relative distinguish name format of the users to be authenticated. For External IdP with only bind operation (remoteAuthProfile=NOSEARCH), it is the full distinguish name of the users to be authenticated.	GET/PUT
searchFilter		Refer to RFC 4511, chapter 4.5.1.	GET

Parameter	Values	Description	REST
searchScope	SUBTREE (default)	Refer to RFC 4511, chapter 4.5.1.	GET
searchAttribute		Refer to RFC 4511, chapter 4.5.1.	GET
searchControls		Refer to RFC 4511, chapter 4.5.1.	GET
isBindPasswordEmpty	true/false	It reports if the BindPassword is already configured or not.	GET

7.1.1 Get External Identity Provider Settings

> This REST endpoint retrieves External Identity Provider settings.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Get External Identity Provider Settings	`GET`	`/oss/idm/config/extidp/settings`

HTTP Response Code: 200

HTTP Response Body:

```
{"isBindPasswordEmpty":true,
"extIdpSettings":{
       "authType":"REMOTEAUTHN",
       "remoteAuthProfile":"NOSEARCH",
       "baseDN":"dc=acme,dc=com",
       "primaryServerAddress":"10.20.30.40:1000",
       "secondaryServerAddress":"[2001:1b70:82a1:149:0:2337:5413:60]:1001",
       "ldapConnectionMode":"LDAP",
       "userBindDNFormat":"uid=$user,ou=pdu nam,dc=acme,dc=com",
       "searchFilter":"",
       "searchScope":"SUBTREE",
       "searchAttribute":"",
       "searchControls":"",
       "bindDN":"",
       "bindPassword":""
       }
}
```

Example 13

```
curl --cacert certificate.pem --cookie cookie.txt "https://<hostname>/oss/idm/co →
nfig/extidp/settings"
```

Result


```
{"isBindPasswordEmpty":true,"extIdpSettings":{"authType":"REMOTEAUTHN","remoteAu →
thProfile":"NOSEARCH","baseDN":"dc=acme,dc=com","primaryServerAddress":"10.20.30 →
.40:1000","secondaryServerAddress":"10.20.30.40:1001","ldapConnectionMode":"LDAP →
","userBindDNFormat":"uid=$user,ou=pdu nam,dc=acme,dc=com","searchFilter":"","se →
archScope":"SUBTREE","searchAttribute":"","searchControls":"","bindDN":"","bindP →
assword":""}}
```


7.1.2 Update External Identity Provider Settings

> This REST endpoint updates the External Identity Provider settings.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Get External Identity Provider Settings	PUT	/oss/idm/config/extidp/settings

JSON Query

```
{
   "authType":"REMOTEAUTHN",
   "remoteAuthProfile":"NOSEARCH",
   "baseDN":"dc=acme,dc=com",
   "primaryServerAddress":"10.20.30.40:1000",
   "secondaryServerAddress":"[2001:1b70:82a1:149:0:2337:5413:60]:1000",
   "ldapConnectionMode":"LDAP",
   "userBindDNFormat":"uid=$user,ou=pdu nam,dc=acme,dc=com",
   "bindDN":"",
   "bindPassword":""
}
```

Available Fields

— authType - indicates authentication and authorization type supported by current ENM installation.

— remoteAuthProfile [this is meaningful when “authType” is REMOTEAUTHN] - indicates remote authentication profile.

— baseDN [this is meaningful when “remoteAuthProfile” is STANDARD] - indicates the distinguish name of the LDAP node root of the subtree spanned by search operations.

— primaryServerAddress [this is meaningful when “authType” is REMOTEAUTHN] - indicates IP address and port of primary External LDAP server.

— secondaryServerAddress [this is optional and meaningful when "authType" is REMOTEAUTHN] - indicates IP address and port of secondary External LDAP server.

— ldapConnectionMode [this is meaningful when “authType” is REMOTEAUTHN] - indicates LDAP connection mode allowed by External LDAP server.

— userBindDNFormat - indicates the Distinguish Name format of the user to bind.

  — In case of “remoteAuthProfile=NOSEARCH”, it must contain the full user Distinguish Name, for instance, assuming the User DN on external IdP is defined as `uid=<userid>,ou=pdu nam,dc=acme,dc=com`, it must be configured as:

    ```
    userBindDNFormat: uid=$user,ou=pdu nam,dc=acme,dc=com
    ```

  — In case of “remoteAuthProfile=STANDARD”, it must contain attribute to be used to retrieve the User DN with LDAP Search, required to perform User Bind, so assuming the User DN on external IdP is defined as `uid=<userid>,ou=pdu nam,dc=acme,dc=com`, it must be configured as:

    ```
    userBindDNFormat: uid=$user
    ```

  Note: In case external IdP is provided by Microsoft Active Directory, depending on how the Users have been defined, it can require to use the sAMAccountName: In that case the suggested setting of userBindDNFormat is:

    ```
    userBindDNFormat: sAMAccountName=$user
    ```

— bindDN [mandatory when “remoteAuthProfile” is STANDARD] - distinguish name of the root of the subtree to span in search operation.

— bindPassword [mandatory when “remoteAuthProfile” is STANDARD] - indicates bind user password.

HTTP Response Code: 200

HTTP Response Body:


```
{"isBindPasswordEmpty":true,
 "extIdpSettings":{
   "authType":"REMOTEAUTHN",
   "remoteAuthProfile":"NOSEARCH",
   "baseDN":"dc=acme,dc=com",
   "primaryServerAddress":"10.20.30.40:1000",
   "secondaryServerAddress":"[2001:1b70:82a1:149:0:2337:5413:60]:1000",
   "ldapConnectionMode":"LDAP",
   "userBindDNFormat":"uid=$user,ou=pdu nam,dc=acme,dc=com",
   "searchFilter":"",
   "searchScope":"SUBTREE",
   "searchAttribute":"",
   "searchControls":"",
   "bindDN":"",
```

```
    "bindPassword":""
  }
}
```

Note:

- Parameters can be updated all at the same time (using one single REST containing all the parameters) or individually (using a REST for the single parameter to be updated).
- PUT REST API supports the following attributes: searchFilter, searchScope, searchAttribute, searchControls. Never change their default value.
- bindPassword in HTTP response always provides an empty value, for security purpose. If this password has been previously configured, the *<isBindPasswordEmpty>* reports value `false`, `true` otherwise.
- isBindPasswordEmpty in HTTP response indicates if bindPassword contains a not-null value.

Example 14

```
curl --cacert certificate.pem --request PUT  --cookie cookie.txt "https://<hostn →
ame>/oss/idm/config/extidp/settings" -H "Content-Type: application/json" -d '{"r →
emoteAuthProfile":"NOSEARCH", "authType":"REMOTEAUTHN", "primaryServerAddress":" →
10.20.30.40:1000", "secondaryServerAddress":"10.20.30.40:1001", "baseDN":"dc=acm →
e,dc=com", "ldapConnectionMode":"LDAP", "userBindDNFormat":"uid=$user,ou=pdu nam →
,dc=acme,dc=com"}'
```

Result

```
{"isBindPasswordEmpty":true,"extIdpSettings":{"authType":"REMOTEAUTHN","remoteAu →
thProfile":"NOSEARCH","baseDN":"dc=acme,dc=com","primaryServerAddress":"10.20.30 →
.40:1000","secondaryServerAddress":"10.20.30.40:1001","ldapConnectionMode":"LDAP →
","userBindDNFormat":"uid=$user,ou=pdu nam,dc=acme,dc=com","searchFilter":"","se →
archScope":"SUBTREE","searchAttribute":"","searchControls":"","bindDN":"","bindP →
assword":""}}
```

7.2 Check Communication against External Identity Provider

> These RESTs check External Identity Provider connectivity and authentication status.

