

SailPoint – Identity Security Cloud

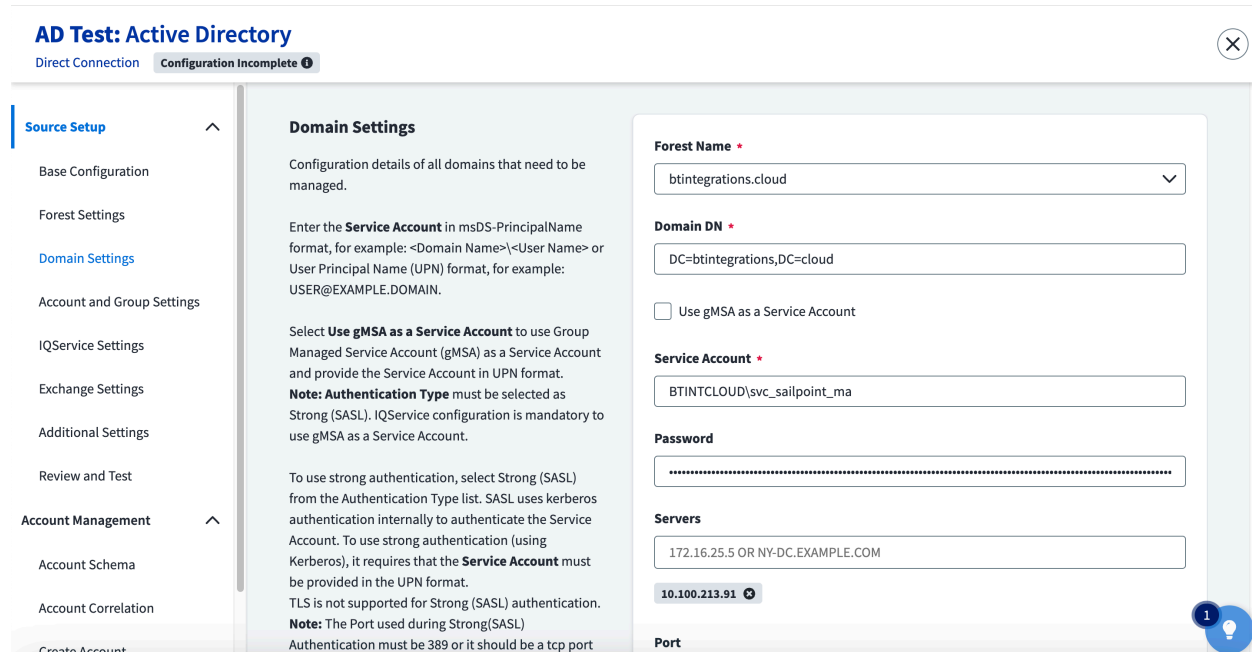
Password Safe Custom Plugin

integrations@beyondtrust.com

August 2024

Context

This Custom Plugin supports Rotating secrets for privileged credentials used by SailPoint Identity Security Cloud for Sources (Connectors).



