Changing or Resetting Passwords

Changing the User Password

The user passwords can be changed using the following methods:

- **Forgot Password:** Use the **Forgot Password** option from the Login page. You need to answer the security questions, or use multi-factor authentication to reset your password.

- **Profile menu:** Click on your Profile dropdown menu located at the top-right corner of the screen and use the **Change Password** option to utilize step-up authentication methods to reset your password.

- **Admin Functions:** Admins can navigate to **Admin Functions** to select a user and click **Manage** to reset the password for the user.

- **Reset User Password or Helpdesk:** Custom SAV roles can be allotted to Helpdesk to provide them access to the **Change password** tile on the ARS Homepage. The Helpdesk can then use the **Reset User Password** option to reset the password for a user. For more details, see Resetting User Password for Others by Helpdesk.

Resetting Security Questions

This feature is used for setting a security question that users are prompted for at the time of changing the password. Users or administrators can reset security questions in Security Manager. End users can reset security questions from the **Reset Security Questions** option after logging in to Security Manager.

To reset the security questions used at the time of changing the password, perform the following steps:

1. Click the **Reset Security Questions** option:

2. The **Reset Security Questions Step 1: Please enter your password** window is displayed with your username.

   Note: This window is not displayed if one of the following is true:

   - If your administrator has configured step-up authentication for the Reset Security Questions functionality.

   - If the external LDAP authentication or Single Sign On is enabled. In this case, you are redirected to the **Reset Security Questions (Please set your challenge questions) Step 2** window.

3. Enter the password and click **Next**. The **Reset Security Questions (Please set your challenge questions) Step 2** window is displayed.

4. Click **Select** to select the required security question and enter an appropriate answer for it. Use the same procedure to add new security questions and their answers.

5. The number of mandatory security questions is captured according to the **Questionnaire list** configured in the password policy and applied across the Security Manager application by your administrator.

6. Click **Save**.

After the successful completion of the **Reset Security Question** form, the security questions and answers in all mapped applications are changed for the user.

Security questions are used to verify your identity during login when you have forgotten your password. If the system administrator has enabled you to set up the security questions, you can perform the following:

- Specify responses that are valid for you when answering administrator-defined questions.

- Specify your own questions and valid responses for them (if your password policy enables this).

During the login process, the Login page automatically redirects you to the Set Security Questions page. You can set up the responses for your security questions on this page. When you log in again and try to reset the forgotten password, Enterprise

Identity Cloud (EIC) prompts the configured questions and asks you to specify answers for them. When your answers matches with the response that you have saved earlier, you are allowed to reset your password.

Changing Account Password for Self

This section provides details on how to change your own password. You can change your password in EIC or change the password of any applications connected to it. You can change your password for one or more applications at the same time, or individually. For more information, see Changing Account Password for Self.

Resetting the Account Password for Others

This section is intended for managers and admins who can change the password of other users. They can also change the password of one or more target application accounts of other users. This is specially useful for managers when they want to reset passwords for their direct reportees. For more information, see Resetting Account Password for Others.

Resetting User Password for Others by Helpdesk

This section explains the process of resetting the user password of other users by Helpdesk or Servicedesk personnel who have access to reset the user password for other users in Enterprise Identity Cloud (EIC).

The **Change password** tile in ARS provides the **Reset User Password** option to reset EIC password. The access to this option is managed via SAV roles. It does not need any administrator-specific privilege. As a Helpdesk personnel, you can verify a user's identity and assist the user with the password change.

To help a user with password change, perform the following steps:

1. Click **ARS** > **Change Password** > **Reset User Password**.

2. In the **User search** form that displays, select a user from the list to see the **User Details** page. Note that the primary and secondary Attributes of the user are displayed. If secondary attributes are not set by an administrator, they will not be displayed.

3. Ask appropriate questions to the user based on the information displayed pertaining to the user. Proceed to the next step after the user answers the questions correctly.

4. Click **Change Password**. You can automatically generate a password or type a password of your choice.

   Note: Auto-generated password is only populated if a **regex** pattern is configured in the USER scope of the password policy.

5. Advise the user to log in with the temporary password and set a new password. The user is sent an email about the password change if the password change notification is set for the user.

Note:

- The passwords set by the Helpdesk are “temporary” and must be changed once the user logs in using the “temporary” password. This can be done in EIC or in the target application (for example, Active Directory) used by the user.

