SailPoint IdentityIQ

Integration Guide with Blue Prism

Version 1.0

Copyright © 2019 SailPoint Technologies, Inc., All Rights Reserved.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Restricted Rights Legend. All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Government's Specially Designated Nationals (SDN) List; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Copyright and Trademark Notices. Copyright © 2019 SailPoint Technologies, Inc. All Rights Reserved. All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet web site are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

"SailPoint Technologies & Design," "SailPoint," "IdentityIQ," "IdentityNow," "SecurityIQ" "IdentityAI" "AccessIQ," "Identity Cube," "Managing the Business of Identity" are registered trademarks of SailPoint Technologies, Inc. "Identity is Everything" and "The Power of Identity" are trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

Table of Contents

1. INTEGRATING SAILPOINT IDENTITYIQ WITH BLUE PRISM 4

1.1. Expose Processes as Web Services 4

1.2. Configure Blue Prism Processes in IdentityIQ 5
1.2.1. Create New Application in IdentityIQ 5
1.2.2. Configure Blue Prism Web Service Settings in IdentityIQ 6
1.2.3. Configure Blue Prism Operations 6
1.2.3.1 Test Connection 7
1.2.3.2 Get All Credentials 8
1.2.3.3 Get Credential 9
1.2.3.4 Get All Access Rights 10
1.2.3.5 Enable Credential 11
1.2.3.6 Disable Credential 11
1.2.3.7 Remove Access Rights 12
1.2.3.8 Add Access Rights 14
1.2.3.9 Delete Credential 15
1.2.4. Configure Account and Group Aggregation 16
1.2.5. Configure Enable and Disable Custom Rule 17
1.2.6. Configure Aggregation Task in IdentityIQ 18

1.3. End to End Checklist 19

2. SUPPORT 20

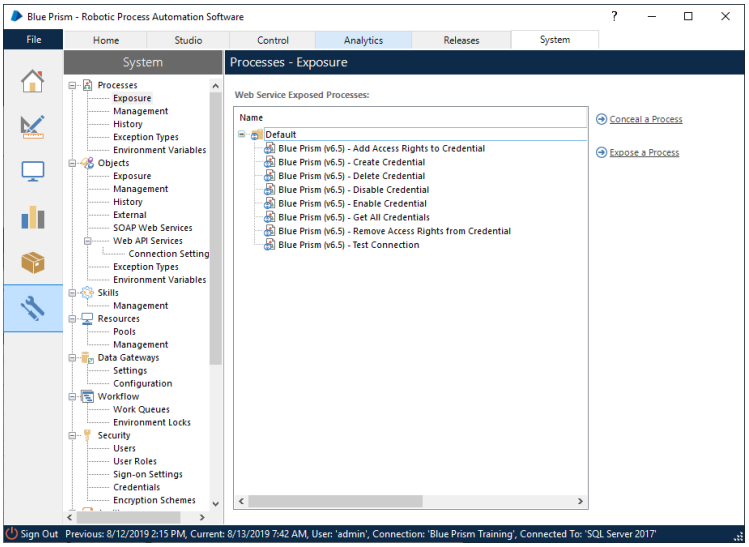
1. Integrating SailPoint IdentityIQ with Blue Prism

The following steps provide guidance on how to configure Blue Prism as a connected application within IdentityIQ. For more in-depth IdentityIQ information, please refer to SailPoint's knowledge base and documentation.

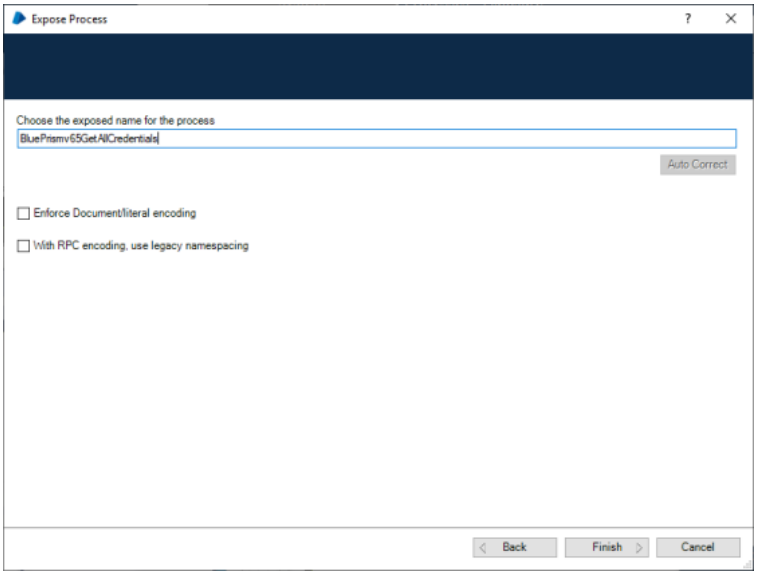
1.1. Expose Processes as Web Services

For additional guidance, please refer to the "v6.3 User Guide – Web Services" document on the Blue Prism portal. Essentially, each process in this package should be exposed as a Web Service by the following steps:

- Navigate to **System** > **Processes** > **Exposure** and select **Expose a Process**



- Select the process and click **Next**, followed by **Finish** to accept the default configuration.



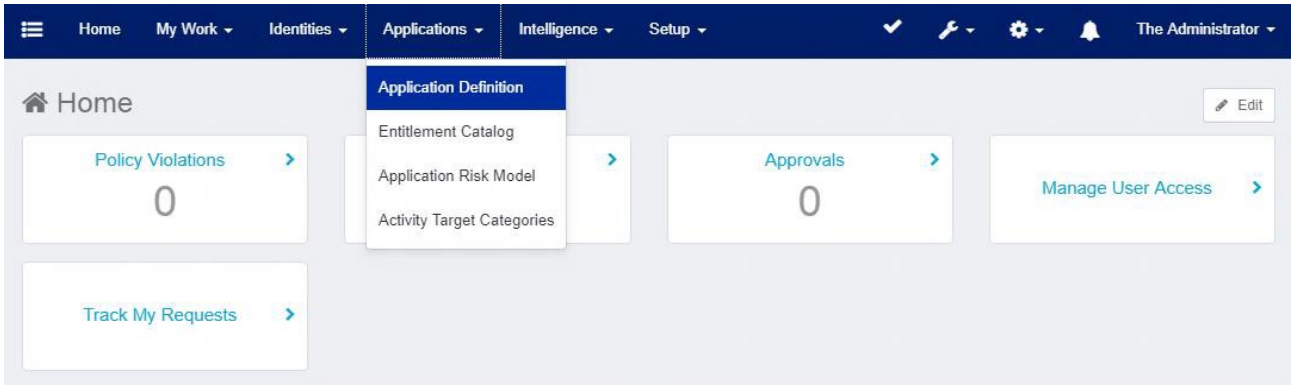
- Repeat the steps for each process included in the package.

