



# Digital Access Extension Programming Interfaces (XPI)

[Smart ID Digital Access component](#) offers the following extension Programming Interfaces (XPIs):

This article is valid for Digital Access 6.0.4 and later.

## Digital Access XPI REST API

See the full documentation in [Digital Access XPI REST API](#).

## Digital Access XPI Web Services

See the full documentation [here](#).

## Use XPI service via SOAP UI tool

[Expand/Collapse All](#)

## Prerequisites

Integration through the Extension Programming Interface (XPI) must be enabled:

1. In Digital Access Admin, go to **Manage System**.
2. Click a registered Policy Service to edit it.
3. Select **Enable XPI: REST** or **Enable XPI: WS**.
4. If you want to enable the XPI and SOAP services, the expose port ID should be 0.0.0.0 in Digital Access Admin.

### XPI: REST and WS

To enable application integration through the Extension Programming Interface (XPI) using REST or Webservice, select Enable XPI: REST or WS and enter the following settings.

Enable XPI:REST  
 Enable XPI:WS

Host:

Port:

Server Certificate:

[Delete...](#)

[Save](#)

5. Delegate the admin privileges to a User storage user or a Local user:
  - a. Go to **Manage system > Delegated Management > Super Administrator > Add Administrator**, read more here: [Create administrative roles in Digital Access](#).
6. **For XPI logging as a Local user:**
  - a. Add a user and enable auth mech.
7. **For XPI logging as a User storage user:**
  - a. Enable auto linking:
    - i. Go to **Manage Accounts and Storage > Global User Account Settings**.
    - ii. On the **User Linking** tab:
      - under **General Settings**, select **Enable PortWise Authentication when automatically linking the user**.
      - under **PortWise Password**, select **Use password from User storage**.

## Related information

- [Add user account in Digital Access](#)
- [Add user group in Digital Access](#)
- [Add user storage in Digital Access](#)
- [User linking in Digital Access](#)
- [User storage in Digital Access](#)

## Example files

- [Authenticate.xml](#)
- [add user.xml](#)

## Step-by-step instruction

Get WSDL in soap UI



1. Get Web Service Description Language (WSDL) in soap UI from <https://da-admin1.test.nexusgroup.com:4443/ws/v4/index.html>
2. Choose the services from the navigation menu. Select and read the detailed information for each service.

**Authentication Web Service**

**Description:** Authentication services

**Namespace:** <http://portwise.com/ws/v1/authentication>

**Endpoint:** <https://<hostname>/ws/v1/services/Authentication>

**Style:** Document/Literal

**WSDL:** <https://<host>/ws/v1/services/Authentication?wsdl>

**Since:** 5.2

**See also:** [Authorization](#)

Authentication is required before any usage of the XPI services, except authorization which may be used for on-demand authentication, i.e. it will ask for additional authentication if the subject does not have the appropriate authentication level. Once authenticated the subject will be populated with security identities, i.e. principals. It is possible to add own principals to the subject; make sure they do not collide with any reserved principal names. Depending on the configuration it may be necessary to authenticate using more than one method when accessing a resource.

When using PortWise OCSA it is possible to use an application generated challenge, which may or may not be a representation of a text to be signed. When using this mode, the challenge should be sent in the subject, with the key 'challenge', and the generated OTP in the password item. Username, challenge and password are mandatory.

## Set up soap request

1. Authentication is required before any usage of the XPI services - import authentication wsdl in request editor:

**WSDL** <https://da-admin1.test.nexusgroup.com:4443/ws/v1/services/Authentication?wsdl>

2. Send a request with inputs in subject:

```
<subject>
<country>?</country>
<credentials>
<key>username</key>
<value>YTE=</value> - username with base64 encoded value
</credentials>
<credentials>
<key>password</key>
<value>bmV4dXNAMTIz</value> - Password with base64 encoded value
</credentials>
</subject>
```

See this example: [Authenticate.xml](#)

- a. A valid response has Session, use it in the following request:

```
<principals>
<key>session</key>
<value>OXg5eWYyM2QxcHRz</value>
</principals>
```

3. Select an admin privileged task, such as a User Account operation.
  - a. To get end point service, choose the service from <https://da-admin1.test.nexusgroup.com:4443/ws/v4/services/UserAccount?wsdl> and import wsdl.
    - i. This is an example of adding a user account:



```
<user:add>
<subject>
<principals>
<key>session</key>
<value>OXg5eWYyM2QxcHRz</value> -> provide session
value from authentication response
</principals>
</subject>
<account>
<enabled>true</enabled>
<displayName>user1</displayName>
<emailAddress>user1@gmail.com</emailAddress>

<globalAccess>
<locked>>false</locked>
<maxRetries>10</maxRetries> - constants
<numRetries>0</numRetries> -constants
</globalAccess>
<userName>user1</userName>
<validFrom>1586975400000</validFrom> date in this
format
<validTo>0</validTo>
</account>
<linkToDirectory>>false</linkToDirectory> - true is
want to link to AD
</user:add>
```

See this example: [add user.xml](#)