- If your system administrator has configured email notification service for sending emails about password changes, the user will receive an email with the new password.

Changing the Account Password for Self

You can manage the passwords of accounts in target applications using the **Change password** tile in the Request home page.

This section provides details on how to change your accounts' passwords. You can change your password for one or more applications, at the same time or individually.

To change your own password, perform the following steps:

1. Select **ARS > Request Home**.

2. Click the **Change Password** tile and click **Change Account Password for Self** as displayed in the following figure:

   Figure: Change Account Password for Self

   Changing your own password is a three-step process as displayed in the following figure:

   Figure: Steps for Changing Password

3. **Select Application:** Select the name of one or more applications for which you want to change the password as displayed in the following figure:

   The following options are available in the columns displayed on this page:

Column	**Description**
Application (read-only)	Displays the name of the application.
Description (read-only)	Displays a detailed description of the application.
Password Policy (read-only)	Displays the appropriate password policy details.
Actions	Click the appropriate action type. The options are: • **Add to Cart**: Click this option to request for changing your own password.

	• **In Cart**: This option is displayed if the application is already in the cart. • **Remove From Cart**: This option is displayed if you have already added an applicat cart. Use this option to change your selected application. • **Add All to Cart:** Click this option to add all the available applications to the cart an the selected applications. • **View Cart:** Click this option to view the total number of applications selected and corresponding endpoints, account names, type, and available action details. When an application is added using **Add to Cart**, the **In Cart** and **Remove from Cart** options are available for the application. • **Checkout**: Click this option to check the selected applications for setting the passw

When an application is added using **Add to Cart**, the **In Cart** and **Remove from Cart** options are available for the application.

4. **Set Password:** Click **Change Password** to set a new password for your target application account. You can also use **Unlock** to unlock your account as displayed in the following figure:

The options on this page are displayed based on the configuration set by your system administrator.

5. The following options are available along with other columns at this stage:

- **View Cart:** Click this option to view the total number of selected applications and corresponding endpoints, account names, type, and available action details.

Column Names	**Description**
Associated Account (read-only)	Displays the accounts associated with the endpoints in separate rows.

Endpoint (read-only)	Displays the endpoint name for the application.
Password Policy	Displays the password policy associated with the user account. Click the :informatio icon to view the policy details.
Status	Displays the password entered or selected to update.
Actions	Displays the action needed to take for an account. • **Change Password:** When you select this option, it displays the **Change passwor** window. ○ **Suggested Password:** The tab displays the system generated password accordi defined password policy. ○ **Type New Password:** The tab displays the field to type a new password once t password is entered, click **Use Password**. • **Unlock**: Select this option to unlock the user account.
reCAPTCHA	Select **I'm not a robot** to verify reCAPTCHA. The reCAPTCHA is a CAPTCHA like a widget designed to establish that a compute human. It is a designed service for verification and identification of bots, if any, and p from spam and abuse.

5. **Next:** Click this option to submit the request.

Change Password from ServiceNow

POST

Change User Password

`{{url}}/ECM/{{path}}/changePassword`

This method resets "password" of a "user" record in SSM. Considering the input parameters, the value of new password should be supplied as `Password` and the `Username` should correspond to the user whose password is being reset.

The `Authorization` must have `Bearer` followed by `Token`.

Mandatory params:

`username`

`password`

Optional params:

`changePasswordAssociatedAccounts` - Values: true/false, default value - true, if true it creates change password tasks else just updates the user password

`endpoint` - list of endpoints comma separated (when changePasswordAssociatedAccounts is true)

`validateagainstpolicy` - Values: Y/N, default is Y. Checks against the password policy

`updateUserPassword` - Default value - true, (when changePasswordAssociatedAccounts is true). If updateUserPassword is true, update user password too along with creating the task. If updateUserPassword is false, just create the changepassword task.

`setarstasksource` - Values: true/false, default is false.If true, it will set source column in arstasks table with 'changeOwnPasswordFromAPI'. When source is 'changeOwnPasswordFromAPI',pwdLastSet is not set to “0” in ADconnector.

HEADERS

Authorization

Bearer {{token}}

BODYurlencoded

username

bliu

password

Hello$?33892@woRLd

changePasswordAssociatedAccounts

true

endpoint

Workday

validateagainstpolicy

Y

updateUserPassword

false

setarstasksource

true

Overview for Configuring Password Synchronization from Active Directory

Synchronizing passwords from Active Directory is not part of the normal user synchronization process. To synchronize passwords, you must install a Password Filter on the Active Directory server. The Password Filter captures passwords when user accounts are created or passwords are changed by users or administrators by any means. The Password Filter encrypts the passwords and sends the password information to EIC.

