BeyondTrust

Privileged Identity 5.5.4
REST API Guide

TC:2/8/2019

Table of Contents

Privileged Identity REST API Guide

This guide outlines the use of the REST-based web service.

The following pages outline the current methods found in the REST-based web service. The methods area grouped together by related functions.

REST: Login

The start of every process begins with authentication and authorization. The end of every process can and should end with the termination of that authentication.

Login (POST)

DoLogin obtains an AuthenticationToken and is the first step to performing any subsequent operations. A successful authentication will provide an authentication token in as `DoLoginResult` as part of `DoLoginResponse` which will be passed to other subsequent commands as `AuthenticationToken`.

Related Commands

- **PowerShell:** Get-LSLoginToken
- **SOAP:** DoLogin

Syntax

```
{
   "Authenticator": "String content",
   "LoginType": 0,
   "MFATokenCode": "String content",
   "OnBehalfOfUser": { "Username": "String content" },
   "Password": "String content",
   "SAMLAudience": "String content",
   "SAMLCert": "String content",
   "SAMLDomainGroups": "String content",
   "SAMLDomainUsers": "String content",
   "SAMLIssuer": "String content",
   "SAMLResponse": "String content",
   "SAMLRoles": "String content",
   "SAMLSubject": "String content",
   "Username": "String content"
}
```

Parameters

- **Authenticator:** *(Optional)* Required when logging in with an LDAP or RADIUS user or Windows domain user not using integrated authentication. LoginType will be set to `FullyQualifiedAccount`.
- **LoginType:** The type of login being performed. Valid options are:
    - **1** - NativeStaticAccount: Use when logging in with Privileged Identity explicit accounts.
    - **2** - FullyQualifiedAccount: Use when logging is with LDAP or RADIUS or Windows domain user not using integrated authentication.
    - **3** - IntegratedAuthentication: Use when logging in with a trusted Windows domain user. No other options are required.
    - **4** - CertificateAuthentication: Use when logging in with a user certificate and no other forms of authentication.
- **MFATokenCode:** *(Optional)* Can be used with identities required to use OATH/Yubico MFA. Supply the current token.
- **OnBehalfOfUser\UserName** *(Optional)* Used for integrations such as McAfee ePO. If performing an impersonated login, specify the target impersonated username.

- **Password:** *(Optional)* The password of the user logging in. This option is not used for Integrated Windows Authentication and may be required when performing certificate-based authentication.
- **SAMLAudience:** Not Used.
- **SAMLCert:** Not Used.
- **SAMLDomainGroups:** Not Used.
- **SAMLDomainUsers:** Not Used.
- **SAMLIssuer:** Not Used.
- **SAMLResponse:** Not Used.
- **SAMLRoles:** Not Used.
- **SAMLSubject:** Not Used.
- **Username:** *(Optional)* The username of the user logging in. This option is not used for Integrated Windows Authentication and may be required when performing certificate-based authentication.

Example Requests

Following are example REST requests showing various types of logins.

Fully Qualified Account Request

```
{
   "Authenticator":"LSDS",
   "LoginType":2,
   "Password":"P@ssw0rd",
   "Username":"lscadmin"
}
```

Integrated Request

```
{
   "LoginType":3
}
```

Output Success

The only output after successfully logging in will be the AuthenticationToken.

Example Success Output

```
"JX825GXEDUQRANCVHWFD6EN4CM8VCKXA"
```

Output Fail

- **Bad Password or Username**

  Login failed or username not found.

- **Time restrictions for operation or Logon permission not granted**

  Identity cannot perform operation at this time, identity has time restrictions.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Login failed or username
not found'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: LoginSAML (POST)

DoLoginSAML is used to obtain an AuthenticationToken and is the first step to performing any subsequent operations using a SAML-based login. A successful authentication will provide a `SessionToken` as part of `DoLoginSAMLResult` which will be passed to other subsequent commands as `AuthenticationToken`.

Related Commands

- **PowerShell:** Get-LSLoginSAMLToken
- **SOAP:** DoLoginSAML

Syntax

```
"String Content of SAMLBase64Response"
```

Parameters

- **SAMLResponse:** The base64 response received externally from the SAML provider.

Example Request

Following is an example REST request for a SAML Login.

Login Request

```
"BASE64 SAML RESPONSE"
```

Output Success

The output after successfully logging in will contain SAML assertions and the SessionToken. SessionToken will be passed to other commands as AuthenticationToken.

Example Success Output

```
{
   "MethodSpecificResultCode": 0,
   "SAMLAudience": "RedIM",
   "SAMLCert": "SAML_CERTIFICATE_INFO_HERE",
   "SAMLDomainGroups": "",
   "SAMLDomainUsers": "",
   "SAMLIssuer": "OneLogin",
   "SAMLRoles": "",
   "SAMLSubject": "user@example.com",
   "SessionToken": "OAGFSAMXQG6D8IYTHVWMZXYJ2B3NB1NJ"
}
```

Output Fail

Login can fail for a number of reasons such as a bad username or password or lack of delegations or a bad SAML response.

- **Bad Password or Username**

  Login failed or username not found.

- **Time restrictions for operation or Logon permission not granted**

  Identity cannot perform operation at this time, identity has time restrictions.

- **Bad SAML response**

  Unexpected token "token_data".

- **Login Attempt falls outside of NotOnOrAfter condition:**

  Failed to generate session, login attempt failed with result: 2147746477.

Example Fail Output

```
{
   "MethodSpecificResultCode": 2147746477,
   "SAMLAudience": null,
   "SAMLCert": null,
   "SAMLDomainGroups": null,
   "SAMLDomainUsers": null,
   "SAMLIssuer": null,
   "SAMLRoles": null,
   "SAMLSubject": null,
   "SessionToken": null
}
```

REST: Logout (POST)

DoLogout terminates an otherwise valid authentication token.

Related Commands

- **SOAP:** DoLogout

Syntax

```
{
   "AuthenticationToken":"String content"
}
```

Parameters

- **AuthenticationToken:** The authentication token to expire, previously received from a login event.

Examples

```
{
   "AuthenticationToken":"69OVX989OP3UGPJIA30RCPW24TAWF4KY"
}
```

Output Success

When a logout is successful, the body of the response will be empty. The web service host will respond with "Status 200 OK".

Example Success Output

```
Status 200 OK
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
```

```
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Session invalid, a
duplicate web session was detected for this identity'. See server logs for more details. The
exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Auditing

This section describes using REST APIs to view the web application audit logs.

Logs/WebLogs (GET)

Logs/WebLogs returns the web audit logs for a given date range, if one is specified.

Permissions Required

- View Web Audit Logs

Related Commands

- **PowerShell:** Get-LSListWebAuditLogs
- **SOAP:** LoggingOps_GetWebAuditLog

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Logs/WebLogs?StartTime=
{STARTTIME}&EndTime={ENDTIME}
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **StartTime:** (Optional) - The start time dateTime object to return logs from. Expected format is:

  `YYYY-MM-DDTHH%3AMM%3ASS`.

  Note the "T" between DD and HH. The hour interval is based on a 24 hour clock. Value must be URL encoded: %3A is the separator between (:) between HH::MM:SS.

- **EndTime:** (Optional) - The start time dateTime object to return logs through. Expected format is:

  `YYYY-MM-DDTHH%3AMM%3ASS`.

  Note the "T" between DD and HH. The hour interval is based on a 24 hour clock. Value must be URL encoded: %3A is the separator between (:) between HH::MM:SS.

Example Request

The request accepts a start and end date for the audit logs as part of FilterSettings. If neither date range is specified, the entire audit log history will be returned.

No date range specified

```
https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/Logs/WebLogs
```

Date range specified

```
https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/Logs/WebLogs?StartTime=2017-05-10T00%3A00%3A00&EndTime=2017-05-11T11%3A59%3A59
```

Output Success

If the command is successful, the web audit logs for the date ranges specified will be provided.

Example Success Output


```
[
   {
      "ClientAgentOperation": false,
      "HTTPSEnabled": false,
      "IPAddress": "fe80::1457:7c44:8b0b:f5ea%14",
      "JobID": "0",
      "OperationAccount": "",
      "OperationResult": 5,
      "OperationSystem": "",
      "ServerName": "",
      "Timestamp": "/Date(1483717789000-0600)/",
      "Username": "[WebApplicationManager]",
      "WebOperation": 16,
      "WebServiceOperation": false
   },
   {
      "ClientAgentOperation": false,
      "HTTPSEnabled": false,
      "IPAddress": "fe80::c1e0:93f:1f9f:c1d5%12",
      "JobID": "0",
      "OperationAccount": "",
      "OperationResult": 5,
      "OperationSystem": "",
      "ServerName": "",
      "Timestamp": "/Date(1483760025000-0600)/",
      "Username": "[WebApplicationManager]",
      "WebOperation": 16,
      "WebServiceOperation": false
   }
]
```


Output Error

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Improperly formatted date/time value**

  Improperly formatted date/time values do not cause an error and will be ignored. All logs will be returned.

- **Start and End times conflict**

  The end/start time specified is before/after the end/start time, this time span is invalid.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'The end time specified is
before the start time, this time span is invalid'. See server logs for more details. The exception
stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Jobs & Job Settings

This section describes using REST APIs to add, edit, list, and delete jobs. Jobs are created for interactive and scheduled management activities.

Jobs (GET)

Jobs returns job information for jobs matching a particular filter, such as the type of job or last result of a job.

Permissions Required

- All Access

Related Commands

- **PowerShell:** Get-LSListJobs

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Jobs?JobOperationType=
{JOBOPERATIONTYPE}&LastResult={LASTRESULT}&MaxCount={MAXCOUNT}
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- **JobOperationType:** (Optional) - An enumerated value that can be passed as an integer or string value. The type of job to filter for. Valid options are:
    - 0 or Unknown
    - 1 or SendMessage
    - 2 or Reboot
    - 3 or AbortReboot
    - 4 or PasswordChange
    - 5 or Refresh_All
    - 6 or Refresh_SystemInfo
    - 7 or WebOperation
    - 8 or UpdateManagementSet
    - 9 or ActivityReport_Manager
    - 10 or ActivityReport_Admin
    - 11 or Refresh_SystemInfoAndCredentialReferences
    - 12 or GenReport_StoredPasswordsTest

- 13 or GenReport_StoredPasswords
- 14 or Refresh_TrustInfo
- 15 or Refresh_TrustInfoForDomain
- 16 or Refresh_CredentialReferences
- 17 or Refresh_InstanceAccounts_SQLServer
- 18 or Refresh_InstanceAccounts_MySQL
- 19 or Refresh_InstanceData_SQLServer
- 20 or Refresh_InstanceData_MySQL
- 21 or Refresh_InstanceAccounts_Oracle
- 22 or Refresh_InstanceData_Oracle
- 23 or GenReport_ComplianceReportingDataSnapshot
- 24 or Refresh_InstanceData_CustomAccountStore
- 25 or Refresh_InstanceAccounts_CustomAccountStore
- 26 or AccountElevation
- 27 or Refresh_InstanceData_Oracle_InternetDirectory
- 28 or Refresh_InstanceAccounts_Oracle_InternetDirectory
- 29 or Refresh_InstanceData_Novell_eDirectory
- 30 or Refresh_InstanceAccounts_Novell_eDirectory
- 31 or Refresh_InstanceAccounts_Sybase
- 32 or Refresh_InstanceData_Sybase
- 33 or Refresh_InstanceData_IBM_Tivoli
- 34 or Refresh_InstanceAccounts_IBM_Tivoli
- 35 or Refresh_InstanceData_BMCThroughIPMI
- 36 or Refresh_InstanceAccounts_BMCThroughIPMI
- 37 or Refresh_InstanceData_ViewDS
- 38 or Refresh_InstanceAccounts_ViewDS
- 39 or UpdateSSHKeyData
- 40 or Refresh_SelectedData
- 41 or Refresh_InstanceAccounts_PostgreSQL
- 42 or Refresh_InstanceData_PostgreSQL
- 43 or GenReport_SecurityPolicyCheck
- 44 or Ops_AppDataStoreMaintenance
- 45 or Refresh_InstanceSystems_CustomAccountStore
- 46 or Refresh_InstanceAccounts_Teradata
- 47 or Refresh_InstanceData_Teradata
- 48 or Refresh_InstanceData_XeroxPhaser
- 49 or GenReport_AuditSettings
- 50 or GenReport_EventLogEvents
- 51 or GenReport_EventLogInfos
- 52 or GenReport_FilePermissions

  - 53 or GenReport_Files
  - 54 or GenReport_GlobalGroups
  - 55 or GenReport_GroupMembership
  - 56 or GenReport_GlobalGroupMembership
  - 57 or GenReport_UserGroupMembership
  - 58 or GenReport_IEUpdates
  - 59 or GenReport_InstalledSoftware
  - 60 or GenReport_LocalGroups
  - 61 or GenReport_LocalUsers
  - 62 or GenReport_LoggedOnUsers
  - 63 or GenReport_NetShares
  - 64 or GenReport_Policies
  - 65 or GenReport_RegistryKeys
  - 66 or GenReport_Rights
  - 67 or GenReport_TrustAccounts
  - 68 or GenReport_UnixAccounts
  - 69 or GenReport_VNCInstances
  - 70 or GenReport_WindowsUpdates
  - 71 or GenReport_WMI
  - 72 or GenReport_SystemInfo
  - 73 or GenReport_NetUses
  - 74 or GenReport_NetSessions
- **LastResult:** (Optional) - An enumerated value that can be passed as an integer or string value. Sets the filter to include only jobs with a specific "Last Result". Valid options are:
  - 0 or Unknown
  - 1 or HasNotRun
  - 2 or Incomplete_InProcess
  - 3 or Complete_WithFailures_CanRetry
  - 4 or Complete_WithFailures_NoRetry
  - 5 or Complete_NoFailures_Rescheduled
  - 6 or Complete_NoFailures
  - 7 or Complete_WithFailures_NoRetry_Rescheduled
  - 8 or Disabled
  - 9 or MissedRun_Rescheduled
  - 10 or MissedRun
  - 11 or Incomplete_PartialRun
- **MaxCountReturned:** (Optional) - Defines the maximum number of jobs to return.

Example Request

No Options - Return Everything

```
http://lsdslscprd.lsds.int/erpmwebserviceanonnossl/authservice.svc/rest/Jobs
```

Filter for Job Type: AccountElevation

```
http://lsdslscprd.lsds.int/erpmwebserviceanonnossl/authservice.svc/rest/Jobs?JobOperationType=26
```

Filter for password change jobs with a result of Complete_WithFailures_NoRetry

```
http://lsdslscprd.lsds.int/erpmwebserviceanonnossl/authservice.svc/rest/Jobs?JobOperationType=4&L
astResult=4
```

Output Success

Output will list all jobs and related descriptions matching any defined filters.

Example Success Output


```
[
   {
      "AssociatedGroup": "[Web Job]",
      "Comment": "Auto-roll on recovery password job created by: lsds\\lscadmin",
      "CreatedBy": "lsds\\erpmweb",
      "CreationTimeUTC": "/Date(1483054229000-0600)/",
      "JobID": "77",
      "JobOperation": 4,
      "JobType": 2,
      "LastResult": 4,
      "LastRunTimeUTC": "/Date(1483499824000-0600)/",
      "NextRunTimeUTC": "/Date(1488369615000-0600)/",
      "PullSystemsFromGroup": false,
      "RefreshGroupBeforeRun": false,
      "RunJobOnNewSystems": false
   }
]
```


Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid identifier name for JobOperationType or LastResult**

  'Invalid enum value '17' cannot be deserialized into type 'AppServiceInterop.AppOperations.EJobOperation'

'Invalid enum value '17' cannot be deserialized into type 'AppServiceInterop.AppOperations.EJobLastResult'

Example Output Fail

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="http://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a> for
constructing valid requests to the service. The exception message is 'Enum value '90' is invalid for
type 'AppServiceInterop.AppOperations.EJobOperation' and cannot be serialized. Ensure that the
necessary enum values are present and are marked with EnumMemberAttribute attribute if the type has
DataContractAttribute attribute.'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Job (GET)

Jobs obtains the current status and other metadata of a particular job.

Permissions Required

- Delegated permissions on the target job.

Related Commands

- **PowerShell:** Get-LSJobStatus
- **SOAP:** JobOps_GetJobStatus

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Job?JobID={JOBID}
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- **JobID:** The ID of the job.

Example Request

```
https://lsdslscprd.lsds.int/erpmwebservice/authservice.svc/rest/Job?JobID=1
```

Output Success

A successful run will return certain metadata about the job.

Example Success Output


```
{
   "AssociatedGroup": "Default",
   "Comment": "Management Set Update Job",
   "CreatedBy": "lsds\\lscadmin",
   "CreationTimeUTC": "/Date(1482288216000-0600)/",
   "JobID": "1",
   "JobOperation": 8,
   "JobType": 0,
   "LastResult": 2,
   "LastRunTimeUTC": "/Date(1490263201000-0500)/",
   "NextRunTimeUTC": "/Date(1490263200000-0500)/",
   "PullSystemsFromGroup": false,
```

```
   "RefreshGroupBeforeRun": false,
   "RunJobOnNewSystems": false
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Non-existent JobID**

  The job specified could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'The job specified could
not be found'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Job/Schedule (GET)

Job/Schedule returns the schedule parameters for a target job ID.

Permissions Required

- Delegated permissions on the job

Related Commands

- **PowerShell:** Get-LSJobSchedule
- **SOAP:** JobOps_GetJobSchedule

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Job/Schedule?JobID={JOBID}
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- **JobID:** The ID of the job to retrieve the schedule for.

Example Request

```
https://serverName/ERPMWebService/AuthService.svc/REST/Job/Schedule?JobID=1
```

Output Success

The scheduling options of the job will be output.

Example Success Output


```
{
   "DayOfMonth": 0,
   "DayOfWeek": 0,
   "DayOfYear": 0,
   "DaysBits": 0,
   "EveryNDays": 30,
   "Hours": 0,
   "Minutes": 0,
   "MonthOfYear": 0,
   "NextRetryTimeUTC": "/Date(1490263201000-0500)/",
   "NumberOfRetries": 0,
   "Reboot": false,
```

```
   "RetryEnabled": true,
   "RunWindowMinutes": 0,
   "ScheduleType": 9,
   "SchedulingPeriod": 0,
   "UpdateNextRunTimeForPartialCompletion": false
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Non-existent JobID**

  The job specified could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_formatting_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'The job specified could
not be found'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Job/WindowsElevation (GET)

Jobs/WindowsElevation obtains the current status and other metadata of a particular job.

Permissions Required

- Delegated permissions on the target job.

Related Commands

- **PowerShell:** Get-LSJobAccountElevationSettings
- **SOAP:** JobOps_GetJobElevationSettings

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Job/WindowsElevation?JobID={JOBID}
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- **JobID:** The ID of the job.

Example Request

```
https://lsdslscprd.lsds.int/erpmwebservice/authservice.svc/rest/Job/WindowsElevation?JobID=68
```

Output Success

A successful run will return certain metadata about the job.

Example Success Output


```
{
   "AccountElevatedState": 2,
   "AccountNameToElevate": "lsds\\lscadmin",
   "DomainElevationGroup": "Administrators",
   "ElevateToDomainGlobalGroup": true,
   "ElevationGroup": "Administrators",
   "ExpirationEmailAddress": "",
   "ExpirationEmailMinutes": 20,
   "ExpirationEmailSent": false,
   "MinutesBeforeRemoval": 360,
   "MinutesBeforeRemovalGlobal": 360,
   "SendExpirationEmail": false,
```

```
   "SendFailureEmail": false,
   "SendSuccessEmail": false
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Non-existent JobID**

  The job specified could not be found.

- **Job is not an account elevation job**

  Could not find job information for the job specified

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'The job specified could
not be found'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Job/PasswordChange (GET)

Jobs/PasswordChange obtains the current status and other metadata of a particular job.

Permissions Required

- Delegated permissions on the target job.

Related Commands

- **PowerShell:** Get-LSJobPasswordChangeSettings
- **SOAP:** JobOps_GetJobPasswordChangeSettings

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Job/PasswordChange?JobID={JOBID}
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- **JobID:** The ID of the job.

Example Request

```
https://lsdslscprd.lsds.int/erpmwebservice/authservice.svc/rest/Job/PasswordChange?JobID=18
```

Output Success

A successful run returns certain metadata about the job.

Example Success Output

```
{
   "AccountComment": "",
   "AccountType": 10,
   "AddMissing": false,
   "AddType": 0,
   "CancelIfCheckedOut": false,
   "ChangeLoginAccount": false,
   "ChangeRootAccount": false,
   "ChangeTwice": false,
   "ClearAutoLogon": false,
   "ConfigFile": "",
   "ConnectionType": 1,
```

```
"CurrentPassword": "",
"DisableAccountLockout": false,
"DomainName": "Azure Active Directory",
"EmailOnChange": "",
"ExplicitPassword": "",
"FirstCharacterSetBits": 15,
"FullAccountName": "James.Kirk@cloudstuff.onmicrosoft.com",
"HostCodePage": 1,
"KeepAccountLockedOutUntilComplete": false,
"KeyLabel": "",
"LastCharacterSetBits": 15,
"LoginName": "",
"LoginPassword": "",
"MiddleCharactersSetBits": 15,
"MinLettersLcase": 0,
"MinLettersUcase": 0,
"MinNumbers": 0,
"MinSymbols": 0,
"NewAccountName": "",
"PasswordChangeType": 1,
"PasswordCharacterSetBits": 15,
"PasswordCompatibilityLevel": 0,
"PasswordConstraints": {
   "DefaultPasswordFilterCompliance": 0,
   "ExplicitPassword": "THEh34t!$0ff",
   "FailGenerationOnMissingPassfiltDLL": false,
   "FirstCharacterSetBits": 15,
   "LastCharacterSetBits": 15,
   "MiddleCharactersSetBits": 15,
   "MinLettersLcase": 0,
   "MinLettersUcase": 0,
   "MinNumbers": 0,
   "MinSymbols": 0,
   "PasswordChangeType": 1,
   "PasswordCharacterSetBits": 15,
   "PasswordCompatibilityLevel": 0,
   "PasswordLength": 14,
   "PasswordSecurityOptions": 0,
   "PasswordSegments": 1,
   "PathToPassfiltDLL": "",
   "SymbolsExcludeProblematicWithAPIs": false,
   "SymbolsExcluded": "",
   "SymbolsSetOverride": ""
},
"PasswordLength": 14,
"PasswordPropagationSettings": {
   "ConstrainToManagedSystems": false,
   "ConstrainToMembersOfGroup": false,
   "ConstrainToSystemsWithNonzeroInUse": false,
   "ExcludeDomainControllers": false,
   "ExcludeSystemWithAccount": false,
   "GroupName": "",
   "PropagateToSystemWithAccountOnly": false,
   "PropagateToTrustingDomains": false
},
```

```
    "PasswordPropagationTargets": {
       "ListTargets": []
    },
    "PasswordSecurityOptions": 0,
    "PasswordSegments": 1,
    "PreventUsernameInPassword": false,
    "ReEnableAccountAfterSetTimeHours": false,
    "ReEnableAccountIfOperationFails": false,
    "RenameAccount": false,
    "SendEmailOnChange": false,
    "SerializedUtilityIDs": "",
    "StoredAccountName": "",
    "StoredNamespace": "",
    "StoredSystemName": "",
    "SymbolsSetOverride": "",
    "TerminalType": 0,
    "Unique": true,
    "UnlockAccount": false,
    "UpdateAutoLogon": false,
    "UpdatedAccountIsRootAccount": false,
    "UseSavedPasswords": false,
    "UseStoredLoginPassword": false
}
```


Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Non-existent JobID**

  The job specified could not be found.

- **Job is not a password change job**

  Could not find job information for the job specified.

Example Fail Output


```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
```

```
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Could not find job
information for the job specified'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Job/PreAndPostRun (GET)

Job/PreAndPostRun obtains the pre and post run job settings for a specific JobID.

Permissions Required

- Delegated permissions on the target job.

Related Commands

- **PowerShell:** Get-LSJobPreAndPostRunSettings
- **SOAP:** JobOps_GetPreAndPostRunSettings

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Job/PreAndPostRun?JobID={JOBID}
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- **JobID:** The ID of the job.

Example Request

```
https://lsdslscprd.lsds.int/erpmwebservice/authservice.svc/rest/Job/PreAndPostRun?JobID=68
```

Output Success

A successful run will return metadata about the job.

Example Success Output

```
{
   "PostRunApplication": "c:\\utils\\sdnutil.exe",
   "PostRunArgs": "-Op Close -Targ vn-custx",
   "PostRunExe": true,
   "PreRunAbortFail": true,
   "PreRunApplication": "c:\\utils\\sdnutil.exe",
   "PreRunArgs": "-Op Open -Targ vn-custx",
   "PreRunExe": true,
   "PreRunWait": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Non-existent JobID**

  The job specified could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'The job specified could
not be found'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Job/SSHKeyChange (GET)

Jobs/SSHKeyChange obtains the current status and other metadata of a particular SSH Key change job.

Permissions Required

- Delegated permissions on the target job.

Related Commands

- **PowerShell:** Get-LSJobSSHKeyChangeSettings
- **SOAP:** JobsOps_GetJobKeyChangeSettings

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Job/SSHKeyChange?JobID={JOBID}
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- **JobID:** The ID of the job.

Example Request

```
https://lsdslscprd.lsds.int/erpmwebservice/authservice.svc/rest/Job/SSHKeyChange?JobID=1199
```

Output Success

A successful run will return certain metadata about the job.

Example Success Output

```
{
   "DeleteKeyFileOnRemoteSystems": true,
   "GenerateNewKeyEachRun": true,
   "KeyLabel": "2B:39:27:15:8C:17:61:32:59:9F:FC:04:A5:EB:B8:11",
   "KeyLengthBits": 4096,
   "KeyType": 0,
   "OldKeyLabel": "",
   "OldKeySig": "",
   "OldPublicKey": "",
   "RemoveOldKey": true,
   "UpdateKeyReferences": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Non-existent JobID**

  The job specified could not be found.

- **Job is not an account elevation job**

  Could not find job information for the job specified.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'The job specified could
not be found'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Job/Logs (GET)

Job/Logs returns the logged operation messages for a job.

> ***Note:*** *The messages that this API returns are not the verbose messages seen in the text log for the specific job. Rather, these are the non-verbose general logs as seen in the logging tab of the job in the management console.*

Permissions Required

- Delegated access on the target job.

Related Commands

- **PowerShell:** Get-LSListJobMessagesForJob
- **SOAP:** JobOps_GetJobLogForJob

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Job/Logs?StartTime={STARTTIME}&EndTime=
{ENDTIME}
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- **StartTime:** *(Optional)* The start time dateTime object to return logs from. Expected format is:

  `YYYY-MM-DDTHH%3AMM%3ASS`

  Note the "T" between DD and HH. The hour interval is based on a 24 hour clock. Value must be URL encoded: %3A is the separator between (:) between HH::MM:SS.

- **EndTime:** *(Optional)* The start time dateTime object to return logs through. Expected format is:

  `YYYY-MM-DDTHH%3AMM%3ASS`

  Note the "T" between DD and HH. The hour interval is based on a 24 hour clock. Value must be URL encoded: %3A is the separator between (:) between HH::MM:SS.

Example Request

The request accepts a start and end date for the audit logs as part of FilterSettings. If neither date range is specified, the entire audit log history will be returned.

No date range specified

```
https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/Job/Logs?JobID=68
```

Date range specified

```
https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/Job/Logs?StartTime=2017-05-10T00%3A00%3A00&EndTime=2017-05-11T11%3A59%3A59
```

Output Success

If the command is successful, the web audit logs for the date ranges specified will be provided.

Example Success Output


```
[
   {
      "InstanceName": "DBAG01",
      "Message": "Account lsds\\lscadmin has been removed from group Administrators on system DBAG01",
      "OperationEntity": "DBAG01",
      "OperationLevel": 2,
      "TimeStamp": "/Date(1482993967000-0600)/"
   },
   {
      "InstanceName": "DBAG02",
      "Message": "Account lsds\\lscadmin has been removed from group Administrators on system DBAG02",
      "OperationEntity": "DBAG02",
      "OperationLevel": 2,
      "TimeStamp": "/Date(1482993967000-0600)/"
   },
   {
      "InstanceName": "DBAG01",
      "Message": "Account lsds\\lscadmin has been temporarily elevated to group Administrators on system DBAG01, elevation will expire in 360 minutes",
      "OperationEntity": "DBAG01",
      "OperationLevel": 2,
      "TimeStamp": "/Date(1482993722000-0600)/"
   },
   {
      "InstanceName": "DBAG02",
      "Message": "Account lsds\\lscadmin has been temporarily elevated to group Administrators on system DBAG02, elevation will expire in 360 minutes",
      "OperationEntity": "DBAG02",
      "OperationLevel": 2,
      "TimeStamp": "/Date(1482993722000-0600)/"
   }
]
```


Output Error

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Improperly formatted date/time value**

  Improperly formatted date/time values do not cause an error and will be ignored. All logs will be returned.

- **Invalid JobID**

  The job specified could not be found.

- **Start and End times conflict**

  The end/start time specified is before/after the end/start time, this time span is invalid.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'The end time specified is
before the start time, this time span is invalid'. See server logs for more details. The exception
stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Job/System (GET)

Job/System lists the status of the work to be performed against each system in the target job ID.

Permissions Required

- Delegated permissions on the target job.

Related Commands

- **PowerShell:** Get-LSListSystemStatusForJob
- **SOAP:** JobOps_GetSystemStatusForJob

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Job/System?JobID={JobID}
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- **JobID:** The ID of the job.

Example Request

```
https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/Job/System?JobID=68
```

Output Success

List all systems and their job state for the job specified.

Example Success Output

```
[
   {
      "AccountStoreName": "DBAG01",
      "LastRunTime": "/Date(1482972367000-0600)/",
      "SystemJobLastResult": 9,
      "SystemName": "DBAG01"
   },
   {
      "AccountStoreName": "DBAG02",
      "LastRunTime": "/Date(1482972367000-0600)/",
      "SystemJobLastResult": 9,
      "SystemName": "DBAG02"
```

```
    }
]
```

Output Error

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid JobID**

  The job specified could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'The job specified could
not be found'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Job/WindowsElevation/Extend (POST)

Job/WindowsElevationExtend changes the de-elevation time, thereby extending or minimizing the elevation time of an account elevation job.

Permissions Required

- Elevate Any Account

Related Commands

- **PowerShell:** Set-LSJobAccountElevationExtension
- **SOAP:** JobOps_SetJobElevationExtension

Syntax

```
{
   "AuthenticationToken":"String content",
   "ElevationExtension":{
      "ExpirationUTC":"\/Date(928167600000-0500)\/",
      "ExtensionMinutes":2147483647
   },
   "JobID":"String content"
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **ExpirationUTC:** The exact date and time to de-elevate the user. Expected format is Microsoft JSON, e.g. "/Date (MillisecondsSinceJan11970)/".
- **ExpirationMinutes:** The number of minutes from now to add to the elevation duration.
- **JobID:** The ID of the target job to extend.

Example Requests

Set a Specific Date and Time for De-Elevation

```
{
   "AuthenticationToken":"3GHMPO3WP5XIDW3GH2YTQQIWYMJFQ8CZ",
   "ElevationExtension":{
      "ExpirationUTC":"\/Date(1501279200000)\/",
      "ExtensionMinutes":0
   },
   "JobID":"1284"
}
```

Add More Time (Minutes) from Now

```
{
   "AuthenticationToken":"3GHMPO3WP5XIDW3GH2YTQQIWYMJFQ8CZ",
   "ElevationExtension":{
      "ExtensionMinutes":240
   },
   "JobID":"1284"
}
```

Output Success

The output message will indicate the job was updated.

Example Success Output

```
{
   "OperationMessage": "Updated elevation expiration for job 1284",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid JobID**

  The job specified could not be found.

- **Elevation duration too large**

  Value was either too large or too small for an Int32.

- **Elevation duration was longer than maximum allowed elevation duration**

  Elevation job could not be created, elevation duration (NNNNNN minutes) is longer than the maximum allowed (XXXX hours).

Example Fail Output

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
   <title>Request Error</title>
   <style>
```

```
      style_info_goes_here
   </style>
</head>
<body>
   <div id="content">
      <p class="heading1">Request Error</p>
      <p xmlns="">
         The server encountered an error processing the request. Please see the
         <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Elevation job could not be
created, elevation duration (777777 minutes) is longer than the maximum allowed (8760 hours)'. See
server logs for more details. The exception stack trace is:
      </p>
      <p>
         stack_trace_info_goes_here
      </p>
   </div>
</body>
</html>
```

REST: Job/System (PUT)

JobOps_AddSystemToJob adds a system to an existing job.

Permissions Required

- Delegated permissions on the job.

Related Commands

- **PowerShell:** New-LSJobAddSystem
- **SOAP:** JobOps_AddSystemToJob

Syntax

```
{
   "AuthenticationToken":"String content",
   "JobID":"String content",
   "SystemName":"String content"
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **JobID:** The ID of the job to add the system (SystemName) to.
- **SystemName:** The name of the system to add to the job.

Example Request

```
{
   "AuthenticationToken":"String content",
   "JobID":"String content",
   "SystemName":"String content"
}
```

Output Success

The output message will indicate SystemName was added to jobID.

Example Success Output

```
{
   "OperationMessage": "Added system dbsmash2008 to job 1259",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid JobID**

  The job specified could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
   <title>Request Error</title>
   <style>
      style_info_goes_here
   </style>
</head>
<body>
   <div id="content">
      <p class="heading1">Request Error</p>
      <p xmlns="">
         The server encountered an error processing the request. Please see the
         <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'The job specified could
not be found'. See server logs for more details. The exception stack trace is:
      </p>
      <p>
         stack_trace_info_goes_here
      </p>
   </div>
</body>
</html>
```

REST: Job/Clone (POST)

Job/Clone adds a system to an existing job.

Permissions Required

- All Access

Related Commands

- **PowerShell:** New-LSJobClone
- **SOAP:** JobOps_CloneJob

Syntax

```
{
   "AuthenticationToken":"String content",
   "JobID":"String content"
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **JobID:** The ID of the job to add the system (SystemName) to.