Capabilities

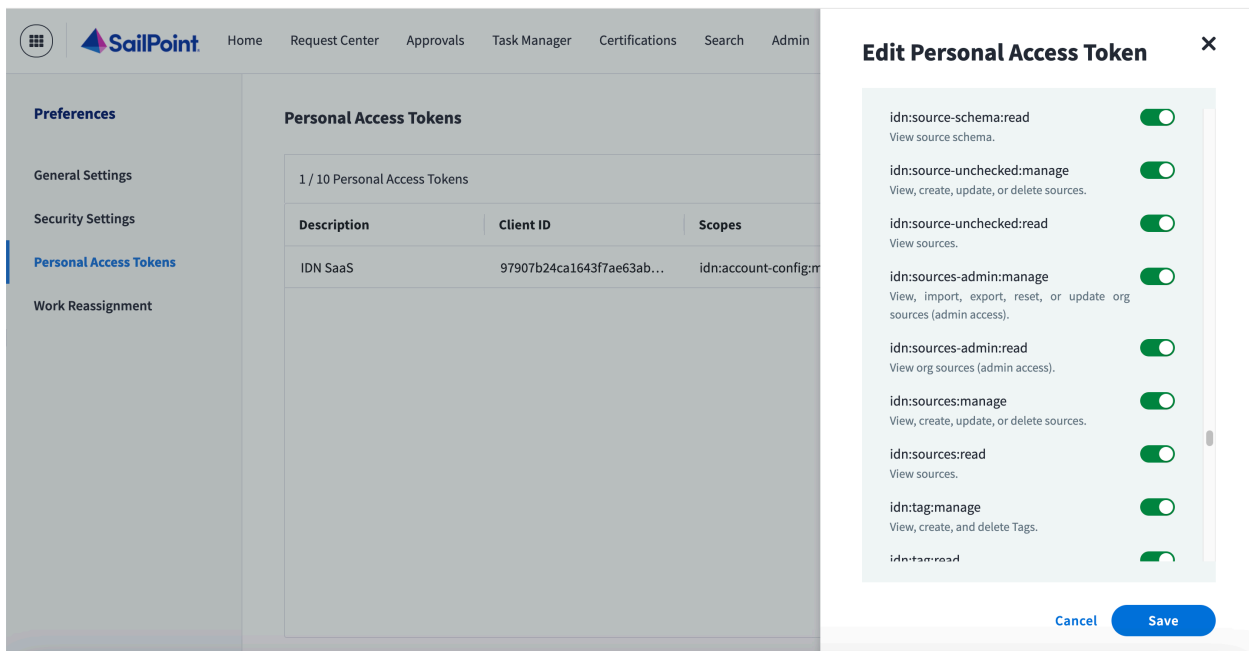
- Change Managed Account Credentials using Functional Account
- Verify Functional Account Credentials

The Plugin has been developed with the Password Safe 24.1.0.0 and 24.1.1.1 Resource Kit and SDK, but the same steps can be used for other versions of the SDK. It is also possible to have multiple .NET versions on the same Visual Studio development workstation simultaneously.

Temporary GitHub Private Repo (ask for invitation) :