1.2. Configure Blue Prism Processes in IdentityIQ

These steps will be carried out within IdentityIQ.

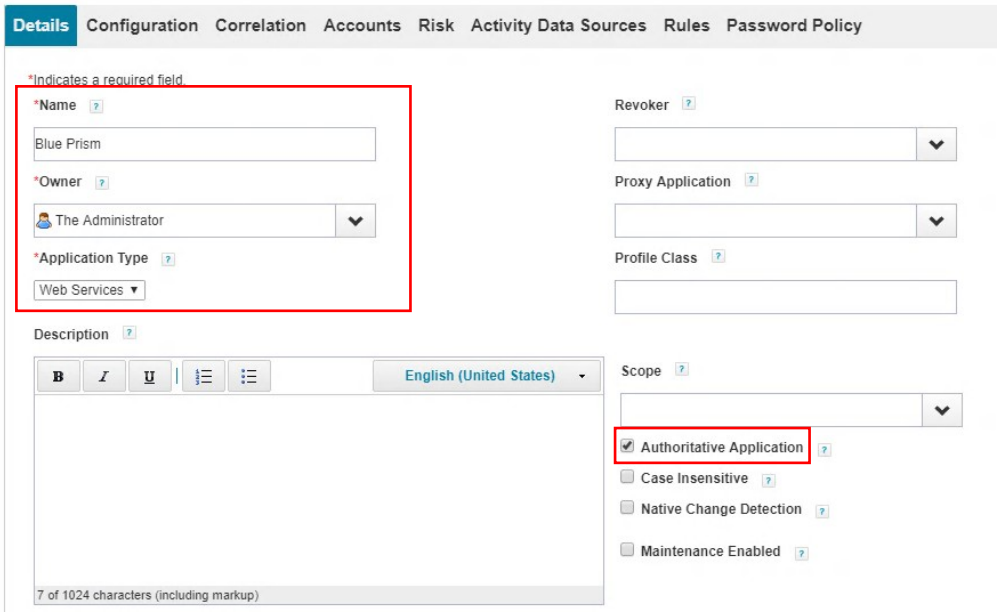
1.2.1. Create New Application in IdentityIQ

Navigate to **Applications** > **Application Definition** from IdentityIQ's home page once logged in as an administrator.



Click **Add New Application**

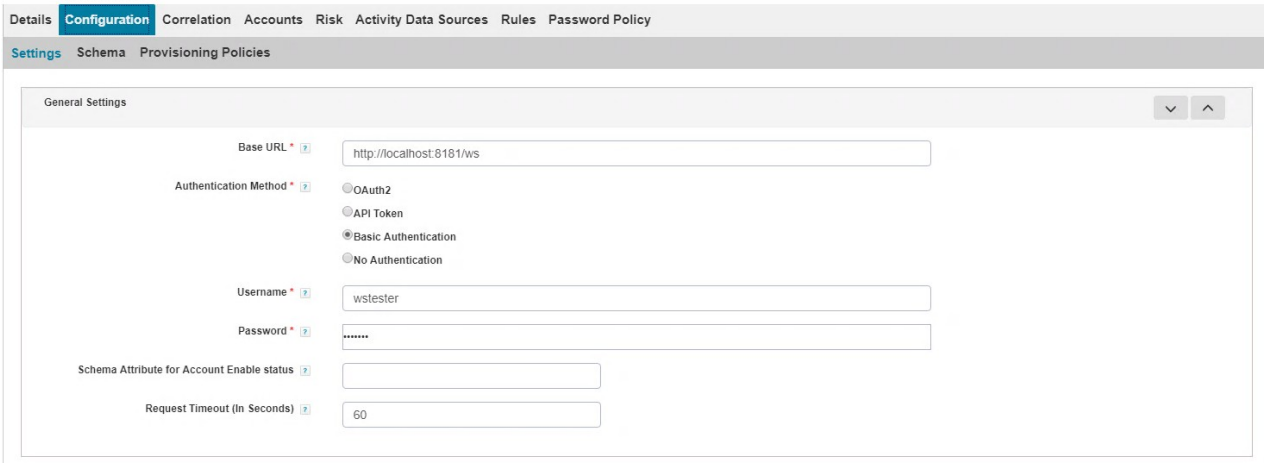
Fill out the basic details as highlighted below



1.2.2. Configure Blue Prism Web Service Settings in IdentityIQ

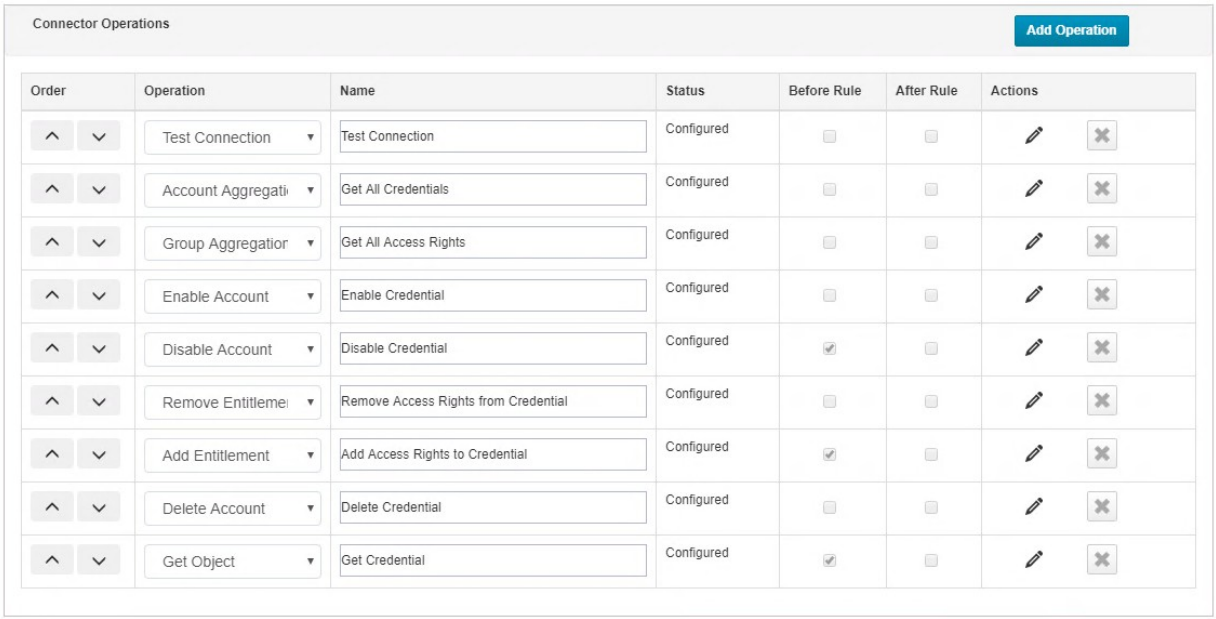
On the **Configuration**>**Settings** tab, enter the following general settings

- Base URL: **http://<hostname>:8181/ws/**
    - The hostname should be the name of the computer where Blue Prism is installed. If Blue Prism and IdentityIQ are installed on the same machine, a value of **localhost** can be used.
- Authentication: **Basic Authentication**
- Username: enter a Blue Prism username that possesses the ability to interact with credentials
- Password: enter the corresponding password for the Blue Prism username



1.2.3. Configure Blue Prism Operations

On the same **Configuration**>**Settings** page, each Blue Prism process should be configured as an IdentityIQ operation.