Example Request

```
{
   "AuthenticationToken":"String content",
   "JobID":"String content"
}
```

Output Success

The output provides the new JobID.

Example Success Output

```
{
   "OperationMessage": "1263",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid JobID**

  The job could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
   <title>Request Error</title>
   <style>
      style_info_goes_here
   </style>
</head>
<body>
   <div id="content">
      <p class="heading1">Request Error</p>
      <p xmlns="">
         The server encountered an error processing the request. Please see the
         <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'The job specified could
not be found'. See server logs for more details. The exception stack trace is:
      </p>
      <p>
         stack_trace_info_goes_here
      </p>
   </div>
</body>
</html>
```

REST: Job/RefreshIPMI (POST)

Job/RefreshIPMI creates a refresh job for IPMI devices.

Permissions Required

- All Access

Related Commands

- **PowerShell:** New-LSJobRefreshAndDiscoveryIPMI
- **SOAP:** JobOps_CreateRefreshIPMISystemJob

Syntax

```
{
   "AuthenticationToken":"String content",
   "JobInfoBase":{
      "AssociatedGroup":"String content",
      "Comment":"String content",
      "CreatedBy":"String content",
      "CreationTimeUTC":"\/Date(928167600000-0500)\/",
      "JobID":"String content",
      "JobOperation":0,
      "JobType":0,
      "LastResult":0,
      "LastRunTimeUTC":"\/Date(928167600000-0500)\/",
      "NextRunTimeUTC":"\/Date(928167600000-0500)\/",
      "PullSystemsFromGroup":true,
      "RefreshGroupBeforeRun":true,
      "RunJobOnNewSystems":true
   },
   "ScheduleInfo":{
      "DayOfMonth":2147483647,
      "DayOfWeek":2147483647,
      "DayOfYear":2147483647,
      "DaysBits":4294967295,
      "EveryNDays":2147483647,
      "Hours":2147483647,
      "Minutes":2147483647,
      "MonthOfYear":2147483647,
      "NextRetryTimeUTC":"\/Date(928167600000-0500)\/",
      "NumberOfRetries":2147483647,
      "Reboot":true,
      "RetryEnabled":true,
      "RunWindowMinutes":2147483647,
      "ScheduleType":0,
      "SchedulingPeriod":2147483647,
      "UpdateNextRunTimeForPartialCompletion":true
   },
   "SystemList":"String content"
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **AssociatedGroup:** Not used for IPMI refresh jobs. Use when adding the target user to all systems in a management set.
- **Comment:** *(Optional)* Add a comment to the job.
- **CreatedBy:** Not used. Will always use the ID of the calling user, most likely that of the COM application identity.
- **CreationTimeUTC:** Not used.
- **JobID:** Not used. Success output will indicate JobID.
- **JobOperation:** Not used.
- **JobType:** Not used.
- **LastResult:** Not used.
- **LastRunTimeUTC:** Not used.
- **NextRunTimeUTC:** *(Optional)* Time to run the job. If left blank, job will be set to run at 00:00:00 (midnight, tonight). Expected format is Microsoft JSON, e.g. "/Date(MillisecondsSinceJan11970)/".
- **PullSystemsFromGroup:** Not used for IPMI refresh jobs. Set to true to add the user to all systems in the management set targeted by AssociatedGroup.
- **RefreshGroupBeforeRun:** Not used for IPMI refresh jobs. Set to true to cause the AssociatedGroup to be updated prior to job run.
- **RunJobOnNewSystems:** Not used for IPMI refresh jobs. Set to true to run the job on new systems as they are added to the AssociatedGroup.
- **DayOfMonth:** *(Optional)* Set the day of the month to run the job. Valid values are 1-31. For months with fewer days than the day of the month defined (e.g. value is 30 but there are only 28 days in the month), the job will run on the last day of the month.
- **DayOfWeek:** *(Optional)* Set the day of the week to run the job. Values are:
    - **0** = Sunday
    - **1** = Monday
    - **2** = Tuesday
    - **3** = Wednesday
    - **4** = Thursday
    - **5** = Friday
    - **6** = Saturday
- **DayOfYear:** Not used.
- **DaysBits:** Not used.
- **EveryNDays:** Sets the amount of days for the job to recur when ScheduleTypes is set to SCHEDULE_TYPE_N_DAYS.
- **Hours:** *(Optional)* Sets the hour at which the job will run. Use a 24 hour clock.
- **Minutes:** *(Optional)* Sets the minutes into the hour (Hours) when the job will run.
- **MonthOfYear:** *(Optional)* Sets the month (number) for the job to run. Values are:
    - **1** = January
    - **2** = February
    - **3** = March
    - **4** = April

  - **5** = May
  - **6** = June
  - **7** = July
  - **8** = August
  - **9** = September
  - **10** = October
  - **11** = November
  - **12** = December
- **NextRetryUTC:** *(Optional)* For new jobs this value should not be used. Expected format is Microsoft JSON, e.g. "/Date (MillisecondsSinceJan11970)/".
- **NumberOfRetries:** *(Optional)* Set the number of retries for the job should it fail. If not defined, it will use the system default.
- **Reboot:** Not used for IPMI refresh jobs.
- **RetryEnabled:** *(Optional)* Set to true to enable retries in the event of failure.
- **RunWindowMinutes:** *(Optional)* Set to value to 1 or more minutes to define the job must run by the specified time plus the run window duration or the job will be skipped. Set to 0 or do not define to indicate it should run despite missing the originally schedule time (default).
- **ScheduleType:** *(Optional)* Defines the type of schedule (one time, recurring, etc.) for the job. If not defined, default value is SCHEDULE_TYPE_INTERACTIVE which means it must be run by hand or will be run immediately based on other scheduling options. Valid values are:
  - **0** = SCHEDULE_TYPE_UNKNOWN
  - **1** = SCHEDULE_TYPE_IMMEDIATELY
  - **2** = SCHEDULE_TYPE_HOURLY - Job will be run once every hour. Set Minutes to define the offset into the hour.
  - **3** = SCHEDULE_TYPE_DAILY- Job will be run once every day on the specified time. Set Hours and Minutes.
  - **4** = SCHEDULE_TYPE_WEEKLY - Job will be run once every week on the specified day and time. Set Hours, Minutes and DayOfWeek.
  - **5** = SCHEDULE_TYPE_MONTHLY - Job will be run once every month on the specified day and time. DayOfMonth, Hours, and Minutes.
  - **6** = SCHEDULE_TYPE_YEARLY - Job will be run once every year on the specified month, day and time. Define DayOfMonth, MonthOfYear, Hours, and Minutes.
  - **7** = SCHEDULE_TYPE_DAYS_OF_WEEK - Job will be run every set day of week. Set DayOfWeek.
  - **8** = SCHEDULE_TYPE_ONCE - Job will be run once at some point in the future. Define DayOfMonth, MonthOfYear, Hours, and Minutes.
  - **9** = SCHEDULE_TYPE_N_DAYS - Job will be run every N days. Set integer value for EveryNDays.
  - **10** = SCHEDULE_TYPE_INTERACTIVE - Default. Job will be run based on NextRunTimeUTC.
  - **11** = SCHEDULE_TYPE_N_HOURS - Job will be run every N hours. Set Hours for the number of hours and Minutes for the offset into each hour when the job will run.
- **SchedulingPeriod:** Not used.
- **UpdateNextRunTimeForPartialCompletion:** *(Optional)* Set to true to define job with multiple systems should update the next run time as seen in the management console display. The default value is false.
- **SystemList:** The target systems. If multiple systems are included, separate them by a semi-colon. For example: "system1;system2".

Example Request

```
{
   "AuthenticationToken":"6O02PLE2VZG9I7W5GGJ89GW7S4GLCJMM",
   "JobInfoBase":{
      "Comment":"refresh those devices",
      "NextRunTimeUTC":"\/Date(928167600000-0500)\/"
   },
   "ScheduleInfo":{
      "DayOfMonth":31,
      "Hours":17,
      "Minutes":16,
      "MonthOfYear":12,
      "NextRetryTimeUTC":"\/Date(928167600000-0500)\/",
      "NumberOfRetries":5,
      "RetryEnabled":true,
      "RunWindowMinutes":20,
      "ScheduleType":8,
      "UpdateNextRunTimeForPartialCompletion":true
   },
   "SystemList":"2.3.4.5"
}
```

Output Success

The output message will indicate the new jobID.

Example Success Output

```
{
   "OperationMessage": "Created refresh job for system 2.3.4.5 with JobID 1296",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
```

```
   <title>Request Error</title>
   <style>
      style_info_goes_here
   </style>
</head>
<body>
   <div id="content">
      <p class="heading1">Request Error</p>
      <p xmlns="">
         The server encountered an error processing the request. Please see the
         <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Invalid authentication
token or token not found'. See server logs for more details. The exception stack trace is:
      </p>
      <p>
         stack_trace_info_goes_here
      </p>
   </div>
</body>
</html>
```

REST: Job/SSHKeyChange (POST)

Job/SSHKeyChange creates a new SSH Key update job.

Permissions Required

- All Access

Related Commands

- **PowerShell:** New-LSJobSSHKeyChange
- **SOAP:** JobOps_CreateKeyChangeJob

Syntax

```
{
   "AuthenticationToken":"String content",
   "JobInfo":{
      "AssociatedGroup":"String content",
      "Comment":"String content",
      "CreatedBy":"String content",
      "CreationTimeUTC":"\/Date(928167600000-0500)\/",
      "JobID":"String content",
      "JobOperation":0,
      "JobType":0,
      "LastResult":0,
      "LastRunTimeUTC":"\/Date(928167600000-0500)\/",
      "NextRunTimeUTC":"\/Date(928167600000-0500)\/",
      "PullSystemsFromGroup":true,
      "RefreshGroupBeforeRun":true,
      "RunJobOnNewSystems":true
   },
   "oKeyChangeSettings":{
      "DeleteKeyFileOnRemoteSystems":true,
      "GenerateNewKeyEachRun":true,
      "KeyLabel":"String content",
      "KeyLengthBits":2147483647,
      "KeyType":2147483647,
      "OldKeyLabel":"String content",
      "OldKeySig":"String content",
      "OldPublicKey":"String content",
      "RemoveOldKey":true,
      "UpdateKeyReferences":true
   },
   "oScheduleInfo":{
      "DayOfMonth":2147483647,
      "DayOfWeek":2147483647,
      "DayOfYear":2147483647,
      "DaysBits":4294967295,
      "EveryNDays":2147483647,
      "Hours":2147483647,
      "Minutes":2147483647,
```

```
        "MonthOfYear":2147483647,
        "NextRetryTimeUTC":"\/Date(928167600000-0500)\/",
        "NumberOfRetries":2147483647,
        "Reboot":true,
        "RetryEnabled":true,
        "RunWindowMinutes":2147483647,
        "ScheduleType":0,
        "SchedulingPeriod":2147483647,
        "UpdateNextRunTimeForPartialCompletion":true
    }
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **AssociatedGroup:** Not used for this job type. Use when adding the target user to all systems in a management set.
- **Comment:** *(Optional)* Add a comment to the job.
- **CreatedBy:** Not used. Will always use the ID of the calling user, most likely that of the COM application identity.
- **CreationTimeUTC:** Not used.
- **JobID:** Not used. Success output will indicate JobID.
- **JobOperation:** Not used.
- **JobType:** Not used.
- **LastResult:** Not used.
- **LastRunTimeUTC:** Not used.
- **NextRunTimeUTC:** *(Optional)* Time to run the job. If left blank, job will be set to run at 00:00:00 (midnight, tonight). Expected format is Microsoft JSON, e.g. "/Date(MillisecondsSinceJan11970)/".
- **PullSystemsFromGroup:** Not used for this job type. Set to true to add the user to all systems in the management set targeted by AssociatedGroup.
- **RefreshGroupBeforeRun:** Not used for this job type. Set to true to cause the AssociatedGroup to be updated prior to job run.
- **RunJobOnNewSystems:** Not used for this job type. Set to true to run the job on new systems as they are added to the AssociatedGroup.
- **KeyLengthBits:** The length of the newly generated key. Values must be set to valid length for the key type, such as 2048, 3072, or 4096. If an invalid key size is set, the default value of 2048 bits will be used.
- **KeyType:** Not used.
- **OldKeyLabel:** Not used.
- **OldKeySig:** Not used.
- **OldPublicKey:** Not used.
- **UpdateReferences:** Set to $True to update allowed ssh key files on target systems by adding new key reference.
- **RemoveOldKey:** Set to $True to remove old ssh key references from target systems.
- **GenerateNewKeyEachRun:** When set to $True a new key is generated and stored/updated in the solution database on every run of the job, and does not perform any subsequent updates to target systems.
- **RemoveOldKeyFiles:** Set to $True to delete previous SSH keys left behind on target systems.
- **DayOfMonth:** Set the day of the month to run the job. Valid values are 1-31. For months with less than days than the day of the month defined (e.g. value is 30 but there is only 28 days in the month), the job will run on the last day of the month.

- **DayOfWeek:** *(Optional)* Set the day of the week to run the job on. Values are:
  - **0** = Sunday
  - **1** = Monday
  - **2** = Tuesday
  - **3** = Wednesday
  - **4** = Thursday
  - **5** = Friday
  - **6** = Saturday
- **DayOfYear:** Not used.
- **DaysBits:** Not used.
- **EveryNDays:** *(Optional)* Set the amount of days for the job to recur when ScheduleTypes is set to SCHEDULE_TYPE_N_DAYS.
- **Hours:** *(Optional)* Set the hour at which the job will run. Use a 24 hour clock.
- **Minutes:** *(Optional)* Set the minutes into the hour (Hours) when the job will run.
- **MonthOfYear:** *(Optional)* Set the month (number) for the job to run. Values are:
  - **1** = January
  - **2** = February
  - **3** = March
  - **4** = April
  - **5** = May
  - **6** = June
  - **7** = July
  - **8** = August
  - **9** = September
  - **10** = October
  - **11** = November
  - **12** = December
- **NextRetryUTC:** *(Optional)* For new jobs this value should not be used. Expected format is Microsoft JSON, e.g. "/Date (MillisecondsSinceJan11970)/".
- **NumberOfRetries:** *(Optional)* Set the number of retries for the job should it fail. If not defined, it will use the system default.
- **Reboot:** Not used for this job type.
- **RetryEnabled:** *(Optional)* Set to 1 to enable retries in the event of failure.
- **RunWindowMinutes:** *(Optional)* Set to value to 1 or more minutes to define the job must run by the specified time plus the run window duration or the job will be skipped. Set to 0 or do not define to indicate it should run despite missing the originally schedule time (default).
- **ScheduleType:** *(Optional)* Defines the type of schedule (one time, recurring, etc.) for the job. If not defined, default value is SCHEDULE_TYPE_INTERACTIVE which means it must be run by hand or will be run immediately based on other scheduling options. Valid values are:
  - **0** = SCHEDULE_TYPE_UNKNOWN
  - **1** = SCHEDULE_TYPE_IMMEDIATELY
  - **2** = SCHEDULE_TYPE_HOURLY - Job will be run once every hour. Set Minutes to define the offset into the hour.

- **3** = SCHEDULE_TYPE_DAILY- Job will be run once every day on the specified time. Set Hours and Minutes.
- **4** = SCHEDULE_TYPE_WEEKLY - Job will be run once every week on the specified day and time. Set Hours, Minutes and DayOfWeek.
- **5** = SCHEDULE_TYPE_MONTHLY - Job will be run once every month on the specified day and time. DayOfMonth, Hours, and Minutes.
- **6** = SCHEDULE_TYPE_YEARLY - Job will be run once every year on the specified month, day and time. Define DayOfMonth, MonthOfYear, Hours, and Minutes.
- **7** = SCHEDULE_TYPE_DAYS_OF_WEEK - Job will be run every set day of week. Set DayOfWeek.
- **8** = SCHEDULE_TYPE_ONCE - Job will be run once at some point in the future. Define DayOfMonth, MonthOfYear, Hours, and Minutes.
- **9** = SCHEDULE_TYPE_N_DAYS - Job will be run every N days. Set integer value for EveryNDays.
- **10** = SCHEDULE_TYPE_INTERACTIVE - Default. Job will be run based on NextRunTimeUTC.
- **11** = SCHEDULE_TYPE_N_HOURS - Job will be run every N hours. Set Hours for the number of hours and Minutes for the offset into each hour when the job will run.

- **SchedulingPeriod:** Not used.
- **UpdateNextRunTimeForPartialCompletion:** *(Optional)* Set to true to define job with multiple systems should update the next run time as seen in the management console display. Default value is false.

Example Request

```
{
   "AuthenticationToken":"O0E18VVM1PDS2DELU7LP3W547RIFOB5F",
   "JobInfo":{
      "Comment":"String content",
      "NextRunTimeUTC":"\/Date(928167600000-0500)\/"
   },
   "oKeyChangeSettings":{
      "DeleteKeyFileOnRemoteSystems":true,
      "GenerateNewKeyEachRun":true,
      "KeyLabel":"dbsmashlnx",
      "KeyLengthBits":4096,
      "RemoveOldKey":true,
      "UpdateKeyReferences":true
   },
   "oScheduleInfo":{
      "DayOfMonth":31,
      "Hours":17,
      "Minutes":16,
      "MonthOfYear":12,
      "NextRetryTimeUTC":"\/Date(928167600000-0500)\/",
      "NumberOfRetries":5,
      "RetryEnabled":true,
      "RunWindowMinutes":20,
      "ScheduleType":8,
      "UpdateNextRunTimeForPartialCompletion":true
   }
}
```

Output Success

The output message will indicate the new jobID.

Example Success Output

```
{
   "OperationMessage": "Created ssh key update job for key with label dbsmashlnx with JobID 1290",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
   <title>Request Error</title>
   <style>
      style_info_goes_here
   </style>
</head>
<body>
   <div id="content">
      <p class="heading1">Request Error</p>
      <p xmlns="">
         The server encountered an error processing the request. Please see the
         <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Invalid authentication
token or token not found'. See server logs for more details. The exception stack trace is:
      </p>
      <p>
         stack_trace_info_goes_here
      </p>
   </div>
</body>
</html>
```

REST: PropagationTargets ConfigurationData

This section defines any ConfigurationData requirements for each propagation target under **InputArgs\PasswordChangeSettings\PropagationTargets\ListTargets**.

The data varies by target and not all propagation targets have configuration data.

builtin:WindowsServices

Used for Windows services. If the Windows services should be restarted following update, set the ConfigurationData to:

```
"ConfigurationData": "<Settings CompactMode=\"1\"/>\r\n"
```

If the Windows services should NOT be restarted following update, set the ConfigurationData to:

```
"ConfigurationData": "<Settings CompactMode="1" m_bRestartServicesAfterUpdate=\"0\"/>/r/n"
```

builtin:WindowsScheduler

Used for Windows scheduled tasks. There is no ConfigurationData for this item.

builtin:WindowsSchedulerAtAccount

Used for Windows AT identity. There is no ConfigurationData for this item.

builtin:COMPlus

Used for Windows COM/MTS applications. There is no ConfigurationData for this item.

builtin:DCOM

Used for Windows DCOM applications. There is no ConfigurationData for this item.

builtin:IIS6Metabase

Used for Windows IIS6 (anonymous, app pool, network credentials). There is no ConfigurationData for this item.

builtin:IIS7ConfigFiles

Used for Windows IIS7 and later (anonymous, app pool, network credentials). There is no ConfigurationData for this item.

builtin:SCOM

Used for Microsoft SCOM RunAs accounts. There is no ConfigurationData for this item.

builtin:SqlServer

Used for SQL Server Credentials (not to be confused with SQL Server Logins). You must define the target named instance for the SQL Server credentials propagation in `m_sInstanceName`.

```
"ConfigurationData": "<Settings CompactMode=\"1\" m_sInstanceName=\"docs_sys\"/>\r\n"
```

builtin:NetConfig

Used for IIS asp.net connection strings. There is no ConfigurationData for this item.

builtin:ReplaceInFiles

Used for string replacement within files. The following ConfigurationData must be defined and set:

- **listFileTargetsForReplace:** Adds one entry for each file to search in the specific propagation and also defines:
  - **sLocalFilePath:** The double quoted path to the file to check for replacement. Path is local relative to target system.
  - **bCreateReferenceBackup:** Set to 1 to create a back of the original file and then define `sReferenceBackupFileFormatString`.
  - **sReferenceBackupFileFormatString:** The double quoted name of the backup file. Replaceable arguments are %filename% and %timestamp%. The default value is "Backup of %filename% (original)".
  - **bBackupExistingFile:** The default value is "0". Set to "1" to create multiple backups of the original file, up to `dwMaxNumberOfBackups`. You must also define bBackupFileFormatString for the secondary backup names. Replaceable arguments are %filename% and %timestamp%. The default value is "Backup of %filename% (original)". The default value is "Backup of %filename% at %timestamp%".
  - **dwMaxNumberOfBackups:** If multiple backups of the original file will be kept, define how many will be kept. The default value is "5".
  - **bReplaceTextFileExistingTypeOnly:** Set to "1" to use the native text file type to determine which text type to search for. Set to "0" to specify the text type. Then define `bReplaceASCII` and `bReplaceUnicode`.
  - **bReplaceASCII:** When `bReplaceTextFileExistingTypeOnly` is set to "0", set `bReplaceASCII` to "1" to search for ASCII text.
  - **bReplaceUNICODE:** When `bReplaceTextFileExistingTypeOnly` is set to "0", set `bReplaceUNICODE` to "1" to search for UNICODE text.
  - **bUseRegexSearch:** Set to "1" to use a regex search to find the old password and define the `sRegexSeach` parameter. Set to "0" to let Privileged Identity attempt to locate the previous password in the target files (password must have been previously managed/imported).
  - **sRegexBuilderString:** Set to an empty value, ""
  - **sRegexSearch:** The regex search pattern to use for the string replacement.
  - **dwSubExpressionNumber_Username:** Not used. Set to "0".
  - **dwSubExpressionNumber_Password:** Set to "1".
  - **dwSubExpressionNumber_Description:** Not used. Set to "0".

The following is an example ConfigurationData for a file called "/usr/bin/redoar/clpwd.py" that will perform a regex search for "password = (.*)":

```
"ConfigurationData": "<Settings CompactMode=\"1\" m_bOperationSupportsPropagation=\"1\" m_
sPropagationCommandLineApp=\"c:\\\\update\\\\updateme.exe\" m_
sPropagationCommandLineParams=\"%NewPassword% %OldUserName%\" m_
sPropagationCommandLineFormat=\"%Application% %Parameters%\" m_eRunLocation=\"2\" m_
eRemoteRunAsCredentialsType=\"2\" m_sRemoteRunAsExplicitUsername=\"demo\\\\bob\" m_
sRemoteRunAsExplicitPassword=\"/\\\\&quot;':;654\" m_bCopyDirectReferencedFiles=\"1\" m_
sFileCopyDestinationDirectory=\"c:\\\\update\" m_bCopyOtherFiles=\"1\"><m_listFilesToCopy
sSourceFilename=\"c:\\\\temp\\\\updateme.exe\"
sDestinationFilename=\"c:\\\\update\\\\updateme.exe\" dwFlags=\"0\"/></Settings>\r\n"
```

builtin:RunProcess

Used to run an arbitrary process. The following ConfigurationData must be defined and set:

- **listFileTargetsForReplace:** Adds one entry for each file to search in the specific propagation and also defines:
  - **m_bOperationSupportsPropagation:** Set to "1".
  - **m_sPropagationCommandLineApp:** Defines the path to the file to run on the target or local system. All forward and backslashes must be escaped by a backslash, e.g. `c:\temp\file.exe`. Should be written as `c:\\temp\\file.exe`.
  - **m_sPropagationCommandLineParams:** The replaceable arguments for the propagation. Valid values are:
    - **%AccountDomain%:** The domain of the account being changed.
    - **%OldUsername%:** The current username of the account being changed.
    - **%NewUsername%:** The new username of the account being changed if changing the account name.
    - **%OldPassword%:** The current password for the account being changed.
    - **%NewPassword%:** The new password for the account being changed.
    - **%System%:** The target system which the change is being propagated to as entered in Privileged Identity.
    - **%SystemNetName%:** The network name for the system which change is being propagated to.
  - **m_sPropagationCommandLineFormat:** Defines the order for processing the file name and its command line parameters. The recommended value is "%Application% %Parameters%".
  - **m_eRunLocation:** Defines the location to run the program from. Valid values are:
    - "1" - Run on the system performing the password change.
    - "2" - Run on the target system. If this value is set, you must also define `m_eRemoteRunAsCredentialsType`.
  - **m_eRemoteRunAsCredentialsType:** Defines which credentials to use to run the program when meRunLocation is set to "2". Valid Values are:
    - "2" - Run under explicitly defined credentials. You must also define `m_sRemoteRunAsExplicitUsername` and `m_sRemoteRunAsExplicitPassword`.
    - "3" - Run under the account used to connect to the system.
    - "4" - Run as the account being updates.
  - **m_sRemoteRunAsExplicitUsername:** When `m_eRemoteRunAsCredentialType` is set to "2", defines the username to run the process as. If supplying a pre-windows 2000 username, e.g. "demo\bob", supply the name escaped like "demo\\bob".
  - **m_sRemoteRunAsExplicitPassword:** When `m_eRemoteRunAsCredentialType` is set to "2", defines the password for the username the process will run as. Backslashes should be escaped with another backslash, e.g. "\\" and other special characters should be turned into their XML/HTML equivalents, for example, a double quote would be passed as "&quote;". This is typically automatically performed by the management console.
  - **m_bCopyDirectReferencedFiles:** Set to "1" to copy the target files from the source Privileged Identity machine to the target system. The file must exist in the exact same location on the source machine that it will be copied to on the target machines. If this value is set to "1", then you must also define `m_sFileCopyDestinationDirectory`.
  - **m_bCopyOtherFiles:** Set to "1" if you will wish to copy secondary files to the target system. Then define the `Settings/m_listFilesToCopy` section.
  - **m_ListFilesToCopy:** If `m_bCopyOtherFiles` is set to "1", define one or more entries for each secondary file to copy to the target system. Then define `sSourceFileName` and `sDestinationFileName`.

- **sSourceFileName:** The escaped path to the source file on the Privileged Identity host system.
- **sDestinationFileName:** The escaped path to the destination location on the target server (including target file name).
- **dwFlags:** Set to "0".

```
"ConfigurationData": "<Settings CompactMode=\"1\" m_bOperationSupportsPropagation=\"1\" m_
sPropagationCommandLineApp=\"c:\\\\update\\\\updateme.exe\" m_
sPropagationCommandLineParams=\"%NewPassword% %OldUserName%\" m_
sPropagationCommandLineFormat=\"%Application% %Parameters%\" m_eRunLocation=\"2\" m_
eRemoteRunAsCredentialsType=\"2\" m_sRemoteRunAsExplicitUsername=\"demo\\\\bob\" m_
sRemoteRunAsExplicitPassword=\"/\\\\&quot;':;654\" m_bCopyDirectReferencedFiles=\"1\" m_
sFileCopyDestinationDirectory=\"c:\\\\update\" m_bCopyOtherFiles=\"1\"><m_listFilesToCopy
sSourceFilename=\"c:\\\\temp\\\\updateme.exe\"
sDestinationFilename=\"c:\\\\update\\\\updateme.exe\" dwFlags=\"0\"/></Settings>\r\n"
```

builtin:Sharepoint

Used for Microsoft SharePoint server. There is no ConfigurationData for this item.

builtin:IBM WebSphere Application Server

Used to update IBM WebSphere Server where the target account matches an account name in WebSphere. If managing local WebSphere accounts, we recommend you manage IBM WebSphere directly.

If using this propagation type, the following ConfigurationData must be defined and set:

- **m_strDefaultPort:** (Optional) - Set the non-SSL port to connect to. Set `m_bUseSSL` to "0".
- **m_strSSLPort:** (Optional) - Set the SSL port to connect to. Set `m_bUseSSL` to "1".
- **m_bUseSSL:** Set to "1" to use SSL and define `m_strSSLPort`. Set to "0" to not use SSL and define `m_strDefaultPort`.
- **m_strLoginUser:** The login name of the user.
- **m_strLoginPassword:** The XML/HTML escaped password for the login user.

```
"ConfigurationData": "<Settings CompactMode=\"1\" m_strDefaultPort=\"9080\" m_strSSLPort=\"9443\"
m_bUseSSL=\"1\" m_strLoginUser=\"wsadmin\" m_strLoginPassword=\"P@ssw0rd\"/>\r\n"
```

builtin:Oracle WebLogic Server

Used to update Oracle WebLogic where the target account matches an account name in WebLogic. If managing local WebLogic accounts, we recommend you manage Oracle WebLogic directly.

If using this propagation type, the following ConfigurationData must be defined and set:

- **m_strDefaultPort:** (Optional) - Set the non-SSL port to connect to. Set `m_bUseSSL` to "0".
- **m_strSSLPort:** (Optional) - Set the SSL port to connect to. Set `m_bUseSSL` to "1".
- **m_bUseSSL:** (Optional) - Set to "1" to use SSL and define `m_strSSLPort`. Set to "0" to not use SSL and define `m_strDefaultPort`.
- **m_strLoginUser:** The login name of the user.
- **m_strLoginPassword:** The XML/HTML escaped password for the login user.

```
"ConfigurationData": "<Settings CompactMode=\"1\" m_strDefaultPort=\"8080\" m_strSSLPort=\"8443\"
m_bUseSSL=\"1\" m_strLoginUser=\"wladmin\" m_strLoginPassword=\"P@ssw0rd\"/>\r\n"
```

builtin:SAP Server

Used to update SAP local accounts where the target account matches an account name in SAP. If managing local SAP accounts, we recommend you manage the SAP instances directly.

If using this propagation type, the following ConfigurationData must be defined and set:

- **m_iSystemNumber:** Defines the system number you are connecting directly. If connecting using a gateway server, this value will be ignored.
- **m_strClient:** Defines your client number if you are connecting directly. If connecting using a gateway server, this value will be ignored.
- **m_strUser:** Defines the name of the management user to connect to SAP as.
- **m_strPassword:** Supplies the escaped value for the password to connect as.
- **m_blsGatewayServer:** Set to "1" to indicate the target SAP server is a gateway server and define `m_strPath`, `m_nPort` or `m_bSecurePortEnabled` and `m_nSecurePort`.
- **m_nPort:** The unsecured port to connect to if `m_bIsGatewayServer` is set to "1" and `m_bSecurePortEnabled` is set to "0". If `m_bSecurePortEnabled` is set to "1", or `m_bSecurePortEnabled` is set to "0", this value will be ignored.
- **m_bSecurePortEnabled:** Defines SSL to be used to connect through a Netweaver Gateway server if set to "1" and `m_bIsGatewayServer` is also set to "1".
- **m_nSecurePort:** The secured port to connect to if `m_bIsGatewayServer` is set to "1" and `m_bSecurePortEnabled` is set to "1". If `m_bSecurePortEnabled` is set to "0" or `m_bSecurePortEnabled` is set to "0", this value will be ignored.
- **m_strPath:** The path on the Netweaver server's URL to locate the Privileged Identity integration. This value is required if `m_bIsGatewayServer` is set to "1".

```
"ConfigurationData": "<Settings CompactMode=\"1\" m_iSystemNumber=\"1\" m_strClient=\"2\" m_
strUser=\"sap*\" m_strPassword=\"P@ssw0rd\" m_bIsGatewayServer=\"1\" m_nPort=\"55636\" m_
bSecurePortEnabled=\"1\" m_nSecurePort=\"65535\" m_strPath=\"/sap/opu/odata/LIEBSOFT/ERPM_USER_
MGMT\"/>\r\n"
```

builtin:UpdateLogonCache

Used for Windows logon cache. There is no ConfigurationData for this item.

builtin:UpdateAutoLogon

Windows automatic logon account. There is no ConfigurationData for this item.

builtin:SQLReportingServices

Used for Microsoft SQL Reporting Services Action Account. There is no ConfigurationData for this item.

REST: Job/RefreshAndDiscoverWindows (POST)

Job/SSHKeyChange creates a new SSH Key update job.