<https://github.com/beyondtrust-integrations/PasswordSafeCustomPlugins>

How to use the example Plugin

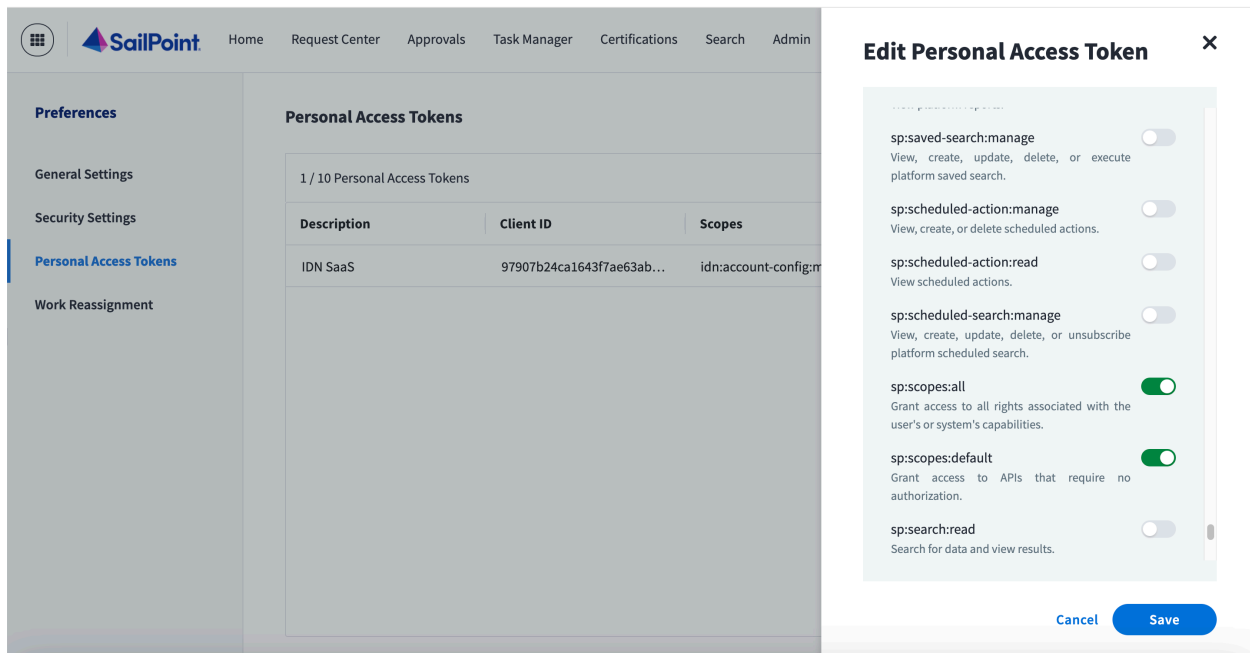


The screenshot displays the SailPoint ISC interface. On the left, the 'Preferences' sidebar is visible, with 'Personal Access Tokens' selected. The main content area shows a table of 'Personal Access Tokens' with columns for Description, Client ID, and Scopes. A single token is listed: 'IDN SaaS' with Client ID '97907b24ca1643f7ae63ab...' and Scopes 'idn:account-config:'. On the right, the 'Edit Personal Access Token' dialog is open, showing a list of permissions with toggle switches. The permissions listed are:

- idn:source-schema:read (View source schema.)
- idn:source-unchecked:manage (View, create, update, or delete sources.)
- idn:source-unchecked:read (View sources.)
- idn:sources-admin:manage (View, import, export, reset, or update org sources (admin access).)
- idn:sources-admin:read (View org sources (admin access).)
- idn:sources:manage (View, create, update, or delete sources.)
- idn:sources:read (View sources.)
- idn:tag:manage (View, create, and delete Tags.)
- idn:tag:read

At the bottom of the dialog are 'Cancel' and 'Save' buttons.

Create a Personal Access Token in ISC and grant permissions for managing Sources.




The screenshot shows the SailPoint Admin console interface. On the left is a sidebar with navigation links: Home, Request Center, Approvals, Task Manager, Certifications, Search, and Admin. Below these is a 'Preferences' section with links for General Settings, Security Settings, Personal Access Tokens (highlighted), and Work Reassignment. The main content area is titled 'Personal Access Tokens' and shows a table with columns 'Description', 'Client ID', and 'Scopes'. A single token is listed with the description 'IDN SaaS', a truncated Client ID, and the scope 'idn:account-config:'. An 'Edit Personal Access Token' modal is open on the right, displaying a list of permissions with toggle switches. The permissions include 'sp:saved-search:manage', 'sp:scheduled-action:manage', 'sp:scheduled-action:read', 'sp:scheduled-search:manage', 'sp:scopes:all', 'sp:scopes:default', and 'sp:search:read'. The 'sp:scopes:all' and 'sp:scopes:default' toggles are turned on, while the others are off. At the bottom of the modal are 'Cancel' and 'Save' buttons.

Scope permission is also needed.

Save the Client ID and Secret for the next steps.

Navigate to Configuration, Privileged Access Management, Platform Plugins, then Create New Platform Plugin.

Edit SailPoint Custom Plu



Drag and drop or click to select a file to upload.

Accepted File Types: PSPLUGIN
Maximum File Size: 5 MB

Upload Plugin

Name

Platform

Publisher

Version

Browse for the Plugin file and Upload the Plugin.

Edit Functional Account ➤

Platform
SailPoint Plugin

Username
svc_isc_fa

[Change Password](#)

Alias

Description (optional)

Workgroup

Password Management
☒ Automatic Password Management

[Update Functional Account](#) [Discard Changes](#)

Create a Functional Account for the Plugin. Use the username is cosmetic and not used. The password format is {client_id}:{client_secret}.