For each operation created in IdentityIQ, click the Pencil icon to edit and fill out the configuration details for each operation as detailed in the following sections.

1.2.3.1 Test Connection

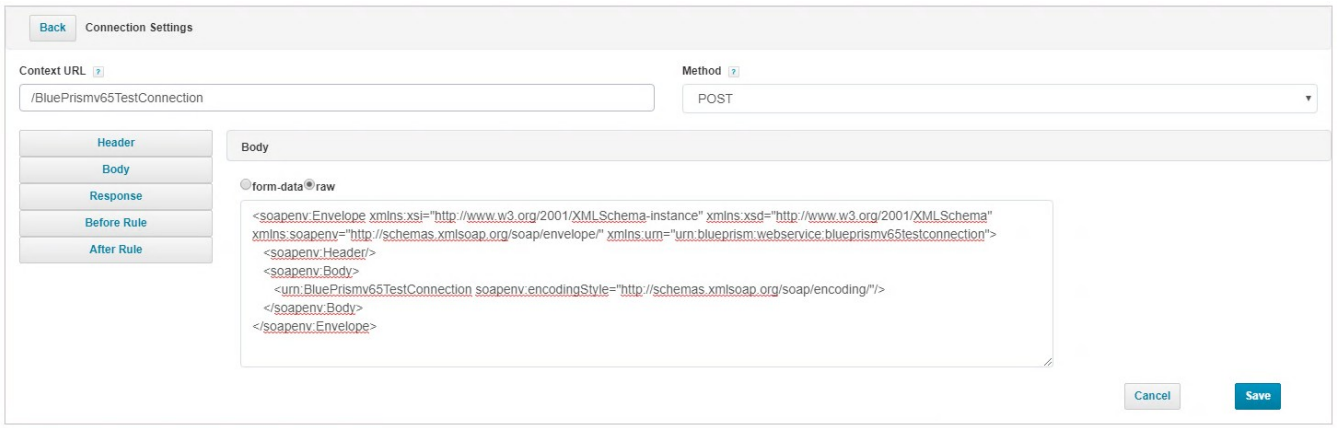
Set the following details on the configuration screen.

Context URL: `/BluePrismv65TestConnection`

Method: `POST`

Body:

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:blueprism:webservice:blueprismv65testconnection">
    <soapenv:Header/>
    <soapenv:Body>
        <urn:BluePrismv65TestConnection
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
    </soapenv:Body>
</soapenv:Envelope>
```



1.2.3.2 Get All Credentials

This operation encompasses the Account Aggregation component in IIQ. It is called regularly to retrieve the updated list of all credentials and their current Access Rights in Blue Prism. Please note that the Response of this operation must be configured using XPath mapping as shown below for the Account Aggregation to function in IIQ.

Context URL: `/BluePrismv65GetAllCredentials`

Method: `POST`

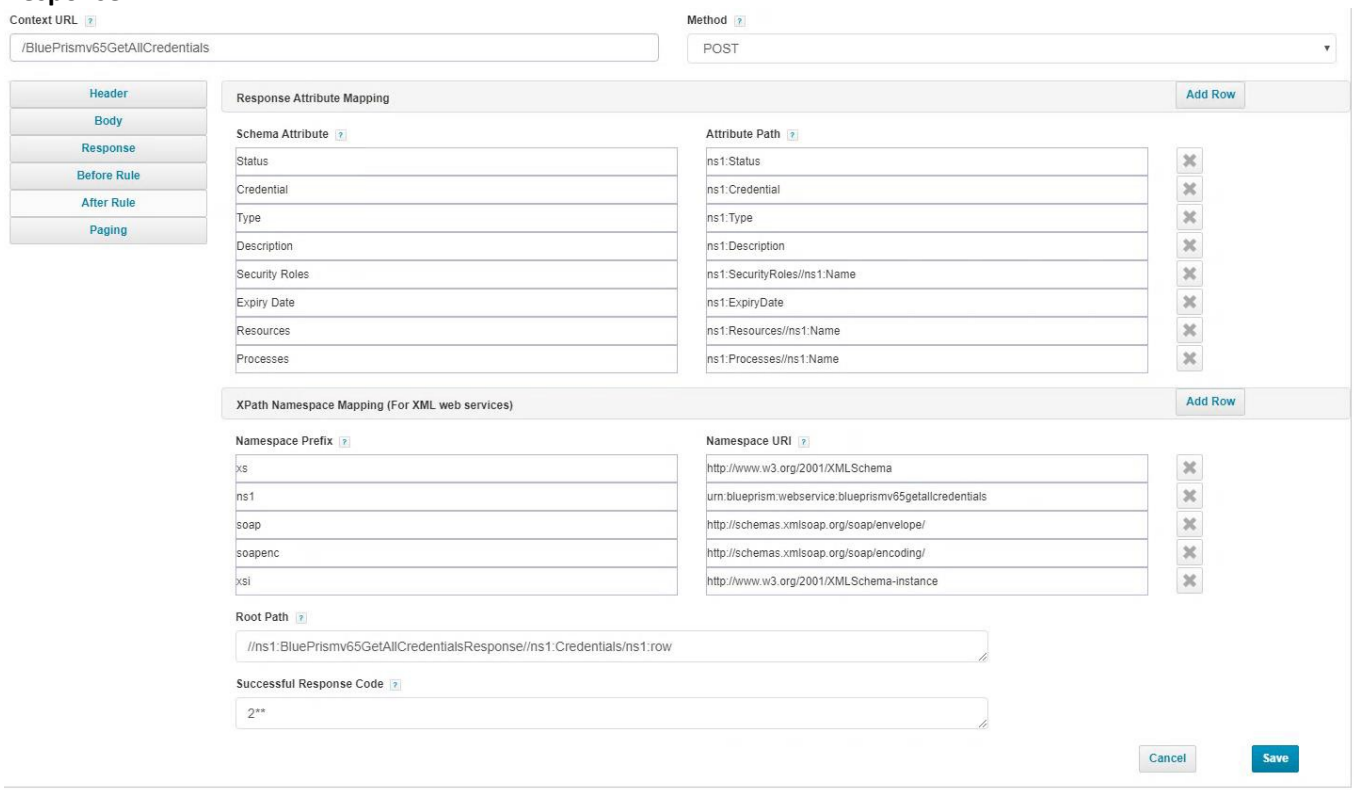
Body:

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:blueprism:webservice:blueprismv65getallcredentials">
    <soapenv:Header/>
    <soapenv:Body>
        <urn:BluePrismv65GetAllCredentials
                soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
    </soapenv:Body>
</soapenv:Envelope>
```