Permissions Required

- All Access

Related Commands

- **PowerShell:** New-LSJobWindowsRefreshAndDiscovery
- **SOAP:** JobOps_CreateRefreshWindowsSystemAndUsageJob

Syntax

```
{
   "AuthenticationToken":"String content",
   "JobInfoBase":{
      "AssociatedGroup":"String content",
      "Comment":"String content",
      "CreatedBy":"String content",
      "CreationTimeUTC":"\/Date(928167600000-0500)\/",
      "JobID":"String content",
      "JobOperation":0,
      "JobType":0,
      "LastResult":0,
      "LastRunTimeUTC":"\/Date(928167600000-0500)\/",
      "NextRunTimeUTC":"\/Date(928167600000-0500)\/",
      "PullSystemsFromGroup":true,
      "RefreshGroupBeforeRun":true,
      "RunJobOnNewSystems":true
   },
   "ScheduleInfo":{
      "DayOfMonth":2147483647,
      "DayOfWeek":2147483647,
      "DayOfYear":2147483647,
      "DaysBits":4294967295,
      "EveryNDays":2147483647,
      "Hours":2147483647,
      "Minutes":2147483647,
      "MonthOfYear":2147483647,
      "NextRetryTimeUTC":"\/Date(928167600000-0500)\/",
      "NumberOfRetries":2147483647,
      "Reboot":true,
      "RetryEnabled":true,
      "RunWindowMinutes":2147483647,
      "ScheduleType":0,
      "SchedulingPeriod":2147483647,
      "UpdateNextRunTimeForPartialCompletion":true
   },
   "SystemList":"String content"
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **AssociatedGroup:** Use when adding the target user to all systems in a management set.
- **Comment:** *(Optional)* Add a comment to the job.
- **CreatedBy:** Not used. Will always use the ID of the calling user, most likely that of the COM application identity.
- **CreationTimeUTC:** Not used.
- **JobID:** Not used. Success output will indicate JobID.
- **JobOperation:** Not used.
- **JobType:** Not used.
- **LastResult:** Not used.
- **LastRunTimeUTC:** Not used.
- **NextRunTimeUTC:** *(Optional)* Time to run the job. If left blank, job will be set to run at 00:00:00 (midnight, tonight). Expected format is Microsoft JSON, e.g. "/Date(MillisecondsSinceJan11970)/".
- **PullSystemsFromGroup:** Not used for this job type. Set to true to add the user to all systems in the management set targeted by AssociatedGroup.
- **RefreshGroupBeforeRun:** Not used for this job type. Set to true to cause the AssociatedGroup to be updated prior to job run.
- **RunJobOnNewSystems:** Set to true to run the job on new systems as they are added to the AssociatedGroup.
- **DayOfMonth:** *(Optional)* Set the day of the month to run the job. Valid values are 1-31. For months with less than days than the day of the month defined (e.g. value is 30 but there is only 28 days in the month), the job will run on the last day of the month.
- **DayOfWeek:** *(Optional)* Set the day of the week to run the job on. Values are:
    - **0** = Sunday
    - **1** = Monday
    - **2** = Tuesday
    - **3** = Wednesday
    - **4** = Thursday
    - **5** = Friday
    - **6** = Saturday
- **DayOfYear:** Not used.
- **DaysBits:** Not used.
- **EveryNDays:** *(Optional)* Set the amount of days for the job to recur when ScheduleTypes is set to SCHEDULE_TYPE_N_DAYS.
- **Hours:** *(Optional)* Set the hour at which the job will run. Use a 24 hour clock.
- **Minutes:** *(Optional)* Set the minutes into the hour (Hours) when the job will run.
- **MonthOfYear:** *(Optional)* Set the month (number) for the job to run. Values are:
    - **1** = January
    - **2** = February
    - **3** = March
    - **4** = April
    - **5** = May

  - **6** = June
  - **7** = July
  - **8** = August
  - **9** = September
  - **10** = October
  - **11** = November
  - **12** = December
- **NextRetryUTC:** *(Optional)* For new jobs this value should not be used. Expected format is Microsoft JSON, e.g. "/Date (MillisecondsSinceJan11970)/".
- **NumberOfRetries:** Sets the number of retries for the job should it fail. If not defined, it will use the system default.
- **Reboot:** Not used for this job type.
- **RetryEnabled:** *(Optional)* Set to 1 to enable retries in the event of failure.
- **RunWindowMinutes:** *(Optional)* Set to value to 1 or more minutes to define the job must run by the specified time plus the run window duration or the job will be skipped. Set to 0 or do not define to indicate it should run despite missing the originally schedule time (default).
- **ScheduleType:** *(Optional)* Defines the type of schedule (one time, recurring, etc.) for the job. If not defined, default value is SCHEDULE_TYPE_INTERACTIVE which means it must be run by hand or will be run immediately based on other scheduling options. Valid values are:
  - **0** = SCHEDULE_TYPE_UNKNOWN
  - **1** = SCHEDULE_TYPE_IMMEDIATELY
  - **2** = SCHEDULE_TYPE_HOURLY - Job will be run once every hour. Set Minutes to define the offset into the hour.
  - **3** = SCHEDULE_TYPE_DAILY- Job will be run once every day on the specified time. Set Hours and Minutes.
  - **4** = SCHEDULE_TYPE_WEEKLY - Job will be run once every week on the specified day and time. Set Hours, Minutes and DayOfWeek.
  - **5** = SCHEDULE_TYPE_MONTHLY - Job will be run once every month on the specified day and time. DayOfMonth, Hours, and Minutes.
  - **6** = SCHEDULE_TYPE_YEARLY - Job will be run once every year on the specified month, day and time. Define DayOfMonth, MonthOfYear, Hours, and Minutes.
  - **7** = SCHEDULE_TYPE_DAYS_OF_WEEK - Job will be run every set day of week. Set DayOfWeek.
  - **8** = SCHEDULE_TYPE_ONCE - Job will be run once at some point in the future. Define DayOfMonth, MonthOfYear, Hours, and Minutes.
  - **9** = SCHEDULE_TYPE_N_DAYS - Job will be run every N days. Set integer value for EveryNDays.
  - **10** = SCHEDULE_TYPE_INTERACTIVE - Default. Job will be run based on NextRunTimeUTC.
  - **11** = SCHEDULE_TYPE_N_HOURS - Job will be run every N hours. Set Hours for the number of hours and Minutes for the offset into each hour when the job will run.
- **SchedulingPeriod:** Not used.
- **UpdateNextRunTimeForPartialCompletion:** *(Optional)* Set to true to define job with multiple systems should update the next run time as seen in the management console display. The default value is false.
- **SystemList:** The target systems. If multiple systems are included, separate them by a semi-colon. For example: "system1;system2".

Example Request


```
{
   "AuthenticationToken":"String content",
   "JobInfoBase":{
      "AssociatedGroup":"String content",
      "Comment":"String content",
      "CreatedBy":"String content",
      "CreationTimeUTC":"\/Date(928167600000-0500)\/",
      "JobID":"String content",
      "JobOperation":0,
      "JobType":0,
      "LastResult":0,
      "LastRunTimeUTC":"\/Date(928167600000-0500)\/",
      "NextRunTimeUTC":"\/Date(928167600000-0500)\/",
      "PullSystemsFromGroup":true,
      "RefreshGroupBeforeRun":true,
      "RunJobOnNewSystems":true
   },
   "ScheduleInfo":{
      "DayOfMonth":2147483647,
      "DayOfWeek":2147483647,
      "DayOfYear":2147483647,
      "DaysBits":4294967295,
      "EveryNDays":2147483647,
      "Hours":2147483647,
      "Minutes":2147483647,
      "MonthOfYear":2147483647,
      "NextRetryTimeUTC":"\/Date(928167600000-0500)\/",
      "NumberOfRetries":2147483647,
      "Reboot":true,
      "RetryEnabled":true,
      "RunWindowMinutes":2147483647,
      "ScheduleType":0,
      "SchedulingPeriod":2147483647,
      "UpdateNextRunTimeForPartialCompletion":true
   },
   "SystemList":"String content"
}
```


Output Success

The output message will indicate the new jobID.

Example Success Output


```
{
   "OperationMessage": "Created refresh job for system lsdslscprd with JobID 1341",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
   <title>Request Error</title>
   <style>
      style_info_goes_here
   </style>
</head>
<body>
   <div id="content">
      <p class="heading1">Request Error</p>
      <p xmlns="">
         The server encountered an error processing the request. Please see the
         <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Invalid authentication
token or token not found'. See server logs for more details. The exception stack trace is:
      </p>
      <p>
         stack_trace_info_goes_here
      </p>
   </div>
</body>
</html>
```

REST: Job (DELETE)

Job deletes a particular job.

Permissions Required

- All Access

Related Commands

- **PowerShell:** Remove-LSJob
- **SOAP:** JobOps_DeleteJob

Syntax

```
https://serverName/ERPMWebService/AuthService.svc/REST/Job
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **JobID:** The ID of the job.

Example Request

```
{
   "AuthenticationToken":"JDPXWBIM1G6VK20Q5F9LAX6688BWG75N",
   "JobID":1341
}
```

Output Success

A successful run will return certain metadata about the job.

Example Success Output

```
{"OperationMessage":"Deleted job 1341","OperationSucceeded":true}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Non-existent JobID**

  The job specified could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'The job specified could
not be found'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Job/System (DELETE)

Job/System removes a system from a specific job.

Permissions Required

- Delegated control of the job.

Related Commands

- **PowerShell:** Remove-LSJobSystem
- **SOAP:** JobOps_RemoveSystemFromJob

Syntax

```
https://serverName/ERPMWebService/AuthService.svc/REST/Job/System
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **JobID:** The ID of the job.
- **SystemName:** The name of the system to remove from the job.

Example Request

```
{
   "AuthenticationToken":"RWFE7OLK5JQ5CA9J96ZUXCWCNLIIOBTX",
   "JobID":1343,
   "SystemName":"lsdslscprd"
}
```

Output Success

A successful run will return certain metadata about the job.

Example Success Output

```
{
   "OperationMessage": "Removed system lsdslscprd from job 1343",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid JobID**

  The job specified could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'The job specified could
not be found'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Job/WindowsElevation (PUT)

Job/WindowsElevation updates the elevation settings of an elevation job.

Permissions Required

- Elevate any account

Related Commands

- **PowerShell:** Set-LSJobAccountElevationSettings
- **SOAP:** JobOps_SetJobElevationSettings

Syntax

```
{
   "AuthenticationToken":"String content",
   "ElevationSettings":{
      "AccountElevatedState":0,
      "AccountNameToElevate":"String content",
      "DomainElevationGroup":"String content",
      "ElevateToDomainGlobalGroup":true,
      "ElevationGroup":"String content",
      "ExpirationEmailAddress":"String content",
      "ExpirationEmailMinutes":2147483647,
      "ExpirationEmailSent":true,
      "MinutesBeforeRemoval":2147483647,
      "MinutesBeforeRemovalGlobal":2147483647,
      "SendExpirationEmail":true,
      "SendFailureEmail":true,
      "SendSuccessEmail":true
   },
   "JobID":"String content"
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **AccountElevatedState:** For new jobs, this should always be 0 (NOT_ELEVATED) or not included.
- **AccountNameToElevate:** Target account to elevate. Format should be DomainName\\UserName.
- **DomainElevationGroup:** *(Optional)* Include this if the target account is being added to a global security group rather than a domain local group if the target system is a domain controller.
- **ElevateToDomainGlobalGroup:** Set to true if adding the user to a global security group, otherwise, set to false.
- **ElevationGroup:** *(Optional)* Include this if the target account is being added to a [domain] local group, rather than a global security group.
- **ExpirationEmailAddress:** Email address to send elevation expiration notice to.
- **ExpirationEmailMinutes:** *(Optional)* The number of minutes prior to the elevation expiring to send the user an email alert.
- **ExpirationEmailSent:** *(Optional)* For new jobs this should always be false.

- **MinutesBeforeRemoval:** *(Optional)* The amount of time in minutes to elevate the target account to a [domain] local group.
- **MinutesBeforeRemovalGlobal:** *(Optional)* The amount of time in minutes to elevate the target account to a global group.
- **SendExpirationEmail:** *(Optional)* Defaults to false if not set to true. If set to true, will send the email address a notification that the elevation is expiring.
- **SendFailureEmail:** *(Optional)* Set to true to send an email to the ExpirationEmail address if the account elevation fails.
- **SendSuccessEmail:** *(Optional)* Set to true to send an email to the ExpirationEmail address if the account elevation succeeds.
- **JobID:** Not used. Success output will indicate JobID.

Example Requests

* Be sure to use two backslashes "\\" for qualified account names.

Minimal Request to a [Domain] Local Group

```
{
   "AuthenticationToken":"YER36N0HIHG20YHB63Y0B212NFBXPONV",
   "ElevationSettings":{
      "AccountNameToElevate":"lsds\\fred",
      "ElevationGroup":"Administrators",
      "ExpirationEmailAddress":"fred@lsds.int",
      "ExpirationEmailMinutes":60,
      "ExpirationEmailSent":false,
      "MinutesBeforeRemoval":720,
      "SendExpirationEmail":true,
   },
   "SystemName":"lsdslscprd"
}
```

Minimal request to a Global Security Group

```
{
   "AuthenticationToken":"YER36N0HIHG20YHB63Y0B212NFBXPONV",
   "ElevationSettings":{
      "AccountNameToElevate":"lsds\\fred",
      "DomainElevationGroup":"CanRequest",
      "ElevateToDomainGlobalGroup":true,
      "ExpirationEmailAddress":"fred@lsds.int",
      "ExpirationEmailMinutes":60,
      "ExpirationEmailSent":true,
      "MinutesBeforeRemovalGlobal":720,
      "SendExpirationEmail":true,
   },
   "JobID":"1284"
}
```

Minimal Request to a [Domain] Local Group sending Email Notifications

```
{
   "AuthenticationToken":"8VL6RCV5SUS8JVH2YY436TZ5O0HP2UW4",
```

```
   "ElevationSettings":{
      "AccountElevatedState":0,
      "AccountNameToElevate":"lsds\\bucky",
      "ElevationGroup":"Administrators",
      "ExpirationEmailAddress":"bucky@lsds.int",
      "ExpirationEmailMinutes":20,
      "ExpirationEmailSent":false,
      "MinutesBeforeRemoval":240,
      "SendExpirationEmail":true,
      "SendFailureEmail":true,
      "SendSuccessEmail":true
   },
   "JobID":"1284"
}
```

Output Success

The output message will include the job ID.

Example Success Output

```
{
   "OperationMessage": "Updated elevation settings for job 1284",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Elevation duration too large**

  Value was either too large or too small for an Int32.

- **Elevation duration was longer than maximum allowed elevation duration**

  Elevation job could not be created, elevation duration (NNNNNN minutes) is longer than the maximum allowed (XXXX hours).

- **Non-existent JobID**

  The job specified could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
```

```
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
   <title>Request Error</title>
   <style>
      style_info_goes_here
   </style>
</head>
<body>
   <div id="content">
      <p class="heading1">Request Error</p>
      <p xmlns="">
         The server encountered an error processing the request. Please see the
         <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Elevation job could not be
created, elevation duration (777777 minutes) is longer than the maximum allowed (8760 hours)'. See
server logs for more details. The exception stack trace is:
      </p>
      <p>
         stack_trace_info_goes_here
      </p>
   </div>
</body>
</html>
```

REST: Job/WindowsElevation/Extend (POST)

Job/WindowsElevationExtend changes the de-elevation time, thereby extending or minimizing the elevation time of an account elevation job.

Permissions Required

- Elevate Any Account

Related Commands

- **PowerShell:** Set-LSJobAccountElevationExtension
- **SOAP:** JobOps_SetJobElevationExtension

Syntax

```
{
   "AuthenticationToken":"String content",
   "ElevationExtension":{
      "ExpirationUTC":"\/Date(928167600000-0500)\/",
      "ExtensionMinutes":2147483647
   },
   "JobID":"String content"
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **ExpirationUTC:** The exact date and time to de-elevate the user. Expected format is Microsoft JSON, e.g. "/Date (MillisecondsSinceJan11970)/".
- **ExpirationMinutes:** The number of minutes from now to add to the elevation duration.
- **JobID:** The ID of the target job to extend.

Example Requests

Set a Specific Date and Time for De-Elevation

```
{
   "AuthenticationToken":"3GHMPO3WP5XIDW3GH2YTQQIWYMJFQ8CZ",
   "ElevationExtension":{
      "ExpirationUTC":"\/Date(1501279200000)\/",
      "ExtensionMinutes":0
   },
   "JobID":"1284"
}
```

Add More Time (Minutes) from Now

```
{
   "AuthenticationToken":"3GHMPO3WP5XIDW3GH2YTQQIWYMJFQ8CZ",
   "ElevationExtension":{
      "ExtensionMinutes":240
   },
   "JobID":"1284"
}
```

Output Success

The output message will indicate the job was updated.

Example Success Output

```
{
   "OperationMessage": "Updated elevation expiration for job 1284",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid JobID**

  The job specified could not be found.

- **Elevation duration too large**

  Value was either too large or too small for an Int32.

- **Elevation duration was longer than maximum allowed elevation duration**

  Elevation job could not be created, elevation duration (NNNNNN minutes) is longer than the maximum allowed (XXXX hours).

Example Fail Output

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
   <title>Request Error</title>
   <style>
```

```
      style_info_goes_here
   </style>
</head>
<body>
   <div id="content">
      <p class="heading1">Request Error</p>
      <p xmlns="">
         The server encountered an error processing the request. Please see the
         <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Elevation job could not be
created, elevation duration (777777 minutes) is longer than the maximum allowed (8760 hours)'. See
server logs for more details. The exception stack trace is:
      </p>
      <p>
         stack_trace_info_goes_here
      </p>
   </div>
</body>
</html>
```

REST: Job/Comment (PUT)

Job/Comment replaces an existing job's comment or sets a new comment for a job. This comment will be visible in the web application and management console.

Permissions Required

- Delegated control of the job.

Related Commands

- **PowerShell:** Set-LSJobComment
- **SOAP:** JobOps_SetJobComment

Syntax

```
{
   "AuthenticationToken":"String content",
   "Comment":"String content",
   "JobID":"String content"
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **Comment:** The new comment to set for the job.
- **JobID:** The ID of the job.

Example Request

```
{
   "AuthenticationToken":"QF2M308GS98BPVGOOW7XUFZ7LRVKFIRT",
   "Comment":"Job Comments Are Helpful!",
   "JobID":"1284"
}
```

Output Success

The output states the job was updated successfully.

Example Success Output

```
{
   "OperationMessage": "Updated job comment for job 1284",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid JobID**

  The job could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'The job specified could
not be found'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Job/PasswordChange (PUT)

Job/PasswordChange allows full [re-]configuration of an existing password change job. For example, if a password change job was initially created as a Windows password change job or did not originally have propagation settings, this method can be used to reconfigure the job as a Linux or Oracle password change job and to add propagation settings.

IMPORTANT!

All password change settings must be defined. Settings not defined will be changed to default settings; existing settings will not be retained.

Permissions Required

- Delegated control of the job.

Related Commands

- **PowerShell:** Set-LSJobPasswordChangeSettings
- **SOAP:** JobOps_SetJobPasswordChangeSettings

Syntax

```
{
   "AuthenticationToken":"String content",
   "JobID":"String content",
   "PasswordChangeSettings":{
      "AccountComment":"String content",
      "AccountType":0,
      "AddMissing":true,
      "AddType":0,
      "CancelIfCheckedOut":true,
      "ChangeLoginAccount":true,
      "ChangeRootAccount":true,
      "ChangeTwice":true,
      "ClearAutoLogon":true,
      "ConfigFile":"String content",
      "ConnectionType":0,
      "CurrentPassword":"String content",
      "DisableAccountLockout":true,
      "DomainName":"String content",
      "EmailOnChange":"String content",
      "ExplicitPassword":"String content",
      "FirstCharacterSetBits":4294967295,
      "FullAccountName":"String content",
      "HostCodePage":2147483647,
      "KeepAccountLockedOutUntilComplete":true,
      "KeyLabel":"String content",
      "LastCharacterSetBits":4294967295,
      "LoginName":"String content",
```

```
"LoginPassword":"String content",
"MiddleCharactersSetBits":4294967295,
"MinLettersLcase":2147483647,
"MinLettersUcase":2147483647,
"MinNumbers":2147483647,
"MinSymbols":2147483647,
"NewAccountName":"String content",
"PasswordChangeType":0,
"PasswordCharacterSetBits":4294967295,
"PasswordCompatibilityLevel":0,
"PasswordConstraints":{
   "DefaultPasswordFilterCompliance":0,
   "ExplicitPassword":"String content",
   "FailGenerationOnMissingPassfiltDLL":true,
   "FirstCharacterSetBits":2147483647,
   "LastCharacterSetBits":2147483647,
   "MiddleCharactersSetBits":2147483647,
   "MinLettersLcase":2147483647,
   "MinLettersUcase":2147483647,
   "MinNumbers":2147483647,
   "MinSymbols":2147483647,
   "PasswordChangeType":0,
   "PasswordCharacterSetBits":2147483647,
   "PasswordCompatibilityLevel":0,
   "PasswordLength":2147483647,
   "PasswordSecurityOptions":2147483647,
   "PasswordSegments":2147483647,
   "PathToPassfiltDLL":"String content",
   "SymbolsExcludeProblematicWithAPIs":true,
   "SymbolsExcluded":"String content",
   "SymbolsSetOverride":"String content"
},
"PasswordLength":2147483647,
"PasswordPropagationSettings":{
   "ConstrainToManagedSystems":true,
   "ConstrainToMembersOfGroup":true,
   "ConstrainToSystemsWithNonzeroInUse":true,
   "ExcludeDomainControllers":true,
   "ExcludeSystemWithAccount":true,
   "GroupName":"String content",
   "PropagateToSystemWithAccountOnly":true,
   "PropagateToTrustingDomains":true
},
"PasswordPropagationTargets":{
   "ListTargets":[{
      "ConfigurationData":"String content",
      "DescriptiveName":"String content",
      "Enabled":true,
      "PasswordChangeJobID":2147483647,
      "RestrictBySystemSet":true,
      "SystemSet":"String content",
      "TargetSystemType_Linux":true,
      "TargetSystemType_Windows":true,
      "TypeName":"String content"
   }]
```

```
        },
        "PasswordSecurityOptions":4294967295,
        "PasswordSegments":2147483647,
        "PreventUsernameInPassword":true,
        "ReEnableAccountAfterSetTimeHours":true,
        "ReEnableAccountIfOperationFails":true,
        "RenameAccount":true,
        "SendEmailOnChange":true,
        "SerializedUtilityIDs":"String content",
        "StoredAccountName":"String content",
        "StoredNamespace":"String content",
        "StoredSystemName":"String content",
        "SymbolsSetOverride":"String content",
        "TerminalType":2147483647,
        "Unique":true,
        "UnlockAccount":true,
        "UpdateAutoLogon":true,
        "UpdatedAccountIsRootAccount":true,
        "UseSavedPasswords":true,
        "UseStoredLoginPassword":true
    }
}
```


Parameters

Job/PasswordChange has multiple sections. To aid in the description of the available parameters, the parameters will be divided into their respective sections.

- **AuthenticationToken:** The authentication token of the calling user.
- **JobID:** The ID of the target job.

/PasswordChangeSettings

- **AccountComment:** *(Optional)* The comment for the target managed account. This will be visible in the web application.
- **AccountType:** *(Optional)* For Windows password change jobs, this value identifies if you are targeting a Windows systems' built-in administrator, built-in guest, or a regular user, or if the job will target another platform such as SQL Server or IPMI. Valid values are:
    - **0** = ACCOUNT_TYPE_USER
    - **1** = ACCOUNT_TYPE_ADMINISTRATOR - set FullAccountName to *Administrator.
    - **2** = ACCOUNT_TYPE_GUEST - set FullAccountName to *Guest.
    - **3** = ACCOUNT_TYPE_SQLSERVER_SA_ACCOUNT
    - **4** = ACCOUNT_TYPE_LINUX_ACCOUNT
    - **5** = ACCOUNT_TYPE_CISCO_ROUTER
    - **6** = ACCOUNT_TYPE_AS400_ACCOUNT
    - **7** = ACCOUNT_TYPE_UNIX_ACCOUNT
    - **8** = ACCOUNT_TYPE_MYSQL_ACCOUNT
    - **9** = ACCOUNT_TYPE_ORACLE_ACCOUNT
    - **10** = ACCOUNT_TYPE_CUSTOM_ACCOUNT
    - **11** = ACCOUNT_TYPE_LDAP

  - **12** = ACCOUNT_TYPE_SYBASE
  - **13** = ACCOUNT_TYPE_OS390_ACCOUNT
  - **14** = ACCOUNT_TYPE_DRAC
  - **15** = ACCOUNT_TYPE_IPMI
  - **16** = ACCOUNT_TYPE_3270_ACCOUNT
  - **17** = ACCOUNT_TYPE_DSRM
- **AddMissing:** *(Optional)* For Windows password change job when AccountType is set to ACCOUNT_TYPE_USER, if the user does not exist, it can be added if the value is set to true.
- **AddType:** *(Optional)* For Windows password change jobs, set any of the following values if you will be creating the target account if it is missing (AddMissing must be set to true). This setting defines what group the missing user will be placed into on the target machine. Valid values are:
  - **0** = ACCOUNT_TYPE_GUEST
  - **1** = ACCOUNT_TYPE_USER
  - **2** = ACCOUNT_TYPE_ADMINISTRATOR
- **CancelIfCheckedOut:** *(Optional)* If set to true, the job will not run if the password is currently checked out to a user.
- **ChangeLoginAccount:** *(Optional)* For SSH-based jobs, sets the option to change the login account when set to true.
- **ChangeRootAccount:** *(Optional)* For SSH-based jobs, sets the option "login account is root" when set to true.
- **ChangeTwice:** *(Optional)* For Windows password change jobs, will spin the password for the target account twice when set to true.
- **ClearAutoLoginAccount:** *(Optional)* For Windows password change jobs, will remove the any configured automatic login account when set to true.
- **ConfigFile:** *(Optional)* This is used for database instance names and for SSH/Telnet-based jobs and defines the name (and possibly the path) for configuration response file to use for the password change process. For database jobs, this specifies the database instance/service name.
- **ConnectionType:** *(Optional)* For SSH/Telnet jobs, set the value to either 0 for SSH or 1 for TELNET.
- **CurrentPassword:** *(Optional)* For SSH/Telnet jobs, this is the password for the target account, if needed.
- **DisableAccountLockout:** Not used during job creation.
- **DomainName:** Not used during job creation.
- **EmailOnChange:** *(Optional)* Emails the clear text password to the target email address when SendEmailOnChange is set to true.
- **ExplicitPassword:** *(Optional)* Defines the password to set on the target account if setting a static password.
- **First Character set bits:** Defines the valid characters for the first character position. Values are cumulative, e.g. a value of 15 enables all possible character types. Possible values are:
  - **1** = Include upper case letters
  - **2** = Include lower case letters
  - **4** = Include numbers
  - **8** = Include symbols
- **FullAccountName:** Supplies the name of the target account. If running against the Windows built-in administrator or built-in guest, set the name to *Administrator or *Guest respectively.
- **HostCodePage:** Not used during job creation.

- **KeepAccountLockedOutUntilComplete:** *(Optional)* For Windows and Oracle database jobs, when UnlockAccount is set to true, this will clear the account lockout flag of the target account AFTER the password change and propagation completes when set to true. If not defined or set to false, the account will be unlocked as soon as the password change job begins.
- **KeyLabel:** *(Optional)* For SSH jobs, this identifies the SSH key to use for authentication.
- **LastCharacterSetBits:** Defines the valid characters for the last character position. Values are cumulative, e.g. a value of 15 enables all possible character types. Possible values are:
    - **1** = Include upper case letters
    - **2** = Include lower case letters
    - **4** = Include numbers
    - **8** = Include symbols
- **LoginName:** *(Optional)* For target systems that require a named login account, specify the name of the login account, such as SSH, Telnet, IPMI, jobs, etc.
- **LoginPassword:** *(Optional)* Defines the static login password for LoginName when the option UseSavedPasswords is set to false.
- **MiddleCharactersSetBits:** Defines the valid characters for the middle character position. Values are cumulative, e.g. a value of 15 enables all possible character types. Possible values are:
    - **1** = Include upper case letters
    - **2** = Include lower case letters
    - **4** = Include numbers
    - **8** = Include symbols
- **MinLettersLcase:** Defines the minimum number of lower case letters.
- **MinLettersUcase:** Defines the minimum number of upper case letters.
- **MinNumbers:** Defines the minimum number of numbers.
- **MinSymbols:** Defines the minimum number of symbols.
- **NewAccountName:** *(Optional)* For Windows password change jobs targeting the built-in administrator or guest, this defines the new name for the account.
- **PasswordChangeType:** Valid values are:
    - **0** = PWD_CHANGE_TYPE_GEN_RANDOM - Set a random password.
    - **1** = PWD_CHANGE_TYPE_EXPLICIT - Set a static password.
- **PasswordCharacterSetBits:** Defines the valid characters for the middle character position. Values are cumulative, e.g. a value of 15 enables all possible character types. Possible values are:
    - **1** = Include upper case letters
    - **2** = Include lower case letters
    - **4** = Include numbers
    - **8** = Include symbols
- **PasswordCompatibilityLevel:** Valid values are:
    - **0** = PWD_COMPAT_LAN_MANAGER - Sets LanMan compatible password constraints.
    - **1** = PWD_COMPAT_NT4 - Sets NT4 compatible password constraints.
    - **2** = PWD_COMPAT_W2K - Sets Windows 2000 and later compatible password constraints.
- **PasswordLength:** *(Optional)* The desired length for a random password. Use when setting a random password. The minimum length is 3 characters and the maximum length is limited based on PasswordCompatibilityLevel configuration.

Maximum values are:

- 14 characters when set to PWD_COMPAT_LAN_MANAGER or PWD_COMPAT_NT4.
- 127 characters when set to PWD_COMPAT_W2K.

- **PasswordSecurityOptions:** *(Optional)* Possible values are:
  - **1** = Symbol in middle
  - **2** = No repeated characters
  - **3** = Both symbol in middle and no repeated characters
- **PasswordSegments:** Defines how many segments the password will be broken into for later retrieval. Set to 1 store the password as 1 segment, meaning only one identity will be required to retrieve the whole password.
- **PreventUsernameInPassword:** For random passwords, set the value to true to ensure the username does not appear anywhere in a random password (statistically improbable!).
- **ReEnableAccountAfterSetTimeHours:** Not used.
- **ReEnableAccountIfOperationFails:** Not used.
- **RenameAccount:** For Windows password change jobs, set to true to rename the target account and define NewAccountName.
- **SendEmailOnChange:** *(Optional)* When set to true, this will send the password in clear text via email to the email address defined in EmailOnChange.
- **SerializedUtilityIDs:** For SSH/Telnet jobs, these are the IDs of the utility accounts that may be used as tertiary login credentials during the password change job. Multiple IDs are separated by a semi-colon, for example "1062;1064;15". The IDs are translated into utility account IDs in the answer file based on the order they are entered here. In the example above, 1062 would be utilityAccount_1.
- **StoredAccountName:** *(Optional)* For non-Windows password change jobs that will use a managed (and central account, e.g. from a directory), to login and change the target account. You must also specify StoredNameSpace and StoredSystemName. UseStoredLoginPassword must also be set to true.
- **StoredNamespace:** *(Optional)* For non-Windows password change jobs that will use a managed (and central account, e.g. from a directory), to login and change the target account. You must also specify StoredAccountName and StoredSystemName. UseStoredLoginPassword must also be set to true.
- **StoredSystemName:** *(Optional)* For non-Windows password change jobs that will use a managed (and central account, e.g. from a directory), to login and change the target account. You must also specify StoredNameSpace and StoredAccountName. UseStoredLoginPassword must also be set to true.
- **SymbolsSetOverride:** *(Optional)* When setting a random password, if desired, define the allowed special symbols for the random password. If not defined, all symbols will be allowed.
- **TerminalType:** Not used during job creation.
- **Unique:** Set to true to define the target account will get a unique random password, should multiple systems be defined in SystemsList. If set to false or not included and a random password is being set and multiple systems are included in SystemsList, the target account's password will be set the same across all target systems. Further, the account will be opted out of password re-randomization following password retrieval via the web application.
- **UnlockAccount:** *(Optional)* For Windows and Oracle database jobs, this will clear the account lockout flag of the target account when set to true.
- **UpdateAutoLogon:** *(Optional)* For Windows password change jobs, this will set the current account to be the automatic login account for the target systems.
- **UpdatedAccountIsRootAccount:** *(Optional)* For SSH/Telnet jobs, set to true when the target account is a root account.
- **UseSavedPasswords:** *(Optional)* For jobs that define a login account on the job, set to true when it is desired to use the stored password for the account. Set to false, when the password defined in the job, LoginPassword, should be used instead of any stored password.

- **UseStoredLoginPassword:** *(Optional)* For jobs that must use a login account on the job, set to true when it is desired to use a managed credential for the login account. You must also define StoredAccountName, StoredNameSpace, and StoredSystemName.

/PasswordChangeSettings/PasswordConstraints

Many items are derived from the PasswordChangeSettings previously defined. Listed below are the new items for which there is no duplicate PasswordChangeSettings element.

- **DefaultPasswordFilterCompliance:** Not used.
- **FailGenerationOnMissingPassfiltDLL:** *(Optional)* Set to false to avoid failing the job if a custom password filter is not defined or unavailable.
- **PathToPassfiltDLL:** *(Optional)* Set to empty value to avoid system trying to use a custom passfilt.dll password filter. Otherwise, define the absolute path the the custom password filter.
- **SymbolsExcludeProblematicWithAPIs:** *(Optional)* Set to true to avoid using symbols known to be problematic with scripts and APIs. These symbols include: /\:;'"
- **SymbolsExcluded:** Defines symbols to exclude from password change jobs.

/PasswordChangeSettings/PasswordPropagationSettings

PasswordPropagationSettings defines the scope of propagation. In other words, what systems will be targeted for password propagation once the password change is made successfully.

- **ConstrainToManagedSystems:** Set to true to limit the scope of propagation to only systems that are managed by Privileged Identity.
- **ConstrainToMembersOfGroup:** Set to true to limit propagation scope to the systems in a specific management set. You must also define the GroupName.
- **ConstrainToSystemsWithNonzeroInUse:** Not used.
- **ExcludeDomainControllers:** *(Optional)* Set to true to avoid attempting propagation of the new password to domain controllers which may otherwise be included in the propagation scope. ExcludeSystemWithAccount must also be set to true.
- **ExcludeSystemWithAccount:** *(Optional)* Set to true to avoid scanning of and attempted propagation to the system where the password was changed.
- **GroupName:** *(Optional)* If ConstraintoMembersOfGroup is set to true, define the management set to limit propagation scope to.
- **PropagateToSystemWithAccountOnly:** *(Optional)* Set to true to scan only the system where the account password was updated. E.g. a local system account where only the local system uses the account.
- **PropagateToTrustingDomains:** *(Optional)* Set to true to cause Privileged Identity to enumerate all trusting domains and attempt scanning and propagating to those trusting systems.

/PasswordChangeSettings/PropagationTargets/ListTargets

This defines what sub-systems to propagate to such as Windows Services, Scheduled Tasks, etc. Create zero or more repetitions of <PasswordPropagationTarget> for each target sub-system. Each propagation target will be wrapped in a <PasswordPropagationTarget> tag.

- **ConfigurationData:** *(Optional)* PropagationTargets ConfigurationData for more information on each propagation target type. This data varies by target. See REST.
- **DescriptiveName:** *(Optional)* A friendly name for the propagation type.
- **Enabled:** *(Optional)* Set to true to enable the propagation type for the job.

- **PasswordChangeJobID:** Not used.
- **RestrictBySystemSet:** *(Optional)* Set to true to limit the propagation type's scope to a specific list of systems. This is useful to ensure a certain type of propagation found on only a subset of systems included in the job's propagation scope are checked for a specific type of propagation. For example, if a job's propagation scope encompasses 1,000 systems,but only 10 of those systems run SharePoint, setting this option and defining SystemSet would configure the SharePoint propagation type to scan only those 10 systems if they were in their own management set.
- **SystemSet:** *(Optional)* Defines the name of a management set when RestrictBySystemSet is set to true.
- **TargetSystemType_Linux:** *(Optional)* Set to true to enable this propagation type for Linux systems (systems under the Linux/Unix node) included in the job's propagation scope.
- **TargetSystemType_Windows:** *(Optional)* Set to true to enable this propagation type for Windows systems included in the job's propagation scope.
- **TypeName:** *(Optional)* If configuring propagations, this value must be defined. Valid values are:
    - **builtin:WindowsServices:** Windows services.
    - **builtin:WindowsScheduler:** Windows scheduled tasks.
    - **builtin:WindowsSchedulerAtAccount:** Windows AT identity.
    - **builtin:COMPlus:** Windows COM.
    - **builtin:DCOM:** Windows DCOM.
    - **builtin:IIS6Metabase:** Windows IIS6 (anonymous, app pool, network credentials).
    - **builtin:IIS7ConfigFiles:** Windows IIS7 and later (anonymous, app pool, network credentials).
    - **builtin:SCOM:** Microsoft SCOM RunAs accounts.
    - **builtin:SqlServer:** SQL Server Credentials (not to be confused with SQL Server Logins).
    - **builtin:NetConfig:** IIS asp.net connection strings.
    - **builtin:ReplaceInFiles:** String replacement within files.
    - **builtin:RunProcess:** Run an arbitrary process.
    - **builtin:Sharepoint:** Microsoft SharePoint server.
    - **builtin:IBM WebSphere Application Server:** IBM WebSphere Server.
    - **builtin:Oracle WebLogic Server:** Oracle Web Logic Server.
    - **builtin:SAP Server:** SAP.
    - **builtin:UpdateLogonCache:** Windows logon cache.
    - **builtin:UpdateAutoLogon:** Windows automatic logon account.
    - **builtin:SQLReportingServices:** Microsoft SQL Reporting Services Action Account.

Example Request

Built-in Windows Administrator Account

The job will be set to target the built-in Windows administrator account, will change the password twice, be 20 characters long,clear the auto-login account, use all possible characters in each position, and will contain a minimum of 1 count of each character type.