Two endpoints are exported supporting the following tests:

- Check connectivity to External Identity Provider server at IP/TCP level providing IP address and TCP port.
- Check authentication against External Identity Provider server at "Bind user" level providing *<BindDN>* and *<BindPassword>* information. In case of *<BindDN>* and *<BindPassword>* are not provided in the REST, those values

are obtained from External Identity Provider settings. This test supports LDAP and LDAPS protocols (LDAPS does not validate server certificate and accept any server certificate).

7.2.1 Connectivity External Identity Provider Status

> This REST endpoint checks External Identity Provider connectivity with the server.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
External Identity Provider Connectivity Status	POST	/oss/idm/config/extidp/settings/test/connectivity

JSON Query

```
{
   "serverAddress":"<extidp_IPADDR>:<extidp_PORT>"
}
```

Available Fields

— serverAddress - For IPv4: <IP server_address>:<port>, for IPv6: [<IP server_address>]:<port>. IP address, and port of External IdP server. A validation rule for both IPv4 and IPv6 is present.

HTTP Response Code: 200

HTTP Response Body:

```
{
   "successfulTest": true,
   "failureReason": ""
}
```

Example 15

This command can be used to test External Identity Provider at IP/TCP transport level:

```
curl --cacert certificate.pem --request POST  --cookie cookie.txt "https://<host
name>/oss/idm/config/extidp/settings/test/connectivity" -H "Content-Type: applic
ation/json" -d '{"serverAddress":"141.137.87.54:7389"}'
```

Result

```
{" successfulTest":true,"failureReason":""}
```

7.2.2 Check External Identity Provider Authentication

> This REST endpoint checks authentication against External Identity Provider at Bind user level.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
External Identity Provider Authentication	POST	/oss/idm/config/extidp/settings/test/authentication

JSON Query

```
{
   "serverAddress":"141.137.87.54:7636",
   "bindDN":"cn=Directory Manager",
   "bindPassword":"ericsson"
}
```

Available Fields

— serverAddress - for IPv4: <IP server_address>:<port>, for IPv6: [<IP server_address>]:<port>. IP address and port of External IdP server. A validation rule for IPv4 is present.

— bindDN - <Proxy_Account_DN>. It is the proxy account Distinguish Name.

— bindPassword - <bindPassword>. It is the proxy account password.

HTTP Response Code: 200

HTTP Response Body:

```
{
   "successfulTest": true,
   "failureReason": ""
}
```

Example 16

```
curl --cacert certificate.pem --request POST  --cookie cookie.txt "https://<host name>/oss/idm/config/extidp/settings/test/authentication" -H "Content-Type: application/json" -d '{"serverAddress":"141.137.87.54:7636","bindDN":"cn=Directory Manager","bindPassword":"ericsson"}'
```

Result

```
{"successfulTest": true,"failureReason": ""}
```

7.3 Troubleshooting Cases

This section shows some examples of correct and error messages.

7.3.1 Configuration

Table 2

Use Case	Example Command	HTTP Response Code	Example Response	Notes or Probable Root Cause
Read "External IdP Settings"	`curl --cacert certificate.pem --request GET -s -i --cookie file.txt https://<host name>/oss/idm/config/extidp/settings`	HTTP/1.1 200 OK	`{"isBindPasswordEmpty":false,"extIdpSettings": {"authType":"LOCAL", "remoteAuthProfile": "STANDARD","baseDN": "dc=acme,dc=com","primaryServerAddress": "141.137.87.54:7389",secondaryServerAddress":"[fe80:aabb:ccdd:eeff::0001]:2001",ldapConnectionMode":"LDAPS","userBindDNFormat":"uid=$user,ou=pdunam,dc=acme,dc=com", "searchFilter":"","searchScope":"SUBTREE","searchAttribute":"","searchControls":"","bindDN":"cn=extldapadmin,ou=people,dc=acme,dc=com","bindPassword":""}}`	
	`curl --cacert certificate.pem --request GET -s -i --cookie file_wrong.txt https://<host name>/oss/idm/config/extidp/settings`	HTTP/1.1 302 Found		Session associated to provided cookie file is not valid or expirated.

Use Case	Example Command	HTTP Response Code	Example Response	Notes or Probable Root Cause
	`curl --cacert certificate.pem --request GET -s -i --cookie file.txt https://<host name>/oss/idm/config/extidp/settings`	HTTP/1.1 403 Forbidden	{"userMessage":"The User does not have permissions to perform this action.","httpStatusCode":403,"internalErrorCode":"SSC-3-read","developerMessage":"com.ericsson.oss.itpf.sdk.security.accesscontrol.SecurityViolationException: access control decision: denied to invoke: read on resource: ext_idp_settings","time":"2018-12-10T14:24:11","links":[],"errorData":null}	User has not privileges to access the resource.
Update "External IdP Settings"	`curl --cacert certificate.pem --request PUT -s -i --cookie file.txt https://<host name>/oss/idm/config/extidp/settings -H "Content-Type: application/json" -d '{"remoteAuthProfile":"FOO","bindDN":"BAR"}'`	HTTP/1.1 412 Precondition Failed	{"constraintViolations":[{"method":"public javax.ws.rs.core.Response com.ericsson.oss.services.security.genericidentityconfigservice.rest.extidpconfiguration.ExtIdpConfigurationRest.updateExtIdpSettings(com.ericsson.oss.services.security.genericidentityconfigservice.extidpsettings.model.ExtIdpSettings)","parameterName":"arg0","kind":"PARAMETER","propertyPath":"ExtIdpConfigurationRest#updateExtIdpSettings(arg0).bindDN","invalidValue":"BAR","message":"must match \"^[^,]+=[^,]+(,[^,]+=[^,]+)*$|^$\""}, {"method":"public javax.ws.rs.core.Response com.ericsson.oss.services.security.genericidentityconfigservice.rest.extidpconfiguration.ExtIdpConfigurationRest.updateExtIdpSettings(com.ericsson.oss.services.security.genericidentityconfigservice.extidpsettings.model.ExtIdpSettings)","parameterName":"arg0","kind":"PARAMETER","propertyPath":"ExtIdpConfigurationRest#updateExtIdpSettings(arg0).remoteAuthProfile","invalidValue":"FOO","message":"Enum value is not valid"}]}	
	`curl --cacert certificate.pem --request PUT -s -i --cookie file.txt https://<hostname>/oss/idm/config/extidp/settings -H "Content-Type: application/json" -d '{"`	HTTP/1.1 200 OK	":false,"extIdpSettings":{"authType":"REMOTEAUTHN","remoteAuthProfile":"NOSEARCH","baseDN":"dc=acme,dc=com","primaryServerAddress":"141.137.87.54:7389","secondaryServerAddress":"[fe80:aabb:ccdd:eeff::0001]:	

Use Case	Example Command	HTTP Response Code	Example Response	Notes or Probable Root Cause
	`remoteAuthProfile":"NOSEARCH","authType":"REMOTEAUTHN"}'`		2001","ldapConnectionMode":"LDAPS","userBindDNFormat":"uid=$user,ou=pdunam,dc=acme,dc=com","searchFilter":"","searchScope":"SUBTREE","searchAttribute":"","searchControls":"","bindDN":"cn=extldapadmin,ou=people, dc=acme,dc=com","bindPassword":""}}	
	`curl --cacert certificate.pem --request PUT -s -i --cookie file.txt https://<host name>/oss/idm/config/extidp/settings -H "Content-Type: application/json" -d '{"remoteAuthProfile":"NOSEARCH","authType":"REMOTEAUTHN"}'`	HTTP/1.1 403 Forbidden	{"userMessage":"The User does not have permissions to perform this action.","httpStatusCode":403,"internalErrorCode":"SSC-3-update","developerMessage":"com.ericsson.oss.itpf.sdk.security.accesscontrol.SecurityViolationException: access control decision: denied to invoke: update on resource: ext_idp_settings","time":"2018-12-10T16:25:23","links":[],"errorData":null}	User has not privileges to access the resource