You can configure an additional level of validation on the Password Filter for the changed password and allow the password change to synchronize only if it is validated. For password synchronization to occur, you must install a password filter (SavPwFilter.dll) on each domain controller and configure the registry to capture password changes for sending them to EIC. The synchronized passwords are then propagated to the endpoints configured for the user. The endpoints are specified as part of the password filter configuration in the **SavPwFilter.json** file. The Password Filter is automatically started when the domain controller is started.

Password Synchronization Flow

The following diagram illustrates the synchronization flow when an Admin user or a Domain joined user initiates a password change.

Figure: Password Synchronization Flow

The following actions occur:

1. When a user changes a password, the Password Filter validates the password with the Password Filter password policy.

    - If the password adheres to the Password Filter password policy, the password is sent to the Active Directory.

    - If the password does not adhere to the Password Filter password policy, the password is return to the user.

2. The Password Filter sends the password to the Active Directory. The Active Directory validates the password against the Active Directory password policy.

   - If the password adheres to the Active Directory password policy, the password is synced with Active Directory.

   - If the password does not adhere to the Active Directory password policy, the password is not synced with Active Directory.

3. The Active Directory sends the validated password to the Password Filter.

4. The Password Filter saves the password in the SQLite database.

5. The SQLite database sends the password to the Password Filter.

6. The Password Filter sends the password to EIC to sync the password with the user profile.
   Note: If the EIC server is down or EIC URL is not responding, the SQLite database queues the changed passwords based on the values specified in the logsize and backuplogfile attributes of the SavPwFilter.json file.

7. EIC sends the synchronized passwords to different endpoints configured for the user.

Installing the Password Filter

This section provides details about installing the Password Filter.

Prerequisites

Ensure that all the prerequisites are met before you install the Password Filter:

- A Windows Server 2012 R2 (64-bit) and later running Active Directory

- Microsoft Visual C++ Redistributable 2015 - 2019 packages are installed on the Windows Server running Active Directory

Installation Worksheet

Use the following information to complete the installation of the Password Filter. You must gather this information before you start the installation process.

Required Information	**Description**
Password Filter Download Directory	PasswordSyncFilter.zip Click this link to download the file.

Configure Saviynt Connection	Specify the EIC connection details in the **SavPwFilter.json** file. The Password Filter use details to establish a connection with EIC for synchronizing passwords.
	To define the JSON, use a format similar to the following:
	`{`
	`"saviynt": {`
	`"baseUrl": "https://<hostname>:<port>/ECM",`
	`"userName": "User name of the administrator",`
	`"password": "Encrypted password of the administrator",`
	`"EnabledVersion": "v5",`
	`"v2": {`
	`"getUserUrl": "/ws/rest/getUser",`
	`"notificationUrl": "/ws/rest/changePassword"`
	`},`
	`"v5": {`
	`"getUserUrl": "/api/v5/getUser",`
	`"notificationUrl": "/api/v5/changePassword",`
	`"oauthUrl": "/api/login",`
	`"oauthRefreshUrl": "/oauth/access_token"`
	`},`
	`"correlation": "username",`
	`"endpoints": "These are the endpoints to which EIC will synchronize the password",`
	`"sourceEndpoint": "Active Directory",`
	`"retry": 5,`
	`"timeout": 60,`
	`"delay": 5`
	`}`
	`}`

where:

- **baseUrl:** Use this attribute to specify the URL where EIC is hosted.

- **userName:** Use this attribute to specify the username of the administrator account req connect to EIC.

- **password:** Use this attribute to specify the encrypted password for the administrator u account required to connect to EIC. The installation folder contains the **SavPasswordEncrypt.exe** utility for encrypting this password. Run this utility fro command prompt to generate the encrypted the password and specify that password fo parameter.

- **EnabledVersion:** Use this attribute to specify the enabled version. Depending on EIC use V2 if basic authentication is enabled, and use V5 if OAuth based authentication is

- **notificationUrl:** Use this attribute to specify the URL of the changePassword REST A changes the password in EIC.

- **correlation:** Use this attribute to correlate an Active Directory user for whom the pass changed with the users in EIC. If a matching user is found, the password is synchroniz Otherwise, the password is not synchronized.