Headers:

Key	Value
charset	utf-8
Accept	text/xml
Content-Type	text/xml

Response:



1.2.3.3 Get Credential

Context URL: `/BluePrismv65GetCredential`

Method: `POST`

Body:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:blueprism:webservice:blueprismv65getcredential">
    <soapenv:Header/>
    <soapenv:Body>
        <urn:BluePrismv65GetCredential>
            <urn:SignInCredentialName>Blue Prism</urn:SignInCredentialName>
            <urn:SignInConnectionName>Default Connection</urn:SignInConnectionName>
            <urn:SingleSignOn>False</urn:SingleSignOn>
            <urn:CredentialName>$plan.nativeIdentity$</urn:CredentialName>
        </urn:BluePrismv65GetCredential>
    </soapenv:Body>
</soapenv:Envelope>
```

1.2.3.4 Get All Access Rights

This operation encompasses the Group Aggregation component in IIQ. It is called regularly to retrieve the updated list of all available Access Rights in Blue Prism. Please note that the Response of this operation must be configured using XPath mapping as shown below for the Group Aggregation to function in IIQ.

Context URL: `/BluePrismv65GetAllAccessRights`

Method: `POST`

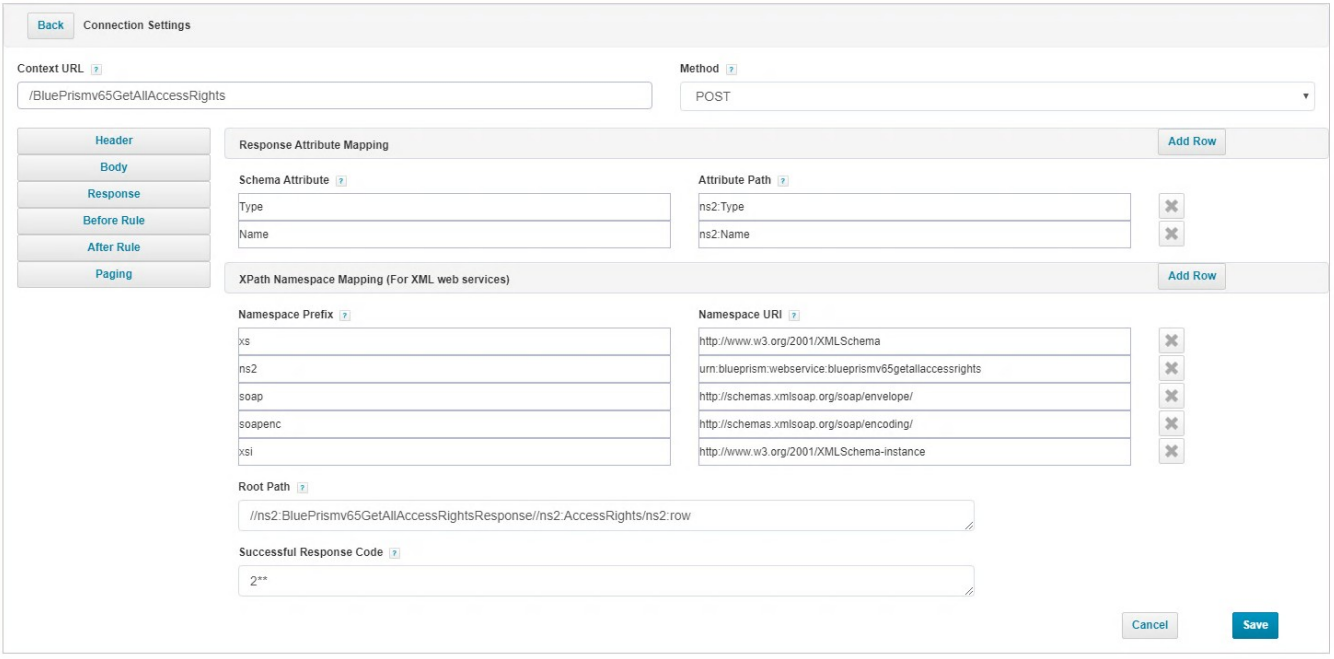
Body:

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:blueprism:webservice:blueprismv65getallaccessrights">
    <soapenv:Header/>
    <soapenv:Body>
        <urn:BluePrismv65GetAllAccessRights
                soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
    </soapenv:Body>
</soapenv:Envelope>
```

Headers:

Key	Value
charset	utf-8
Accept	text/xml
Content-Type	text/xml

Response:



1.2.3.5 Enable Credential

Context URL: `/BluePrismv65EnableCredential`

Method: `POST`

Body:

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:blueprism:webservice:blueprismv65enablecredential">
    <soapenv:Header/>
    <soapenv:Body>
        <urn:BluePrismv65EnableCredential
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
            <SignInConnectionName xsi:type="xsd:string">Default Connection</SignInConnectionName>
            <SignInCredentialName xsi:type="xsd:string">Blue Prism</SignInCredentialName>
            <SingleSignOn xsi:type="xsd:boolean">False</SingleSignOn>
            <CredentialName xsi:type="xsd:string">$plan.nativeIdentity$</CredentialName>
        </urn:BluePrismv65EnableCredential>
    </soapenv:Body>
</soapenv:Envelope>
```

1.2.3.6 Disable Credential

Context URL: `/BluePrismv65DisableCredential`

Method: `POST`

Body:

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:blueprism:webservice:blueprismv65disablecredential">
    <soapenv:Header/>
    <soapenv:Body>
        <urn:BluePrismv65DisableCredential
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
            <SignInConnectionName xsi:type="xsd:string">Default Connection</SignInConnectionName>
            <SignInCredentialName xsi:type="xsd:string">Blue Prism</SignInCredentialName>
            <SingleSignOn xsi:type="xsd:boolean">False</SingleSignOn>
            <CredentialName xsi:type="xsd:string">$plan.nativeIdentity$</CredentialName>
        </urn:BluePrismv65DisableCredential>
    </soapenv:Body>
</soapenv:Envelope>
```