```
{
   "AuthenticationToken":"YOMORP6VD3TUUCO68QE4MXC3GYWUWL45",
   "JobID":"1402",
   "PasswordChangeSettings":{
```

```
      "AccountComment":"builtin admin",
      "AccountType":1,
      "AddType":2,
      "CancelIfCheckedOut":true,
      "ChangeTwice":false,
      "FirstCharacterSetBits":15,
      "FullAccountName":"*Administrator",
      "LastCharacterSetBits":15,
      "MiddleCharactersSetBits":15,
      "MinLettersLcase":1,
      "MinLettersUcase":1,
      "MinNumbers":1,
      "MinSymbols":1,
      "PasswordChangeType":0,
      "PasswordCharacterSetBits":15,
      "PasswordCompatibilityLevel":2,
      "PasswordConstraints":{
         "FailGenerationOnMissingPassfiltDLL":false,
         "PathToPassfiltDLL":""
      },
      "PasswordLength":20,
      "PasswordSecurityOptions":3,
      "PasswordSegments":1,
      "PreventUsernameInPassword":true,
      "Unique":true
   }
}
```

Named Windows Account

The job will create a Windows account named firecall if needed and make it an administrator on systems included in the job, set the password to be 20 characters long,clear the auto-login account, use all possible characters in each position, and will contain a minimum of 1 count of each character type.

```
{
   "AuthenticationToken":"YOMORP6VD3TUUCO68QE4MXC3GYWUWL45",
   "JobID":"1402",
   "PasswordChangeSettings":{
      "AccountComment":"break the glass account",
      "AccountType":0,
      "AddType":2,
      "CancelIfCheckedOut":true,
      "ChangeTwice":false,
      "FirstCharacterSetBits":15,
      "FullAccountName":"firecall",
      "LastCharacterSetBits":15,
      "MiddleCharactersSetBits":15,
      "MinLettersLcase":1,
      "MinLettersUcase":1,
      "MinNumbers":1,
      "MinSymbols":1,
      "PasswordChangeType":0,
      "PasswordCharacterSetBits":15,
      "PasswordCompatibilityLevel":2,
```

```
      "PasswordConstraints":{
         "FailGenerationOnMissingPassfiltDLL":false,
         "PathToPassfiltDLL":""
      },
      "PasswordLength":20,
      "PasswordSecurityOptions":3,
      "PasswordSegments":1,
      "PreventUsernameInPassword":true,
      "Unique":true
   }
}
```

Oracle Password Change with Propagation to .Net Data Source Web Servers

The job will be set to manage an Oracle database account named oltpacct with a login account named redimsvcacct. The job will target a server called DBORA12c and the Oracle database service called orcl12c.lsds.int. The password will be set to 20 characters long and avoid problematic special characters, use all possible characters in each position and will contain a minimum of 1 count of each character type. The password will then be propagated to the IIS servers the "web Servers" management set.

```
{
   "AuthenticationToken":"YOMORP6VD3TUUCO68QE4MXC3GYWUWL45",
   "JobID":"1402",
   "PasswordChangeSettings":{
      "AccountComment":"OLTP DB Account",
      "AccountType":9,
      "CancelIfCheckedOut":true,
      "ChangeTwice":false,
      "ConfigFile":"orcl12c.lsds.int",
      "FirstCharacterSetBits":15,
      "FullAccountName":"oltpacct",
      "LastCharacterSetBits":15,
      "LoginName":"redimsvcacct",
      "MiddleCharactersSetBits":15,
      "MinLettersLcase":1,
      "MinLettersUcase":1,
      "MinNumbers":1,
      "MinSymbols":1,
      "PasswordChangeType":0,
      "PasswordCharacterSetBits":15,
      "PasswordCompatibilityLevel":2,
      "PasswordConstraints":{
         "FailGenerationOnMissingPassfiltDLL":false,
         "PathToPassfiltDLL":"",
         "SymbolsExcludeProblematicWithAPIs":true
      },
      "PasswordLength":20,
      "PasswordPropagationSettings":{
         "ConstrainToManagedSystems":false,
         "ConstrainToMembersOfGroup":true,
         "ConstrainToSystemsWithNonzeroInUse":false,
         "ExcludeDomainControllers":false,
         "ExcludeSystemWithAccount":false,
         "GroupName":"Web Servers",
         "PropagateToSystemWithAccountOnly":false,
```

```
            "PropagateToTrustingDomains":false
         },
         "PasswordPropagationTargets":{
            "ListTargets":[{
               "ConfigurationData":"",
               "DescriptiveName":"IIS Propagation",
               "Enabled":true,
               "RestrictBySystemSet":true,
               "SystemSet":"Web Servers",
               "TargetSystemType_Linux":false,
               "TargetSystemType_Windows":true,
               "TypeName":"builtin:NetConfig"
            }]
         },
         "PasswordSecurityOptions":3,
         "PasswordSegments":1,
         "PreventUsernameInPassword":false,
         "Unique":true,
         "UseSavedPasswords":true,
         "UseStoredLoginPassword":false
      }
   }
```

Output Success

The output message will indicate the job was updated successfully.

Example Success Output

```
{
   "OperationMessage": "Updated password change settings for job 1402",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid JobID**

  The job specified could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
```

```
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
   <title>Request Error</title>
   <style>
      style_info_goes_here
   </style>
</head>
<body>
   <div id="content">
      <p class="heading1">Request Error</p>
      <p xmlns="">
         The server encountered an error processing the request. Please see the
         <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Invalid authentication
token or token not found'. See server logs for more details. The exception stack trace is:
      </p>
      <p>
         stack_trace_info_goes_here
      </p>
   </div>
</body>
</html>
```

REST: PropagationTargets ConfigurationData

This section defines any ConfigurationData requirements for each propagation target under **InputArgs\PasswordChangeSettings\PropagationTargets\ListTargets**.

The data varies by target and not all propagation targets have configuration data.

builtin:WindowsServices

Used for Windows services. If the Windows services should be restarted following update, set the ConfigurationData to:

```
"ConfigurationData": "<Settings CompactMode=\"1\"/>\r\n"
```

If the Windows services should NOT be restarted following update, set the ConfigurationData to:

```
"ConfigurationData": "<Settings CompactMode="1" m_bRestartServicesAfterUpdate=\"0\"/>/r/n"
```

builtin:WindowsScheduler

Used for Windows scheduled tasks. There is no ConfigurationData for this item.

builtin:WindowsSchedulerAtAccount

Used for Windows AT identity. There is no ConfigurationData for this item.

builtin:COMPlus

Used for Windows COM/MTS applications. There is no ConfigurationData for this item.

builtin:DCOM

Used for Windows DCOM applications. There is no ConfigurationData for this item.

builtin:IIS6Metabase

Used for Windows IIS6 (anonymous, app pool, network credentials). There is no ConfigurationData for this item.

builtin:IIS7ConfigFiles - Windows IIS7 and later (anonymous, app pool, network credentials).

Used for Windows IIS7 and later (anonymous, app pool, network credentials). There is no ConfigurationData for this item.

builtin:SCOM

Used for Microsoft SCOM RunAs accounts. There is no ConfigurationData for this item.

builtin:SqlServer

Used for SQL Server Credentials (not to be confused with SQL Server Logins). You must define the target named instance for the SQL Server credentials propagation in `m_sInstanceName`.

```
"ConfigurationData": "<Settings CompactMode=\"1\" m_sInstanceName=\"docs_sys\"/>\r\n"
```

builtin:NetConfig

Used for IIS asp.net connection strings. There is no ConfigurationData for this item.

builtin:ReplaceInFiles

Used for string replacement within files. The following ConfigurationData must be defined and set:

- **listFileTargetsForReplace:** Adds one entry for each file to search in the specific propagation and also defines:
  - **sLocalFilePath:** The double quoted path to the file to check for replacement. Path is local relative to target system.
  - **bCreateReferenceBackup:** Set to 1 to create a back of the original file and then define `sReferenceBackupFileFormatString`.
  - **sReferenceBackupFileFormatString:** The double quoted name of the backup file. Replaceable arguments are %filename% and %timestamp%. The default value is "Backup of %filename% (original)".
  - **bBackupExistingFile:** The default value is "0". Set to "1" to create multiple backups of the original file, up to dwMaxNumberOfBackups. You must also define `bBackupFileFormatString` for the secondary backup names. Replaceable arguments are %filename% and %timestamp%. The default value is "Backup of %filename% (original)". The default value is "Backup of %filename% at %timestamp%".
  - **dwMaxNumberOfBackups:** If multiple backups of the original file will be kept, define how many will be kept. Default value is "5".
  - **bReplaceTextFileExistingTypeOnly:** Set to "1" to use the native text file type to determine which text type to search for. Set to "0" to specify the text type. Then define `bReplaceASCII` and `bReplaceUnicode`.
  - **bReplaceASCII:** When `bReplaceTextFileExistingTypeOnly` is set to "0", set `bReplaceASCII` to "1" to search for ASCII text.
  - **bReplaceUNICODE:** When `bReplaceTextFileExistingTypeOnly` is set to "0", set `bReplaceUNICODE` to "1" to search for UNICODE text.
  - **bUseRegexSearch:** Set to "1" to use a regex search to find the old password and define the `sRegexSeach` parameter. Set to "0" to let Privileged Identity attempt to locate the previous password in the target files (password must have been previously managed/imported).
  - **sRegexBuilderString:** Set to an empty value, ""
  - **sRegexSearch:** The regex search pattern to use for the string replacement.
  - **dwSubExpressionNumber_Username:** Not used. Set to "0".
  - **dwSubExpressionNumber_Password:** Set to "1".
  - **dwSubExpressionNumber_Description:** Not used. Set to "0".

The following is an example ConfigurationData for a file called "/usr/bin/redoar/clpwd.py" that will perform a regex search for "password = (.*)":

```
"ConfigurationData": "<Settings CompactMode=\"1\" m_bOperationSupportsPropagation=\"1\" m_
sPropagationCommandLineApp=\"c:\\\\update\\\\updateme.exe\" m_
sPropagationCommandLineParams=\"%NewPassword% %OldUserName%\" m_
sPropagationCommandLineFormat=\"%Application% %Parameters%\" m_eRunLocation=\"2\" m_
eRemoteRunAsCredentialsType=\"2\" m_sRemoteRunAsExplicitUsername=\"demo\\\\bob\" m_
sRemoteRunAsExplicitPassword=\"/\\\\&quot;':;654\" m_bCopyDirectReferencedFiles=\"1\" m_
sFileCopyDestinationDirectory=\"c:\\\\update\" m_bCopyOtherFiles=\"1\"><m_listFilesToCopy
sSourceFilename=\"c:\\\\temp\\\\updateme.exe\"
sDestinationFilename=\"c:\\\\update\\\\updateme.exe\" dwFlags=\"0\"/></Settings>\r\n"
```

builtin:RunProcess

Used to run an arbitrary process. The following ConfigurationData must be defined and set:

- **listFileTargetsForReplace:** Adds one entry for each file to search in the specific propagation and also defines:
  - **m_bOperationSupportsPropagation:** Set to "1".
  - **m_sPropagationCommandLineApp:** Defines the path to the file to run on the target or local system. All forward and backslashes must be escaped by a backslash, e.g. `c:\temp\file.exe`. Should be written as `c:\\temp\\file.exe`.
  - **m_sPropagationCommandLineParams:** The replaceable arguments for the propagation. Valid values are:
    - **%AccountDomain%:** The domain of the account being changed.
    - **%OldUsername%:** The current username of the account being changed.
    - **%NewUsername%:** The new username of the account being changed if changing the account name.
    - **%OldPassword%:** The current password for the account being changed.
    - **%NewPassword%:** The new password for the account being changed.
    - **%System%:** The target system which the change is being propagated to as entered in Privileged Identity.
    - **%SystemNetName%:** The network name for the system which change is being propagated to.
  - **m_sPropagationCommandLineFormat:** Defines the order for processing the file name and its command line parameters. Recommended value is "%Application% %Parameters%".
  - **m_eRunLocation:** Defines the location to run the program from. Valid values are:
    - "1" - Run on the system performing the password change.
    - "2" - Run on the target system. If this value is set, you must also define `m_eRemoteRunAsCredentialsType`.
  - **m_eRemoteRunAsCredentialsType:** Defines which credentials to use to run the program when meRunLocation is set to "2". Valid Values areL
    - "2" - Run under explicitly defined credentials. You must also define `m_sRemoteRunAsExplicitUsername` and `m_sRemoteRunAsExplicitPassword`.
    - "3" - Run under the account used to connect to the system.
    - "4" - Run as the account being updated.
  - **m_sRemoteRunAsExplicitUsername:** When `m_eRemoteRunAsCredentialType` is set to "2", defines the username to run the process as. If supplying a pre-windows 2000 username, e.g. "demo\bob", supply the name escaped like "demo\\bob".
  - **m_sRemoteRunAsExplicitPassword:** When `m_eRemoteRunAsCredentialType` is set to "2", defines the password for the username the process will run as. backslashes should be escaped with another backslash, e.g. "\\" and other special characters should be turned into their XML/HTML equivalents, for example, a double quote would be passed as "&quote;". This is typically automatically performed by the management console.
  - **m_bCopyDirectReferencedFiles:** Set to "1" to copy the target files from the source Privileged Identity machine to the target system. The file must exist in the exact same location on the source machine that it will be copied to on the target machines. If this value is set to "1", then you must also define `m_sFileCopyDestinationDirectory`.
  - **m_bCopyOtherFiles:** Set to "1" if you will wish to copy secondary files to the target system. Then define the `Settings/m_listFilesToCopy` section.
  - **m_ListFilesToCopy:** If `m_bCopyOtherFiles` is set to "1", define one or more entries for each secondary file to copy to the target system. Then define `sSourceFileName` and `sDestinationFileName`.

- **sSourceFileName:** The escaped path to the source file on the Privileged Identity host system.
- **sDestinationFileName:** The escaped path to the destination location on the target server (including target file name).
- **dwFlags:** Set to "0"

```
"ConfigurationData": "<Settings CompactMode=\"1\" m_bOperationSupportsPropagation=\"1\" m_
sPropagationCommandLineApp=\"c:\\\\update\\\\updateme.exe\" m_
sPropagationCommandLineParams=\"%NewPassword% %OldUserName%\" m_
sPropagationCommandLineFormat=\"%Application% %Parameters%\" m_eRunLocation=\"2\" m_
eRemoteRunAsCredentialsType=\"2\" m_sRemoteRunAsExplicitUsername=\"demo\\\\bob\" m_
sRemoteRunAsExplicitPassword=\"/\\\\&quot;':;654\" m_bCopyDirectReferencedFiles=\"1\" m_
sFileCopyDestinationDirectory=\"c:\\\\update\" m_bCopyOtherFiles=\"1\"><m_listFilesToCopy
sSourceFilename=\"c:\\\\temp\\\\updateme.exe\"
sDestinationFilename=\"c:\\\\update\\\\updateme.exe\" dwFlags=\"0\"/></Settings>\r\n"
```

builtin:Sharepoint

Used for Microsoft SharePoint server. There is no ConfigurationData for this item.

builtin:IBM WebSphere Application Server

Used to update IBM WebSphere Server where the target account matches an account name in WebSphere. If managing local WebSphere accounts, it is recommended to manage IBM WebSphere directly.

If using this propagation type, the following ConfigurationData must be defined and set:

- **m_strDefaultPort:** *(Optional)* Set the non-SSL port to connect to. Set `m_bUseSSL` to "0".
- **m_strSSLPort:** *(Optional)* Set the SSL port to connect to. Set `m_bUseSSL` to "1".
- **m_bUseSSL:** Set to "1" to use SSL and define `m_strSSLPort`. Set to "0" to not use SSL and define `m_strDefaultPort`.
- **m_strLoginUser:** The login name of the user.
- **m_strLoginPassword:** The XML/HTML escaped password for the login user.

```
"ConfigurationData": "<Settings CompactMode=\"1\" m_strDefaultPort=\"9080\" m_strSSLPort=\"9443\"
m_bUseSSL=\"1\" m_strLoginUser=\"wsadmin\" m_strLoginPassword=\"P@ssw0rd\"/>\r\n"
```

builtin:Oracle WebLogic Server

Used to update Oracle WebLogic where the target account matches an account name in WebLogic. If managing local WebLogic accounts, it is recommended to manage Oracle WebLogic directly.

If using this propagation type, the following ConfigurationData must be defined and set:

- **m_strDefaultPort:** *(Optional)* Set the non-SSL port to connect to. Set `m_bUseSSL` to "0".
- **m_strSSLPort:** *(Optional)* Set the SSL port to connect to. Set `m_bUseSSL` to "1".
- **m_bUseSSL:** *(Optional)* Set to "1" to use SSL and define `m_strSSLPort`. Set to "0" to not use SSL and define `m_strDefaultPort`.
- **m_strLoginUser:** The login name of the user.
- **m_strLoginPassword:** The XML/HTML escaped password for the login user.

```
"ConfigurationData": "<Settings CompactMode=\"1\" m_strDefaultPort=\"8080\" m_strSSLPort=\"8443\"
m_bUseSSL=\"1\" m_strLoginUser=\"wladmin\" m_strLoginPassword=\"P@ssw0rd\"/>\r\n"
```

builtin:SAP Server

Used to update SAP local accounts where the target account matches an account name in SAP. If managing local SAP accounts, it is recommended to manage the SAP instances directly.

If using this propagation type, the following ConfigurationData must be defined and set:

- **m_iSystemNumber:** Defines the system number you are connecting directly. If connecting using a gateway server, this value will be ignored.
- **m_strClient:** Defines your client number if you are connecting directly. If connecting using a gateway server, this value will be ignored.
- **m_strUser:** Defines the name of the management user to connect to SAP as.
- **m_strPassword:** Supplies the escaped value for the password to connect as.
- **m_blsGatewayServer:** Set to "1" to indicate the target SAP server is a gateway server and define `m_strPath`, `m_nPort` or `m_bSecurePortEnabled` and `m_nSecurePort`.
- **m_nPort:** The unsecured port to connect to if `m_bIsGatewayServer` is set to "1" and `m_bSecurePortEnabled` is set to "0". If `m_bSecurePortEnabled` is set to "1", or `m_bSecurePortEnabled` is set to "0", this value will be ignored.
- **m_bSecurePortEnabled:** Defines that SSL will be used to connect through a Netweaver Gateway server if set to "1" and `m_bIsGatewayServer` is also set to "1".
- **m_nSecurePort:** The secured port to connect to if `m_bIsGatewayServer` is set to "1" and `m_bSecurePortEnabled` is set to "1". If `m_bSecurePortEnabled` is set to "0" or `m_bSecurePortEnabled` is set to "0", this value will be ignored.
- **m_strPath:** The path on the Netweaver server's URL to locate the Privileged Identity integration. This value is required if `m_bIsGatewayServer` is set to "1".

```
"ConfigurationData": "<Settings CompactMode=\"1\" m_iSystemNumber=\"1\" m_strClient=\"2\" m_
strUser=\"sap*\" m_strPassword=\"P@ssw0rd\" m_bIsGatewayServer=\"1\" m_nPort=\"55636\" m_
bSecurePortEnabled=\"1\" m_nSecurePort=\"65535\" m_strPath=\"/sap/opu/odata/LIEBSOFT/ERPM_USER_
MGMT\"/>\r\n"
```

builtin:UpdateLogonCache

Used for Windows logon cache. There is no ConfigurationData for this item.

builtin:UpdateAutoLogon

Windows automatic logon account. There is no ConfigurationData for this item.

builtin:SQLReportingServices

Used for Microsoft SQL Reporting Services Action Account. There is no ConfigurationData for this item.

REST: Job/SpinPassword (POST)

Job/SpinPassword generates a new password randomization job. When using this function via PowerShell, almost every value is hard coded and cannot be changed. When calling this method directly, the available functionality is almost identical to "REST: Job/PasswordChange (PUT)" on page 1 and "REST: Job/PasswordChange (POST)" on page 1, which allows full configuration of a job and its settings. The important distinction is that this will not use a JobID as input as it is creating a new job and cannot specifically define a schedule, but it will define a job which runs once, N minutes from now against a target system.

Permissions Required

- All Access

Related Commands

- **PowerShell:** Set-LSJobPasswordSpin
- **SOAP:** JobOps_SpinPassword

Syntax

```
{
   "AuthenticationToken":"String content",
   "MinutesUntilSpin":2147483647,
   "PasswordChangeSettings":{
      "AccountComment":"String content",
      "AccountType":0,
      "AddMissing":true,
      "AddType":0,
      "CancelIfCheckedOut":true,
      "ChangeLoginAccount":true,
      "ChangeRootAccount":true,
      "ChangeTwice":true,
      "ClearAutoLogon":true,
      "ConfigFile":"String content",
      "ConnectionType":0,
      "CurrentPassword":"String content",
      "DisableAccountLockout":true,
      "DomainName":"String content",
      "EmailOnChange":"String content",
      "ExplicitPassword":"String content",
      "FirstCharacterSetBits":4294967295,
      "FullAccountName":"String content",
      "HostCodePage":2147483647,
      "KeepAccountLockedOutUntilComplete":true,
      "KeyLabel":"String content",
      "LastCharacterSetBits":4294967295,
      "LoginName":"String content",
      "LoginPassword":"String content",
      "MiddleCharactersSetBits":4294967295,
      "MinLettersLcase":2147483647,
      "MinLettersUcase":2147483647,
      "MinNumbers":2147483647,
      "MinSymbols":2147483647,
```

```
"NewAccountName":"String content",
"PasswordChangeType":0,
"PasswordCharacterSetBits":4294967295,
"PasswordCompatibilityLevel":0,
"PasswordConstraints":{
   "DefaultPasswordFilterCompliance":0,
   "ExplicitPassword":"String content",
   "FailGenerationOnMissingPassfiltDLL":true,
   "FirstCharacterSetBits":2147483647,
   "LastCharacterSetBits":2147483647,
   "MiddleCharactersSetBits":2147483647,
   "MinLettersLcase":2147483647,
   "MinLettersUcase":2147483647,
   "MinNumbers":2147483647,
   "MinSymbols":2147483647,
   "PasswordChangeType":0,
   "PasswordCharacterSetBits":2147483647,
   "PasswordCompatibilityLevel":0,
   "PasswordLength":2147483647,
   "PasswordSecurityOptions":2147483647,
   "PasswordSegments":2147483647,
   "PathToPassfiltDLL":"String content",
   "SymbolsExcludeProblematicWithAPIs":true,
   "SymbolsExcluded":"String content",
   "SymbolsSetOverride":"String content"
},
"PasswordLength":2147483647,
"PasswordPropagationSettings":{
   "ConstrainToManagedSystems":true,
   "ConstrainToMembersOfGroup":true,
   "ConstrainToSystemsWithNonzeroInUse":true,
   "ExcludeDomainControllers":true,
   "ExcludeSystemWithAccount":true,
   "GroupName":"String content",
   "PropagateToSystemWithAccountOnly":true,
   "PropagateToTrustingDomains":true
},
"PasswordPropagationTargets":{
   "ListTargets":[{
      "ConfigurationData":"String content",
      "DescriptiveName":"String content",
      "Enabled":true,
      "PasswordChangeJobID":2147483647,
      "RestrictBySystemSet":true,
      "SystemSet":"String content",
      "TargetSystemType_Linux":true,
      "TargetSystemType_Windows":true,
      "TypeName":"String content"
   }]
},
"PasswordSecurityOptions":4294967295,
"PasswordSegments":2147483647,
"PreventUsernameInPassword":true,
"ReEnableAccountAfterSetTimeHours":true,
"ReEnableAccountIfOperationFails":true,
```