Edit SailPoint Identity Security Cloud


[View Advanced Details...](#)


Entity Type

Asset

Platform

SailPoint Plugin

 Collapse All

 Expand All

Identification

Name

SailPoint Identity Security Cloud

Description

DNS Name

https://company5176-poc.api.identitynow-demo.co

IP Address

127.0.0.1

☐ Allow use as an Application Host

Associated Managed Systems: 0

Workgroup

Default Workgroup

Automatic Password Change Options

Collapse all

Credentials

Functional Account

SailPoint ISC FA

[Create New Functional Account ...](#)

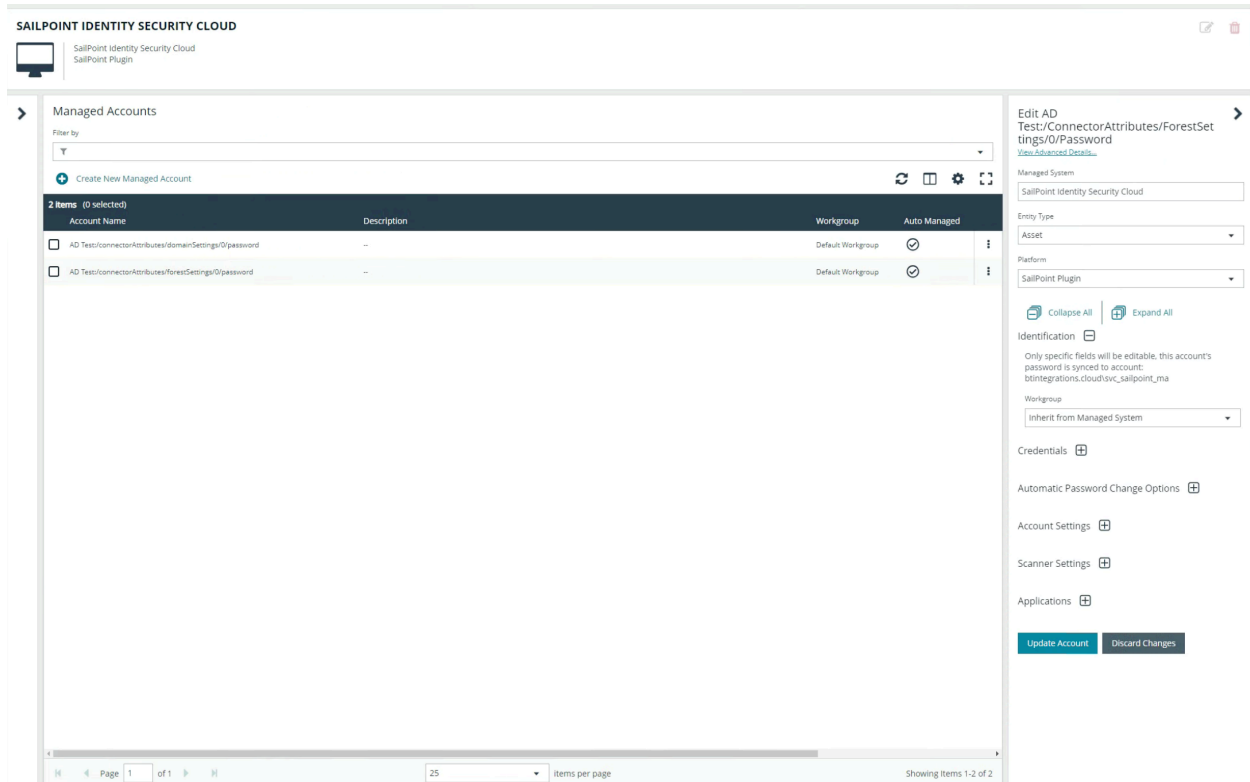
General Settings

Update Managed System

Discard Changes

Create a Managed System for the Plugin. DNS Name is is the API Url for ISC.

Note: The API Url has an extra .api part.



Account Name	Description	Workgroup	Auto Managed
AD Test/connectorAttributes/domainSettings/0/password	--	Default Workgroup	✓
AD Test/connectorAttributes/forestSettings/0/password	--	Default Workgroup	✓