7.3.2 Monitoring

Table 3

Use Case	Example Command	HTTP Response Code	Example Response	Notes or Probable Root Cause
Connectivity test	`curl --cacert certificate.pem --request POST -s -i --cookie file.txt https://<host name>/oss/idm/config/extidp/settings/test/connectivity -H "Content-Type: application/json" -d '{"serverAddress":"141.137.87.54:7389"}'`	HTTP/1.1 200 OK	{"successfulTest":true,"failureReason":""}	
	`curl --cacert certificate.pem --request POST -s -i --cookie file.txt https://<host name>/oss/idm/config/extidp/settings/test/connectivity -H "Content-Type: application/json" -d '{"serverAddres`	HTTP/1.1 200 OK	{"successfulTest":false,"failureReason":"ldap connection failure"}	Wrong port or Wrong IP address

Use Case	Example Command	HTTP Response Code	Example Response	Notes or Probable Root Cause
	s":"141.137.87.54:1111"}'			
	curl --cacert certificate.pem --request POST -s -i --cookie file.txt https://<host name>/oss/idm/config/extidp/settings/test/connectivity -H "Content-Type: application/json" -d '{"serverAddress":"1411.137.87.54:1111"}'	HTTP/1.1 412 Precondition Failed	{"constraintViolations":[{"method":"public javax.ws.rs.core.Response com.ericsson.oss.services.security.genericidentityconfigservice.rest.extidpconfiguration.ExtIdpConfigurationRest.testExtIdpConnectivity(com.ericsson.oss.services.security.genericidentityconfigservice.extidpsettings.model.ExtIdpTestParam)","parameterName":"arg0","kind":"PARAMETER","propertyPath":"ExtIdpConfigurationRest#testExtIdpConnectivity(arg0).serverAddress","invalidValue":"141.137.87.54.1111","message":"must match \"(((((25[0-5]|(2[0-4]|1{0,1}[0-9]){0,1}[0-9])\\.){3,3}(25[0-5]|(2[0-4]|1{0,1}[0-9]){0,1}[0-9]))|\\[(([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,7}:|([0-9a-fA-F]{1,4}:){1,6}:[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,5}(:[0-9a-fA-F]{1,4}){1,2}|([0-9a-fA-F]{1,4}:){1,4}(:[0-9a-fA-F]{1,4}){1,3}|([0-9a-fA-F]{1,4}:){1,3}(:[0-9a-fA-F]{1,4}){1,4}|([0-9a-fA-F]{1,4}:){1,2}(:[0-9a-fA-F]{1,4}){1,5}|[0-9a-fA-F]{1,4}:((:[0-9a-fA-F]{1,4}){1,6})|:((:[0-9a-fA-F]{1,4}){1,7}|:)|fe80:(:[0-9a-fA-F]{0,4}){0,4}%[0-9a-zA-Z]{1,}|::(ffff(:0{1,4}){0,1}:){0,1}((25[0-5]|(2[0-4]|1{0,1}[0-9]){0,1}[0-9])\\.){3,3}(25[0-5]|(2[0-4]|1{0,1}[0-9]){0,1}[0-9])|([0-9a-fA-F]{1,4}:){1,4}:((25[0-5]|(2[0-4]|1{0,1}[0-9]){0,1}[0-9])\\.){3,3}(25[0-5]|(2[0-4]|1{0,1}[0-9]){0,1}[0-9]))\\]):(6553[0-5]|655[0-2][0-9]|65[0-4][0-9]{2}|6[0-4][0-9]{3}|[1-5][0-9]{4}|[1-9][0-9]{3}|[1-9][0-9]{2}|[1-9][0-9]|[1-9]))|^$\""}]}	Wrong IP address format
	curl --cacert certificate.pem --request POST -s -i --cookie file.txt https://<host name>/oss/idm/config/extidp/settings/test/connectivity -H "Content-Type: application/json" -d	HTTP/1.1 403 Forbidden	{"userMessage":"The User does not have permissions to perform this action.","httpStatusCode":403,"internalErrorCode":"SSC-3-execute","developerMessage":"com.ericsson.oss.itpf.sdk.security.accesscontrol.SecurityViolationException: access control	

Use Case	Example Command	HTTP Response Code	Example Response	Notes or Probable Root Cause
	'{"serverAddress":"141.137.87.54:7636"}'		decision: denied to invoke: execute on resource: ext_idp_settings","time":"2018-12-10T16:28:34","links":[],"errorData":null}	
Authentication Test	curl --cacert certificate.pem --request POST -s -i --cookie file.txt https://<host name>/oss/idm/config/extidp/settings/test/authentication -H "Content-Type: application/json" -d '{"serverAddress":"141.137.87.54:7636"}'	HTTP/1.1 200 OK	{"successfulTest":true,"failureReason":""}	
	curl --cacert certificate.pem --request POST -s -i --cookie file.txt https://<host name>/oss/idm/config/extidp/settings/test/authentication -H "Content-Type: application/json" -d '{"serverAddress":"141.137.87.54:7636","bindDN":"cn=extldapadmin,ou=people,dc=acme,dc=com","bindPassword":"Externalldapadmin01","ldapConnectionMode":"LDAPS"}'	HTTP/1.1 200 OK	{"successfulTest":true,"failureReason":""}	The only mandatory parameter is serverAddress. The other parameters, if present, are used instead of the values actually configured in ENM.
	curl --cacert certificate.pem --request POST -s -i --cookie file.txt https://<host name>/oss/idm/config/extidp/settings/test/authentication -H "Content-Type: application/json" -d '{"serverAddress":"141.137.87.54:8080"}'	HTTP/1.1 200 OK	{"successfulTest":false,"failureReason":"ldap authentication failure: Connect Error: Connection refused"}	Failure due to server port not supporting neither LDAP nor LDAPS
	curl --cacert certificate.pem --request POST -s -i --cookie file.txt https://<host name>/oss/idm/config/extidp/settings/test/authentication -H "Content-Type: application/json" -d '{"serverAddr	HTTP/1.1 200 OK	{"successfulTest":false,"failureReason":"ldap authentication failure: Connect Error: Unrecognized SSL message, plaintext connection?"}	Failure due to server port = LDAP port and client configured as LDAPS

Use Case	Example Command	HTTP Response Code	Example Response	Notes or Probable Root Cause
	ess":"141.137.87.54:7389","ldapConnectionMode":"LDAPS"}'			
	curl --cacert certificate.pem --request POST -s -i --cookie file.txt https://<host name>/oss/idm/config/extidp/settings/test/authentication -H "Content-Type: application/json" -d '{"serverAddress":"141.137.87.54:7636","ldapConnectionMode":"LDAP"}'	HTTP/1.1 200 OK	{"successfulTest":false,"failureReason":"ldap authentication failure: Server Connection Closed"}	Failure due to server port = LDAPS port and client configured as LDAP
	curl --cacert certificate.pem --request POST -s -i --cookie file.txt https://<host name>/oss/idm/config/extidp/settings/test/authentication -H "Content-Type: application/json" -d '{"foo":"141.137.87.54:7636"}'	HTTP/1.1 400 Bad Request	Unrecognized field "foo" (Class com.ericsson.oss.services.security.genericidentityconfigservice.extidpsettings.model.ExtIdpTestParam), not marked as ignorable at [Source: org.jboss.resteasy.core.interception.MessageBodyReaderContextImpl$InputStreamWrapper@508009a9; line: 1, column: 11] (through reference chain: com.ericsson.oss.services.security.genericidentityconfigservice.extidpsettings.model.ExtIdpTestParam["foo"])	Wrong field name

Note: In the examples, IPv4 addresses are used for serverAddress, but also IPv6 address are supported in the format specified in Table 1.