1.2.3.7 Remove Access Rights

Context URL: /BluePrismv65RemoveAccessRights

Method: POST

Headers:

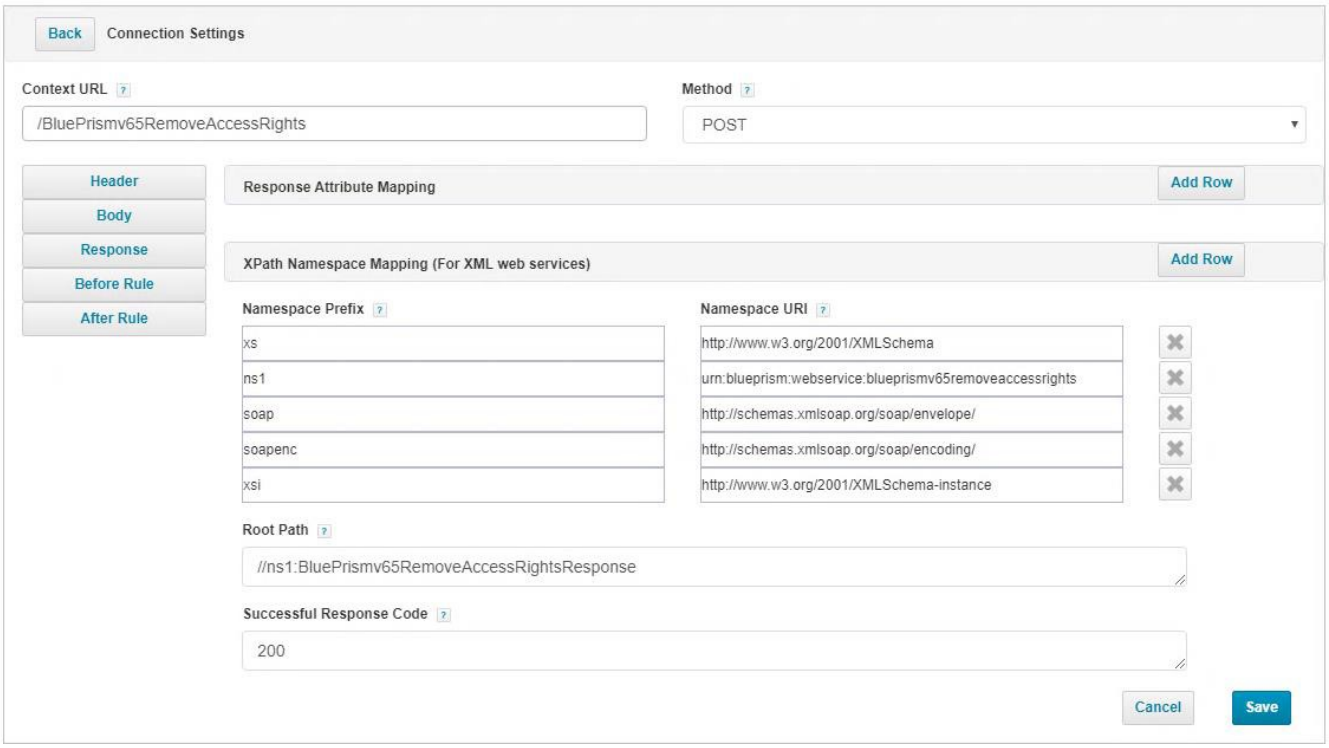
Key	Value
charset	utf-8
Accept	text/xml
Content-Type	text/xml