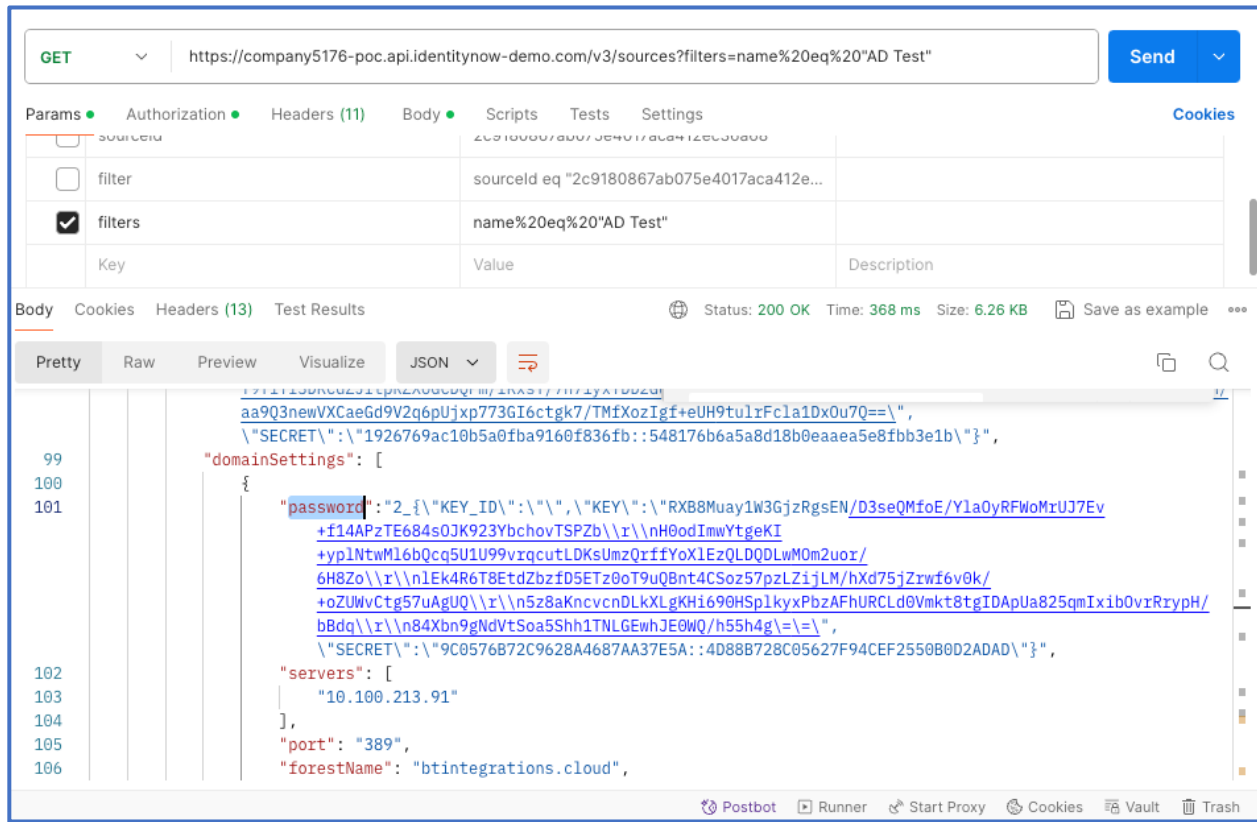
Create a Managed Account with the format {Source Name:password-JSONPATH}.

Note: the JSONPATH format can be identified using a tool like Postman and is specific to the Source type in ISC. You can refer to SailPoint API V3 documentation:

<https://developer.sailpoint.com/docs/api/v3/update-source>

For example, for Active Directory, if we want to update the Domain service account password, the JSONPATH is /ConnectorAttributes/ForestSettings/0/Password

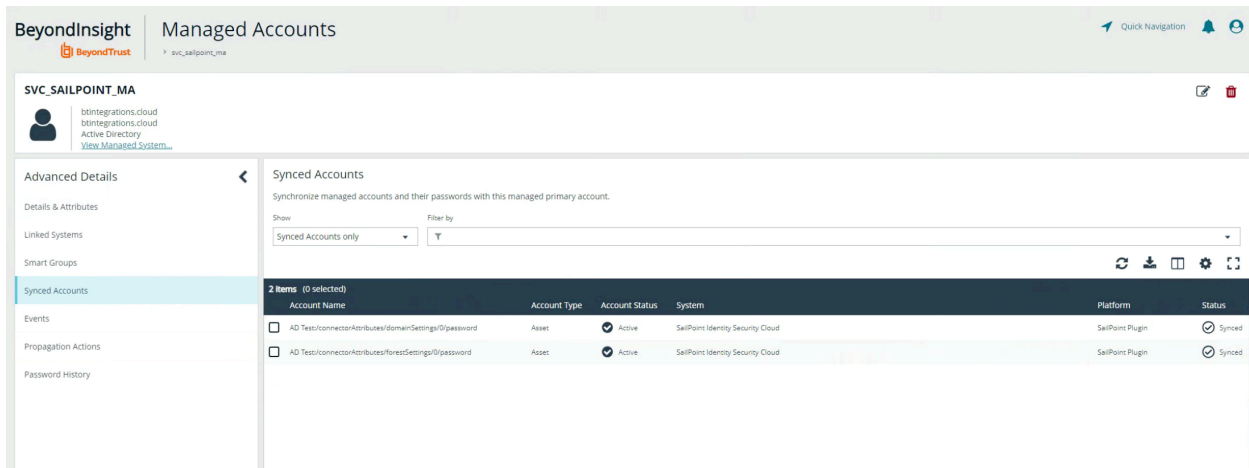
You can also refer to <https://jsonpatch.com/>