8 Federated Identity Management Interface

Federated Identity Management is a component of the Identity Management Service that provides federated users management to the security solution through REST API.

Sync State Parameters

Table 4

Sync State Parameter	Description
adminState	String ("enabled", "disabled") - this field contains the administrative state of the synchronization.
operState	String ("init", "notConfigured", "disabled", "idle", "periodicSyncInProgress", "forcedSyncInProgress", "testSyncInProgress", "forcedDeleteInProgress") - this field contains the operational state of the synchronization.
progressReport	String ("", "externallySearching", "internallySearching", "merging", "performingCRUD") - this field contains the progress report for asynchronous operations (Periodic Sync, Forced Sync, Test Sync, and Forced Delete). For synchronous operations, the field contains an empty string.

Sync Period Parameters

Table 5

Sync Period Parameters	Description
intervalDurationInHours	Integer (an integer greater than 0) - this field contains the interval duration of periodic synchronization timer. Default value is 24.
initialExpiration	String ("HH:mm" where HH in the range [00-23] and mm in the range [00-59] or "" empty string) - this field contains the initial expiration (in terms

Sync Period Parameters	Description
	of time of day hours and minutes Local Time) of periodic synchronization timer. When it contains an empty string, the initial expiration is to be considered when the administrative state is set to "enabled" otherwise the first timer expiration occurs at next suitable occurrence of specified time after enabling the synchronization. Default value is "00:00".

Sync Advanced Settings Parameters

Table 6

Sync Advanced Settings Parameters	Description
name	String - this field contains the name of the configuration.
searchPageSize	Integer (an integer greater than 0) - the search page size used in the search requests. It is greater than zero and less than max-search-size configured on external server.
searchRequests	JSON object - this field contains a JSON list of search requests. Each search request contains parameters to perform the search request (relative base DN, scope, filter, requested attributes) and parameters to parse the attributes values contained in the correspondent search result entries to extract the relevant user information.
relativeBaseDn	String (Distinguished Name format) - this field contains the relative DN respect of the base DN of the external server for the starting point of the search. The search is executed starting from "<relativeBaseDn>,<baseDn>". So the relativeBaseDn SHALL NOT contain the base DN. If the relativeBaseDn is null or empty, the search is executed starting from the base DN.
scope	String ("base", "one", "sub", "children") - this field contains the scope of the search.

Sync Advanced Settings Parameters	Description
filter	String - this field contains the filter of the search as defined in RFC 4515.
attributes	JSON object - this field contains a JSON map of requested attributes: the key is the attribute name, the value is a JSON object containing the parameters to parse the attribute values to extract the relevant user information. The set of keys of this field provides the requested attributes used in the search request.
valueRegex	String - this field contains the regular expression (in Java format) to parse an attribute value.
valueMatchingGroups	JSON object - this field contains a JSON map of matching groups possibly extracted with the regular expression: the key is a tag ("username", "userDn", "memberOf", "groupDn", "member", "role", "tg") specifying which information is contained in a matching group, the value is a JSON list containing the indexes of the matching groups containing such tag.
roleMappingType	String ("none", "format", "map") - this field contains the type of role mapping to be applied to all external roles retrieved from the external server to get the correspondent ENM custom role.
roleFormat	String (with format "\[<prefix>]${role}\[<suffix>]" where ${role} is the mandatory placeholder for the external role name) - this field contains the format to obtain the local role name starting from the external role name (${role} is its mandatory placeholder) adding an optional prefix <prefix>, an optional suffix <suffix>, or both. This field is mandatory if roleMappingType is equal to "format", it is ignored otherwise and in this case this field can be left null or empty.
rolesMap	JSON object - this field contains a JSON map of each external role name (the key) to the correspondent local

Sync Advanced Settings Parameters	Description
	role name (the value). This field is mandatory if roleMappingType is equal to "map", it is ignored otherwise and in this case this field can be left null or empty.

Sync Report Parameters

Table 7

Sync Report Parameters	Description
actionReport	JSON object - this field contains action-related report information.
action	String ("testSync", "forcedDelete", "forcedSync", "periodicSync") - this field contains the action type.
startTime	String (with format "yyyy-MM-dd HH:mm:ss") - this field contains when the action started.
duration	String (with format "HH:mm:ss.SSS") - this field contains the action duration.
result	String ("successful", "failed") - this field contains the action result.
tasksReport	JSON object - this field contains a JSON list of task reports. For each task of the action, the task report contains task-related report information.
task	String ("externalSearch", "internalSearch", "merge","performCrud") - this field contains the task type.
startTime	String (with format "yyyy-MM-dd HH:mm:ss") - this field contains when the task started.
duration	String (with format "HH:mm:ss.SSS") - this field contains the task duration.
result	String ("successful", "failed") - this field contains the task result.
counters	JSON object - this field contains a JSON map of counters; the key is the counter, the value is a JSON object containing value and associated diagnostic messages of the counter.

Sync Report Parameters	Description
value	Integer (an integer greater than or equal to 0) - this field contains the numeric value of the counter.
diagnosticMessages	JSON object - this field contains a JSON list of strings. Each string contains additional diagnostic information associated to the counter. The list can be empty.
privilegesReport	JSON object - this field contains privileges-related report information.
requiredEnmRoles	JSON object - this field contains a JSON list of strings representing the set of required ENM Custom Roles. A Custom Role is required if associated to at least one federated user.
requiredTGs	JSON object - this field contains a JSON list of strings representing the set of required Target Groups. A Target Group is required if associated to at least one federated user.
unmappedRoles	JSON object - this field contains a JSON list of strings representing the set of external roles correctly parsed for at least one federated user but that cannot be mapped to a local role.

Report Counters

The available counters depend on the task they are related to.

Table 8

Report Counters	Description	Available in Tasks
numBindRequestsError	Number of failed LDAP bind requests.	externalSearch, internalSearch, performCrud
numEnmFederatedUsers	Number of internal federated users.	merge
numExtFederatedUsers	Number of external federated users.	merge
numLdapEntries	Number of search result entries contained in all successful search results.	externalSearch, internalSearch, performCrud

Report Counters	Description	Available in Tasks
numLdapErrors	Number of generic LDAP errors (neither bind nor search request errors).	externalSearch, internalSearch, performCrud
numLdapUsersWithoutEnmPrivileges	Number of LDAP search result entries returned by the server but not containing any privileges matching the rules configured in the sync advanced settings.	externalSearch
numSearchRequestsError	Number of failed LDAP search requests.	externalSearch, internalSearch, performCrud
numSearchRequestsSuccess	Number of successful LDAP search requests.	externalSearch, internalSearch, performCrud
numSearchResultsEmpty	Number of successful LDAP search results containing an empty collection.	externalSearch, internalSearch, performCrud
numSearchResultsSuccess	Number of successful LDAP search results containing a not empty collection.	externalSearch, internalSearch, performCrud
numUserCheckOnCreateError	Number of checks on federated users create failed because of generic error.	performCrud
numUserCheckOnCreateTimeout	Number of checks on federated users create failed because of timeout.	performCrud
numUserCheckOnDeleteError	Number of checks on federated users delete failed because of generic error.	performCrud
numUserCheckOnDeleteTimeout	Number of checks on federated users delete failed because of timeout.	performCrud
numUserCheckOnUpdateError	Number of checks on federated users update failed because of generic error.	performCrud