Body:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:blueprism:webservice:blueprismv65removeaccessrights">
    <soapenv:Header/>
    <soapenv:Body>
        <urn:BluePrismv65RemoveAccessRights>
            <urn:SignInCredentialName>Blue Prism</urn:SignInCredentialName>
            <urn:SignInConnectionName>Default Connection</urn:SignInConnectionName>
            <urn:SingleSignOn>False</urn:SingleSignOn>
            <urn:CredentialName>$plan.nativeIdentity$</urn:CredentialName>
            <urn:SecurityRoles>
                  <urn:row>
                     <urn:Name>$plan.SecurityRoles$</urn:Name>
                     <urn:Enabled>False</urn:Enabled>
                  </urn:row>
               </urn:SecurityRoles>
            <urn:Processes>
                  <urn:row>
                     <urn:Name>$plan.Processes$</urn:Name>
                     <urn:Enabled>False</urn:Enabled>
                  </urn:row>
               </urn:Processes>
               <urn:Resources>
                     <urn:row>
                     <urn:Name>$plan.Resources$</urn:Name>
                     <urn:Enabled>False</urn:Enabled>
                  </urn:row>
               </urn:Resources>
            </urn:BluePrismv65RemoveAccessRights>
     </soapenv:Body>
  </soapenv:Envelope>
```

Remove Access Rights, continued

Response:



1.2.3.8 Add Access Rights

Context URL: `/BluePrismv65AddAccessRights`

Method: `POST`

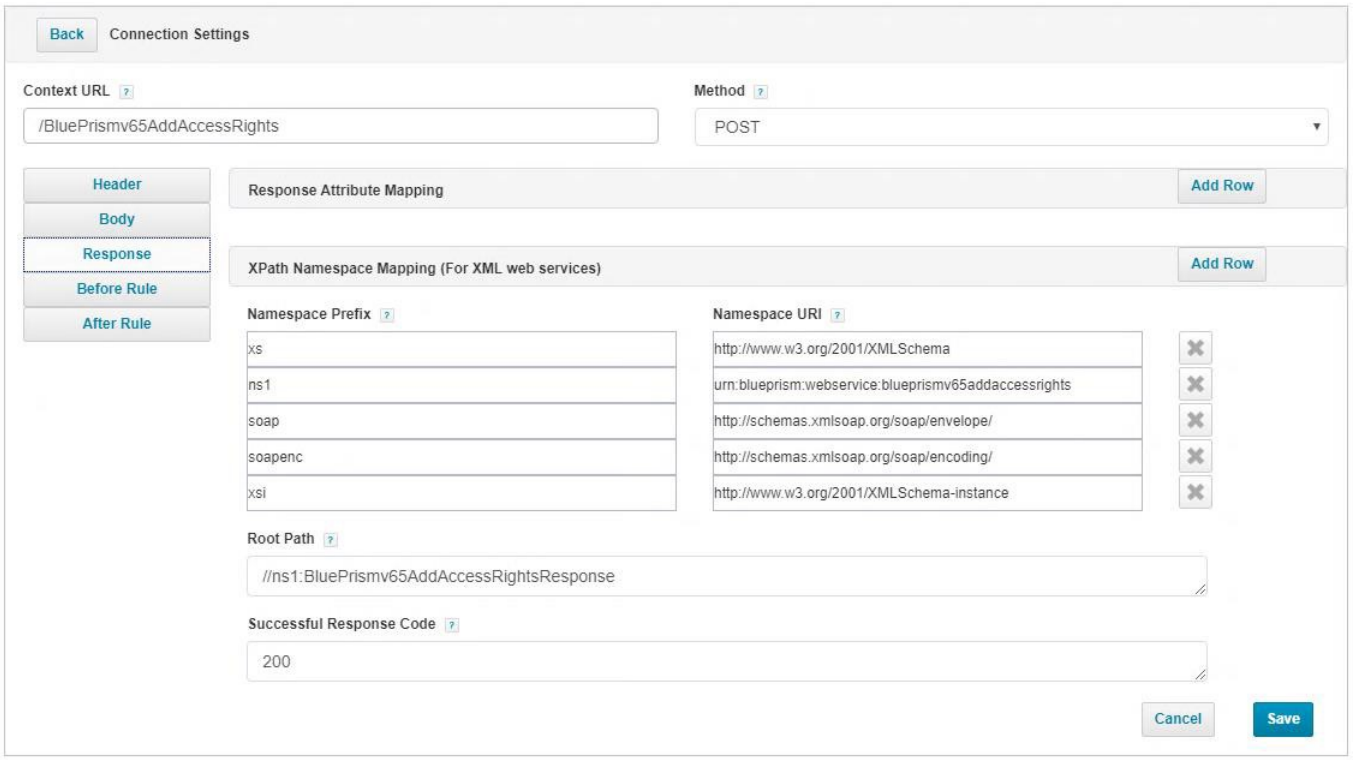
Headers:

Key	Value
charset	utf-8
Accept	text/xml
Content-Type	text/xml

Body:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:blueprism:webservice:blueprismv65addaccessrights">
    <soapenv:Header/>
    <soapenv:Body>
        <urn:BluePrismv65AddAccessRights>
            <urn:SignInCredentialName>Blue Prism</urn:SignInCredentialName>
            <urn:SignInConnectionName>Default Connection</urn:SignInConnectionName>
            <urn:SingleSignOn>False</urn:SingleSignOn>
            <urn:CredentialName>$plan.nativeIdentity$</urn:CredentialName>
            <urn:SecurityRoles>
                <urn:row>
                    <urn:Name>$plan.SecurityRoles$</urn:Name>
                    <urn:Enabled>True</urn:Enabled>
                </urn:row>
            </urn:SecurityRoles>
            <urn:Processes>
                <urn:row>
                    <urn:Name>$plan.Processes$</urn:Name>
                    <urn:Enabled>True</urn:Enabled>
                </urn:row>
            </urn:Processes>
            <urn:Resources>
                <urn:row>
                    <urn:Name>$plan.Resources$</urn:Name>
                    <urn:Enabled>True</urn:Enabled>
                </urn:row>
            </urn:Resources>
        </urn:BluePrismv65AddAccessRights>
    </soapenv:Body>
</soapenv:Envelope>
```

Response:



1.2.3.9 Delete Credential

Context URL: `/BluePrismv65DeleteCredential`

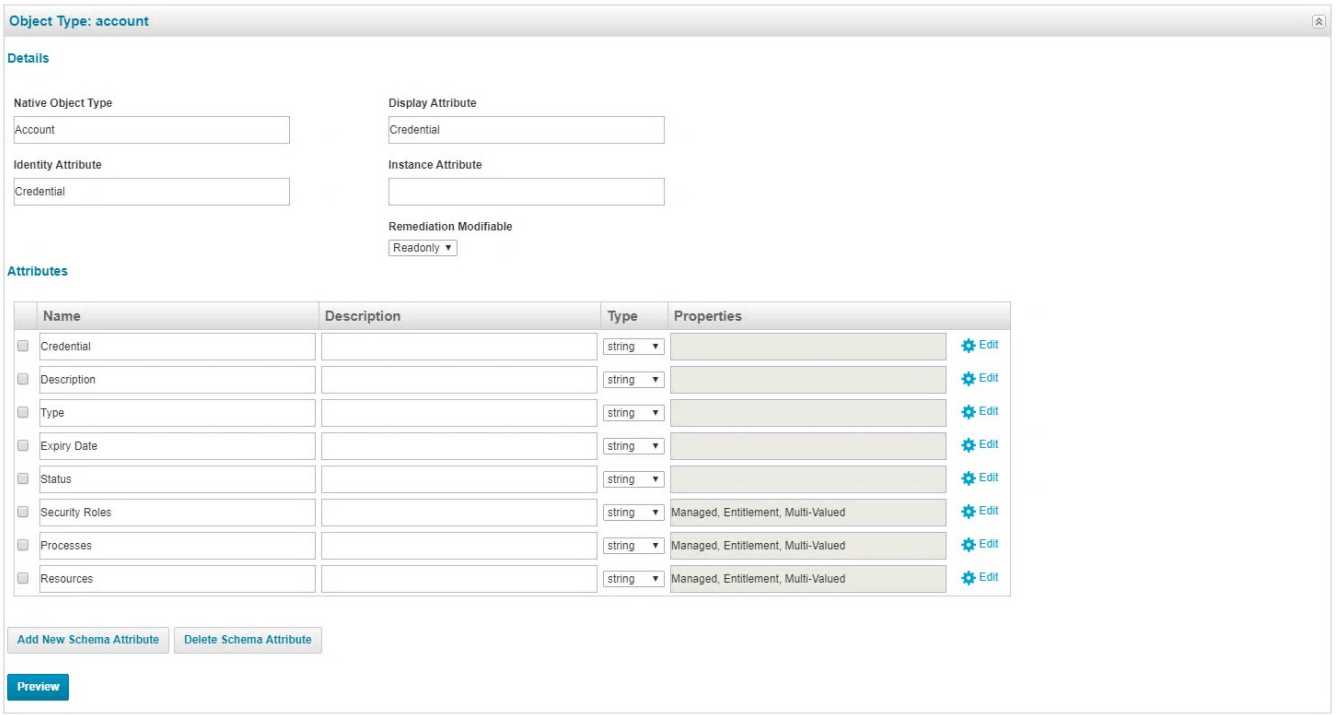
Method: `POST`

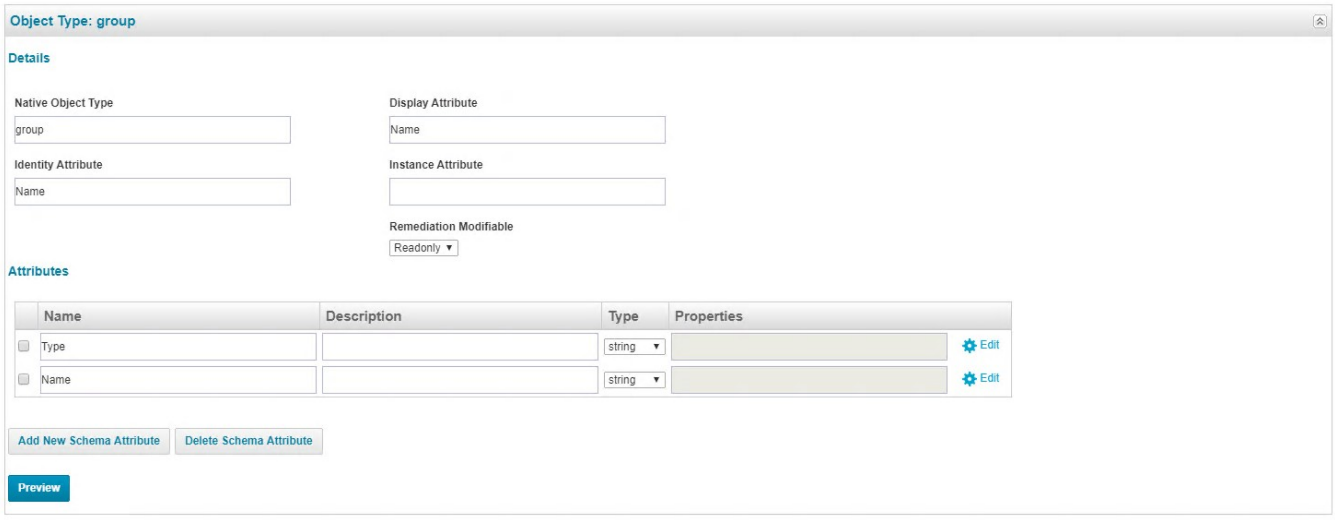
Body:

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:blueprism:webservice:blueprismv65deletecredential">
    <soapenv:Header/>
    <soapenv:Body>
        <urn:BluePrismv65DeleteCredential
soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
            <SignInConnectionName xsi:type="xsd:string">Default Connection</SignInConnectionName>
            <SignInCredentialName xsi:type="xsd:string">Blue Prism</SignInCredentialName>
            <SingleSignOn xsi:type="xsd:boolean">False</SingleSignOn>
            <CredentialName xsi:type="xsd:string">$plan.nativeIdentity$</CredentialName>
        </urn:BluePrismv65DeleteCredential>
    </soapenv:Body>
</soapenv:Envelope>
```

1.2.4. Configure Account and Group Aggregation

In the **Configuration**>**Schema** tab, set the following values for Account Aggregation and Group Aggregation.





1.2.5. Configure Enable and Disable Custom Rule

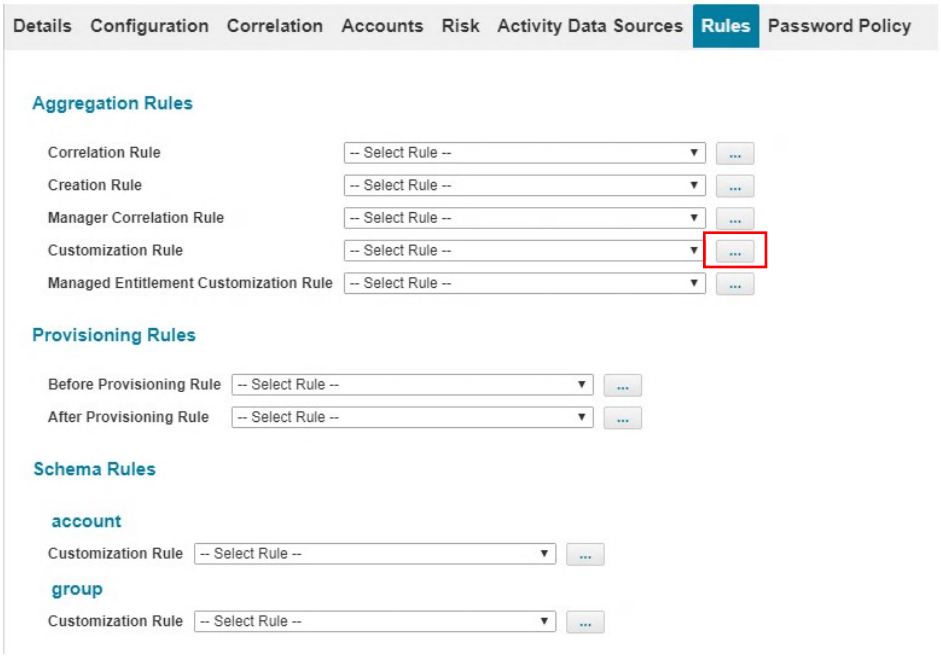
In order for the IdentityIQ interface to accurately reflect whether a Blue Prism credential is enabled or disabled (i.e. the "Mark as Invalid" checkbox is unchecked or checked, respectively), a custom rule must be created to set the "**IIQDisabled**" attribute for the credential when it changes status.

To do so, click **Applications** > **Application**

Definition Select the Blue Prism application

Select **"Rules"**

Within the **Aggregation Rules** heading, select the **ellipses button** to open the editor for the Customization Rule



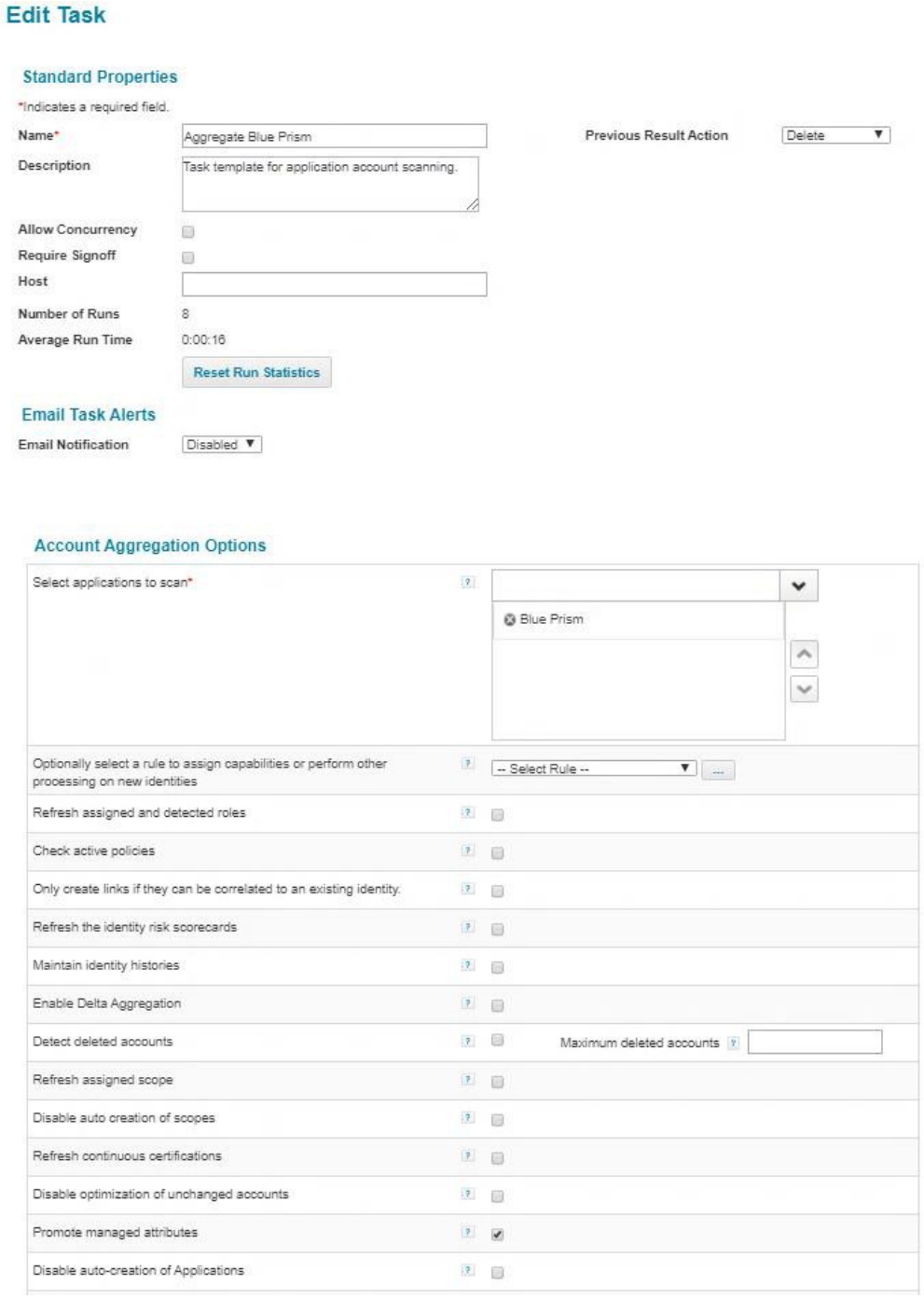
Give the rule a title, enter the following code, and save the rule:

```
String acctName = object.getIdentity();
// If Status has been populated with "Invalid" set the account to disabled.
String statusString = object.getAttribute("Status");
if ( (null != statusString) && (0 != statusString.length()) ) {
   if ("Invalid".equalsIgnoreCase(statusString)) {
      object.put("IIQDisabled", true);
   }
}
return object;
```

1.2.6. Configure Aggregation Task in IdentityIQ

The final step is to configure the Account and Group Aggregation operations as a Task in IdentityIQ. Once complete, this task will be able to execute the Blue Prism processes and gather the Credentials and Access Rights for usage in IdentityIQ.

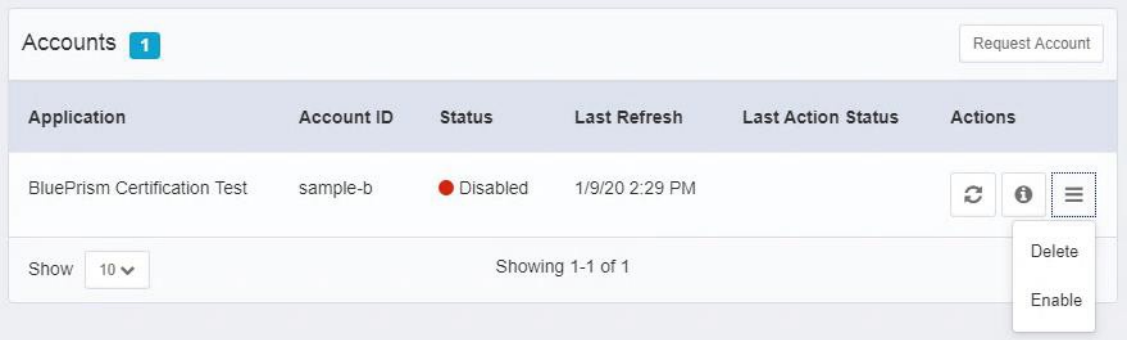
- Navigate to **Setup** > **Tasks** from the topmost toolbar in IdentityIQ.
- Select Create **New Task** > **Account Aggregation**
- Complete the form to match the following information and Save.



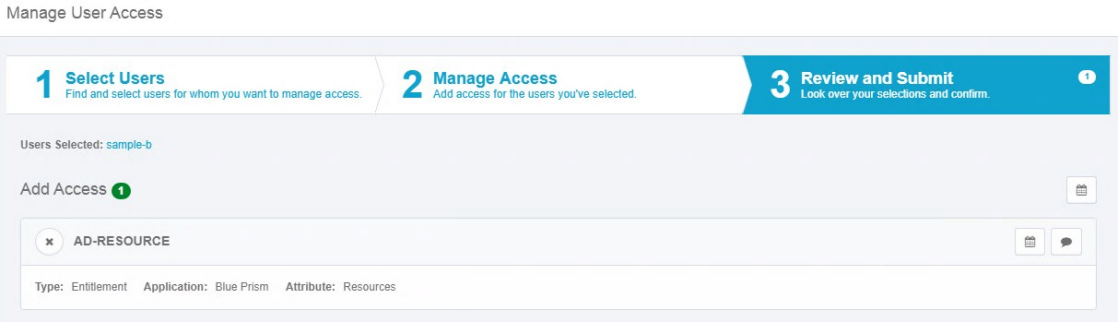
1.3. End to End Checklist

With the integration steps completed, the following actions should be functional within IdentityIQ

1. Enable, disable, and delete credentials from **Manage Access** > **Manage Accounts**



2. Add and Remove Access Rights from a Credential from **Manage Access** > **Manage User Access**



3. The Aggregation Task (in Setup > Tasks) can execute and gather current information about each Blue Prism credential and Access Rights.

2. Support

Support for this integration can be found in Compass.

SailPoint's knowledgebase, downloads, forums, requests for new Compass logins, and other useful information can be accessed on our Compass community: https://community.sailpoint.com/
If you have any issues with your Compass account or need to reset your password, please either use the links provided or send an email to compass@sailpoint.com. Please do not raise a ticket with Support as our Support organization does not administer Compass.