```
        "RenameAccount":true,
        "SendEmailOnChange":true,
        "SerializedUtilityIDs":"String content",
        "StoredAccountName":"String content",
        "StoredNamespace":"String content",
        "StoredSystemName":"String content",
        "SymbolsSetOverride":"String content",
        "TerminalType":2147483647,
        "Unique":true,
        "UnlockAccount":true,
        "UpdateAutoLogon":true,
        "UpdatedAccountIsRootAccount":true,
        "UseSavedPasswords":true,
        "UseStoredLoginPassword":true
    },
    "StoredCredential":{
        "AccountName_FullyQualified":"String content",
        "AccountSupplementaryData":{
            "Flag_AccountDisabled":true,
            "Flag_AccountLocked":true,
            "Flag_PasswordCantChange":true,
            "Flag_PasswordExpired":true,
            "Flag_PasswordNotRequired":true,
            "PasswordAge":"P428DT10H30M12.3S"
        },
        "Comment":"String content",
        "CredentialType":0,
        "IsSecretDataInStore":true,
        "IsSetToSpin":true,
        "LastSetTimeUTC":"String content",
        "ManagementStatusData":{
            "CheckedOutToUser":"String content",
            "PasswordCheckedOut":true
        },
        "Password":"String content",
        "RowID":2147483647,
        "SupplementaryData_ePO":{
            "AccessToAccountCredentials":true,
            "AccountDisabled":true,
            "AccountLocked":true,
            "Managed":true,
            "PasswordAge":4294967295,
            "PasswordCantChange":true,
            "PasswordNotRequired":true,
            "Passwordexpire":true
        },
        "SystemName":"String content",
        "Username":"String content"
    }
}
```


Parameters

Job/PasswordChange has multiple sections. To aid in the description of the available parameters, the parameters will be divided into their respective sections.

/

- **AuthenticationToken:** The authentication token of the calling user.
- **JobID:** The ID of the target job.

/PasswordChangeSettings

- **AccountComment:** *(Optional)* The comment for the target managed account. This will be visible in the web application.
- **AccountType:** *(Optional)* For Windows password change jobs, this value identifies if you are targeting a Windows systems' built-in administrator, built-in guest, or a regular user, or if the job will target another platform such as SQL Server or IPMI. Valid values are:
  - **0** = ACCOUNT_TYPE_USER
  - **1** = ACCOUNT_TYPE_ADMINISTRATOR - set FullAccountName to *Administrator.
  - **2** = ACCOUNT_TYPE_GUEST - set FullAccountName to *Guest.
  - **3** = ACCOUNT_TYPE_SQLSERVER_SA_ACCOUNT
  - **4** = ACCOUNT_TYPE_LINUX_ACCOUNT
  - **5** = ACCOUNT_TYPE_CISCO_ROUTER
  - **6** = ACCOUNT_TYPE_AS400_ACCOUNT
  - **7** = ACCOUNT_TYPE_UNIX_ACCOUNT
  - **8** = ACCOUNT_TYPE_MYSQL_ACCOUNT
  - **9** = ACCOUNT_TYPE_ORACLE_ACCOUNT
  - **10** = ACCOUNT_TYPE_CUSTOM_ACCOUNT
  - **11** = ACCOUNT_TYPE_LDAP
  - **12** = ACCOUNT_TYPE_SYBASE
  - **13** = ACCOUNT_TYPE_OS390_ACCOUNT
  - **14** = ACCOUNT_TYPE_DRAC
  - **15** = ACCOUNT_TYPE_IPMI
  - **16** = ACCOUNT_TYPE_3270_ACCOUNT
  - **17** = ACCOUNT_TYPE_DSRM
- **AddMissing:** *(Optional)* For Windows password change job when AccountType is set to ACCOUNT_TYPE_USER, if the user does not exist, it can be added if the value is set to true.
- **AddType:** *(Optional)* For Windows password change jobs, set any of the following values if you will be creating the target account if it is missing (AddMissing must be set to true). This setting defines what group the missing user will be placed into on the target machine. Valid values are:
  - **0** = ACCOUNT_TYPE_GUEST
  - **1** = ACCOUNT_TYPE_USER
  - **2** = ACCOUNT_TYPE_ADMINISTRATOR
- **CancelIfCheckedOut:** *(Optional)* If set to true, the job will not run if the password is currently checked out to a user.
- **ChangeLoginAccount:** *(Optional)* For SSH-based jobs, sets the option to change the login account when set to true.
- **ChangeRootAccount:** *(Optional)* For SSH-based jobs, sets the option "login account is root" when set to true.
- **ChangeTwice:** *(Optional)* For Windows password change jobs, will spin the password for the target account twice when set to true.

- **ClearAutoLoginAccount:** *(Optional)* For Windows password change jobs, will remove the any configured automatic login account when set to true.
- **ConfigFile:** *(Optional)* This is used for database instance names and for SSH/Telnet-based jobs, this defines the name (and possibly the path) for configuration response file to use for the password change process. For database jobs, this specifies the database instance/service name.
- **ConnectionType:** *(Optional)* For SSH/Telnet jobs, set the value to either 0 for SSH or 1 for TELNET.
- **CurrentPassword:** *(Optional)* For SSH/Telnet jobs, this is the password for the target account, if needed.
- **DisableAccountLockout:** Not used during job creation.
- **DomainName:** Not used during job creation.
- **EmailOnChange:** *(Optional)* Will email the clear text password to the target email address when SendEmailOnChange is set to true.
- **ExplicitPassword:** *(Optional)* Defines the password to set on the target account if setting a static password.
- **First Character set bits:** Defines the valid characters for the first character position. Values are cumulative, e.g. a value of 15 enables all possible character types. Possible values are:
    - **1** = include upper case letters
    - **2** = include lower case letters
    - **4** = include numbers
    - **8** = include symbols
- **FullAccountName:** Supplies the name of the target account. If running against the Windows built-in administrator or built-in guest, set the name to *Administrator or *Guest respectively.
- **HostCodePage:** Not used during job creation.
- **KeepAccountLockedOutUntilComplete:** *(Optional)* For Windows and Oracle database jobs, when UnlockAccount is set to true, this will clear the account lockout flag of the target account AFTER the password change and propagation completes when set to true. If not defined or set to false, the account will be unlocked as soon as the password change job begins.
- **KeyLabel:** *(Optional)* For SSH jobs, this identifies the SSH key to use for authentication.
- **LastCharacterSetBits:** Defines the valid characters for the last character position. Values are cumulative, e.g. a value of 15 enables all possible character types. Possible values are:
    - **1** = include upper case letters
    - **2** = include lower case letters
    - **4** = include numbers
    - **8** = include symbols
- **LoginName:** *(Optional)* For target systems that require a named login account, specify the name of the login account, such as SSH, Telnet, IPMI, jobs, etc.
- **LoginPassword:** *(Optional)* Defines the static login password for LoginName when the option UseSavedPasswords is set to false.
- **MiddleCharactersSetBits:** Defines the valid characters for the middle character position. Values are cumulative, e.g. a value of 15 enables all possible character types. Possible values are:
    - **1** = include upper case letters
    - **2** = include lower case letters
    - **4** = include numbers
    - **8** = include symbols
- **MinLettersLcase:** Defines the minimum number of lower case letters.

- **MinLettersUcase:** Defines the minimum number of upper case letters.
- **MinNumbers:** Defines the minimum number of numbers.
- **MinSymbols:** Defines the minimum number of symbols.
- **NewAccountName:** *(Optional)* For Windows password change jobs targeting the built-in administrator or guest, this defines the new name for the account.
- **PasswordChangeType:** Valid values are:
  - **0** = PWD_CHANGE_TYPE_GEN_RANDOM - Set a random password.
  - **1** = PWD_CHANGE_TYPE_EXPLICIT - Set a static password.
- **PasswordCharacterSetBits:** Defines the valid characters for the middle character position. Values are cumulative, e.g. a value of 15 enables all possible character types. Possible values are:
  - **1** = Include upper case letters
  - **2** = Include lower case letters
  - **4** = Include numbers
  - **8** = Include symbols
- **PasswordCompatibilityLevel:** Valid values are:
  - **0** = PWD_COMPAT_LAN_MANAGER - Sets LanMan compatible password constraints.
  - **1** = PWD_COMPAT_NT4 - Sets NT4 compatible password constraints.
  - **2** = PWD_COMPAT_W2K - Sets Windows 2000 and later compatible password constraints.
- **PasswordLength:** *(Optional)* The desired length for a random password. Use when setting a random password. The minimum length is 3 characters and the maximum length is limited based on PasswordCompatibilityLevel configuration. Maximum values are:
  - 14 characters when set to PWD_COMPAT_LAN_MANAGER or PWD_COMPAT_NT4.
  - 127 characters when set to PWD_COMPAT_W2K.
- **PasswordSecurityOptions:** Possible values are:
  - **1** = symbol in middle
  - **2** = no repeated characters
  - **3** = both symbol in middle and no repeated characters
- **PasswordSegments:** Defines how many segments the password will be broken into for later retrieval. Set to 1 store the password as 1 segment, meaning only one identity will be required to retrieve the whole password.
- **PreventUsernameInPassword:** For random passwords, set the value to true to ensure the username does not appear anywhere in a random password, though the likelihood of this is statistically improbable.
- **ReEnableAccountAfterSetTimeHours:** Not used.
- **ReEnableAccountIfOperationFails:** Not used.
- **RenameAccount:** *(Optional)* For Windows password change jobs, set to true to rename the target account and define NewAccountName.
- **SendEmailOnChange:** *(Optional)* When set to true, this will send the password in clear text via email to the email address defined in EmailOnChange.
- **SerializedUtilityIDs:** For SSH/Telnet jobs, these are the IDs of the utility accounts that may be used as tertiary login credentials during the password change job. Multiple IDs are separated by a semi-colon, for example "1062;1064;15". The IDs are translated into utility account IDs in the answer file based on the order they are entered here. In the example above, 1062 would be utilityAccount_1.

- **StoredAccountName:** *(Optional)* For non-Windows password change jobs that will use a managed (and central account, e.g. from a directory), to login and change the target account. You must also specify StoredNameSpace and StoredSystemName. UseStoredLoginPassword must also be set to true.
- **StoredNamespace:** *(Optional)* For non-Windows password change jobs that will use a managed (and central account, e.g. from a directory), to login and change the target account. You must also specify StoredAccountName and StoredSystemName. UseStoredLoginPassword must also be set to true.
- **StoredSystemName:** *(Optional)* For non-Windows password change jobs that will use a managed (and central account, e.g. from a directory), to login and change the target account. You must also specify StoredNameSpace and StoredAccountName. UseStoredLoginPassword must also be set to true.
- **SymbolsSetOverride:** *(Optional)* When setting a random password, if desired, define the allowed special symbols for the random password. If not defined, all symbols will be allowed.
- **TerminalType:** Not used during job creation.
- **Unique:** Set to true to define the target account will get a unique random password, should multiple systems be defined in SystemsList. If set to false or not included and a random password is being set and multiple systems are included in SystemsList, the target account's password will be set the same across all target systems. Further, the account will be opted out of password re-randomization following password retrieval via the web application.
- **UnlockAccount:** *(Optional)* For Windows and Oracle database jobs, this will clear the account lockout flag of the target account when set to true.
- **UpdateAutoLogon:** *(Optional)* For Windows password change jobs, this will set the current account to be the automatic login account for the target systems.
- **UpdatedAccountIsRootAccount:** (Optional) - For SSH/Telnet jobs, set to true when the target account is a root account.
- **UseSavedPasswords:** *(Optional)* For jobs that define a login account on the job, set to true when it is desired to use the stored password for the account. Set to false, when the password defined in the job, LoginPassword, should be used instead of any stored password.
- **UseStoredLoginPassword:** *(Optional)* For jobs that must use a login account on the job, set to true when it is desired to use a managed credential for the login account. You must also define StoredAccountName, StoredNameSpace, and StoredSystemName.

/PasswordChangeSettings/PasswordConstraints

Many items are derived from the PasswordChangeSettings previously defined. Listed below are the new items for which there is no duplicate PasswordChangeSettings element.

- **DefaultPasswordFilterCompliance:** Not used.
- **FailGenerationOnMissingPassfiltDLL:** *(Optional)* Set to false to avoid failing the job if a custom password filter is not defined or unavailable.
- **PathToPassfiltDLL:** *(Optional)* Set to empty value to avoid system trying to use a custom passfilt.dll password filter. Otherwise, define the absolute path the the custom password filter.
- **SymbolsExcludeProblematicWithAPIs:** (Optional) - Set to true to avoid using symbols known to be problematic with scripts and APIs. These symbols include: /\:;'"
- **SymbolsExcluded:** *(Optional)* Define symbols to exclude from password change jobs.

/PasswordChangeSettings/PasswordPropagationSettings

PasswordPropagationSettings defines the scope of propagation. In other words, what systems will be targeted for password propagation once the password change is made successfully.

- **ConstrainToManagedSystems:** *(Optional)* Set to true to limit the scope of propagation to only systems that are managed by Privileged Identity.

- **ConstrainToMembersOfGroup:** Set to true to limit propagation scope to the systems in a specific management set. You must also define the GroupName.
- **ConstrainToSystemsWithNonzeroInUse:** Not used.
- **ExcludeDomainControllers:** *(Optional)* Set to true to avoid attempting propagation of the new password to domain controllers which may otherwise be included in the propagation scope. ExcludeSystemWithAccount must also be set to true.
- **ExcludeSystemWithAccount:** *(Optional)* Set to true to avoid scanning of and attempted propagation to the system where the password was changed.
- **GroupName:** *(Optional)* If ConstraintoMembersOfGroup is set to true, define the management set to limit propagation scope to.
- **PropagateToSystemWithAccountOnly:** *(Optional)* Set to true to scan only the system where the account password was updated. For example, a local system account where only the local system uses the account.
- **PropagateToTrustingDomains:** *(Optional)* Set to true to cause Privileged Identity to enumerate all trusting domains and attempt scanning and propagating to those trusting systems.

/PasswordChangeSettings/PropagationTargets/ListTargets

This defines what sub-systems to propagate to such as Windows Services, Scheduled Tasks, etc.. Create zero or more repetitions of <PasswordPropagationTarget> for each target sub-system. Each propagation target will be wrapped in a <PasswordPropagationTarget> tag.

- **ConfigurationData:** *(Optional)* PropagationTargets ConfigurationData for more information on each propagation target type. This data varies by target. See REST.
- **DescriptiveName:** *(Optional)* A friendly name for the propagation type.
- **Enabled:** (Optional) - Set to true to enable the propagation type for the job.
- **PasswordChangeJobID:** Not used.
- **RestrictBySystemSet:** *(Optional)* Set to true to limit the propagation type's scope to a specific list of systems. This is useful to ensure a certain type of propagation found on only a subset of systems included in the job's propagation scope are checked for a specific type of propagation. For example, if a job's propagation scope encompasses 1,000 systems,but only 10 of those systems run SharePoint, setting this option and defining SystemSet would configure the SharePoint propagation type to scan only those 10 systems if they were in their own management set.
- **SystemSet:** (Optional) - Define the name of a management set when RestrictBySystemSet is set to true.
- **TargetSystemType_Linux:** *(Optional)* Set to true to enable this propagation type for Linux systems (systems under the Linux/Unix node) included in the job's propagation scope.
- **TargetSystemType_Windows:** *(Optional)* Set to true to enable this propagation type for Windows systems included in the job's propagation scope.
- **TypeName:** *(Optional)* If configuring propagations, this value must be defined. Valid values are:
    - **builtin:WindowsServices:** Windows services.
    - **builtin:WindowsScheduler:** Windows scheduled tasks.
    - **builtin:WindowsSchedulerAtAccount:** Windows AT identity.
    - **builtin:COMPlus:** Winuniquedows COM.
    - **builtin:DCOM:** Windows DCOM.
    - **builtin:IIS6Metabase:** Windows IIS6 (anonymous, app pool, network credentials).
    - **builtin:IIS7ConfigFiles:** Windows IIS7 and later (anonymous, app pool, network credentials).
    - **builtin:SCOM:** Microsoft SCOM RunAs accounts.
    - **builtin:SqlServer:** SQL Server Credentials (not to be confused with SQL Server Logins).

- **builtin:NetConfig:** IIS asp.net connection strings.
- **builtin:ReplaceInFiles:** String replacement within files.
- **builtin:RunProcess:** Run an arbitrary process.
- **builtin:Sharepoint:** Microsoft SharePoint server.
- **builtin:IBM WebSphere Application Server:** IBM WebSphere Server.
- **builtin:Oracle WebLogic Server:** Oracle Web Logic Server.
- **builtin:SAP Server:** SAP.
- **builtin:UpdateLogonCache:** Windows logon cache.
- **builtin:UpdateAutoLogon:** Windows automatic logon account.
- **builtin:SQLReportingServices:** Microsoft SQL Reporting Services Action Account.

InputArgs\StoredCredential

- **AccountName_FullyQualified:** Set the value to Namespace\UserName. See the Namespace Values addenda in the administrator's guide.
- **AccountSupplementaryData:** Not used for this operation.
  - **Flag_AccountDisabled:** Not used for this operation.
  - **Flag_AccountLocked:** Not used for this operation.
  - **Flag_PasswordCantChange:** Not used for this operation.
  - **Flag_PasswordExpired:** Not used for this operation.
  - **Flag_PasswordNotRequired:** Not used for this operation.
  - **PasswordAge:** Not used for this operation.
- **Comment:** Not used for this operation.
- **CredentialType:** Set to 1.
- **IsCredentialSecretDataInStore:** Not used for this operation.
- **IsSetToSpin:** Not used for this operation.
- **LastSetTimeUTC:** Not used for this operation.
- **ManagementSetStatusData:** Not used for this operation.
  - **CheckedOutToUser:** Not used for this operation.
  - **PasswordCheckedOut:** Not used for this operation.
- **Password:** Not used for this operation.
- **RowID:** Not used for this operation.
- **SupplementaryData_ePO:** Not used for this operation.
  - **AccessToAccountCredentials:** Not used for this operation.
  - **AccountDisabled:** Not used for this operation.
  - **AccountLocked:** Not used for this operation.
  - **Managed:** Not used for this operation.
  - **PasswordAge:** Not used for this operation.
  - **PasswordCantChange:** Not used for this operation.

- **PasswordNotRequired:** Not used for this operation.
- **Passwordexpire:** Not used for this operation.

- **SystemName:** The target system name.
- **Username:** The target username.

Example Requests

Linux Root Account

```
{
   "AuthenticationToken": "String content",
   "MinutesUntilSpin": 30,
   "PasswordChangeSettings": {
      "AccountType": 4,
      "CancelIfCheckedOut": true,
      "ChangeLoginAccount": true,
      "ChangeRootAccount": true,
      "ChangeTwice": false,
      "ConfigFile": "Response",
      "ConnectionType": 0,
      "DisableAccountLockout": false,
      "FirstCharacterSetBits": 15,
      "FullAccountName": "root",
      "HostCodePage": 0,
      "LastCharacterSetBits": 15,
      "LoginName": "root",
      "MiddleCharactersSetBits": 15,
      "MinLettersLcase": 1,
      "MinLettersUcase": 1,
      "MinNumbers": 1,
      "MinSymbols": 1,
      "PasswordChangeType": 0,
      "PasswordCharacterSetBits": 15,
      "PasswordCompatibilityLevel": 2,
      "PasswordConstraints": {
         "FailGenerationOnMissingPassfiltDLL": false
      },
      "PasswordLength": 14,
      "PasswordSecurityOptions": 3,
      "Unique": true,
      "UpdatedAccountIsRootAccount": true,
      "UseSavedPasswords": true,
      "UseStoredLoginPassword": false
   },
   "StoredCredential": {
      "AccountName_FullyQualified": "[Linux]\\root",
      "CredentialType": 1,
      "SystemName": "smeagles",
      "Username": "root"
   }
}
```

Output Success

The output message will indicate the job was updated successfully.

Example Success Output

```
{
   "OperationMessage": "Created password spin job with JobID 1407",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
   <title>Request Error</title>
   <style>
      style_info_goes_here
   </style>
</head>
<body>
   <div id="content">
      <p class="heading1">Request Error</p>
      <p xmlns="">
         The server encountered an error processing the request. Please see the
         <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Invalid authentication
token or token not found'. See server logs for more details. The exception stack trace is:
      </p>
      <p>
         stack_trace_info_goes_here
      </p>
   </div>
</body>
</html>
```

REST: Job/PreAndPostRun (PUT)

Job/PreAndPostRun sets and replaces pre and post run job settings on the target job.

Permissions Required

- Delegated control of the job.

Related Commands

- **PowerShell:** Set-LSJobPreAndPostRunSettings
- **SOAP:** JobOps_SetPreAndPostRunSettings

Syntax

```
{
   "AuthenticationToken":"String content",
   "JobID":"String content",
   "oPreAndPostSettings":{
      "PostRunApplication":"String content",
      "PostRunArgs":"String content",
      "PostRunExe":true,
      "PreRunAbortFail":true,
      "PreRunApplication":"String content",
      "PreRunArgs":"String content",
      "PreRunExe":true,
      "PreRunWait":true
   }
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **JobID:** The ID of the job.
- **oPreAndPostRunSettings:** The pre and/or post run settings to apply to the target job.
    - **PostRunApplication:** The path of the executable to run on the Privileged Identity host, after the job completes.
    - **PostRunArguments:** Command line arguments for the post run executable.
    - **PostRunExe:** Set to true to run a PostRun application.
    - **PreRunAbortFail:** Set to true to abort the the job if the pre-run operation fails or returns a non-zero code.
    - **PreRunApplication:** The path of the executable to run on the Privileged Identity host, before the job starts.
    - **PreRunArgs:** Command line arguments for the pre-run executable.
    - **PreRunExe:** Set to true to run a Pre-Run application.
    - **PreRunWait:** Set to true to wait for the pre-run application to exit and supply a non-zero return code before continuing to process the job. Set to false to run the pre-run operation and immediately continue processing the password change.

Example Request

```
{
   "AuthenticationToken":"U84TTBJSOLUWF76XD9J4XPUE4SJ42T2E",
   "JobID":"1407",
   "oPreAndPostSettings":{
      "PostRunApplication":"c:\\utils\\sdnutil.exe",
      "PostRunArgs":"-Op Close -Targ vn-custx",
      "PostRunExe":true,
      "PreRunAbortFail":true,
      "PreRunApplication":"c:\\utils\\sdnutil.exe",
      "PreRunArgs":"Op Open -Targ vn-custx",
      "PreRunExe":true,
      "PreRunWait":true
   }
}
```

Output Success

The output message will indicate the job was updated successfully.

Example Success Output

```
{
   "OperationMessage": "Updated pre and post run settings for job 1407",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid JobID**

  The job specified could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
```

```
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'The job specified could
not be found'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Job/RunNow (POST)

Job/RunNow updates the specified job's next run time to "run now", where run now is "now" plus 1 minute to account for transaction submission delays.

Permissions Required

- Delegated control of the job.

Related Commands

- **PowerShell:** Set-LSJobRun
- **SOAP:** JobsOps_RunJob

Syntax

```
{
   "AuthenticationToken":"String content",
   "JobID":"String content"
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **JobID:** The ID of the job.

Example Request

```
{
   "AuthenticationToken":"FPTLVO5H5BUVMW1XLRQ3K2U1GJYDO694",
   "JobID":"1398"
}
```

Output Success

The output message will indicate the job was updated successfully.

Example Success Output

```
{
   "OperationMessage": "Updated job to run now job 1398",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid JobID**

  The job specified could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'The job specified could
not be found'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Job/Schedule (PUT)

Job/Schedule sets a job schedule for a target job.

Permissions Required

- Delegated control of the job.

Related Commands

- **PowerShell:** Set-LSJobSchedule
- **SOAP:** JobOps_SetJobSchedule

Syntax

```
{
   "AuthenticationToken":"String content",
   "JobID":"String content",
   "ScheduleInfo":{
      "DayOfMonth":2147483647,
      "DayOfWeek":2147483647,
      "DayOfYear":2147483647,
      "DaysBits":4294967295,
      "EveryNDays":2147483647,
      "Hours":2147483647,
      "Minutes":2147483647,
      "MonthOfYear":2147483647,
      "NextRetryTimeUTC":"\/Date(928167600000-0500)\/",
      "NumberOfRetries":2147483647,
      "Reboot":true,
      "RetryEnabled":true,
      "RunWindowMinutes":2147483647,
      "ScheduleType":0,
      "SchedulingPeriod":2147483647,
      "UpdateNextRunTimeForPartialCompletion":true
   }
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **JobID:** The ID of the target job.
- **ScheduleInfo:** The job's schedule object.
    - **DayOfMonth:** *(Optional)* Set the day of the month to run the job. Valid values are 1-31. For months with fewer days than the day of the month defined (e.g. value is 30 but there are only 28 days in the month), the job will run on the last day of the month.

- **DayOfWeek:** *(Optional)* Set the day of the week to run the job on. Values are:
  - **0** = Sunday
  - **1** = Monday
  - **2** = Tuesday
  - **3** = Wednesday
  - **4** = Thursday
  - **5** = Friday
  - **6** = Saturday
- **DayOfYear:** Not used.
- **DaysBits:** Not used.
- **EveryNDays:** *(Optional)* Set the amount of days for the job to recur when ScheduleTypes is set to SCHEDULE_TYPE_N_DAYS.
- **Hours:** *(Optional)* Set the hour at which the job will run. Use a 24 hour clock.
- **Minutes:** *(Optional)* Set the minutes into the hour (Hours) when the job will run.
- **MonthOfYear:** *(Optional)* Set the month (number) for the job to run. Values are:
  - **1** = January
  - **2** = February
  - **3** = March
  - **4** = April
  - **5** = May
  - **6** = June
  - **7** = July
  - **8** = August
  - **9** = September
  - **10** = October
  - **11** = November
  - **12** = December
- **NextRetryUTC:** *(Optional)* For new jobs this value should not be used. Expected format is Microsoft JSON, e.g. "/Date (MillisecondsSinceJan11970)/".
- **NumberOfRetries:** *(Optional)* Set the number of retries for the job should it fail. If not defined, it will use the system default.
- **Reboot:** *(Optional)* Set to true to reboot Windows systems following the password change. Systems defined in SystemList will be affected.
- **RetryEnabled:** *(Optional)* Set to true to enable retries in the event of failure.
- **RunWindowMinutes:** *(Optional)* Set to value to 1 or more minutes to define the job must run by the specified time plus the run window duration or the job will be skipped. Set to 0 or do not define to indicate it should run despite missing the originally schedule time (default).
- **ScheduleType:** *(Optional)* Define the type of schedule (one time, recurring, etc.) for the job. If not defined, default value is SCHEDULE_TYPE_INTERACTIVE which means it must be run by hand or will be run immediately based on other scheduling options. Valid values are:

- **0** = SCHEDULE_TYPE_UNKNOWN
- **1** = SCHEDULE_TYPE_IMMEDIATELY
- **2** = SCHEDULE_TYPE_HOURLY - Job will be run once every hour. Set Minutes.
- **3** = SCHEDULE_TYPE_DAILY- Job will be run once every day on the specified time. Set Hours and Minutes.
- **4** = SCHEDULE_TYPE_WEEKLY - Job will be run once every week on the specified day and time. Set Hours, Minutes and DayOfWeek.
- **5** = SCHEDULE_TYPE_MONTHLY - Job will be run once every month on the specified day and time. DayOfMonth, Hours, and Minutes.
- **6** = SCHEDULE_TYPE_YEARLY - Job will be run once every year on the specified month, day and time. Define DayOfMonth, MonthOfYear, Hours, and Minutes.
- **7** = SCHEDULE_TYPE_DAYS_OF_WEEK - Job will be run every set day of week. Set DayOfWeek.
- **8** = SCHEDULE_TYPE_ONCE - Job will be run once at some point in the future. Define DayOfMonth, MonthOfYear, Hours, and Minutes.
- **9** = SCHEDULE_TYPE_N_DAYS - Job will be run every N days. Set integer value for EveryNDays.
- **10** = SCHEDULE_TYPE_INTERACTIVE - Default. Job will be run based on NextRunTimeUTC.
- **11** = SCHEDULE_TYPE_N_HOURS - Job will be run every N hours. Set Hours for the number of hours and Minutes for number of minutes to offset.

- **SchedulingPeriod:** Not used.
- **UpdateNextRunTimeForPartialCompletion:** *(Optional)* Set to true to define job with multiple systems should update the next run time as seen in the management console display. The default value is false.

Example Request

```
{
   "AuthenticationToken":"DKXYP1TPG36UQXMD9FW5BXPZKL2X33XW",
   "JobID":"1398",
   "ScheduleInfo":{
      "DayOfMonth":27,
      "Hours":0,
      "Minutes":30,
      "NextRetryTimeUTC":"\/Date(1501761662000)\/",
      "NumberOfRetries":3,
      "Reboot":false,
      "RetryEnabled":true,
      "RunWindowMinutes":20,
      "ScheduleType":5,
      "UpdateNextRunTimeForPartialCompletion":true
   }
}
```

Output Success

The output message will indicate the job was updated successfully.

Example Success Output

```
{
   "OperationMessage": "Updated schedule for job 1398",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid JobID**

  The job specified could not be found.

Example Fail Output

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
   <s:Body>
      <s:Fault>
         <faultcode>s:Client</faultcode>
         <faultstring xml:lang="en-US">The job specified could not be found</faultstring>
         <detail>
            <RouletteAppService_FaultException
xmlns="http://schemas.datacontract.org/2004/07/RouletteAppService_WCF"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
               <Component>AppProcessingComponent</Component>
               <Description>The job specified could not be found</Description>
               <ErrorCode>2147614729</ErrorCode>
            </RouletteAppService_FaultException>
         </detail>
      </s:Fault>
   </s:Body>
</s:Envelope>
```

REST: Job/SSHKeyChange (PUT)

Job/SSHKeyChange defines SSH key change job settings for an existing job.

Permissions Required

- Delegated control of the job

Related Commands

- **PowerShell:** Set-LSJobSSHKeyChangeSettings
- **SOAP:** JobOps_SetJobKeyChangeSettings

Syntax

```
{
   "AuthenticationToken":"String content",
   "JobID":"String content",
   "oKeyChangeSettings":{
      "DeleteKeyFileOnRemoteSystems":true,
      "GenerateNewKeyEachRun":true,
      "KeyLabel":"String content",
      "KeyLengthBits":2147483647,
      "KeyType":2147483647,
      "OldKeyLabel":"String content",
      "OldKeySig":"String content",
      "OldPublicKey":"String content",
      "RemoveOldKey":true,
      "UpdateKeyReferences":true
   }
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **JobID:** -The ID of the target job.
- **JobSSHKeySettings:** The new SSH key settings for the job.
    - **DeleteKeyFileOnRemoteSystems:** When set to $true, a new key is generated and stored in the solution database on the first run only, and removes any physical files found where it has the authority to remove (rm) the keys files.
    - **GenerateNewKeyForEachRun:** When set to true, a new key is generated and stored/updated in the solution database on every run of the job, and does not perform any subsequent updates to target systems.
    - **KeyLabel:** The label of the key to be updated.
    - **KeyLengthBits:** Length of the new key to generate. The bit length will default to the current length of the key. Available options are 2048, 3072, and 4096 bits.
    - **KeyType:** Currently, this functionality is limited to OpenSSH v2 RSA type keys and cannot be configured. Set this value to 0.
    - **OldKeyLabel:** Not used. Reserved for future use.

- **OldKeySig:** Not used. Reserved for future use.
- **OldPublicKey:** Not used. Reserved for future use.
- **RemoveOldKey:** When set to true, a new key will be generated and stored in the database on the first run only. Then, the previous key references will be removed from the the authorized key files on the target systems, which breaks any access reliant on the old key based on discovered information.
- **UpdateKeyReferences:** When set to true, a new key will be generated and stored in the solution database on the first job run only, and update the authorized key files on the target systems. Subsequent job runs will continue trying to update the target systems' authorized keys to reference the new SSH key that was generated on the first job run. That means if a system was offline or otherwise inaccessible when the job ran previously, it will be updated on a subsequent run. This job will distribute key files to the systems. It only updates the authorized key files on the target systems.

Example Request

```
{
   "AuthenticationToken":"TAXLRKL5OZ21287CYTW80OP320IRHGHZ",
   "JobID":"1199",
   "oKeyChangeSettings":{
      "DeleteKeyFileOnRemoteSystems":true,
      "GenerateNewKeyEachRun":true,
      "KeyLabel":"dbsmashlnx",
      "KeyLengthBits":4096,
      "KeyType":0,
      "RemoveOldKey":true,
      "UpdateKeyReferences":true
   }
}
```

Output Success

The output message will indicate the job was updated successfully.

Example Success Output

```
{
   "OperationMessage": "Updated ssh key change settings for job 1199",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid JobID**

  The job specified could not be found.

Example Fail Output

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
   <s:Body>
      <s:Fault>
         <faultcode>s:Client</faultcode>
         <faultstring xml:lang="en-US">The job specified could not be found</faultstring>
         <detail>
            <RouletteAppService_FaultException
xmlns="http://schemas.datacontract.org/2004/07/RouletteAppService_WCF"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
               <Component>AppProcessingComponent</Component>
               <Description>The job specified could not be found</Description>
               <ErrorCode>2147614729</ErrorCode>
            </RouletteAppService_FaultException>
         </detail>
      </s:Fault>
   </s:Body>
</s:Envelope>
```

REST: SharedCredentialList (PUT)

SharedCredentialList (PUT) allows you to change the settings of a shared credential list.

Permissions Required

- Manage External Lists
- All Access

Related Commands

- **PowerShell:** Set-LSSharedCredentialList
- **SOAP:** AccountStoreOps_EditSharedCredentialList_Input

Parameters

- **AuthenticationToken:** Authentication token of the calling user.
  - **AllowAdd:** Set to `$true` to allow new passwords to be added to the shared credential list.
  - **AllowDelegate:** Set to `$true` to allow other users to manage the delegation of the shared credential list.
  - **AllowEdit:** Set to `$true` to allow existing passwords in the shared credential list to be edited.
  - **Comment:** Include a comment.
  - **Count:** Number of passwords included in the shared credential list.
  - **Name:** The name of the shared credential list.
  - **RowID:**
  - **NewListName:** (string) Provide a new name for the shared credential list, if needed.

Example Request

```
{
   "AuthenticationToken":"String content",
   "CredentialList": {
               "AllowAdd":true,

               "AllowDelegate":true,
               "AllowDelete":true,
               "AllowEdit":true,
               "Comment":"String content",
               "Count":2147483647,
               "Name":"String content",
               "RowID":2147483647
       },
       "NewListName":String content"
}
```

Example Response

```
{
        "OperationMessage":"String content",
        "OperationSucceeded":true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid List**

  The shared credential list could not be found.

- **Edit Failed**

  Failed to edit the shared credential list.

REST: Delegations

This section covers REST APIs pertaining to setting, editing, or removing delegations. Delegations are used to grant access to many items such as password, account elevation, file store, etc.

REST: Delegation/AccountMask (GET)

Delegation/AccountMask is used to return the entire list of defined account masks.

Permissions Required

- View Delegations

Related Commands

- **PowerShell:** Get-LSListDelegationAccountMasks
- **SOAP:** DelegationOps_GetAccountMaskPermissionsList

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Delegation/AccountMask
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- None

Example Request

```
https://lsdslscprd.lsds.int/erpmwebservice/authservice.svc/rest/Delegation/AccountMask
```

Output Success

If no account masks are defined, the output will be empty. If lists are defined, the output will contain the account mask and associated identity.

Example Success Output

```
[
   {
      "AccountMask": "admin*",
      "IdentityName": "pat"
```

```
   }
]
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Session invalid, a
duplicate web session was detected for this identity'. See server logs for more details. The
exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/Identity (GET)

Delegation/Identity is used to return the entire list of delegated identities and their global permissions. Use "Delegation/Permission (GET)" on page 1 to return the list of all permissions for all permission types for all identities.

Permissions Required

- View Delegations

Related Commands

- **PowerShell:** Get-LSListDelegationIdentities
- **SOAP:** DelegationOps_GetIdentities

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Delegation/Identity
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- None

Example Request

```
https://lsdslscprd.lsds.int/erpmwebservice/authservice.svc/rest/Delegation/Identity
```

Output Success

If no delegation identities defined, the output will be empty. If identities are defined, the output will contain the list of identities and their global permissions. Multiple **DelegationIdentity** objects will be listed for multiple identities.

Example Success Output


```
[
   {
      "AccountName": "Recovery User",
      "AlertOnRecovery": false,
      "AlertOnRequest": false,
      "DisplayName": "",
      "EmailAddress": "",
      "IsDomainAccount": 4,
      "Password": "",
      "PermissionAccessRemoteSessions": false,
```

```
    "PermissionAddPasswordsForManagedSystems": false,
    "PermissionAllAccess": false,
    "PermissionCreateRefreshSystemJob": false,
    "PermissionEditDelegation": false,
    "PermissionEditPasswordLists": false,
    "PermissionEditStoredPasswords": false,
    "PermissionElevateAccountPermissions": false,
    "PermissionElevateAnyAccountPermissions": false,
    "PermissionGrantPasswordRequests": false,
    "PermissionIgnorePasswordCheckout": false,
    "PermissionLogon": true,
    "PermissionPersonalStore": false,
    "PermissionRequestPasswords": false,
    "PermissionRequestRemoteAccess": false,
    "PermissionRequireOATH": false,
    "PermissionRequireRSASecurID": false,
    "PermissionSelfRecovery": false,
    "PermissionViewAccounts": true,
    "PermissionViewDashboards": false,
    "PermissionViewDelegation": false,
    "PermissionViewFileStore": false,
    "PermissionViewJobs": false,
    "PermissionViewPasswordActivity": false,
    "PermissionViewPasswordHistory": false,
    "PermissionViewPasswords": true,
    "PermissionViewScheduler": false,
    "PermissionViewSystems": false,
    "PermissionViewWebLogs": false
  },
  {
    "AccountName": "Request User",
    "AlertOnRecovery": false,
    "AlertOnRequest": false,
    "DisplayName": "",
    "EmailAddress": "",
    "IsDomainAccount": 4,
    "Password": "",
    "PermissionAccessRemoteSessions": false,
    "PermissionAddPasswordsForManagedSystems": false,
    "PermissionAllAccess": false,
    "PermissionCreateRefreshSystemJob": false,
    "PermissionEditDelegation": false,
    "PermissionEditPasswordLists": false,
    "PermissionEditStoredPasswords": false,
    "PermissionElevateAccountPermissions": false,
    "PermissionElevateAnyAccountPermissions": false,
    "PermissionGrantPasswordRequests": false,
    "PermissionIgnorePasswordCheckout": false,
    "PermissionLogon": true,
    "PermissionPersonalStore": false,
    "PermissionRequestPasswords": true,
    "PermissionRequestRemoteAccess": true,
    "PermissionRequireOATH": false,
    "PermissionRequireRSASecurID": false,
    "PermissionSelfRecovery": false,
```

```
      "PermissionViewAccounts": true,
      "PermissionViewDashboards": false,
      "PermissionViewDelegation": false,
      "PermissionViewFileStore": false,
      "PermissionViewJobs": false,
      "PermissionViewPasswordActivity": false,
      "PermissionViewPasswordHistory": false,
      "PermissionViewPasswords": false,
      "PermissionViewScheduler": false,
      "PermissionViewSystems": false,
      "PermissionViewWebLogs": false
   }
]
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Session invalid, a
duplicate web session was detected for this identity'. See server logs for more details. The
exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/Identity/ManagementSet (GET)

Delegation/Identity/ManagementSet lists management sets the specific identity has global delegations for.

Permissions Required

- View Delegations

Related Commands

- **PowerShell:** Get-LSListDelegationManagementSetsForIdentity
- **SOAP:**DelegationOps_GetManagedGroupsForIdentity

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Delegation/Identity/ManagementSet?Identity
={IDENTITY}
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- **Identity:** The identity for which to obtain the list of assigned management sets.

Example Request

```
https://lsdslscprd.lsds.int/erpmwebservice/authservice.svc/rest/Delegation/Identity/ManagementSet
?Identity=lsds%5cInfrastructureAdmins
```

***Note:** If the identity name uses characters such as back slashes or spaces, the name must be URL encoded. a back slash is represented by %5c while a space is represented by %20.*

Output Success

Successful output will list all management sets associated with the identity via global delegations. The list will be empty if no management sets are defined for the target identity.

Example Success Output

```
[
   {
      "ManagedGroupName": "All Windows Systems"
   },
```

```
    {
       "ManagedGroupName": "esx"
    },
    {
       "ManagedGroupName": "IPMI"
    }
]
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid or non-existent identity**

  No files were found with this name, or you do not have permission to the view files.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'A database call
unexpectedly returned no data or a file was not found'. See server logs for more details. The
exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/File (GET)

Delegation/File returns a list of identities and permissions assigned via file store delegations for a specific file.

Permissions Required

- View Delegations

Related Commands

- **PowerShell:** Get-LSListDelegationPermissionsOnFile
- **SOAP:** DelegationOps_StoredFile_GetPermissions

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Delegation/File?FileID={FILEID}
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- **FileID:** The ID of the target file. Hint: this can be retrieved from the web application or Files (GET).

Example Request

```
https://lsdslscprd.lsds.int/erpmwebservice/authservice.svc/rest/Delegation/File?FileID=2
```

Output Success

If file store delegations are defined on specific files, the output will contain an entry for each file delegation for the specific file.

Example Success Output


```
[
   {
      "FileName": "LSC Certificate for Web-1.cer",
      "IdentityName": "lsds\\lscadmin",
      "PermissionDelegate": true,
      "PermissionDelete": true,
      "PermissionDownload": true,
      "PermissionGrant": true,
      "PermissionRequest": false,
      "PermissionUpdate": true,
      "PermissionView": true
   },
```

```
    {
       "FileName": "LSC Certificate for Web-1.cer",
       "IdentityName": "pat",
       "PermissionDelegate": false,
       "PermissionDelete": true,
       "PermissionDownload": true,
       "PermissionGrant": false,
       "PermissionRequest": false,
       "PermissionUpdate": false,
       "PermissionView": true
    }
]
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid or non-existent identity**

  The identity name could not be found. Or, the edit process failed.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'A database call
unexpectedly returned no data or a file was not found'. See server logs for more details. The
exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/Job (GET)

Delegation/Job returns a list of per-job permissions.