Report Counters	Description	Available in Tasks
numUserCheckOnUpdateTimeout	Number of checks on federated users update failed because of timeout.	performCrud
numUserCreate	Number of federated users to be created in Local IdP since they are present in external IdP and not present in local IdP.	merge
numUserCreateError	Number of failed federated users create (sum of numUserCreateErrorDueToInternalLogicException and numUserCreateErrorDueToEntityNotFound and numUserCreateErrorDueToGenericError).	perform crud
numUserCreateErrorDueToEntityNotFound	Number of failed federated users create because of entity not found error (for example, create with not existing roles and/or target groups).	performCrud
numUserCreateErrorDueToGenericError	Number of failed federated users create because of generic error (for example, unexpected internal error).	performCrud
numUserCreateErrorDueToInternalLogicException	Number of failed federated users create because of internal logic error (for example, create of an already existent user).	performCrud
numUserCreateSuccess	Number of successful federated users create in Local IdP.	performCrud
numUserDelete	Number of federated users to be deleted from Local IdP since they are not present in external	merge

Report Counters	Description	Available in Tasks
	IdP and present in local IdP.	
numUserDeleteError	Number of failed federated users delete.	performCrud
numUserDeleteSuccess	Number of successful federated users delete from Local IdP.	perfornCrud
numUsersInCommon	Number of common federated users present in both external and local IdP with the same privileges.	merge
numUsersWithoutEnmPrivileges	Number of LDAP search result entries returned by the server, containing at least a privilege matching the rules configured in the sync advanced settings but not containing any privileges after applying the role mapping.	externalSearch
numUserUpdate	Number of federated users to be updated in Local IdP since they are present in both external and local IdP with different privileges.	merge
numUserUpdateError	Number of failed federated users update (sum of numUserUpdateErrorDueToEntityNotFound and numUserUpdateErrorDueToGenericError).	performCrud
numUserUpdateErrorDueToEntityNotFound	Number of failed federated users update because of entity not found error (for example, update with not existing roles and/or target groups).	performCrud
numUserUpdateErrorDueToGenericError	Number of failed federated users update because of generic error (for example,	performCrud

Report Counters	Description	Available in Tasks
	unexpected internal error).	
numUserUpdateSuccess	Number of successful federated users update in Local IdP.	performCrud

8.1 Get Federated Identity Synchronization State

> This REST endpoint is used to get the state of the Federated Identity Synchronization.

Both administrative and operational states are returned. If an asynchronous operation is in progress, its progress report is returned too.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Get state of federated identity synchronization	`GET`	`/oss/fidm/sync/state`

Available Path Parameters

None

Available Query Parameters

None

JSON Query

None

Available Query Fields

Not Applicable

HTTP Response Code: 200

```
{
  "adminState" : "enabled",
```

```
  "operState" : "forcedSyncInProgress",
  "progressReport" : "externallySearching"
}
```

Available Response Fields

— adminState - the administrative state.

— operState - the operational state.

— progressReport - the progress report.

Example 17

This command can be used to retrieve state of synchronization:

```
curl --cacert <certificate.pem> -b <cookie.txt> -H Accept:application/json -H Co →
ntent-Type:application/json -X GET "https://<hostName>/oss/fidm/sync/state"
```

Result:

```
{"adminState":"enabled","operState":"forcedSyncInProgress","progressReport":"per →
formingCrud"}
```

8.2 Set Federated Identity Synchronization State

> This REST endpoint is used to set the administrative state of the Federated Identity Synchronization.

Both updated administrative and operational states are returned. The progress report is returned too.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Set administrative state of federated identity synchronization	PUT	/oss/fidm/sync/state

Available Path Parameters

None

Available Query Parameters

None

JSON Query

```
{
  "adminState" : "disabled"
}
```

Available Query Fields

— adminState [mandatory] the administrative state to set.

HTTP Response Code: 200

```
{
  "adminState" : "disabled",
  "operState" : "disabled",
  "progressReport" : ""
}
```

Available Response Fields

— adminState - the updated administrative state.

— operState - the updated operational state.

— progressReport - the updated progress report.

Example 18

This command can be used to set administrative state of synchronization:

```
curl --cacert <certificate.pem> -b <cookie.txt> -H Accept:application/json -H Co →
ntent-Type:application/json -X PUT "https://<hostName>/oss/fidm/sync/state" -d ' →
{"adminState":"disabled"}'
```

Result:

```
{"adminState":"disabled","operState":"disabled","progressReport":""}
```

8.3 Get Federated Identity Synchronization Period

> This REST endpoint is used to get the period of the Federated Identity Synchronization.

The period is expressed in terms of interval duration (in hours) and initial expiration of periodic synchronization timer.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Get period of federated identity synchronization	GET	/oss/fidm/sync/period

Available Path Parameters

None

Available Query Parameters

None

JSON Query

None

Available Query Fields

Not Applicable

HTTP Response Code: 200

```
{
  "intervalDurationInHours" : 12,
  "initialExpiration" : 02:00
}
```

Available Response Fields

— intervalDurationInHours - the interval duration (in hours) of the periodic synchronization timer.

— initialExpiration - the initial expiration of the periodic synchronization timer.

Example 19

This command can be used to get synchronization period:

```
curl --cacert <certificate.pem> -b <cookie.txt> -H Accept:application/json -H Co
ntent-Type:application/json -X GET "https://<hostName>/oss/fidm/sync/period"
```

Result:

```
{"intervalDurationInHours" : 12,"initialExpiration" : "02:00"}
```

8.4 Set Federated Identity Synchronization Period

> This REST endpoint is used to set the period of the Federated Identity Synchronization.

The period is expressed in terms of interval duration (in hours) of periodic synchronization timer. It is also possible to specify the initial expiration time as a string whose format is "HH:mm": the first timer expiration occurs at next suitable occurrence of specified time when administrative state is set to "enabled" . If the initial expiration is an empty string, a synchronization is performed when the administrative state of the synchronization is set to "enabled".

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Set period of federated identity synchronization	PUT	/oss/fidm/sync/period

Available Path Parameters

None

Available Query Parameters

None

JSON Query

```
{
  "intervalDurationInHours" : 12,
```

```
  "initialExpiration" : "02:00"
}
```

Available Query Fields

— intervalDurationInHours - the interval duration (in hours) of the periodic synchronization timer to set.

— initialExpiration - the initial expiration of the periodic synchronization timer to set.

HTTP Response Code: 200

```
{
  "intervalDurationInHours" : 12,
  "initialExpiration" : 02:00
}
```

Available Response Fields

— intervalDurationInHours [mandatory] - the updated interval duration (in hours) of the periodic synchronization timer.

— initialExpiration [mandatory] - the updated initial expiration of the periodic synchronization timer.