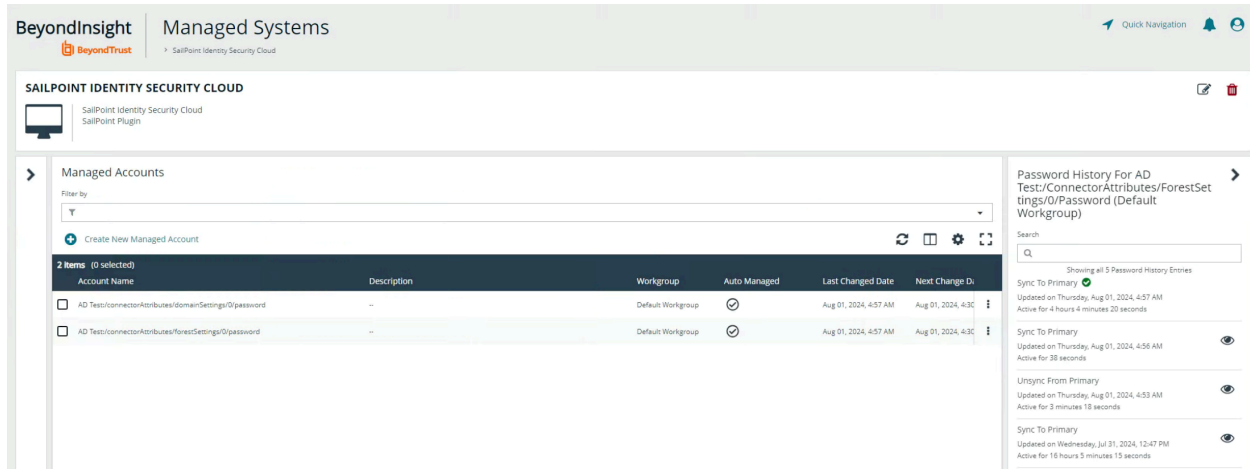
Using Postman to identify the location of password values within the Source.

At this point, you should be able to successfully Test Functional Account and Change Password for Managed Account.