> ***Note:*** *Job permissions added prior to version 5.5.2.1 will be unavailable for reporting.*

Permissions Required

- View Delegations

Related Commands

- **PowerShell:** Get-LSListDelegationPermissionsOnJobs
- **SOAP:** DelegationOps_GetPermissionsOnJobs

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Delegation/Job
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- None.

Example Request

```
https://lsdslscprd.lsds.int/erpmwebservice/authservice.svc/rest/Delegation/Job
```

Output Success

If per-job delegations are defined, a list of each delegation on each job is returned.

Example Success Output


```
[
   {
      "AccountName": "",
      "AccountStoreType": 0,
      "Application": "",
      "FileName": "",
      "IdentityID": 12,
      "IdentityName": "pat",
```

```
    "JobID": "3",
    "ManagementSetName": "",
    "Namespace": "",
    "OfflineTenant": "",
    "PermissionAccessJobs": false,
    "PermissionAccessPersonalPasswords": false,
    "PermissionAccessRemoteSessions": false,
    "PermissionAddPassword": false,
    "PermissionAlertOnChange": false,
    "PermissionAlertOnIncident": false,
    "PermissionAllAccess": false,
    "PermissionChangeDelegation": false,
    "PermissionChangePasswords": false,
    "PermissionChangePasswordsOnManagedSystems": false,
    "PermissionChangeSharedCredentialLists": false,
    "PermissionCreateModifyManagementSets": false,
    "PermissionCreateRefreshJobs": false,
    "PermissionDeletePassword": false,
    "PermissionEditWebPanels": false,
    "PermissionElevateAnyAccount": false,
    "PermissionGrantPasswordRequests": false,
    "PermissionIgnorePasswordCheckout": false,
    "PermissionLogon": false,
    "PermissionModifyElevationJob": false,
    "PermissionModifyPasswordChangeJob": false,
    "PermissionModifyRefreshJob": false,
    "PermissionRead": true,
    "PermissionRequestPasswords": false,
    "PermissionRequestRemoteAccess": false,
    "PermissionRequire2Factor": false,
    "PermissionRequireOATH": false,
    "PermissionSelfAccountElevation": false,
    "PermissionSelfRecovery": false,
    "PermissionType": 9,
    "PermissionViewAccounts": false,
    "PermissionViewDashboards": false,
    "PermissionViewDelegation": false,
    "PermissionViewFileStore": false,
    "PermissionViewPasswordActivity": false,
    "PermissionViewPasswordHistory": false,
    "PermissionViewPasswords": false,
    "PermissionViewSchedulerService": false,
    "PermissionViewSystems": false,
    "PermissionViewWebLogs": false,
    "PermissionWrite": true,
    "RestrictionDayOfMonthEnd": 0,
    "RestrictionDayOfMonthStart": 0,
    "RestrictionDayOfWeekEnd": 0,
    "RestrictionDayOfWeekStart": 0,
    "RestrictionEndTimeUTC": "/Date(-2208967200000-0600)/",
    "RestrictionStartTimeUTC": "/Date(-2208967200000-0600)/",
    "ScheduleRestrictionType": 0,
    "SharedCredentialListName": "",
    "SystemName": ""
}
```

```
]
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Session invalid, a
duplicate web session was detected for this identity'. See server logs for more details. The
exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/ManagementSet (GET)

Delegation/ManagementSet returns a list of per-management set permissions.

Permissions Required

- View Delegations

Related Commands

- **PowerShell:** Get-LSListDelegationPermissionsOnManagementSets
- **SOAP:** DelegationOps_GetPermissionsOnManagementSets

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Delegation/ManagementSet
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- None.

Example Request

```
https://lsdslscprd.lsds.int/erpmwebservice/authservice.svc/rest/Delegation/ManagementSet
```

Output Success

If per-job delegations are defined, a list of each delegation on each job will be returned.

Example Success Output


```
[
   {
      "AlertForChange": false,
      "AlertForIncident": true,
      "IdentityName": "pat",
      "ManagementSetName": "All Windows Systems",
      "PermissionAllowRemoteSessions": false,
      "PermissionChangeGroupMembership": false,
      "PermissionElevateAccountPermissions": false,
      "PermissionGrantPasswordRequests": false,
      "PermissionRequestPasswords": false,
      "PermissionRequestRemoteAccess": false,
```

```
      "PermissionViewAccounts": false,
      "PermissionViewPasswords": false,
      "PermissionViewSystems": false
   }
]
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Session invalid, a
duplicate web session was detected for this identity'. See server logs for more details. The
exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/Permission (GET)

Delegation/Permission returns all identities and all permissions across all delegated objects, such as global, per-management set, per-system, file store, etc.

Permissions Required

- View Delegations

Related Commands

- **PowerShell:** Get-LSListDelegationPermissions
- **SOAP:** DelegationOps_GetPermissions

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Delegation/Permission
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- None

Example Request

```
https://lsdslscprd.lsds.int/erpmwebservice/authservice.svc/rest/Delegation/Permission
```

Output Success

Output will indicate all global permissions for the identities as well as object specific permissions.

Example Success Output


```
[
   {
      "AccountName": "",
      "AccountStoreType": 0,
      "Application": "",
      "FileName": "",
      "IdentityID": 5,
      "IdentityName": "[WebApplicationManager]",
      "JobID": "0",
      "ManagementSetName": "",
      "Namespace": "",
```

```
        "OfflineTenant": "",
        "PermissionAccessJobs": false,
        "PermissionAccessPersonalPasswords": false,
        "PermissionAccessRemoteSessions": false,
        "PermissionAddPassword": false,
        "PermissionAlertOnChange": false,
        "PermissionAlertOnIncident": false,
        "PermissionAllAccess": true,
        "PermissionChangeDelegation": false,
        "PermissionChangePasswords": false,
        "PermissionChangePasswordsOnManagedSystems": false,
        "PermissionChangeSharedCredentialLists": false,
        "PermissionCreateModifyManagementSets": false,
        "PermissionCreateRefreshJobs": false,
        "PermissionDeletePassword": false,
        "PermissionEditWebPanels": false,
        "PermissionElevateAnyAccount": false,
        "PermissionGrantPasswordRequests": false,
        "PermissionIgnorePasswordCheckout": false,
        "PermissionLogon": false,
        "PermissionModifyElevationJob": false,
        "PermissionModifyPasswordChangeJob": false,
        "PermissionModifyRefreshJob": false,
        "PermissionRead": false,
        "PermissionRequestPasswords": false,
        "PermissionRequestRemoteAccess": false,
        "PermissionRequire2Factor": false,
        "PermissionRequireOATH": false,
        "PermissionSelfAccountElevation": false,
        "PermissionSelfRecovery": false,
        "PermissionType": 1,
        "PermissionViewAccounts": false,
        "PermissionViewDashboards": false,
        "PermissionViewDelegation": false,
        "PermissionViewFileStore": false,
        "PermissionViewPasswordActivity": false,
        "PermissionViewPasswordHistory": false,
        "PermissionViewPasswords": false,
        "PermissionViewSchedulerService": false,
        "PermissionViewSystems": false,
        "PermissionViewWebLogs": false,
        "PermissionWrite": false,
        "RestrictionDayOfMonthEnd": 0,
        "RestrictionDayOfMonthStart": 0,
        "RestrictionDayOfWeekEnd": 0,
        "RestrictionDayOfWeekStart": 0,
        "RestrictionEndTimeUTC": "/Date(-2208967200000-0600)/",
        "RestrictionStartTimeUTC": "/Date(-2208967200000-0600)/",
        "ScheduleRestrictionType": 0,
        "SharedCredentialListName": "",
        "SystemName": ""
    }
]
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Session invalid, a
duplicate web session was detected for this identity'. See server logs for more details. The
exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/SelfRecoveryPermission (GET)

Delegation/AccountMask is used to return a list of self-recovery rules.

Permissions Required

- View Delegations

Related Commands

- **PowerShell:** Get-LSListDelegationPermissionsForSelfRecovery
- **SOAP:** DelegationOps_GetSelfRecoveryPermissionList

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Delegation/SelfRecoveryPermission
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- **SystemFilter:** *(Optional)* The DOS style filter for system names.
- **AccountFilter:** *(Optional)* Tthe DOS style filter for target account names (not identities).

Example Request

No Filter, Return All

```
https://lsdslscprd.lsds.int/erpmwebservice/authservice.svc/rest/Delegation/SelfRecoveryPermission
```

Filtered with Account and System Names

```
https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/Delegation/SelfRecoveryPermission
?SystemFilter=lsc*&AccountFilter=*erpm*
```

Output Success

If no defined self-recovery permissions, the output list will be empty. If permissions are defined, the output will contain the account and associated identity.

Example Success Output

```
[
   {
      "AccountName": "erpmlauncher",
      "IdentityName": "pat",
      "Namespace": "LSC",
      "SystemName": "lsc.ent"
   }
]
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Session invalid, a
duplicate web session was detected for this identity'. See server logs for more details. The
exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/SharedCredentialList (GET)

Delegation/SharedCredentialList returns a list of shared credential list permissions.

Permissions Required

Any of the following permissions:

- View Delegation
- Manage delegations on the target list
- Manage External Lists

Related Commands

- **PowerShell:** Get-LSListDelegationPermissionsOnSharedCredentialList
- **SOAP:** DelegationOps_GetPermissionsForSharedCredentialList

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Delegation/SharedCredentialList?Name=
{NAME}
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.
- **Name:** The URL encoded version of the target shared credential list name

Parameters

- None.

Example Request

```
https://lsdslscprd.lsds.int/erpmwebservice/authservice.svc/rest/Delegation/SharedCredentialList?N
ame=list-0001
```

Output Success

If shared credential list delegations are defined, a list of each delegation on each shared credential list will be returned.

Example Success Output

```
[
   {
      "CredentialListName": "List-0001",
      "IdentityName": "pat",
```

```
      "PermissionAddPassword": false,
      "PermissionChangeDelegation": true,
      "PermissionDeletePassword": false,
      "PermissionEditPassword": false,
      "PermissionGrantRequest": false,
      "PermissionRecoverPassword": false,
      "PermissionRequestPassword": false,
      "PermissionViewList": true
   }
]
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid shared credential list or list not found**

  The shared credential list could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Could not find a shared
credential list with the name specified'. See server logs for more details. The exception stack
trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/StoredCredential (GET)

Delegation/StoredCredential returns a list of identities and permissions assigned via per-account delegations.

Permissions Required

- View Delegations

Related Commands

- **PowerShell:** Get-LSListDelegationPermissionsOnAccounts
- **SOAP:** DelegationOps_GetPermissionsOnAccounts

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Delegation/StoredCredential
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- None.

Example Request

```
https://lsdslscprd.lsds.int/erpmwebservice/authservice.svc/rest/Delegation/StoredCredential
```

Output Success

If per-account delegation are defined, the output will contain an entry for each per-account delegation.

Example Success Output


```
[
   {
      "AccountName": "bob",
      "AlertForChange": false,
      "AlertForIncident": false,
      "IdentityName": "pat",
      "Namespace": "DTVM",
      "PermissionAllowRemoteSessions": false,
      "PermissionGrantPasswordRequests": false,
      "PermissionRequestPasswords": false,
      "PermissionRequestRemoteAccess": false,
      "PermissionViewAccounts": true,
```

```
      "PermissionViewPasswords": true,
      "SystemName": "dtvm"
   }
]
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Session invalid, a
duplicate web session was detected for this identity'. See server logs for more details. The
exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/System (GET)

Delegation/System returns a list of per-system permissions.

Permissions Required

- View Delegations

Related Commands

- **PowerShell:** Get-LSListDelegationPermissionsOnSystems
- **SOAP:** DelegationOps_GetPermissionsonSystems

Syntax

The body will be empty. You must add additional headers.

```
https://serverName/ERPMWebService/AuthService.svc/REST/Delegation/System
```

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

- None.

Example Request

```
https://lsdslscprd.lsds.int/erpmwebservice/authservice.svc/rest/Delegation/System
```

Output Success

If per-job delegations are defined, a list of each delegation on each job will be returned.

Example Success Output


```
[
   {
      "AlertForChange": false,
      "AlertForIncident": false,
      "IdentityName": "pat",
      "PermissionAllowRemoteSessions": false,
      "PermissionElevateAccountPermissions": false,
      "PermissionGrantPasswordRequests": false,
      "PermissionRequestPasswords": false,
      "PermissionRequestRemoteAccess": true,
      "PermissionViewAccounts": false,
      "PermissionViewPasswords": true,
```

```
      "PermissionViewSystems": false,
      "SystemName": "10.1.0.95"
   }
]
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Invalid authentication
token or token not found'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/AccountMask (POST)

Delegation/AccountMask creates an account mask for a target identity.

Permissions Required

- Manage Delegations

Related Commands

- **PowerShell:** Set-LSDelegationPermissionAccountMask
- **SOAP:** DelegationOps_AccountMaskPermission_Add

Syntax

```
{
   "AuthenticationToken":"String content",
   "Permission":{
      "AccountMask":"String content",
      "IdentityName":"String content"
   }
}
```

Parameters

- **AuthenticationToken:** Authentication token of the calling user.
- **AccountMask:** The new account mask to associate with the identity.
- **IdentityName:** The target identity. For domain identities, be sure to use two backslashes in the identity name.

Example Request

```
{
   "AuthenticationToken":"0YW0HGFEAMQROOLSKZOV2B6RT1J1E3AK",
   "Permission":{
      "AccountMask":"svc*",
      "IdentityName":"lsds\\cletus"
   }
}
```

Output Success

A successful operation will state "*Created account mask for identity IDENTITY to MASK*".

Example Success Output

```
{
   "OperationMessage": "Created account mask for identity lsds\\cletus to svc*",
```

```
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid identity**

  The identity name could not be found. Or, the edit process failed.

- **Account mask already exists**

  The identity name already exists. Or, the creation process failed.

Example Fail Output - Account mask already exists

```
{
   "OperationMessage": "Account mask for identity lsds\\cletus to svc* already exists",
   "OperationSucceeded": false
}
```

Example Fail Output - Invalid identity

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'A database call
unexpectedly returned no data or a file was not found'. See server logs for more details. The
exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
```

```
        </div>
    </body>
</html>
```

REST: Delegation/File/Identity (POST)

Delegation/File/Identity adds permissions to a file in the file store for an identity. If theidentity already has permissions, those permissions are replaced. This is functionally equivalent to "Delegation/File (PUT)" on page 1 and uses the same structures. Please see "Delegation/File (PUT)" on page 1 for more information on parameters and success or error output.

REST: Delegation/ManagementSet (POST)

Delegation/ManagementSet adds or updates per-management set delegations. The management set must already exist to apply the per-management set permissions to.

Permissions Required

- Manage Delegations

Related Commands

- **PowerShell:** Set-LSDelegationPermissionOnManagementSet
- **SOAP:** DelegationOps_SetPermissionOnManagementSet

Syntax

```
{
   "AuthenticationToken":"String content",
   "Permission":{
      "AlertForChange":true,
      "AlertForIncident":true,
      "IdentityName":"String content",
      "ManagementSetName":"String content",
      "PermissionAllowRemoteSessions":true,
      "PermissionChangeGroupMembership":true,
      "PermissionElevateAccountPermissions":true,
      "PermissionGrantPasswordRequests":true,
      "PermissionRequestPasswords":true,
      "PermissionRequestRemoteAccess":true,
      "PermissionViewAccounts":true,
      "PermissionViewPasswords":true,
      "PermissionViewSystems":true
   }
}
```

Parameters

Any permissions not included will be set to false.

- **AuthenticationToken:** Authentication token of the calling user.
- **DelegationPermissionOnManagementSet:**
    - **AlertForChange - bool:** False or true to disable or enable alert emails during a password request for the target account when CHANGE is selected.
    - **AlertForIncident - bool:** False or true to disable or enable alert emails during a password request for the target account when INCIDENT is selected.
    - **IdentityName:** Name of the target identity. For domain identities, be sure to use two backslashes in the identity name.
    - **ManagementSetName:** Name of the target management set.
    - **PermissionAllowRemoteSessions - bool:** False or true to disable or enable RDP/SSH/Telnet access to the target system (web site).

- **PermissionChangeGroupMembership - bool:** False or true to disable or enable adding/removing systems to/from the management set.
- **PermissionElevateAccountPermissions - bool:** False or true to enable the user for self elevation.
- **PermissionGrantPasswordRequests - bool:** False or true to disable or enable granting password requests for the target account.
- **PermissionRequestPasswords - bool:** False or true to disable or enable requesting access to the password.
- **PermissionRequestRemoteAccess - bool:** False or true to disable or enable requesting RDP/SSH/Telnet access to the target system (web site).
- **PermissionViewAccounts - bool:** False or true to disable or enable viewing of the account. This value should be set to 1 in order to view the account in the web site.
- **PermissionViewPasswords - bool:** False or true to disable or enable recovering of the password.
- **PermissionViewSystems - bool:** False or true to disable or enable viewing of the systems. This value should be set to 1 in order to view the systems in the web site. If this is set to 0, then the user will also be unable to view accounts in the web site regardless of the permission to do so.

Example Request

```
{
   "AuthenticationToken":"FV1ILHIUEQOQIUHFRXDZJZMJKC1AKWCH",
   "Permission":{
      "AlertForChange":true,
      "AlertForIncident":true,
      "IdentityName":"lsds\\cletus",
      "ManagementSetName":"Web Servers",
      "PermissionAllowRemoteSessions":false,
      "PermissionChangeGroupMembership":false,
      "PermissionElevateAccountPermissions":true,
      "PermissionGrantPasswordRequests":false,
      "PermissionRequestPasswords":true,
      "PermissionRequestRemoteAccess":true,
      "PermissionViewAccounts":true,
      "PermissionViewPasswords":false,
      "PermissionViewSystems":true
   }
}
```

Output Success

A successful operation will state "*Updated delegation permission for identity IDENTITY on management set MANAGEMENTSET*".

Example Success Output

```
{
   "OperationMessage": "Updated delegation permission for identity lsds\\cletus on management set
Web Servers",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid identity**

  The database call unexpectedly returned no data. Or the file was not found.

- **Invalid management set**

  The management set specified could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Login failed or username
not found'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/Identity (POST)

Delegation/Identity creates and adds a new delegation identity. Using this programmatic method also allows you to define global delegation permissions for the account.

Permissions Required

- Manage Delegation

Related Commands

- **PowerShell:** New-LSDelegationIdentity
- **SOAP:** DelegationOps_CreateIdentity

Syntax

```
{
   "AuthenticationToken":"String content",
   "Identity":{
      "AccountName":"String content",
      "AlertOnRecovery":true,
      "AlertOnRequest":true,
      "DisplayName":"String content",
      "EmailAddress":"String content",
      "IsDomainAccount":0,
      "Password":"String content",
      "PermissionAccessRemoteSessions":true,
      "PermissionAddPasswordsForManagedSystems":true,
      "PermissionAllAccess":true,
      "PermissionCreateRefreshSystemJob":true,
      "PermissionEditDelegation":true,
      "PermissionEditPasswordLists":true,
      "PermissionEditStoredPasswords":true,
      "PermissionElevateAccountPermissions":true,
      "PermissionElevateAnyAccountPermissions":true,
      "PermissionGrantPasswordRequests":true,
      "PermissionIgnorePasswordCheckout":true,
      "PermissionLogon":true,
      "PermissionPersonalStore":true,
      "PermissionRequestPasswords":true,
      "PermissionRequestRemoteAccess":true,
      "PermissionRequireOATH":true,
      "PermissionRequireRSASecurID":true,
      "PermissionSelfRecovery":true,
      "PermissionViewAccounts":true,
      "PermissionViewDashboards":true,
      "PermissionViewDelegation":true,
      "PermissionViewFileStore":true,
      "PermissionViewJobs":true,
      "PermissionViewPasswordActivity":true,
      "PermissionViewPasswordHistory":true,
      "PermissionViewPasswords":true,
```

```
        "PermissionViewScheduler":true,
        "PermissionViewSystems":true,
        "PermissionViewWebLogs":true
    }
}
```

Parameters

- **AuthenticationToken:** The authentication token of the requesting user.
- **AccountName:** The name for the new identity.
- **AlertOnRecovery:** (Optional) - Set to true to send emails to EmailAddress when a password is recovered for a system associated with the identity. Set to false to never send an email to the user via the associated EmailAddress.
- **AlertOnRequest:** (Optional) - Set to true to send emails to EmailAddress when a password or remote access is requested for a system associated with the identity. Set to false to never send an email to the user via the associated EmailAddress.
- **DisplayName:** (Optional) - The display name used for the account. If not defined, the AccountName will be used.
- **EmailAddress:** (Optional) - The email address for the identity to send email alerts to.
- **IsDomainAccount:** - Valid values are:
    - **0** = MANAGER_TYPE_EXPLICIT_USER - Explicit user account. IdentityName and Password are required.
    - **1** = MANAGER_TYPE_DOMAIN_USER - Domain user from a Windows domain. Supply the Pre-Windows 2000 name as the IdentityName.
    - **2** = MANAGER_TYPE_DOMAIN_GROUP - Domain-based global security group from a Windows domain. Supply the Pre-Windows 2000 name as the IdentityName.
    - **3** = MANAGER_TYPE_SELF_RECOVERY - Not used.
    - **4** = MANAGER_TYPE_ROLE - Privileged Identity role. User objects from other LDAP sources must be added separately. Supply the name of the role as the IdentityName.
    - **5** = MANAGER_TYPE_RADIUS - RADIUS user. Supply the name of the AuthenticationServerName\UserName as the IdentityName.
    - **6** = MANAGER_TYPE_CERTIFICATE - Certificate-based identity. Supply the name of the user to be associated with the token as the IdentityName. Note that the certificate must already have been enrolled via the console.
    - **7** = MANAGER_TYPE_LDAP_USER - A specific user from an LDAP directory. Supply AuthenticationServerName\UserName name as the IdentityName.
- **Password:** The password for the identity. If your account is not an explicit user, simply specify an empty string.

The following values are all boolean values. Set to true to enable or false to disable. Each of the following values are optional.

- **PermissionAccessRemoteSessions:** Allow remote sessions.
- **PermissionAddPasswordsForManagedSystems:** Add/Edit/Delete Passwords for only Managed Systems.
- **PermissionAllAccess:** Grant All Access.
- **PermissionCreateRefreshSystemJob:**
- **PermissionEditDelegation:** Manage Delegation.
- **PermissionEditPasswordLists:** Manage External Lists.
- **PermissionEditStoredPasswords** Add/Edit/Delete Passwords.
- **PermissionElevateAccountPermissions** Elevate Account Access.
- **PermissionElevateAnyAccountPermissions** Elevate Any Account.

- **PermissionGrantPasswordRequests** Grant Requests.
- **PermissionIgnorePasswordCheckout** Ignore Password Checkout.
- **PermissionLogon** Logon.
- **PermissionPersonalStore** Not used.
- **PermissionRequestPasswords** Request Password Access.
- **PermissionRequestRemoteAccess** Request Remote Access.
- **PermissionRequireOATH** Require OATH/Yubico.
- **PermissionRequireRSASecurID** Require Ext 2-Factor Auth.
- **PermissionSelfRecovery** Not used.
- **PermissionViewAccounts** View Accounts.
- **PermissionViewDashboards** View Dashboards.
- **PermissionViewDelegation** View Delegation.
- **PermissionViewFileStore** Access File Repository.
- **PermissionViewJobs** Manage Scheduled Jobs
- **PermissionViewPasswordActivity** View Password Activity.
- **PermissionViewPasswordHistory** View Password History.
- **PermissionViewPasswords** Recover Passwords.
- **PermissionViewScheduler** Not used.
- **PermissionViewSystems** View Systems.
- **PermissionViewWebLogs** View Web Activity Logs.

Example Request

PowerShell Equivalent for Domain User

```
{
   "AuthenticationToken":"8DDNRPUYVA1IBGPGI0I9HV6KUVTC8TZ8",
   "Identity":{
      "AccountName":"lsds\\cletus",
      "IsDomainAccount":1,
      "Password":""
   }
}
```

Domain User with Permissions

```
{
   "AuthenticationToken":"8DDNRPUYVA1IBGPGI0I9HV6KUVTC8TZ8",
   "Identity":{
      "AccountName":"lsds\\cletus",
      "AlertOnRecovery":true,
      "AlertOnRequest":false,
      "DisplayName":"",
      "EmailAddress":"sales@example.com",
      "IsDomainAccount":1,
```

```
      "Password":"",
      "PermissionAccessRemoteSessions":true,
      "PermissionAddPasswordsForManagedSystems":true,
      "PermissionAllAccess":false,
      "PermissionCreateRefreshSystemJob":false,
      "PermissionEditDelegation":false,
      "PermissionEditPasswordLists":false,
      "PermissionEditStoredPasswords":false,
      "PermissionElevateAccountPermissions":false,
      "PermissionElevateAnyAccountPermissions":false,
      "PermissionGrantPasswordRequests":false,
      "PermissionIgnorePasswordCheckout":false,
      "PermissionLogon":true,
      "PermissionPersonalStore":true,
      "PermissionRequestPasswords":false,
      "PermissionRequestRemoteAccess":false,
      "PermissionRequireOATH":true,
      "PermissionRequireRSASecurID":false,
      "PermissionSelfRecovery":true,
      "PermissionViewAccounts":true,
      "PermissionViewDashboards":true,
      "PermissionViewDelegation":false,
      "PermissionViewFileStore":true,
      "PermissionViewJobs":false,
      "PermissionViewPasswordActivity":false,
      "PermissionViewPasswordHistory":true,
      "PermissionViewPasswords":true,
      "PermissionViewScheduler":false,
      "PermissionViewSystems":true,
      "PermissionViewWebLogs":false
   }
}
```

Output Success

The output states the identity was added.

Example Success Output

```
{
   "OperationMessage": "Identity with name lsds\\cletus created",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Identity already exists**

  The identity name already exists. Or, the creation process failed.

Example Fail Output

```
{
   "OperationMessage": "Identity with name lsds\\cletus already exists, create failed",
   "OperationSucceeded": false
}
```

REST: Delegation/Identity/Role (POST)

Delegation/Identity/Role adds a user from an authentication server (LDAP) to a role.

Permissions Required

- Manage delegations

Related Commands

- **PowerShell:** Set-LSDelegationPermissionRoleMapping
- **SOAP:** DelegationOps_RoleMappingPermission_Add

Syntax

```
{
   "AuthenticationToken":"String content",
   "Permission":{
      "Authenticator":"String content",
      "CredentialName":"String content",
      "RoleName":"String content"
   }
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **AuthenticationServer:** The source authentication server entry.
- **IdentityName:** The target identity role.
- **CredentialName:** The user to add from the source authentication server to the identity role.

Example Request

```
{
   "AuthenticationToken":"9UN88FJX2TPVLJD3WV7736Z1K1AEC7Y2",
   "Permission":{
      "Authenticator":"lsds.int",
      "CredentialName":"alberto",
      "RoleName":"Administrator User"
   }
}
```

Output Success

A successful update states "*Permission for role ROLE on authenticator AUTHENTICATIONSERVER created for credential CREDENTIALNAME*".

Example Success Output

```
{
   "OperationMessage": "Permission for role Administrator User on authenticator lsds.int created for
credential alberto",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid role or Invalid authentication server**

  Permission for the role on the authentication server could not be created for the credential. Or, the role could not be found.

Example Fail Output

```
{
   "OperationMessage": "Permission for role Administrator User XX on authenticator lsds.int could
not be created for credential alberto - Role could not be found",
   "OperationSucceeded": false
}
```

REST: Delegation/Job (POST)

Delegation/Job grants an identity full control of a job.

Permissions Required

- Manage Delegations

Related Commands

- **PowerShell:** Set-LSDelegationPermissionOnJob
- **SOAP:** DelegationOps_SetPermissionOnJob

Syntax

```
{
   "AuthenticationToken":"String content",
   "Permission":{
      "AccountName":"String content",
      "AccountStoreType":4294967295,
      "Application":"String content",
      "FileName":"String content",
      "GlobalGroup":"String content",
      "IdentityID":4294967295,
      "IdentityName":"String content",
      "JobID":"String content",
      "LocalGroup":"String content",
      "ManagementSetName":"String content",
      "MaxTimeMinutes":2147483647,
      "Namespace":"String content",
      "OfflineTenant":"String content",
      "PermissionAccessJobs":true,
      "PermissionAccessPersonalPasswords":true,
      "PermissionAccessRemoteSessions":true,
      "PermissionAddPassword":true,
      "PermissionAlertOnChange":true,
      "PermissionAlertOnIncident":true,
      "PermissionAllAccess":true,
      "PermissionChangeDelegation":true,
      "PermissionChangePasswords":true,
      "PermissionChangePasswordsOnManagedSystems":true,
      "PermissionChangeSharedCredentialLists":true,
      "PermissionCreateModifyManagementSets":true,
      "PermissionCreateRefreshJobs":true,
      "PermissionDeletePassword":true,
      "PermissionEditWebPanels":true,
      "PermissionElevateAnyAccount":true,
      "PermissionGrantPasswordRequests":true,
      "PermissionIgnorePasswordCheckout":true,
      "PermissionLogon":true,
      "PermissionModifyElevationJob":true,
      "PermissionModifyPasswordChangeJob":true,
```

```
        "PermissionModifyRefreshJob":true,
        "PermissionRead":true,
        "PermissionRequestPasswords":true,
        "PermissionRequestRemoteAccess":true,
        "PermissionRequire2Factor":true,
        "PermissionRequireOATH":true,
        "PermissionSelfAccountElevation":true,
        "PermissionSelfRecovery":true,
        "PermissionType":0,
        "PermissionViewAccounts":true,
        "PermissionViewDashboards":true,
        "PermissionViewDelegation":true,
        "PermissionViewFileStore":true,
        "PermissionViewPasswordActivity":true,
        "PermissionViewPasswordHistory":true,
        "PermissionViewPasswords":true,
        "PermissionViewSchedulerService":true,
        "PermissionViewSystems":true,
        "PermissionViewWebLogs":true,
        "PermissionWrite":true,
        "RestrictionDayOfMonthEnd":4294967295,
        "RestrictionDayOfMonthStart":4294967295,
        "RestrictionDayOfWeekEnd":4294967295,
        "RestrictionDayOfWeekStart":4294967295,
        "RestrictionEndTimeUTC":"\/Date(928167600000-0500)\/",
        "RestrictionStartTimeUTC":"\/Date(928167600000-0500)\/",
        "ScheduleRestrictionType":4294967295,
        "SharedCredentialListName":"String content",
        "SystemName":"String content"
    }
}
```


Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- Permission:
    - **AccountName:** Not used for this operation.
    - **AccountStoreType:** Not used for this operation.
    - **Application:** Not used for this operation.
    - **FileName:** Not used for this operation.
    - **IdentityID:** Not used for this operation.
    - **IdentityName:** The target identity. For domain identities, be sure to use two backslashes,in the identity name, e.g. LSDS\\lscadmin.
    - **JobID:** - the target job id.
    - **ManagementSetName:** - not used for this operation.
    - **MaxTimeMinutes** - not used for this operation.
    - **Namespace:** Not used for this operation.
    - **OfflineTenant:** Not used for this operation.
    - **PermissionAccessJobs:** Not used for this operation.

- **PermissionAccessPersonalPasswords:** Not used for this operation.
- **PermissionAccessRemoteSessions:** Not used for this operation.
- **PermissionAddPassword:** Not used for this operation.
- **PermissionAlertOnChange:** Not used for this operation.
- **PermissionAlertOnIncident:** Not used for this operation.
- **PermissionAllAccess:** Not used for this operation.
- **PermissionChangeDelegation:** Not used for this operation.
- **PermissionChangePasswords:** Not used for this operation.
- **PermissionChangePasswordsOnManagedSystems:** Not used for this operation.
- **PermissionChangeSharedCredentialLists:** Not used for this operation.
- **PermissionCreateModifyManagementSets:** Not used for this operation.
- **PermissionCreateRefreshJobs:** Not used for this operation.
- **PermissionDeletePassword:** Not used for this operation.
- **PermissionEditWebPanels:** Not used for this operation.
- **PermissionElevateAnyAccount:** Not used for this operation.
- **PermissionGrantPasswordRequests:** Not used for this operation.
- **PermissionIgnorePasswordCheckout:** Not used for this operation.
- **PermissionLogon:** Not used for this operation.
- **PermissionModifyElevationJob:** Not used for this operation.
- **PermissionModifyPasswordChangeJob:** Not used for this operation.
- **PermissionModifyRefreshJob:** Not used for this operation.
- **PermissionRead:** Not used for this operation.
- **PermissionRequestPasswords:** Not used for this operation.
- **PermissionRequestRemoteAccess:** Not used for this operation.
- **PermissionRequire2Factor:** Not used for this operation.
- **PermissionRequireOATH:** Not used for this operation.
- **PermissionSelfAccountElevation:** Not used for this operation.
- **PermissionSelfRecovery:** Not used for this operation.
- **PermissionType:** Not used for this operation.
- **PermissionViewAccounts:** Not used for this operation.
- **PermissionViewDashboards:** Not used for this operation.
- **PermissionViewDelegation:** Not used for this operation.
- **PermissionViewFileStore:** Not used for this operation.
- **PermissionViewPasswordActivity:** Not used for this operation.
- **PermissionViewPasswordHistory:** Not used for this operation.
- **PermissionViewPasswords:** Not used for this operation.
- **PermissionViewSchedulerService:** Not used for this operation.
- **PermissionViewSystems:** Not used for this operation.
- **PermissionViewWebLogs:** Not used for this operation.
- **PermissionWrite:** Not used for this operation.

- **RestrictionDayOfMonthEnd:** Not used for this operation.
- **RestrictionDayOfMonthStart:** Not used for this operation.
- **RestrictionDayOfWeekEnd:** Not used for this operation.
- **RestrictionDayOfWeekStart:** Not used for this operation.
- **RestrictionEndTimeUTC:** Not used for this operation.
- **RestrictionStartTimeUTC:** Not used for this operation.
- **ScheduleRestrictionType:** Not used for this operation.
- **SharedCredentialListName:** Not used for this operation.
- **SystemName:** Not used for this operation.

Example Request

```
{
   "AuthenticationToken":"LVEEQGCFXVJAY6MON1A05FAETIINS0EB",
   "Permission":{
      "IdentityName":"lsds\\cletus",
      "JobID":"66"
   }
}
```

Output Success

A successful operation will state "*Updated delegation permission for identity IDENTITY on job JOBID*".

Example Success Output

```
{
   "OperationMessage": "Updated delegation permission for identity lsds\\cletus on job 66",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid identity**

  Log in failed, or the username provided was not found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Login failed or username
not found'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/Identity/ManagementSet (POST)

Delegation/Identity/ManagementSet associates an existing management set with an existing delegation identity. Management sets are added at the global delegation level.