Example 20

This command can be used to set synchronization period:

```
curl --cacert <certificate.pem> -b <cookie.txt> -H Accept:application/json -H Co →
ntent-Type:application/json -X PUT "https://<hostName>/oss/fidm/sync/period" -d →
'{"intervalDurationInHours":12,"initialExpiration":"02:00"}'
```

Result:

```
{"intervalDurationInHours" : 12,"initialExpiration" : "02:00"}
```

8.5 Import Federated Identity Synchronization Advanced Settings Configuration

> This REST endpoint is used to import the Federated Identity Synchronization Advanced Settings Configuration.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Import federated identity synchronization advanced settings configuration	POST	/oss/fidm/sync/import

Available Path Parameters

None

Available Query Parameters

None

JSON Query

```
{
  "name": "Acme Users",
  "searchPageSize": 100,
  "searchRequests": [
    {
      "relativeBaseDn": "ou=people",
      "scope": "sub",
      "filter": "(&(objectClass=*)(acmeapplicationaut=enm@ACME_* →
))",
      "attributes": {
        "dn": {
          "valueRegex": "^(.+)$",
          "valueMatchingGroups": {
            "userDn": [
              1
            ]
          }
        },
        "uid": {
          "valueRegex": "^([^\b]+)$",
          "valueMatchingGroups": {
            "username": [
              1
            ]
          }
        },
        "acmeapplicationaut": {
          "valueRegex": "enm@([^:]+)(?::(.+))?",
          "valueMatchingGroups": {
            "role": [
              1
            ],
```

```
            "tg": [
              2
            ]
          }
        }
      }
    }
  ],
  "roleMapping": {
    "roleMappingType": "none",
    "roleFormat": null,
    "rolesMap": null
  }
}
```

Available Query Fields

- name [mandatory] - the name of the configuration.
- searchPageSize [mandatory] - the search page size used in the search requests.
- searchRequests [mandatory] -a JSON list of search requests; each request is a JSON object containing:
  - relativeBaseDn [mandatory] - the relative DN respect of the base DN of the external server for the starting point of the search.
  - scope [mandatory] - the scope of the search.
  - fiter [mandatory] - the filter of the search as defined in RFC4515, Reference [2].
  - attributes [mandatory] - a JSON map of search attributes; the key is the `attributeName`, the value is a JSON object containing:
    - valueRegex [mandatory] - the regular expression (in Java format) to parse the attribute value.
    - valueMatchingGroups [mandatory] - a JSON map of matching groups possibly extracted with the regular expression; the key is a tag specifying which information is involved, the value is the index of the matching group containing such tag.
- rolemapping [mandatory] - a JSON object containing:
  - roleMappingType [mandatory] - the type of role mapping.
  - roleFormat [mandatory] - the format to get the local role name from the external role name.
  - rolesMap [mandatory] - a JSON map of each external role name (the key) to the correspondent local role name (the value).

HTTP Response Code: 200

```
{
  "adminState" : "disabled",
  "operState" : "disabled",
  "progressReport" : ""
}
```

Available Response Fields

- adminState - the new administrative state.
- operState - the new operational state.
- progressReport - the new progress report.

Example 21

This command can be used to import synchronization advanced settings configuration:

```
curl --cacert <certificate.pem> -b <cookie.txt> -H Accept:application/json -H Co →
ntent-Type:application/json -X POST "https://<hostName>/oss/fidm/sync/period" -d →
 '{"name":"Acme Users","searchPageSize":100,"searchRequests":[{"relativeBaseDn": →
"ou=people","scope":"sub","filter":"(&(objectClass=*)(acmeapplicationaut=enm@ACM →
E_*))","attributes":{"dn":{"valueRegex":"^(.+)$","valueMatchingGroups":{"userDn" →
:[1]}},"uid":{"valueRegex":"^([^\b]+)$","valueMatchingGroups":{"username":[1]}}, →
"acmeapplicationaut":{"valueRegex":"enm@([^:]+)(?::(.+))?","valueMatchingGroups" →
:{"role":[1],"tg":[2]}}}}],"roleMapping":{"roleMappingType":"none","roleFormat": →
null,"rolesMap":null}}'
```

Result:

```
{"adminState":"disabled","operState":"disabled","progressReport":""}
```

8.6 Export Federated Identity Synchronization Advanced Settings Configuration

> This REST endpoint is used to retrieve the Federated Identity Synchronization Advanced Settings Configuration.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Export federated identity synchronization advanced settings configuration	GET	/oss/fidm/sync/export

Available Path Parameters

None

Available Query Parameters

None

JSON Query

None

Available Query Fields

Not Applicable

HTTP Response Code: 200

```
{ "name": "Acme Users", "searchPageSize": 100, "searchRequests": [ { "relativeBa
seDn": "ou=people", "scope": "sub", "filter": "(&(objectClass=*)(acmeapplication
aut=enm@ACME_*))", "attributes": { "dn": { "valueRegex": "^(.+)$", "valueMatchin
gGroups": { "userDn": [ 1 ] } }, "uid": { "valueRegex": "^([^\b]+)$", "valueMatc
hingGroups": { "username": [ 1 ] } }, "acmeapplicationaut": { "valueRegex": "enm
@([^:]+)(?::(.+))?", "valueMatchingGroups": { "role": [ 1 ], "tg": [ 2 ] } } }
 ], "roleMapping": { "roleMappingType": "none", "roleFormat": null, "rolesMap":
null } }
```

Available Response Fields

— name - the name of the configuration.

— searchPageSize - the search page size used in the search requests.

— searchRequests - a JSON list of search requests; each request is a JSON object containing:

  — relativeBaseDn - the relative DN respect of the base DN of the external server for the starting point of the search.

  — scope - the scope of the search.

  — fiter - the filter of the search as defined in RFC4515, Reference [2].

  — attributes - a JSON map of search attributes; the key is the `attributeName`, the value is a JSON object containing:

- valueRegex - the regular expression (in Java format) to parse the attribute value.
- valueMatchingGroups - a JSON map of matching groups possibly extracted with the regular expression; the key is a tag specifying which information is involved, the value is the index of the matching group containing such

— rolemapping - a JSON object containing:

  — roleMappingType - the type of role mapping.

  — roleFormat - the format to get the local role name from the external role name.

  — rolesMap - a JSON map of each external role name (the key) to the correspondent local role name (the value).

Example 22

This command can be used to export synchronization advanced settings configuration:

```
curl --cacert <certificate.pem> -b <cookie.txt> -H Accept:application/json -H Co
ntent-Type:application/json -X GET "https://<hostName>/oss/fidm/sync/export"
```

Result:


```
{"name":"Acme Users","searchPageSize":100,"searchRequests":[{"relativeBaseDn":"o
u=people","scope":"sub","filter":"(&(objectClass=*)(acmeapplicationaut=enm@ACME_
*))","attributes":{"dn":{"valueRegex":"^(.+)$","valueMatchingGroups":{"userDn":[
1]}},"uid":{"valueRegex":"^([^\b]+)$","valueMatchingGroups":{"username":[1]}},"a
cmeapplicationaut":{"valueRegex":"enm@([^:]+)(?::(.+))?","valueMatchingGroups":{
"role":[1],"tg":[2]}}}}],"roleMapping":{"roleMappingType":"none","roleFormat":nu
ll,"rolesMap":null}}
```


8.7 Test Federated Identity Synchronization

> This REST endpoint is used to trigger the Federated Identity Synchronization test.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Test federated identity synchronization	POST	/oss/fidm/sync/test

Available Path Parameters

None

Available Query Parameters

None

JSON Query

None

Available Query Fields

Not Applicable

HTTP Response Code: 200

```
{
  "adminState" : "disabled",
  "operState" : "testSyncInProgress",
  "progressReport" : ""
}
```

Available Response Fields

— adminState - the new administrative state.

— operState - the new operational state.

— progressReport - the new progress report.

Example 23

This command can be used to test synchronization advanced settings configuration:

```
curl --cacert <certificate.pem> -b <cookie.txt> -H Accept:application/json -H Co →
ntent-Type:application/json -X POST "https://<hostName>/oss/fidm/sync/test"
```

Result:

```
{"adminState":"disabled","operState":"testSyncInProgress","progressReport":""}
```

8.8 Federated Identity Synchronization Forced Delete

> This REST endpoint is used to trigger the Federated Identity Synchronization forced delete to remove all federated users from Local server.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Federated identity synchronization forced delete	POST	/oss/fidm/sync/delete

Available Path Parameters

None

Available Query Parameters

None

JSON Query

None

Available Query Fields

Not Applicable

HTTP Response Code: 200

```
{
  "adminState" : "disabled",
  "operState" : "forcedDeleteInProgress",
  "progressReport" : ""
}
```

Available Response Fields

— adminState - the new administrative state.