- **endpoints:** Use this attribute to specify the endpoints to which the password change m propogated.

- **sourceEndpoint:** Use this attribute to specify the name of the Active Directory endpo

- **retry:** Use this attribute to define the number of times the password filter attempts to resynchronize the changed password to EIC if the password synchronization fails.

- **timeout:** Use this attribute to specify the time period within which the connection betv Password Filter and EIC must be established. Otherwise, the connection times out.

- **delay:** Use this attribute to specify the amount of time in seconds between two passwo synchronization retries.

Disable Password Change Notification	The Password Filter automatically notifies the password change to EIC. To stop the notif make the following entry in the **SavPwFilter.json** file: `"notification": {"enabled": false},`

Enforce Password Policy	The Password Filter can optionally apply a password policy on the changed password bef sending it to EIC. This provides an additional layer of validation of changed passwords. I password does not comply with the password policy, it is not synchronized and an error m displayed.
	By default, this setting is disabled. To enable it, make the following entry in the **SavPwFilter.json** file:
	`"filter": { "enabled": true, "policy": { "enforce":  "local", "local":`
	`"minChars": 6, "maxChars": 20, "lowerCases": 1, "upperCases": 1, "numbe`
	`"specials": 1 } } }`

Configure log file rotation policy	The Password Filter can rotate the log files based on the values specified in the `logsize` and `backuplogfile` attributes.
	To define log file details, make the following entry in the **SavPwFilter.json** file:
	`"log": {`
	`"logfile": "log\\SavPwFilter.log",`
	`"loglevel": 0,`
	`"logsize": 10,`
	`"backuplogfile": 5,`
	`"verbose": 0`
	`}`
	where,
	• `logfile` - Use this attribute to define the location of log files.
	• `loglevel` - Use this attribute to define a log level. You can cloose a log level as show
	○ `0` for Debug level logs
	○ `1` for Info level logs
	○ `2` for Warn level logs

	○ `3` for Error level logs ○ `4` for Exception level logs ○ `5` for Disable level logs • `logsize` - Use this attribute to define the maximum file size (in MB) allowed for writi When the log file reaches this size, a backup of the log file is taken and the log is writt new file. • `backuplogfile` - Use this attribute to define the maximum number of backup log file maintained. • `verbose` - Use this attribute to add additional details in the log file.

Installation Procedure

The software required to install and configure the Password Filter is available in the **PasswordSyncFilter.zip** file. This file contains the following contents:

- **SavPWFilter.dll:** Synchronizes the changed passwords.

- **SavPasswordEncrypt.exe:** Generates an encrypted password for the administrator user account for establishing a connection with EIC. You must specify the encrypted password in the password entry in the **SavPwFilter.json** file.

- **SavPWFilter.json:** Contains the settings for configuring the Password Filter.

Perform the following steps to install and configure the Password Filter:

1. Create a new folder named SavPwFilter in the **C:\** directory of the Active Directory domain controller server.

2. Copy the **PasswordSyncFilter.zip** file to the folder that you created in Step 1 and extract the contents of the file.

3. Locate the **SavPasswordEncrypt.exe** file in the extracted contents and run the file in the command prompt to encrypt the administrator user password.

4. Locate the **SavPwFilter.json** file in the extracted contents and define the following settings for your requirement**:**

    1. **Connection with EIC**

    2. **Disable Password Change Notification**

    3. **Enforce Password Policy**

    4. **Configure log file rotation policy**

5. Enable Local Security Authority (LSA) protection for the Password Filter to successfully load it as a protected process on the Active Directory domain controller server.

6. Open the Registry Editor (RegEdit.exe) and navigate to the registry key located at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages.

7. Add the following value to the registry key: **C:\SavPwFilter\SavPwFilter.dll.**

8. Restart the Active Directory domain controller server.

By default, logging is enabled for password change requests sent from the Active Directory server and captured in the SavPWFilter.log file located in the Password Filter installation folder (**C:\SavPwFilter**). To change the log details, modify the log entries in the **SavPWFilter.json** file.

Uninstallation Procedure

1. Open the Registry Editor and navigate to the registry key located at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages.

2. Remove the following value from the registry key: **C:\SavPwFilter\SavPwFilter.dll.**

3. Restart the Active Directory domain controller server.

4. Delete the SavPwFilter folder from the **C:\** directory of the Active Directory domain controller server where SavPwFilter.dll was saved.