Permissions Required

- Manage Delegations

Related Commands

- **PowerShell:** New-LSDelegationManagementSetForIdentity
- **SOAP:** DelegationOps_GetManagedGroupsForIdentity

Syntax

```
{
   "AuthenticationToken":"String content",
   "GroupName":"String content",
   "IdentityName":"String content"
}
```

Parameters

- **AuthenticationToken:** The authentication token of the requesting user.
- **GroupName:** The management set to associate with IdentityName.
- **IdentityName:** The identity that will have a management set associated with it. For domain identities, be sure to use two backslashes in the identity name.

Example Request

```
{
   "AuthenticationToken":"FKVM4T464CWG1OUF499XCWIZUFMGHXMD",
   "GroupName":"Web Servers - DMZ",
   "IdentityName":"lsds\\lscadmin"
}
```

Output Success

The output states the identity is now managing the management set.

Example Success Output

```
{
   "OperationMessage": "Identity with name lsds\\lscadmin is now managing the management set Web
Servers - DMZ",
```

```
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid IdentityName**

  The database call unexpectedly returned no data. Or the file was not found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'A database call
unexpectedly returned no data or a file was not found'. See server logs for more details. The
exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/SelfRecoveryPermission (POST)

DelegationOps_SelfRecoveryPermission_Add creates new self-recovery delegations.

Permissions Required

- Manage Delegations

Related Commands

- **PowerShell:** New-LSDelegationPermissionForSelfRecovery
- **SOAP:** DelegationOps_SelfRecoveryPermission_Add

Syntax

```
{
   "AuthenticationToken":"String content",
   "Permission":{
      "AccountName":"String content",
      "IdentityName":"String content",
      "Namespace":"String content",
      "SystemName":"String content"
   }
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **AccountName:** The target account name associated with the SystemName and NameSpace.
- **IdentityName:** The identity to create the new self-recovery rule. For domain identities, be sure to use two backslashes in the identity name.
- **NameSpace:** - The target namespace. See Namespace Values in the Administrator's Guide Addenda section.
- **SystemName:** - The target system.

Example Request

```
{
   "AuthenticationToken":"W6Y1TEUHVNNGVEC1C824J67Q9PHTQIXN",
   "Permission":{
      "AccountName":"wsdmzsvcacct",
      "IdentityName":"lsds\\lscadmin",
      "Namespace":"lsds",
      "SystemName":"lsds.int"
   }
}
```

Output Success

The output message will indicate the self-recovery permissions was created.

Example Success Output

```
{
   "OperationMessage": "Created self recovery permission for identity lsds\\lscadmin to
(lsds.int)'lsds\\wsdmzsvcacct'",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Delegation already Exists**

  The self recovery permission for the identity already exists.

Example Fail Output

```
{
   "OperationMessage": "Self recovery permission for identity lsds\\lscadmin to
(lsds.int)'lsds\\wsdmzsvcacct' already exists",
   "OperationSucceeded": false
}
```

REST: Delegation/SharedCredentialList (POST)

Delegation/SharedCredentialList adds or updates shared credential list delegations. The shared credential list set must already exist to apply the permissions.

Permissions Required

Either:

- Manage Permissions on the list
- Manage External Lists

Related Commands

- **PowerShell:** Set-LSDelegationPermissionOnSharedCredentialList
- **SOAP:** DelegationOps_SetPermissionsForSharedCredentialList

Syntax

```
{
   "AuthenticationToken":"String content",
   "Permission":{
      "CredentialListName":"String content",
      "IdentityName":"String content",
      "PermissionAddPassword":true,
      "PermissionChangeDelegation":true,
      "PermissionDeletePassword":true,
      "PermissionEditPassword":true,
      "PermissionGrantRequest":true,
      "PermissionRecoverPassword":true,
      "PermissionRequestPassword":true,
      "PermissionViewList":true
   }
}
```

Parameters

Any permissions not included will be set to false.

- **AuthenticationToken:** The authentication token of the calling user.
- **DelegationSharedCredentialListPermission:**
    - **CredentialListName:** The name of the shared credential list.
    - **IdentityName:** The name of the target identity. For domain identities, be sure to use two backslashes in the identity name.
    - **PermissionAddPassword :** Boolean. False or true to disable or enable adding passwords to the target SCL.
    - **PermissionChangeDelegation:** Boolean. False or true to disable or enable changing permissions on the target SCL.
    - **PermissionDeletePassword:** Boolean. False or true to disable or enable deleting passwords from the target SCL.
    - **PermissionEditPassword:** Boolean. False or true to disable or enable modifying passwords in the target SCL.

- **PermissionGrantRequest:** Boolean. False or true to disable or enable granting requests to passwords in the target SCL.
- **PermissionRecoverPassword:** Boolean. False or true to disable or enable viewing passwords from the target SCL.
- **PermissionRequestPassword:** Boolean. False or true to disable or enable requesting passwords from the target SCL.
- **PermissionViewList** Boolean. False or true to disable or enable viewing the list of credentials stored in the SCL.

Example Request

```
{
   "AuthenticationToken":"CE4SFC9027R2FARIORJIZOKLBTIY6A4N",
   "Permission":{
      "CredentialListName":"List-0001",
      "IdentityName":"lsds\\cletus",
      "PermissionAddPassword":false,
      "PermissionChangeDelegation":false,
      "PermissionDeletePassword":false,
      "PermissionEditPassword":false,
      "PermissionGrantRequest":false,
      "PermissionRecoverPassword":false,
      "PermissionRequestPassword":true,
      "PermissionViewList":true
   }
}
```

Output Success

A successful operation will state "*Updated delegation on shared credential list LIST, identity IDENTITY now has permissions*".

Example Success Output

```
{
   "OperationMessage": "Updated delegation on shared credential list List-0001, identity
lsds\\cletus now has permissions",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid list**

  The shared credential list could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Could not find a shared
credential list with the name specified'. See server logs for more details. The exception stack
trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/StoredCredential (POST)

Delegation/StoredCredential adds or updates per-account delegations. A stored password for the target system, account, and namespace must already exist to apply the per-account permissions to.

Permissions Required

- Manage Delegations

Related Commands

- **PowerShell:**Set-LSDelegationPermissionOnAccount
- **SOAP:** DelegationOps_SetPermissionOnAccount

Syntax

```
{
   "AuthenticationToken":"String content",
   "Permission":{
      "AccountName":"String content",
      "AlertForChange":true,
      "AlertForIncident":true,
      "IdentityName":"String content",
      "Namespace":"String content",
      "PermissionAllowRemoteSessions":true,
      "PermissionGrantPasswordRequests":true,
      "PermissionRequestPasswords":true,
      "PermissionRequestRemoteAccess":true,
      "PermissionViewAccounts":true,
      "PermissionViewPasswords":true,
      "SystemName":"String content"
   }
}
```

Parameters

Any permissions not included will be set to **False**.

- **AuthenticationToken:** The authentication token of the calling user.
- Permission:
    - **AccountName:** *(String)* The name of the target account on the target system.
    - **AlertForIncident:** *(Boolean)* False or true to disable or enable alert emails during a password request for the target account when INCIDENT is selected.
    - **AlertForChange:** *(Boolean)* False or true to disable or enable alert emails during a password request for the target account when CHANGE is selected.
    - **IdentityName:** *(String)* The name of the target identity. For domain identities, be sure to use two backslashes in the identity name.
    - **Namespace:** *(String)* The namespace of the target system. See Namespace Values for a list of pre-defined values.

- **PermissionAllowRemoteSessions:** *(Boolean)* False or true to disable or enable RDP/SSH/Telnet access with the target account (web site).
- **PermissionGrantPasswordRequests:** *(Boolean)* False or true to disable or enable granting password requests for the target account.
- **PermissionRequestPasswords:** *(Boolean)* False or true to disable or enable requesting access to the password.
- **PermissionRequestRemoteAccess:** *(Boolean)* False or true to disable or enable requesting remote access with the account.
- **PermissionViewAccounts:** *(Boolean)* False or true to disable or enable viewing of the account. This value should be set to 1 in order to view the account in the web site.
- **PermissionViewPasswords:** *(Boolean)* False or true to disable or enable recovering of the password.
- **SystemName:** *(String)* The name of the target system. For systems that include additional identifiers, like LDAP directories or database, be sure to use two backslashes in the system name.

Example Request

```
{
   "AuthenticationToken":"2FKAMM4HPEQQ61KKCC4JPDGUQJ9LWO2U",
   "Permission":{
      "AccountName":"sa",
      "AlertForChange":true,
      "AlertForIncident":false,
      "IdentityName":"lsds\\cletus",
      "Namespace":"[sql server]",
      "PermissionAllowRemoteSessions":true,
      "PermissionGrantPasswordRequests":true,
      "PermissionRequestPasswords":false,
      "PermissionRequestRemoteAccess":true,
      "PermissionViewAccounts":true,
      "PermissionViewPasswords":true,
      "SystemName":"dbag02\\mssqlserver"
   }
}
```

Output Success

A successful update will state "*Updated delegation permission for identity IDENTITY on account (SYSTEMNAME)'NAMESPACE\ACCOUNTNAME*"

Example Success Output

```
{
   "OperationMessage": "Updated delegation permission for identity lsds\\cletus on account
(dbag02\\mssqlserver)'[sql server]\\sa'",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid identity**

  Log in failed, or the username provided was not found.

- **Invalid SystemName** -or- **Namespace** -or- **AccountName**

  The specified password was not found in the store.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Password specied was not
found in store'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/System (POST)

Delegation/System adds or updates per-system delegations. The system must already exist to apply the per-system permissions.

Permissions Required

- Manage delegations

Related Commands

- **PowerShell:** Set-LSDelegationPermissionOnSystem
- **SOAP:** DelegationOps_SetPermissionsOnSystem

Syntax

```
{
   "AuthenticationToken":"String content",
   "Permission":{
      "AlertForChange":true,
      "AlertForIncident":true,
      "IdentityName":"String content",
      "PermissionAllowRemoteSessions":true,
      "PermissionElevateAccountPermissions":true,
      "PermissionGrantPasswordRequests":true,
      "PermissionRequestPasswords":true,
      "PermissionRequestRemoteAccess":true,
      "PermissionViewAccounts":true,
      "PermissionViewPasswords":true,
      "PermissionViewSystems":true,
      "SystemName":"String content"
   }
}
```

Parameters

Any permissions not included will be set to 0 (False).

- **AuthenticationToken:** The authentication token of the calling user.
- **DelegationPermissionOnSystem:**
  - **AlertForIncident:** *(Boolean)* False or true to disable or enable alert emails during a password request for the target account when INCIDENT is selected.
  - **AlertForChange:** *(Boolean)* False or true to disable or enable alert emails during a password request for the target account when CHANGE is selected.
  - **IdentityName:** The name of the target identity.
  - **PermissionAllowRemoteSessions:** *(Boolean)* False or true to disable or enable RDP/SSH/Telnet access with the target account (web site).
  - **PermissionElevateAccountPermissions** *(Boolean)* False or true to disable or enable self-service account elevation.
  - **PermissionGrantPasswordRequests:** *(Boolean)* False or true to disable or enable granting password requests for the target account.

- **PermissionRequestPasswords:** *(Boolean)* False or true to disable or enable requesting access to the password.
- **PermissionRequestRemoteAccess:** *(Boolean)* False or true to disable or enable requesting remote access to the system using RDP/SSH/Telnet access with the target account (web site).
- **RemoteAccessPermissionViewAccounts:** *(Boolean)* False or true to disable or enable viewing of the account. This value should be set to 1 in order to view the account in the web site.
- **PermissionViewPasswords:** *(Boolean)* False or true to disable or enable recovering of the password.
- **PermissionViewSystems:** *(Boolean)* False or true to disable or enable viewing the system. The value should be set to 1 in order to view the system and its accounts in the web interface.
- **SystemName:** The name of the target system.

Example Request

```
{
   "AuthenticationToken":"BRWQM47FE9E340ZHADIES7H8RHQ9PWPH",
   "Permission":{
      "AlertForChange":true,
      "AlertForIncident":true,
      "IdentityName":"lsds\\cletus",
      "PermissionAllowRemoteSessions":true,
      "PermissionElevateAccountPermissions":true,
      "PermissionGrantPasswordRequests":true,
      "PermissionRequestPasswords":false,
      "PermissionRequestRemoteAccess":false,
      "PermissionViewAccounts":true,
      "PermissionViewPasswords":true,
      "PermissionViewSystems":true,
      "SystemName":"radaus2k3"
   }
}
```

Output Success

A successful update will state "*Updated delegation permission for identity IDENTITY on system SYSTEM*".

Example Success Output

```
{
   "OperationMessage": "Updated delegation permission for identity lsds\\cletus on system
radaus2k3",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid identity**

  Log in failed, or the username provided was not found.

- **Invalid system**

  The system information could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Could not find system
information with the system specified'. See server logs for more details. The exception stack trace
is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/File (PUT)

Delegation/File adds permissions to a file in the file store for an identity. If the identity already has permissions, those permissions are replaced. Delegation/File/Identity (POST) performs the same function as this API, using the POST method.

Permissions Required

- Change permissions for the target file

Related Commands

- **PowerShell:** Set-LSDelegationPermissionForIdentityOnFile
- **SOAP:** DelegationOps_StoredFile_SetPermissions

Syntax

```
{
   "AuthenticationToken":"String content",
   "FilePermission":{
      "FileName":"String content",
      "IdentityName":"String content",
      "PermissionDelegate":true,
      "PermissionDelete":true,
      "PermissionDownload":true,
      "PermissionGrant":true,
      "PermissionRequest":true,
      "PermissionUpdate":true,
      "PermissionView":true
   }
}
```

Parameters

- **AuthenticationToken:** Authentication token of the calling user.
- **IdentityName - string:** Name of identity of which to modify/add permissions. For domain identities, be sure to use two backslashes in the identity name.
- **DelegationFilePermission:** An object containing the file permissions.
    - **FileName - string:** The name of the file.
    - **PermissionDelegate - bool:** False or true to disable or enable managing delegations for the file.
    - **PermissionDelete - bool:** False or true to disable or enable deleting the file.
    - **PermissionDownload - bool:** False or true to disable or enable downloading/checking out the file.
    - **PermissionGrant - bool:** False or true to disable or enable granting requests for access to the file.
    - **PermissionRequest - bool:** False or true to disable or enable requesting the file.
    - **PermissionUpdate - bool:** False or true to disable or enable updating the file with a new version.
    - **PermissionView - bool:** False or true to disable or enable viewing the file.

Example Request

```
{
   "AuthenticationToken":"2XH8T5KKQCDH8NIJPNLFJ9D0RGZVSATR",
   "FilePermission":{
      "FileName":"tuscany.txt",
      "IdentityName":"lsds\\cletus",
      "PermissionDelegate":true,
      "PermissionDelete":false,
      "PermissionDownload":true,
      "PermissionGrant":false,
      "PermissionRequest":true,
      "PermissionUpdate":false,
      "PermissionView":true
   }
}
```

Output Success

A successful update will state "*File permissions updated for file: FILENAME (File ID: XX) - Manager IDENTITY has permissions: PERMISSIONS*".

Example Success Output

```
{
   "OperationMessage": "File permissions updated for file: tuscany.txt (File ID: 3) - Manager
lsds\\cletus has permissions: Read Download Delegate Request ",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid identity**

  The identity name could not be found. Or, the edit process failed.

- **Invalid file or no permissions**

  No files were found with this name, or you do not have permission to the view files.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'No files were found with
this name or insufficient permission to view files'. See server logs for more details. The exception
stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/Identity (PUT)

Delegation/Identity is used to configure the web application global delegations of an existing target identity. This function replaces the existing settings and permissions for a delegation identity with those specified in the **IdentitySettings** parameter. If the intent is to modify specific settings for a user and change only some of the parameters, call Delegation/Identity (GET) and enumerate the resulting structure to get the existing settings for the target identity, then make changes to that object and pass it back as the input parameter.

Permissions Required

- Manage Delegations

Related Commands

- **PowerShell:** Set-LSDelegationIdentitySettings
- **SOAP:** DelegationOps_SetIdentitySettings

Syntax

```
{
   "AuthenticationToken":"String content",
   "Identity":{
      "AccountName":"String content",
      "AlertOnRecovery":true,
      "AlertOnRequest":true,
      "DisplayName":"String content",
      "EmailAddress":"String content",
      "IsDomainAccount":0,
      "Password":"String content",
      "PermissionAccessRemoteSessions":true,
      "PermissionAddPasswordsForManagedSystems":true,
      "PermissionAllAccess":true,
      "PermissionCreateRefreshSystemJob":true,
      "PermissionEditDelegation":true,
      "PermissionEditPasswordLists":true,
      "PermissionEditStoredPasswords":true,
      "PermissionElevateAccountPermissions":true,
      "PermissionElevateAnyAccountPermissions":true,
      "PermissionGrantPasswordRequests":true,
      "PermissionIgnorePasswordCheckout":true,
      "PermissionLogon":true,
      "PermissionPersonalStore":true,
      "PermissionRequestPasswords":true,
      "PermissionRequestRemoteAccess":true,
      "PermissionRequireOATH":true,
      "PermissionRequireRSASecurID":true,
      "PermissionSelfRecovery":true,
      "PermissionViewAccounts":true,
      "PermissionViewDashboards":true,
      "PermissionViewDelegation":true,
      "PermissionViewFileStore":true,
      "PermissionViewJobs":true,
```

```
        "PermissionViewPasswordActivity":true,
        "PermissionViewPasswordHistory":true,
        "PermissionViewPasswords":true,
        "PermissionViewScheduler":true,
        "PermissionViewSystems":true,
        "PermissionViewWebLogs":true
    }
}
```

Parameters

- **AuthenticationToken:** Authentication token of the calling user.
- **Identity:** Includes one enumerated type and multiple values:
    - **AccountName:** String. The name of the identity. For domain identities, be sure to use two backslashes in the identity name.
    - **AlertOnRecovery:** Boolean. Used in conjunction with EmailAddress. Set to true to enable email notifications when a password or access request is made for a system or account the identity can grant access requests for.
    - **AlertOnRequest:** Boolean. Used in conjunction with EmailAddress. Set to true to enable email notifications when a password or access request is made for a system or account the identity can grant access requests for.
    - **DisplayName:** String. Sets the display name of the account. If omitted, uses AccountName. For domain identities, be sure to use two backslashes in the identity name.
    - **EmailAddress:** - String. Email address for the identity.
    - **IsDomainAccount:** Enumerated value, eManagerType. Available values are:
        - **0** = MANAGER_TYPE_EXPLICIT_USER
        - **1** = MANAGER_TYPE_DOMAIN_USER
        - **2** = MANAGER_TYPE_DOMAIN_GROUP
        - **3** = MANAGER_TYPE_SELF_RECOVERY
        - **4** = MANAGER_TYPE_ROLE
        - **5** = MANAGER_TYPE_RADIUS
        - **6** = MANAGER_TYPE_CERTFICATE
        - **7** = MANAGER_TYPE_LDAP_USER
    - **Password:** String. Will set the password for an explicit account.
    - **PermissionAccessRemoteSessions:** Boolean. False or true to disable or enable access to remote sessions (RDP & SSH/Telnet).
    - **PermissionAddPasswordsForManagedSystems:** Boolean. False or true to disable or enable adding/editing stored managed passwords.
    - **PermissionAllAccess:** Boolean. False or true to disable or enable All Access.
    - **PermissionCreateRefreshSystemJob:** Boolean. False or true to disable or enable creating new jobs.
    - **PermissionEditDelegation:** Boolean. False or true to disable or enable managing delegations.
    - **PermissionEditPasswordLists:** Boolean. False or true to disable or enable editing of passwords in password lists.
    - **PermissionEditStoredPasswords:** Boolean. False or true to disable or enable editing stored passwords.
    - **PermissionElevateAccountPermissions:** Boolean. False or true to disable or enable Elevate Account (self-elevation).
    - **PermissionElevateAnyAccountPermissions:** Boolean. False or true to disable or enable Elevate Any Account.

- **PermissionGrantPasswordRequests:** Boolean. False or true to disable or enable Grant Password Requests.
- **PermissionIgnorePasswordCheckout:** Boolean. False or true to disable or enable Ignore Password Checkout (programmatic access only).
- **PermissionLogon:** Boolean. False or true to disable or enable web logon.
- **PermissionPersonalStore:** Bool. False or true to disable or enable access to the personal password store.
- **PermissionRequestPasswords:** Boolean. False or true to disable or enable Request Passwords.
- **PermissionRequestRemoteAccess:** - Boolean. False or true to disable or enable Request Passwords.
- **PermissionRequireOATH:** Boolean. False or true to disable or enable requirement for OATH two factor authentication.
- **PermissionRequireRSASecurID:** Boolean. False or true to disable or enable requirement of two factor authentication.
- **PermissionSelfRecovery:** Boolean. False or true to disable or enable access to Self-Recovery.
- **PermissionViewAccounts:** Boolean. False or true to disable or enable View Accounts.
- **PermissionViewDashboards:** Boolean. False or true to disable or enable access to the dashboards (when enabled).
- **PermissionViewDelegation:** Boolean. False or true to disable or enable Viewing Delegations.
- **PermissionViewFileStore:** Boolean. False or true to disable or enable access to File Repository.
- **PermissionViewJobs:** Boolean. False or true to disable or enable View Jobs.
- **PermissionViewPasswordActivity:** Boolean. False or true to disable or enable access to the Password Activity.
- **PermissionViewPasswordHistory:** Boolean. False or true to disable or enable access to managed Password History.
- **PermissionViewPasswords:** Boolean. False or true to disable or enable Recover Passwords.
- **PermissionViewScheduler:** Boolean. False or true to disable or enable Manage Scheduled Jobs.
- **PermissionViewSystems:** Boolean. False or true to disable or enable View Systems.
- **PermissionViewWebLogs:** Boolean. False or true to disable or enable View Web Logs.

Example Request


```
{
   "AuthenticationToken":"01A5JAVQ32QV2BC9CZARMUSJF0ESJQOH",
   "Identity":{
      "AccountName":"lsds\\corky",
      "AlertOnRecovery":true,
      "AlertOnRequest":true,
      "DisplayName":"lsds\\corky",
      "EmailAddress":"corky@lsds.int",
      "IsDomainAccount":1,
      "PermissionAccessRemoteSessions":true,
      "PermissionAddPasswordsForManagedSystems":true,
      "PermissionAllAccess":false,
      "PermissionCreateRefreshSystemJob":true,
      "PermissionEditDelegation":true,
      "PermissionEditPasswordLists":true,
      "PermissionEditStoredPasswords":true,
      "PermissionElevateAccountPermissions":true,
      "PermissionElevateAnyAccountPermissions":true,
      "PermissionGrantPasswordRequests":true,
      "PermissionIgnorePasswordCheckout":true,
      "PermissionLogon":true,
```

```
      "PermissionPersonalStore":true,
      "PermissionRequestPasswords":false,
      "PermissionRequestRemoteAccess":false,
      "PermissionRequireOATH":false,
      "PermissionRequireRSASecurID":false,
      "PermissionSelfRecovery":true,
      "PermissionViewAccounts":true,
      "PermissionViewDashboards":true,
      "PermissionViewDelegation":false,
      "PermissionViewFileStore":true,
      "PermissionViewJobs":false,
      "PermissionViewPasswordActivity":true,
      "PermissionViewPasswordHistory":true,
      "PermissionViewPasswords":true,
      "PermissionViewScheduler":false,
      "PermissionViewSystems":true,
      "PermissionViewWebLogs":true
   }
}
```

Output Success

A successful update states "*Identity with name IDENTITY updated - Added permissions: PERMISSIONS Removed permissions: PERMISSIONS*". Permissions added or removed will be listed in series, separated by commas.

Example Success Output

```
{
   "OperationMessage": "Identity with name lsds\\corky updated - Added permissions: view dashboards
Removed permissions: request passwords, request remote access, require 2 factor, require OATH",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid Identity**

  The identity name could not be found. Or, the edit process failed.

Example Fail Output

```
{
   "OperationMessage": "Identity with name lsds\\reynaldo could not be found, edit failed",
```

```
   "OperationSucceeded": false
}
```

REST: Delegation/AccountMask (DELETE)

Delegation/AccountMask removes an account mask associated with a target identity.

Permissions Required

- Manage Delegations

Related Commands

- **PowerShell:** Remove-LSDelegationPermissionAccountMask
- **SOAP:** DelegationOps_AccountMaskPermission_Remove

Syntax

```
{
   "AuthenticationToken":"String content",
   "Permission":{
      "AccountMask":"String content",
      "IdentityName":"String content"
   }
}
```

Parameters

- **AuthenticationToken:** Authentication token of the calling user.
- **AccountMask:** The account mask to disassociate from the target identity.
- **IdentityName:** The name of the target identity. For domain identities, be sure to use two backslashes in the identity name.

Example Request

```
{
   "AuthenticationToken":"VQVUW68JF1X5T3ISRPNWZP9NJ0PRQ7AQ",
   "Permission":{
      "AccountMask":"*admin",
      "IdentityName":"lsds\\cletus"
   }
}
```

Output Success

Successful removal will state "*Removed account mask for identity IDENTITY from MASK*".

Example Success Output

```
{
   "OperationMessage": "Removed account mask for identity lsds\\cletus from *admin",
```

```
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid identity name**

  The database call unexpectedly returned no data. Or the file was not found.

- **Invalid account mask**

  No account mask for identity IDENTITY to MASK exists.

Example Fail Output - Invalid Account Mask

```
{
   "OperationMessage": "No account mask for identity lsds\\cletus to *admin exists",
   "OperationSucceeded": false
}
```

Example Fail Output - Invalid Identity Name

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'A database call
unexpectedly returned no data or a file was not found'. See server logs for more details. The
exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
```

```
        </div>
    </body>
</html>
```

REST: Delegation/File/Identity (DELETE)

Delegation/File/Identity remove all permissions from a file for the target identity.

Permissions Required

- Access File Repository
- Change permissions on target file

Related Commands

- **PowerShell:** Remove-LSDelegationPermissionForIdentityOnFile
- **SOAP:** DelegationOps_StoredFile_RemoveIdentityPermissions

Syntax

```
{
   "AuthenticationToken":"String content",
   "FileName":"String content",
   "IdentityName":"String content"
}
```

Parameters

- **AuthenticationToken:** Authentication token of the calling user.
- **FileName:** The name of the file to remove all permissions associated with the target identity.
- **IdentityName:** The name of the target identity. For domain identities, be sure to use two backslashes in the identity name.

Example Request

```
{
   "AuthenticationToken":"CQF27GXV5XUYGJFMX316OVKY8M1TJDK5",
   "FileName":"tuscany.txt",
   "IdentityName":"lsds\\cletus"
}
```

Output Success

Successful removal will state "*Removed permissions from identity IDENTITY on file FILE*".

Example Success Output

```
{
   "OperationMessage": "Removed permissions from identity lsds\\cletus on file tuscany.txt",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid file name**

  No files were found with this name, or you do not have permission to the view files.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'No files were found with
this name or insufficient permission to view files'. See server logs for more details. The exception
stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/Identity (DELETE)

Delegation/Identity removes a specific delegation identity and any permissions associated with the identity.

Permissions Required

- Manage Delegations

Related Commands

- **PowerShell:** Remove-LSDelegationIdentity
- **SOAP:** DelegationOps_DeleteIdentity

Syntax

```
{
   "AuthenticationToken":"String content",
   "IdentityName":"String content"
}
```

Parameters

- **AuthenticationToken:** Authentication token of the calling user.
- **IdentityName:** The identity to create the new self-recovery rule. For domain identities, be sure to use two backslashes in the identity name.

Example Request

```
{
   "AuthenticationToken":"IDM2PZMH7N62STY70822YQ1PIPMUXONB",
   "IdentityName":"gyro"
}
```

Output Success

A successful removal will indicate "*Identity with name NAME deleted*".

Example Success Output

```
{
   "OperationMessage": "Identity with name gyro deleted",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid identity specified**

  The database call unexpectedly returned no data. Or the file was not found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Could not find delegation
identity'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/Identity/Role (DELETE)

Delegation/Identity/Role removes usernames from identity role mappings.

Permissions Required

- Manage Delegations

Related Commands

- **PowerShell:** Remove-LSDelegationPermissionRoleMapping
- **SOAP:** DelegationOps_RoleMappingPermission_Remove

Syntax

```
{
   "AuthenticationToken":"String content",
   "Permission":{
      "Authenticator":"String content",
      "CredentialName":"String content",
      "RoleName":"String content"
   }
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **AuthenticationServer:** The authentication server entry the CredentialName is associated with.
- **CredentialName:** The name of the account from the authentication server entry to remove from the identity-role.
- **RoleName:** The name of the identity role to modify.

Example Request

```
{
   "AuthenticationToken":"DI80PBVDSKOC1YB1MMO408FB62RI3QBC",
   "Permission":{
      "Authenticator":"lsds.int",
      "CredentialName":"lscadmin",
      "RoleName":"Administrator User"
   }
}
```

Output Success

A successful removal will state *"Permission for role ROLE on authenticator AUTHENTICATIONSERVER deleted for credential CREDENTIAL*".

Example Success Output

```
{
   "OperationMessage": "Permission for role Administrator User on authenticator lsds.int deleted for
credential lscadmin",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid identity** -or- **Invalid authentication server** -or- **Invalid credential**

  Permission for the role on the authentication server does not exist for the credential.

Example Fail Output

```
{
   "OperationMessage": "Permission for role Administrator User on authenticator lsds.int does not
exist for credential lscadmin",
   "OperationSucceeded": true
}
```

REST: Delegation/Job (DELETE)

Delegation/Job removes permissions for a specific job from an identity.

Permissions Required

- Manage Delegations

Related Commands

- **PowerShell:** Remove-LSDelegationPermissionOnJob
- **SOAP:** DelegationOps_RemovePermissionOnJob

Syntax

```
{
   "AuthenticationToken":"String content",
   "IdentityName":"String content",
   "JobID":"String content"
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **IdentityName:** The target identity. For domain identities, be sure to use two backslashes in the identity name.
- **JobID:** The target job.

Example Request

```
{
   "AuthenticationToken":"02OQ286UEYTEXI2LQFEG0HBNFVHOC7BT",
   "IdentityName":"lsds\\cletus",
   "JobID":"10"
}
```

Output Success

A successful removal will state "*Updated delegation on job JOBID, identity IDENTITY permissions removed*".

Example Success Output

```
<pre xml:space="preserve">{
   "AuthenticationToken":"02OQ286UEYTEXI2LQFEG0HBNFVHOC7BT",
   "IdentityName":"lsds\\cletus",
   "JobID":"10"
}</pre>
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid AccountName**

  Login failed. Or, the username could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Login failed or username
not found'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/ManagementSet (DELETE)

Delegation/ManagementSet removes the per-management set permissions assigned to a target identity for a specific management set.

Permissions Required

- Manage Delegations

Related Commands

- **PowerShell:** Remove-LSDelegationPermissionOnManagementSet
- **SOAP:** DelegationOps_RemovePermissionOnManagementSet

Syntax

```
{
   "AuthenticationToken":"String content",
   "IdentityName":"String content",
   "ManagementSetName":"String content"
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **IdentityName:** The target identity. For domain identities, be sure to use two backslashes in the identity name.
- **ManagementSet:** The target management set.

Example Request

```
{
   "AuthenticationToken":"I4TAU5IYUK92ZILW9JKZ01QTC08CEZKC",
   "IdentityName":"lsds\\cletus",
   "ManagementSetName":"WebService Management Set"
}
```

Output Success

Successful removal will state "*Updated delegation on management set MANAGEMENTSET, identity IDENTITY permissions removed*".

Example Success Output

```
{
   "OperationMessage": "Updated delegation on management set WebService Management Set, identity
lsds\\cletus permissions removed",
```

```
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid identity** -or- **Invalid management set**

  The specific permission could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Could not find the
permission specified'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/ManagementSet (DELETE)

Delegation/ManagementSet modifies global delegation permissions to remove target management set delegation from the target identity.

Permissions Required

- Manage Delegations

Related Commands

- **PowerShell:** Remove-LSDelegationManagementSetFromIdentity
- **SOAP:** DelegationOps_RemoveManagedGroupFromIdentity

Syntax

```
{
   "AuthenticationToken":"String content",
   "IdentityName":"String content",
   "ManagementSetName":"String content"
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **IdentityName:** The name of the target identity.
- **ManagementName:** The name of the target group to disassociate from the calling user. For domain identities, be sure to use two backslashes in the identity name.

Example Request

```
{
   "AuthenticationToken":"156IN9G9MSO15Z3FY9E4QO7RDYYV3Q8N",
   "IdentityName":"lsds\\cletus",
   "ManagementSetName":"WebService Management Set"
}
```

Output Success

Successful removal will state "*Identity with name NAME is no longer managing the management set MANAGEMENTSET, identity IDENITY permissions removed*".

Example Success Output

```
{
   "OperationMessage": "Updated delegation on management set WebService Management Set, identity
```

```
lsds\\cletus permissions removed",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid identity name**

  The specific permission could not be found.