— operState - the new operational state.

— progressReport - the new progress report.

Example 24

This command can be used to remove all federated users:

```
curl --cacert <certificate.pem> -b <cookie.txt> -H Accept:application/json -H Co →
ntent-Type:application/json -X POST "https://<hostName>/oss/fidm/sync/delete"
```

Result:

```
{"adminState":"disabled","operState":"forcedDeleteInProgress","progressReport":" →
"}
```

8.9 Federated Identity Synchronization Forced Sync

> This REST endpoint is used to trigger the Federated Identity Synchronization forced sync to forcefully execute synchronization.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Federated identity synchronization forced sync	POST	/oss/fidm/sync/forced

Available Path Parameters

None

Available Query Parameters

None

JSON Query

None

Available Query Fields

Not Applicable

HTTP Response Code: 200

```
{
```

```
  "adminState" : "enabled",
  "operState" : "forcedSyncInProgress",
  "progressReport" : ""
}
```

Available Response Fields

- adminState - the new administrative state.
- operState - the new operational state.
- progressReport - the new progress report.

Example 25

This command can be used to remove all federated users:

```
curl --cacert <certificate.pem> -b <cookie.txt> -H Accept:application/json -H Co
ntent-Type:application/json -X POST "https://<hostName>/oss/fidm/sync/forced"
```

Result:

```
{"adminState":"enabled","operState":"forcedSyncInProgress","progressReport":""}
```

8.10 Federated Identity Synchronization Restore to Defaults

> This REST endpoint is used to trigger the Federated Identity Synchronization restore to defaults.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Federated identity synchronization restore to defaults.	POST	/oss/fidm/sync/restore

Available Path Parameters

None

Available Query Parameters

None

JSON Query

None

Available Query Fields

Not Applicable

HTTP Response Code: 200

```
{
  "adminState" : "disabled",
  "operState" : "notConfigured",
  "progressReport" : ""
}
```

Available Response Fields

- adminState - the new administrative state.
- operState - the new operational state.
- progressReport - the new progress report.

Example 26

This command can be used to restore to defaults:

```
curl --cacert <certificate.pem> -b <cookie.txt> -H Accept:application/json -H Co →
ntent-Type:application/json -X POST "https://<hostName>/oss/fidm/sync/restore"
```

Result:

```
{"adminState":"disabled","operState":"notConfigured","progressReport":""}
```

8.11 Get Federated Identity Last Synchronization Report

> This REST endpoint is used to retrieve the Federated Identity last synchronization report.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Description	Method	Path
Get federated identity the Federated Identity last synchronization report	GET	/oss/fidm/sync/report

Available Path Parameters

None

Available Query Parameters

None

JSON Query

None

Available Query Fields

Not Applicable

HTTP Response Code: 200


```
{
  "actionReport" : {
    "startTime" : "2020-04-15 02:00:00",
    "duration" : "00:00:04.791",
    "result" : "successful",
    "action" : "periodicSync"
  },
  "taskReports" : [ {
    "startTime" : "2020-04-15 02:00:00",
    "duration" : "00:00:00.314",
    "result" : "successful",
    "task" : "externalSearch",
    "counters" : {
      "numSearchResultsSuccess" : {
        "value" : 1,
        "diagnosticMessages" : [ ]
      },
      "numLdapEntries" : {
        "value" : 11,
        "diagnosticMessages" : [ ]
      },
      "numSearchRequestsSuccess" : {
        "value" : 1,
        "diagnosticMessages" : [ ]
      }
    }
  }, {
    "startTime" : "2020-04-15 02:00:01",
    "duration" : "00:00:03.276",
    "result" : "successful",
    "task" : "internalSearch",
    "counters" : {
      "numSearchResultsSuccess" : {
        "value" : 1,
        "diagnosticMessages" : [ ]
      },
      "numLdapEntries" : {
```

```
        "value" : 9,
        "diagnosticMessages" : [ ]
      },
      "numSearchRequestsSuccess" : {
        "value" : 1,
        "diagnosticMessages" : [ ]
      }
    }
  }, {
    "startTime" : "2020-04-15 02:00:04",
    "duration" : "00:00:00.001",
    "result" : "successful",
    "task" : "merge",
    "counters" : {
      "numEnmFederatedUsers" : {
        "value" : 9,
        "diagnosticMessages" : [ ]
      },
      "numUsersInCommon" : {
        "value" : 6,
        "diagnosticMessages" : [ ]
      },
      "numExtFederatedUsers" : {
        "value" : 11,
        "diagnosticMessages" : [ ]
      },
      "numUserCreate" : {
        "value" : 2,
        "diagnosticMessages" : [ ]
      },
      "numUserUpdate" : {
        "value" : 3,
        "diagnosticMessages" : [ ]
      },
      "numUserDelete" : {
        "value" : 0,
        "diagnosticMessages" : [ ]
      }
    }
  }, {
    "startTime" : "2020-04-15 02:00:04",
    "duration" : "00:00:00.771",
    "result" : "successful",
    "task" : "performCrud",
    "counters" : {
      "numUserCreateErrorDueToEntityNotFound" : {
        "value" : 1,
        "diagnosticMessages" : [ ]
      },
      "numUserCreateSuccess" : {
        "value" : 0,
        "diagnosticMessages" : [ ]
      },
      "numUserCreateErrorDueToInternalLogicException" : {
        "value" : 1,
        "diagnosticMessages" : [ ]
      },
      "numUserUpdateSuccess" : {
        "value" : 0,
        "diagnosticMessages" : [ ]
      },
      "numUserUpdateErrorDueToEntityNotFound" : {
        "value" : 3,
        "diagnosticMessages" : [ ]
      },
      "numUserUpdateError" : {
        "value" : 3,
        "diagnosticMessages" : [ ]
      },
      "numUserCreateError" : {
        "value" : 2,
        "diagnosticMessages" : [ ]
      }
    }
  } ],
  "privilegesReport" : {
    "requiredEnmRoles" : [ "ACME_NodeSecurity_Operator", "ACME_PKI_Operator", "A →
CME_NodeSecurity_Administrator" ],
    "requiredTGs" : [ "NORTH", "WEST", "SOUTH", "EAST" ],
    "unmappedRoles" : [ ]
```

```
    }
}
```

Available Response Fields

- actionReport - a JSON object containing following action-related fields:
  - action - the action type.
  - startTime - when the action started.
  - duration - the duration of the action.
  - result - the action result.
- tasksReport - a JSON list containing, for each task of the action, following task-related fields:
  - task - the task type.
  - startTime - when the task started.
  - duration - the duration of the task.
  - result - the task result.
  - counters - a JSON map of counters; the key is the counter, the value is a JSON object containing:
    - value - the numeric value of the counter.
    - diagnosticMessage - a JSON list of diagnostic messages associated to the counter.
- privilegesReport - a JSON object containing following privileges-related fields:
  - requiredEnmRoles - the set of required ENM Custom Roles.
  - requiredTGs - the set of required Target Groups.
  - unmappedRoles - the set of external roles correctly parsed for at least one federated user but that cannot be mapped to a local role.