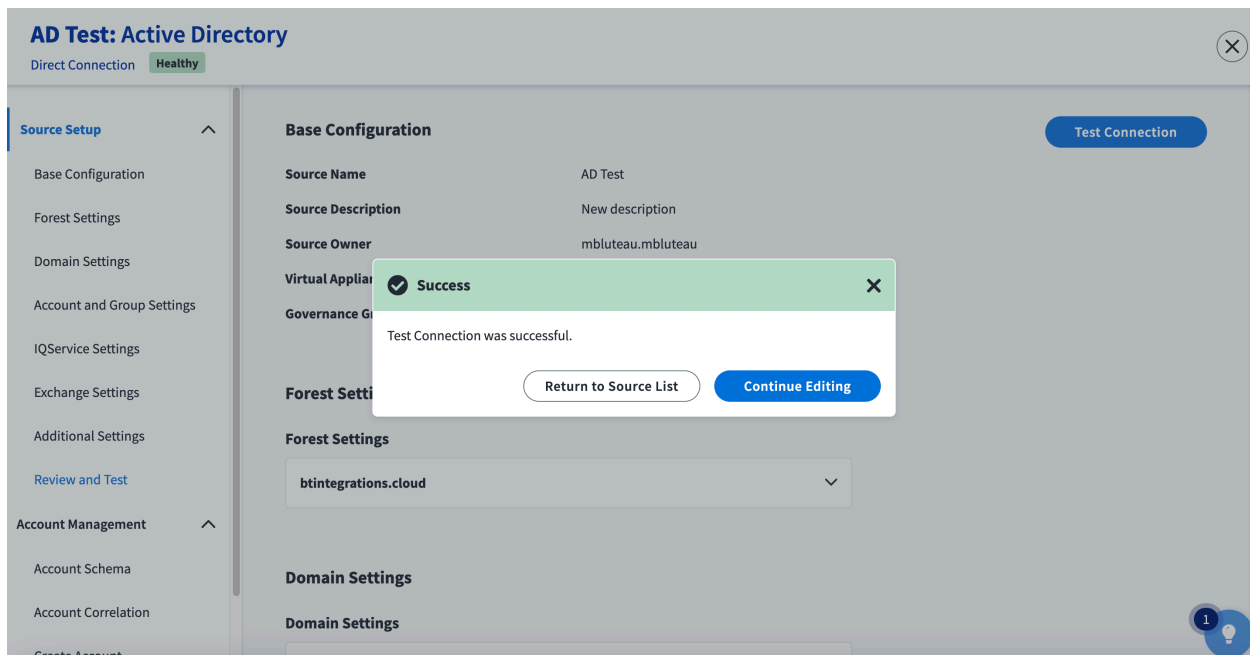
However, the typical configuration would be to Synchronize the AD Managed Account with either the Domain or Forest Managed Account, or both:



We are Synchronizing the AD Managed account used by SailPoint ISC for both Domain and Forest service account with both credentials for the AD Source.

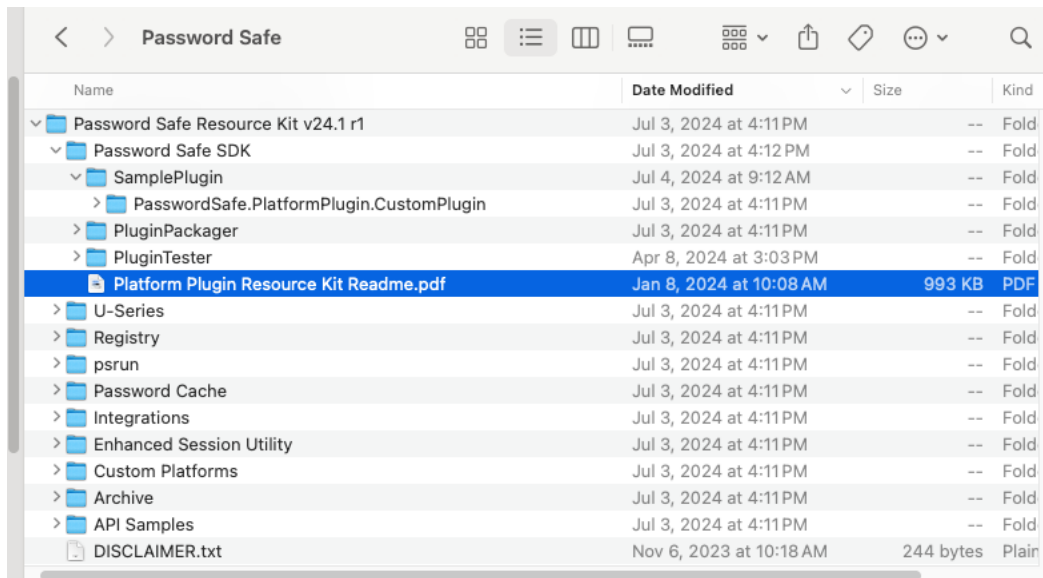


For the SailPoint Managed Account, we should see Sync to Primary whenever a Password Change is triggered for the AD Managed Account.



We can confirm that SailPoint has up-to-date password values by using Test Connection via the Source.

How to get the SDK



Follow the steps in Readme pdf to create a new project using the SamplePlugin.

Note: Multiple versions of .NET can coexist on the same Visual Studio workstation.