- **No existing association of identity and management set Invalid management set name**

  The management set specified could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Could not find the
permission specified'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/SelfRecoveryPermission (DELETE)

Delegation/SelfRecoveryPermission removes a self-recovery permission associated with the target identity.

Permissions Required

- Manage Delegations

Related Commands

- **PowerShell:** Remove-LSDelegationPermissionForSelfRecovery
- **SOAP:** DelegationOps_SelfRecoveryPermission_Remove

Syntax

```
{
   "AuthenticationToken":"String content",
   "Permission":{
      "AccountName":"String content",
      "IdentityName":"String content",
      "Namespace":"String content",
      "SystemName":"String content"
   }
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **AccountName:** The target account defined in the self recovery permission.
- **IdentityName:** The target identity to remove the self recovery permission for. For domain identities, be sure to use two backslashes in the identity name.
- **NameSpace:** The target name space defined in the self recovery permission.
- **SystemName:** The target system name defined in the self recovery permission.

Example Request

```
{
   "AuthenticationToken":"IMC5XI96ZN4PAASFJ4PKZL8VBB3EW7EG",
   "Permission":{
      "AccountName":"Administrator",
      "IdentityName":"lsds\\cletus",
      "Namespace":"lsdslscprd",
      "SystemName":"lsdslscprd"
   }
}
```

Output Success

Successful removal will state "Removed permissions from identity IDENTITY on file FILE".

Example Success Output

```
{
   "OperationMessage": "Removed self recovery permission for identity lsds\\cletus from
(lsdslscprd)'lsdslscprd\\Administrator'",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid AccountName** -or- **Invalid SystemName** -or- **NameSpace** -or- **AccountName**

  No self recovery permission exists for the identity.

Example Fail Output

```
{
   "OperationMessage": "No self recovery permission for identity lsds\\cletus to
(lsdslscprd)'lsdslscprd\\Administrator' exists",
   "OperationSucceeded": false
}
```

REST: Delegation/SharedCredentialList (DELETE)

Delegation/SharedCredentialList removes an identity's permissions from a shared credential list.

Permissions Required

- Manage permissions for the target shared credential list

Related Commands

- **PowerShell:**Remove-LSDelegationPermissionOnSharedCredentialList
- **SOAP:** DelegationOps_RemovePermissionForSharedCredentialList

Syntax

```
{
   "AuthenticationToken":"String content",
   "IdentityName":"String content",
   "SharedCredentialListName":"String content"
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **IdentityName:** The target identity. For domain identities, be sure to use two backslashes in the identity name.
- **SharedCredentialList:** The target management set.

Example Request

```
{
   "AuthenticationToken":"70DATPFXCR8XC2X50N88HPP5ONDS0VWY",
   "IdentityName":"lsds\\cletus",
   "SharedCredentialListName":"List-0001"
}
```

Output Success

Successful removal will state "*Updated delegation on shared credential list SHAREDCREDENTIALLIST, identity IDENTITY permissions removed*".

Example Success Output

```
{
   "OperationMessage": "Updated delegation on shared credential list List-0001, identity
lsds\\cletus permissions removed",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid identity**

  Log in failed, or the username provided was not found.

- **Invalid shared credential list**

  The shared credential list could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Could not find shared
credential list with the name specified'. See server logs for more details. The exception stack
trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/StoredCredential (DELETE)

Delegation/StoredCredential removes a per-account permission.

Permissions Required

- Manage Delegations

Related Commands

- **PowerShell:** Remove-LSDelegationPermissionOnAccount
- **SOAP:** DelegationOps_RemovePermissionOnAccount

Syntax

```
{
   "AuthenticationToken":"String content",
   "AccountIdentificationInfo":{
      "AccountName":"String content",
      "AccountStore":{
         "CustomTypeName":"String content",
         "TargetName":"String content",
         "Type":0
      },
      "PasswordList":"String content"
   },
   "IdentityName":"String content"
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **AccountName:** The target account defined in the per-account permission formatted as Namespace\\AccountName. Be sure to use two backslashes in the account name.
- **AccountStore:**
    - **CustomTypeName:** (Optional) - Required when Type is set to "Custom"
    - **TargetName:** The target system name defined in the per-account permission.
    - **Type:** Identifies the namespace. Valid options are:
        - **0** = Unknown
        - **1** = OS_Windows
        - **2** = OS_UnixAndCompat
        - **3** = OS_AS400
        - **4** = OS_OS390
        - **5** = CommType_TN3270
        - **6** = BMC_IPMI_Generic
        - **7** = BMC_DRAC

- **8** = Router_Cisco
- **9** = DB_SQLServer
- **10** = DB_Oracle
- **11** = DB_Sybase
- **12** = DB_MySql
- **13** = DB_DB2
- **14** = Directory_OracleInternetDirectory
- **15** = Directory_Novell_eDirectory
- **16** = Directory_IBM_Tivoli
- **17** = Directory_ViewDS
- **18** = Custom
- **19** = PasswordList
- **20** = DB_PostgreSQL
- **21** = DB_Teradata
- **22** = OS_XeroxPhaser
- **23** = External

- **PasswordList:** Not used.
- **IdentityName:** The target identity to remove the self recovery permission for. For domain identities, be sure to use two backslashes in the identity name.

Example Request

```
{
   "AuthenticationToken":"0YO029FVJDDGLB4HQGL0IXCJNM951C6C",
   "AccountIdentificationInfo":{
      "AccountName":"lsds\\svcpool-1",
      "AccountStore":{
         "TargetName":"lsds.int",
         "Type":1
      }
   },
   "IdentityName":"lsds\\cletus"
}
```

Output Success

Successful removal will state "*Updated delegation on account (SYSTEMNAME)'NAMESPACE\ACCOUNT', identity IDENTITY permissions removed*".

Example Success Output

```
{
   "OperationMessage": "Updated delegation on account (lsds.int)'lsds\\svcpool-1', identity
lsds\\cletus permissions removed",
```

```
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid AccountName** -or- **Invalid SystemName** -or- **NameSpace** -or- **AccountName**

  The specific permission could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Could not find the
permission specified'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
</html>
```

REST: Delegation/System (DELETE)

Delegation/System removes a per-system permission.

Permissions Required

- Manage Delegations

Related Commands

- **PowerShell:** Remove-LSDelegationPermissionOnSystem
- **SOAP:** DelegationOps_RemovePermissionOnSystem

Syntax

```
{
   "AuthenticationToken":"String content",
   "IdentityName":"String content",
   "TargetIdentificationInfo":{
      "CustomTypeName":"String content",
      "TargetName":"String content",
      "Type":0
   }
}
```

Parameters

- **AuthenticationToken:** The authentication token of the calling user.
- **IdentityName:** The target identity. For domain identities, be sure to use two backslashes in the identity name.
- **CustomTypeName:** Reserved for future use.
- **TargetName:** The target system.
- **Type:** Identifies the namespace. Valid options are:
    - **0** = Unknown
    - **1** = OS_Windows
    - **2** = OS_UnixAndCompat
    - **3** = OS_AS400
    - **4** = OS_OS390
    - **5** = CommType_TN3270
    - **6** = BMC_IPMI_Generic
    - **7** = BMC_DRAC
    - **8** = Router_Cisco
    - **9** = DB_SQLServer
    - **10** = DB_Oracle
    - **11** = DB_Sybase

- **12** = DB_MySql
- **13** = DB_DB2
- **14** = Directory_OracleInternetDirectory
- **15** = Directory_Novell_eDirectory
- **16** = Directory_IBM_Tivoli
- **17** = Directory_ViewDS
- **18** = Custom
- **19** = PasswordList
- **20** = DB_PostgreSQL
- **21** = DB_Teradata
- **22** = OS_XeroxPhaser
- **23** = External

Example Request

```
{
   "AuthenticationToken":"216PNASKU8L4U9ILJ8CHC7AJXT1KW82S",
   "IdentityName":"lsds\\cletus",
   "TargetIdentificationInfo":{
      "TargetName":"dbag01",
      "Type":1
   }
}
```

Output Success

Successful removal will state "*Updated delegation on system SYSTEM, identity IDENTITY permissions removed*".

Example Success Output

```
{
   "OperationMessage": "Updated delegation on system dbag01, identity lsds\\cletus permissions
removed",
   "OperationSucceeded": true
}
```

Output Fail

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

- **Invalid identity** -or- **Invalid system**

  The specific permission could not be found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="https://lsdslscprd.lsds.int/ERPMWebService/AuthService.svc/REST/help">service help page</a>
for constructing valid requests to the service. The exception message is 'Could find the permission
specified'. See server logs for more details. The exception stack trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
   </body>
```

SSHKey (GET)

SSHKey retrieves a stored SSH key and returns it as a HEX encoded string.

Permissions Required

- All Access

Related Commands

- **SOAP:** AccountStoreOps_GetSSHKey

Syntax

```
https://serverName/ERPMWebService/AuthService.svc/REST/SSHKey?KeyLabel={KEYLABEL}&Comment=
{COMMENT}
```

Parameters

- **KeyLength:** The length of the SSH Key in bits.
- **KeySignature:** Signature for the key.
- **KeyType:** The type of SSH Key, such RSA or ECDSA.
- **Passphrase:** The passphrase associated with the SSH key.
- **PrivateKeyData:** The private key data.
- **PublicKeyData:** The public key data
- **PuttyKeyData:** The Putty key data.
- **User:** User associated with the SSH key.

Request

XML

The request body should be left empty.

JSON

The request body should be left empty.

Response

A successful operation will get the SSH Key Label and return the HEX-encoded string.

XML

JSON

```
[{
        "KeyLength":"String content",
```

```
        "KeySignature":"String content",
        "KeyType":"String content",
        "Passphrase":"String content",
        "PrivateKeyData":"String content",
        "PublicKeyData": "String content",
        "PuttyKeyData": "String content",
        "User": "String content"

}]
```

Example - XML

Request

The request body should be left empty.

Response

```
<SSHKeyData xmlns="http://example.com/2004/07/RouletteAppService_WCF">
       <KeyLength>2048</KeyLength>
       <KeyLabel>Demo</KeyLabel>
       <KeySignature>A4:D0:28:36:CF:9C:1D:24:1D:</KeySignature>
       <KeyType>RSA</KeyType>
       <Passphrase>P@ssw0rd</Passphrase>
       <PrivateKeyData>""-----BEGIN RSA PRIVATE KEY-----\r\nProc-Type: 4,ENCRYPTED\r\nDEK-Info: AES-128-
CBC,D7B79BBC75767334071B90871AE1CD88\r\n\r\nZoKGSr9gYBFos4I+XzkB61mRJIIvkCTjW8Nwznqply85vDcnrECCADNm
rLew7raP\r\nUYNCvzO6E/JtPf5RlDrTvZ8UP4O3cZ0QXkgbUft2vV3NaQtMWGhIIOo/J1k9chC6\r\njOyBD5sFqsuW4jDStMH2
6M+3PjOwE7r2BUKzr44zv8Db2f36arwiZr6w1VYRN/uj\r\nnnQfLFnR+Wph0Va/lVGzLaPbL/LtO+o2QOFz5Dte27m1TfMu87Tw
3l3ugAzeiy9x\r\n2sZgTTfgXNF3L94i/bIgLhuahZRhe171Vs69rJP58h40PsmP3j3w3iEfyxNRJpwg\r\nmw14Wkaz5YW/GqZ0
ivMFfZcVuzIXBJstb9dBtcmGs3zHGDV5pa7aEvi/B+ygxJUA\r\nbUwNX8TuuUFnrlltZcPGp9fM1eMQtykxlLZxT8oZBkhuhwNr
PtS2J5ZH7jUauCJ9\r\n40hhqLj/gBg7Jd+eyTaDgpfVDTcyVDjwcvfml6PAUI1YgKPfBNZ4b0y0Rw6Kibrc\r\nDBrHCz07Y1/U
BtBj9eEnlnI+8Dv6sIf+9cnDLGzSS/RoBD8Ppv3r8xtd7sfAoXUe\r\nSqFBXic0dVdRg5MfeLaxYa/K/L/cj3Po6ChveKxKTwYz
mV4RnlLTih6ifDpR9C8v\r\ny4qlP80Dg8qxaJWk+2c/ZFzMCHkGaqXXQe6baNLlqn8/chYevtUv856nZA7Y2Hcq\r\nxFdXaw3I
5NKREbnjTs7mBA7b3Im30nq6eW+ZSIBQZ6b39W5GmEn5IzG3bVSMOBWi\r\nhm1DJwWN5b+x+MbJrk/fUKmHIWhXb0VcrZQ8rvUB
cEGYyfrItCYRvtSYNPY2Qo7w\r\nrNi8Yt4P+UpAaprK79z2auE5wJLmjKarTGc3A+byCbwRUvL8D7hZUJBSTsHHnorM\r\nsfIZ
6yJSSiv7MxC/c3imCI3JvhHMrR1gye2lDIJ4HQ1IignPYZvkioyMLcV1VZ9I\r\nHSCsUQVDmgpOPKMaLcjafoOOh6ESwFMau9/1
fp+mVy8b+j2f1Jj8DO/JYS1gOEMY\r\nOoCgyK67HPbcuKqBIM9JU6oiU6Nbvwo5I911R4v42RzckHwcUZx7N1eCzoZIEPRY\r\n
0TlO7pT/9GJueb0+3aNPCvF/GFqtHFFVAf2jpd4tlkMfQKH4/am9p+JBPwthtgzt\r\nx8f9GpeiM11erx0BRG1sY48B+Jv9K1kQ
Mv1COV+gvT4DsFu7hzMvjFPDxyoqNL2R\r\nkZescXl4t8Wmzl79pgp6lqZaFV+sIZWWruhYlBFLs9TlTZZTsPJUkFHT4Mca/lkj
\r\nZvAm7MEgTJtZNwxuOkTqfrOHZEGVmDeljamAFCFIZMnW400eaoaOhOjKFbJDvSJl\r\nGImnpmq/NO6tLaVDTZbnIIPJRAWr
X7MLunGiTT/j3wXniQsZvw5FQPZP+dWSJA3U\r\n81hHmhAUaw8r9RIgoVFMeuv4qdy3bhVJiSqzaZRjknX4OiNrVapIGBZG9Qth
ZvKW\r\nStEreMEnbQQkq6DEKtPYD4sq64uLExLtV5CjZA5UnwWkO54aqIOGZbM8Nkexhkbw\r\nf2VAf8WfzbmNH5WCrOYPfwTU
vUNQATt6VBkDX/+MIQ4wBfOC8MAKGwuVm5FvGYYW\r\n-----END RSA PRIVATE KEY-----\r\n</PrivateKeyData>
       <PublicKeyData></PublicKeyData>
       <PuttyKeyData></PuttyKeyData>
       <User></User>
</SSHKeyData>
```

Example - JSON

Request

The request body should be left empty.

Response

```
{
	"KeyLength":"2048",
	"KeySignature":"A4:D0:28:36:CF:9C:1D:24:1D:",
	"KeyType":"RSA",
	"Passphrase":"P@ssw0rd",
	"PrivateKeyData": "-----BEGIN RSA PRIVATE KEY-----\r\nProc-Type: 4,ENCRYPTED\r\nDEK-Info: AES-128-
CBC,D7B79BBC75767334071B90871AE1CD88\r\n\r\nZoKGSr9gYBFos4I+XzkB61mRJIIvkCTjW8Nwznqply85vDcnrECCADNm
rLew7raP\r\nUYNCvzO6E/JtPf5RlDrTvZ8UP4O3cZ0QXkgbUft2vV3NaQtMWGhIIOo/J1k9chC6\r\njOyBD5sFqsuW4jDStMH2
6M+3PjOwE7r2BUKzr44zv8Db2f36arwiZr6w1VYRN/uj\r\nnnQfLFnR+Wph0Va/lVGzLaPbL/LtO+o2QOFz5Dte27m1TfMu87Tw
3l3ugAzeiy9x\r\n2sZgTTfgXNF3L94i/bIgLhuahZRhe171Vs69rJP58h40PsmP3j3w3iEfyxNRJpwg\r\nmw14Wkaz5YW/GqZ0
ivMFfZcVuzIXBJstb9dBtcmGs3zHGDV5pa7aEvi/B+ygxJUA\r\nbUwNX8TuuUFnrlltZcPGp9fM1eMQtykxlLZxT8oZBkhuhwNr
PtS2J5ZH7jUauCJ9\r\n40hhqLj/gBg7Jd+eyTaDgpfVDTcyVDjwcvfml6PAUI1YgKPfBNZ4b0y0Rw6Kibrc\r\nDBrHCz07Y1/U
BtBj9eEnlnI+8Dv6sIf+9cnDLGzSS/RoBD8Ppv3r8xtd7sfAoXUe\r\nSqFBXic0dVdRg5MfeLaxYa/K/L/cj3Po6ChveKxKTwYz
mV4RnlLTih6ifDpR9C8v\r\ny4qlP80Dg8qxaJWk+2c/ZFzMCHkGaqXXQe6baNLlqn8/chYevtUv856nZA7Y2Hcq\r\nxFdXaw3I
5NKREbnjTs7mBA7b3Im30nq6eW+ZSIBQZ6b39W5GmEn5IzG3bVSMOBWi\r\nhm1DJwWN5b+x+MbJrk/fUKmHIWhXb0VcrZQ8rvUB
cEGYyfrItCYRvtSYNPY2Qo7w\r\nrNi8Yt4P+UpAaprK79z2auE5wJLmjKarTGc3A+byCbwRUvL8D7hZUJBSTsHHnorM\r\nsfIZ
6yJSSiv7MxC/c3imCI3JvhHMrR1gye2lDIJ4HQ1IignPYZvkioyMLcV1VZ9I\r\nHSCsUQVDmgpOPKMaLcjafoOOh6ESwFMau9/1
fp+mVy8b+j2f1Jj8DO/JYS1gOEMY\r\nOoCgyK67HPbcuKqBIM9JU6oiU6Nbvwo5I911R4v42RzckHwcUZx7N1eCzoZIEPRY\r\n
0TlO7pT/9GJueb0+3aNPCvF/GFqtHFFVAf2jpd4tlkMfQKH4/am9p+JBPwthtgzt\r\nx8f9GpeiM11erx0BRG1sY48B+Jv9K1kQ
Mv1COV+gvT4DsFu7hzMvjFPDxyoqNL2R\r\nkZescXl4t8Wmzl79pgp6lqZaFV+sIZWWruhYlBFLs9TlTZZTsPJUkFHT4Mca/lkj
\r\nZvAm7MEgTJtZNwxuOkTqfrOHZEGVmDeljamAFCFIZMnW400eaoaOhOjKFbJDvSJl\r\nGImnpmq/NO6tLaVDTZbnIIPJRAWr
X7MLunGiTT/j3wXniQsZvw5FQPZP+dWSJA3U\r\n81hHmhAUaw8r9RIgoVFMeuv4qdy3bhVJiSqzaZRjknX4OiNrVapIGBZG9Qth
ZvKW\r\nStEreMEnbQQkq6DEKtPYD4sq64uLExLtV5CjZA5UnwWkO54aqIOGZbM8Nkexhkbw\r\nf2VAf8WfzbmNH5WCrOYPfwTU
vUNQATt6VBkDX/+MIQ4wBfOC8MAKGwuVm5FvGZZW\r\n-----END RSA PRIVATE KEY-----\r\n",
	"PublicKeyData": "",
	"PuttyKeyData": "",
	"User": ""

}
```

REST: SSHKeys (GET)

SSHKeys (GET) lists information for each stored SSH key.

Permissions Required

- All Access

Related Commands

- **SOAP:** AccountStoreOps_GetSSHKeyList

Syntax

```
https://serverName/ERPMWebService/AuthService.svc/REST/SSHKeys
```

Parameters

- **KeyLabel:** IP Address of the target machine.
- **KeySignature:** Signature for the key.
- **KeyType:** The label associated with the SSH key.
- **Target:** The target machine.
- **User:** User associated with the SSH key.

Request

XML

The request body should be left empty.

JSON

The request body should be left empty.

Response

A successful operation will remove the mapping.

XML

```
<ArrayOfSSHKeyMetadata xmlns="http://schemas.datacontract.org/2004/07/RouletteAppService_WCF">
       <SSHKeyMetadata>
              <KeyLabel>String content</KeyLabel>
              <KeySignature>String content</KeySignature>
              <KeyType>String content</KeyType>
              <Target>String content</Target>
              <User>String content</User>
       </SSHKeyMetadata>
</ArrayOfSSHKeyMetadata>
```

JSON

```
[{
	"KeyLabel":"String content",
	"KeySignature":"String content",
	"KeyType":"String content",
	"Target":"String content",
	"User":"String content"
}]
```

Example - XML

Request

The request body should be left empty.

Response

```
<ArrayOfSSHKeyMetadata xmlns="http://schemas.datacontract.org/2004/07/RouletteAppService_WCF">
	<SSHKeyMetadata>
		<KeyLabel>Demo</KeyLabel>
		<KeySignature>A4:D0:28:36:CF:9C:1D:24:1D:</KeySignature>
		<KeyType>Private Key</KeyType>
		<Target></Target>
		<User></User>
	</SSHKeyMetadata>
</ArrayOfSSHKeyMetadata>
```

Example - JSON

Request

The request body should be left empty.

Response

```
[{
	"KeyLabel":"Demo",
	"KeySignature":"A4:D0:28:36:CF:9C:1D:24:1D:",
	"KeyType":"Private Key",
	"Target":"",
	"User":""
}]
```

REST: SSH Keys Find (GET)

SSHKeys/Find lists information for stored SSH keys associated with a system.

Permissions Required

- All Access

Related Commands

- **SOAP:** AccountStoreOps_GetSSHKeyListForSystem

Syntax

```
https://serverName/ERPMWebService/AuthService.svc/REST/SSHKeys/Find?Search={SEARCH}
```

Parameters

- **KeyLabel:** IP Address of the target machine.
- **KeySignature:** Signature for the key.
- **KeyType:** The type of SSH Key, such RSA or ECDSA.
- **Target:** The target machine.
- **User:** User associated with the SSH key.

Note: *This API call expects the name of an account store/system as the search parameter. The call returns key meta data for each key mapping that matches the search; however, it does not return any meta data for keys mapped to all targets.*

Request

XML

The request body should be left empty.

JSON

The request body should be left empty.

Response

A successful operation will return a list of keys.

XML

```
<ArrayOfSSHKeyMetadata xmlns="http://schemas.datacontract.org/2004/07/RouletteAppService_WCF">
<SSHKeyMetadata>String content</SSHKeyMetadata>
       <KeyLabel>String content</KeyLabel>
       <KeySignature>String content</KeySignature>
       <KeyType>String content</KeyType>
```

```
        <Target>String content</Target>
        <User>String content</User>
        </SSHKeyData>
</ArrayOfSSHKeyMetadata>
```

JSON

```
[{
        "KeyLabel":"String content",
        "KeySignature":"String content",
        "KeyType":"String content",
        "Target":"String content",
        "User": "String content"

}]
```

Example - XML

Request

The request body should be left empty.

Response

```
<ArrayOfSSHKeyMetadata xmlns="http://example.com/2004/07/RouletteAppService_WCF">
<SSHKeyMetadata>
        <KeyLabel>Demo</KeyLabel>
        <KeySignature>A4:D0:28:36:CF:9C:1D:24:1D:</KeySignature>
        <KeyType>String content</KeyType>
        <Target>String content</Target>
        <User>String content</User>
        </SSHKeyData>
</ArrayOfSSHKeyMetadata>
```

Example - JSON

Request

The request body should be left empty.

Response

```
{
        "KeyLength":"2048",
        "KeySignature":"A4:D0:28:36:CF:9C:1D:24:1D:",
        "KeyType":"RSA",
        "Passphrase":"P@ssw0rd",
        "PrivateKeyData": "-----BEGIN RSA PRIVATE KEY-----\r\nProc-Type: 4,ENCRYPTED\r\nDEK-Info: AES-128-
CBC,D7B79BBC75767334071B90871AE1CD88\r\n\r\nZoKGSr9gYBFos4I+XzkB61mRJIIvkCTjW8Nwznqply85vDcnrECCADNm
rLew7raP\r\nUYNCvzO6E/JtPf5RlDrTvZ8UP4O3cZ0QXkgbUft2vV3NaQtMWGhIIOo/J1k9chC6\r\njOyBD5sFqsuW4jDStMH2
6M+3PjOwE7r2BUKzr44zv8Db2f36arwiZr6w1VYRN/uj\r\nnnQfLFnR+Wph0Va/lVGzLaPbL/LtO+o2QOFz5Dte27m1TfMu87Tw
3l3ugAzeiy9x\r\n2sZgTTfgXNF3L94i/bIgLhuahZRhe171Vs69rJP58h40PsmP3j3w3iEfyxNRJpwg\r\nmw14Wkaz5YW/GqZ0
```

```
ivMFfZcVuzIXBJstb9dBtcmGs3zHGDV5pa7aEvi/B+ygxJUA\r\nbUwNX8TuuUFnrlltZcPGp9fM1eMQtykxlLZxT8oZBkhuhwNr
PtS2J5ZH7jUauCJ9\r\n40hhqLj/gBg7Jd+eyTaDgpfVDTcyVDjwcvfml6PAUI1YgKPfBNZ4b0y0Rw6Kibrc\r\nDBrHCz07Y1/U
BtBj9eEnlnI+8Dv6sIf+9cnDLGzSS/RoBD8Ppv3r8xtd7sfAoXUe\r\nSqFBXic0dVdRg5MfeLaxYa/K/L/cj3Po6ChveKxKTwYz
mV4RnlLTih6ifDpR9C8v\r\ny4qlP80Dg8qxaJWk+2c/ZFzMCHkGaqXXQe6baNLlqn8/chYevtUv856nZA7Y2Hcq\r\nxFdXaw3I
5NKREbnjTs7mBA7b3Im30nq6eW+ZSIBQZ6b39W5GmEn5IzG3bVSMOBWi\r\nhm1DJwWN5b+x+MbJrk/fUKmHIWhXb0VcrZQ8rvUB
cEGYyfrItCYRvtSYNPY2Qo7w\r\nrNi8Yt4P+UpAaprK79z2auE5wJLmjKarTGc3A+byCbwRUvL8D7hZUJBSTsHHnorM\r\nsfIZ
6yJSSiv7MxC/c3imCI3JvhHMrR1gye2lDIJ4HQ1IignPYZvkioyMLcV1VZ9I\r\nHSCsUQVDmgpOPKMaLcjafoOOh6ESwFMau9/1
fp+mVy8b+j2f1Jj8DO/JYS1gOEMY\r\nOoCgyK67HPbcuKqBIM9JU6oiU6Nbvwo5I911R4v42RzckHwcUZx7N1eCzoZIEPRY\r\n
0TlO7pT/9GJueb0+3aNPCvF/GFqtHFFVAf2jpd4tlkMfQKH4/am9p+JBPwthtgzt\r\nx8f9GpeiM11erx0BRG1sY48B+Jv9K1kQ
Mv1COV+gvT4DsFu7hzMvjFPDxyoqNL2R\r\nkZescXl4t8Wmzl79pgp6lqZaFV+sIZWWruhYlBFLs9TlTZZTsPJUkFHT4Mca/lkj
\r\nZvAm7MEgTJtZNwxuOkTqfrOHZEGVmDeljamAFCFIZMnW400eaoaOhOjKFbJDvSJl\r\nGImnpmq/NO6tLaVDTZbnIIPJRAWr
X7MLunGiTT/j3wXniQsZvw5FQPZP+dWSJA3U\r\n81hHmhAUaw8r9RIgoVFMeuv4qdy3bhVJiSqzaZRjknX4OiNrVapIGBZG9Qth
ZvKW\r\nStEreMEnbQQkq6DEKtPYD4sq64uLExLtV5CjZA5UnwWkO54aqIOGZbM8Nkexhkbw\r\nf2VAf8WfzbmNH5WCrOYPfwTU
vUNQATt6VBkDX/+MIQ4wBfOC8MAKGwuVm5FvGZZW\r\n-----END RSA PRIVATE KEY-----\r\n",
       "PublicKeyData": "",
       "PuttyKeyData": "",
       "User": ""

}
```

SSHKey/New (POST)

SSHKey/New creates a new SSH key.

Permissions Required

- All Access

Related Commands

- **SOAP:** AccountStoreOps_GenerateSSHKey

Syntax

```
https://serverName/ERPMWebService/AuthService.svc/REST/SSHKey/New
```

Parameters

- **KeyID:** The label associated with the SSH key.
- **KeyLength:** The length of the SSH Key in bits.
- **KeyType:** The type of SSH Key, such RSA or ECDSA.
- **Passphrase:** The passphrase associated with the SSH key.

Request

XML

JSON

```
{
        "AuthenticationToken":"String content",
        "KeyID":"String content",
        "KeyLength":2147483647,
        "KeyType":"String content",
        "Passphrase":"String content"
{
```

Reponse

A successful operation will generate a new SSH key.

XML

JSON

```
{
        "OperationMessage":"String content",
```

```
        "OperationSucceeded":true
{
```

Example - XML

Request

Response

Example - JSON

Request

```
{
        "AuthenticationToken":"Q1IDOFJ15ZL10SZD5PND2VPGET2GERDO",
        "KeyID":"Demo",
        "KeyLength":2147483647,
        "KeyType":"RSA",
        "Passphrase":"P@ssw0rd"
{
```

Response

```
{
        "OperationMessage":"Created new key with id Demo",
        "OperationSucceeded":true
{
```

SSHKey/Map (POST)

SSHKey/Map maps a stored SSH key to an account store and identity.

Permissions Required

- All Access

Related Commands

- **SOAP:** AccountStoreOps_MapSSHKeyToStore

Syntax

```
https://serverName/ERPMWebService/AuthService.svc/REST/SSHKey/Map
```

Parameters

- **TargetName:** IP Address of the target machine.
- **Type** The type of system.
- **KeyID:** The label associated with the SSH key.
- **Username:** The identity you wish to map the SSH key to in the system.

Request

XML

JSON

```
{
        "AuthenticationToken":"String content",
        "AccountStore":{
                "CustomTypeName":"String content",
                "TargetName":"String content",
                "Type":0
        },
        "KeyID":"String content",
        "Username":"String content"
}
```

Reponse

A successful operation will map the SSH key to a specific account store and user.

XML

JSON

```
{
        "OperationMessage":"String content",
        "OperationSucceeded":true
{
```

Example - XML

Request

Response

Example - JSON

Request

```
{
        "AuthenticationToken":"Q1IDOFJ15ZL10SZD5PND2VPGET2GERDO",
        "AccountStore":{
                "TargetName":"10.10.32.20",
                "Type":0
        },
        "KeyID":"Demo",
        "Username":"tcdemo"
}
```

Response

```
{
  "OperationMessage":"Key Demo successfully mapped to target 10.10.32.20 for   user tcdemo",
  "OperationSucceeded":true
{
```

SSHKey/Map (DELETE)

SSHKey/Map removes a stored SSH key mapping to an account store and a user.

Permissions Required

- All Access

Related Commands

- **SOAP:** AccountStoreOps_RemoveSSHKeyMapping

Syntax

```
https://serverName/ERPMWebService/AuthService.svc/REST/SSHKey/Map
```

Parameters

- **TargeName:** IP Address of the target machine.
- **Type:** The type of system
- **KeyID:** The label associated with the SSH key.

Request

XML

JSON

```
{
        "AuthenticationToken":"String content",
        "AccountStore":{
                "CustomTypeName":"String content",
                "TargetName":"String content",
                "Type":0
        },
        "KeyID":"String content",
}
```

Response

A successful operation will remove the mapping.

XML

JSON

```
{
        "OperationMessage":"String content",
```

```
        "OperationSucceeded":true
{
```

Example - XML

Response

Example - JSON

Request

```
{
        "AuthenticationToken":"Q1IDOFJ15ZL10SZD5PND2VPGET2GERDO",
        "AccountStore":{
                "TargetName":"10.10.32.20",
                "Type":0
        },
        "KeyID":"Demo",
}
```

Response

```
{
  "OperationMessage":"Successfully removed mapping for key Demo to target 10.10.32.20",
  "OperationSucceeded":true
{
```

REST: Test & System Configuration

Config/AccountTypes (GET)

Config_GetAccountTypes lists all configured system types and accounts stored. It returns a string valued list.

Permissions Required

- Logon

Related Commands

- **SOAP:** Config_GetAccountTypes

Syntax

The body will be empty. You must add additional headers.

Additional Headers

- **AuthenticationToken:** The authentication token of the requesting user.

Parameters

There are no additional parameters for this request.

Example Request

The body will be empty. You must add additional headers.

Output Success

A successful request will list all available account store and system types.

Example Success Output

```
{
  "ListValues": [
    {
      "Value": "Windows"
    },
    {
      "Value": "Sybase"
    },
    {
      "Value": "SQL Server"
    },
    {
      "Value": "Azure Active Directory"
```

```
    },
    {
      "Value": "Amazon Web Services"
    },
    {
      "Value": "RackSpace Public Cloud"
    },
    {
      "Value": "SalesForce"
    },
    {
      "Value": "SoftLayer"
    },
    {
      "Value": "VMWare (ESX)"
    }
  ]
}
```

Output Error

- **Session previously expired**

  The session was invalid, or a duplicate web session was detected for this identity.

- **Invalid authentication token**

  An invalid authentication token was used, or the token was not found.

Example Fail Output

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
   <head>
      <title>Request Error</title>
      <style>style_info_goes_here</style>
   </head>
   <body>
      <div id="content">
         <p class="heading1">Request Error</p>
         <p xmlns="">
            The server encountered an error processing the request. Please see the
            <a rel="help-page"
href="http://lsdslscprd.lsds.int/ERPMWebServiceAnonNoSSL/AuthService.svc/REST/help">service help
page</a> for constructing valid requests to the service. The exception message is 'Invalid
authentication token or token not found'. See server logs for more details. The exception stack
trace is:
         </p>
         <p>
            stack_trace_info_goes_here
         </p>
      </div>
```

```
    </body>
</html>
```