Example 27

This command can be used to get last synchronization report:

```
curl --cacert <certificate.pem> -b <cookie.txt> -H Accept:application/json -H Co
ntent-Type:application/json -X GET "https://<hostName>/oss/fidm/sync/report"
```

Result:

```
{"actionReport":{"startTime":"2020-04-15 02:00:00","duration":"00:00:04.791","re
sult":"successful","action":"periodicSync"},"taskReports":[{"startTime":"2020-04
```

```
-15 02:00:00","duration":"00:00:00.314","result":"successful","task":"externalSe
arch","counters":{"numSearchResultsSuccess":{"value":1,"diagnosticMessages":[]},
"numLdapEntries":{"value":11,"diagnosticMessages":[]},"numSearchRequestsSuccess"
:{"value":1,"diagnosticMessages":[]}}},{"startTime":"2020-04-15 02:00:01","durat
ion":"00:00:03.276","result":"successful","task":"internalSearch","counters":{"n
umSearchResultsSuccess":{"value":1,"diagnosticMessages":[]},"numLdapEntries":{"v
alue":9,"diagnosticMessages":[]},"numSearchRequestsSuccess":{"value":1,"diagnost
icMessages":[]}}},{"startTime":"2020-04-15 02:00:04","duration":"00:00:00.001","
result":"successful","task":"merge","counters":{"numEnmFederatedUsers":{"value":
9,"diagnosticMessages":[]},"numUsersInCommon":{"value":6,"diagnosticMessages":[]
},"numExtFederatedUsers":{"value":11,"diagnosticMessages":[]},"numUserCreate":{"
value":2,"diagnosticMessages":[]},"numUserUpdate":{"value":3,"diagnosticMessages
":[]},"numUserDelete":{"value":0,"diagnosticMessages":[]}}},{"startTime":"2020-0
4-15 02:00:04","duration":"00:00:00.771","result":"successful","task":"performCr
ud","counters":{"numUserCreateErrorDueToEntityNotFound":{"value":1,"diagnosticMe
ssages":[]},"numUserCreateSuccess":{"value":0,"diagnosticMessages":[]},"numUserC
reateErrorDueToInternalLogicException":{"value":1,"diagnosticMessages":[]},"numU
serUpdateSuccess":{"value":0,"diagnosticMessages":[]},"numUserUpdateErrorDueToEn
tityNotFound":{"value":3,"diagnosticMessages":[]},"numUserUpdateError":{"value":
3,"diagnosticMessages":[]},"numUserCreateError":{"value":2,"diagnosticMessages":
[]}}}],"privilegesReport":{"requiredEnmRoles":["ACME_NodeSecurity_Operator","ACM
E_PKI_Operator","ACME_NodeSecurity_Administrator"],"requiredTGs":["NORTH","WEST"
,"SOUTH","EAST"],"unmappedRoles":[]}}
```


8.12 Error Code Responses - Federated Identity Management

%s - this sign in the message indicates dynamic parameters like name of a field, value of a field.

Use Case	REST	httpStatusCode	internalErrorCode	userMessage in REST	userMessage in UI
IDAM-FIDMNBI06 NBI Get Federated Users Synchronization Status	GET /oss/fidm/sync/state	403	FIDM-3-read	The User does not have permissions to perform this action.	N/A
IDAM-FIDMNBI02 NBI Enable / Disable Federated Users Synchronization	PUT /oss/fidm/sync/state	403	FIDM-3-update	The User does not have permissions to perform this action.	N/A
		400	FIDM-1	— Missing mandatory query parameter adminState. — The query parameter value pair adminState: %s is incorrect.	N/A
		422	FIDM-5-28-39	External IdP synchronization is still initializing.	N/A
		422	FIDM-5-28-40	External IdP synchronization is not yet configured.	N/A
		422	FIDM-5-28-42	External IdP synchronization is in progress.	N/A
IDAM-FIDMNBI011 NBI Get Federated Users Synchronize Period	GET /oss/fidm/sync/period	403	FIDM-3-read	The User does not have permissions to perform this action.	N/A

Use Case	REST	httpStatusCode	internalErrorCode	userMessage in REST	userMessage in UI
		422	FIDM-5-28-39	External IdP synchronization is still initializing.	N/A
IDAM-FIDMNBI05 NBI Update Federated Users Synchronize Period	PUT /oss/fidm/sync/period	403	FIDM-3-update	The User does not have permissions to perform this action.	N/A
		400	FIDM-1	— Missing mandatory query parameter %s. — The query parameter value pair %s: %s is incorrect.	N/A
		422	FIDM-5-28-39	External IdP synchronization is still initializing.	N/A
		422	FIDM-5-28-20	External IdP synchronization operation not allowed in current state.	N/A
IDAM-FIDMNBI03 NBI Import Federated Users Synchronizer Advanced Settings	POST /oss/fidm/sync/import	403	FIDM-3-execute	The User does not have permissions to perform this action.	N/A
		422	FIDM-5-28-39	External IdP synchronization is still initializing.	N/A
		422	FIDM-5-28-20	External IdP synchronization operation not allowed in current state.	N/A
IDAM-FIDMNBI04 NBI Export Federated Users Synchronizer Advanced Settings	GET /oss/fidm/sync/export	403	FIDM-3-read	The User does not have permissions to perform this action.	N/A
		422	FIDM-5-28-39	External IdP synchronization is still initializing.	N/A
		422	FIDM-5-28-40	External IdP synchronization is not yet configured.	N/A
IDAM-FIDMNBI01 NBI Test Federated Users Synchronize Setting	POST /oss/fidm/sync/test	403	FIDM-3-execute	The User does not have permissions to perform this action.	N/A
		422	FIDM-5-28-39	External IdP synchronization is still initializing.	N/A
		422	FIDM-5-28-40	External IdP synchronization is not yet configured.	N/A
		422	FIDM-5-28-20	External IdP synchronization operation not allowed in current state.	N/A
IDAM-FIDMNBI09 NBI Delete Federated Users	POST /oss/fidm/sync/delete	403	FIDM-3-execute	The User does not have permissions to perform this action.	N/A

Use Case	REST	httpStatusCode	internalErrorCode	userMessage in REST	userMessage in UI
		422	FIDM-5-28-39	External IdP synchronization is still initializing.	N/A
		422	FIDM-5-28-40	External IdP synchronization is not yet configured.	N/A
		422	FIDM-5-28-20	External IdP synchronization operation not allowed in current state.	N/A
IDAM-FIDMNBI08 NBI Force Federated Users Synchronization	POST /oss/fidm/sync/forced	403	FIDM-3-execute	The User does not have permissions to perform this action.	N/A
		422	FIDM-5-28-39	External IdP synchronization is still initializing.	N/A
		422	FIDM-5-28-40	External IdP synchronization is not yet configured.	N/A
		422	FIDM-5-28-20	External IdP synchronization operation not allowed in current state.	N/A
		422	FIDM-5-28-42	External IdP synchronization is in progress.	N/A
IDAM-FIDMNBI07 NBI Get Last Federated Users Synchronization Report	GET /oss/fidm/sync/report	403	FIDM-3-read	The User does not have permissions to perform this action.	N/A
		422	FIDM-5-28-39	External IdP synchronization is still initializing.	N/A
		422	FIDM-5-28-41	External IdP synchronization never executed.	N/A
IDAM-FIDMNBI10 NBI Federated Users Synchronizer Restore to Default Advanced Settings	POST /oss/fidm/sync/restore	403	FIDM-3-execute	The User does not have permissions to perform this action.	N/A
		422	FIDM-5-28-39	External IdP synchronization is still initializing.	N/A
		422	FIDM-5-28-20	External IdP synchronization operation not allowed in current state.	N/A
		422	FIDM-5-28-42	External IdP synchronization is in progress.	N/A

Reference List

[1] *ENM Public Key Infrastructure System Administrator Guide*, 2/1543-aom 901 151-3 Uen
[2] *RFC4515*, https://tools.ietf.org/search/rfc4515
[3] *ENM Network Integration Guideline*, 1/102 72-aom 901 151 Uen