# SSF Tools: Password Expiration Reminder User Guide

# Document Revision History

| Revision Date | Written/Edited By | Comments |
|---|---|---|
| June 2017 | Kaveh Ahmadian | Password Expiration Reminder v1 initial release with SSD v4. |
| | | |

# Table of Contents

# Introduction

Password Expiration Reminder provides a mechanism to send notifications to users through IdentityIQ when the passwords on their accounts in integrated target systems are about to expire. It is also possible to configure steps to be taken when an account password has expired.

The tool is implemented via an IdentityIQ Advanced Policy that executes the Rule for each configured Application, which in turn determines if an account password has expired or if a reminder notification needs to be sent. If expired, a policy violation occurs, and additional actions may be configured via a custom Workflow (see below).

# Components

The following components are used in the Password Expiration Reminder solution:

| File | Location in SSD | Description |
|---|---|---|
| Password_Expiration_Configuration_Custom.xml | config/SSF_Tools/PasswordExpirationReminder/Source/Custom/ | Custom object that defines the Rules used by the Password Expiration Policy. |
| Password_Expiration_Policy.xml | config/SSF_Tools/PasswordExpirationReminder/Source/Policy/ | Policy that executes Rules for each configured Application, driving the process that causes email notifications to be sent. Defines Policy Violations for passwords that have expired. |
| Password_Expiration_Policy_Rule.xml | config/SSF_Tools/PasswordExpirationReminder/Source/Rule/ | The main Password Expiration Policy Rule which determines whether any passwords are due to expire or have expired by running the Rules for the Applications related to the identity's accounts. Launches the Password Expiration Reminder Workflow to notify of expiring passwords. Sets Policy Violations for expired passwords. |
| Sample_AD_Password_Expiration_Rule.xml | config/SSF_Tools/PasswordExpirationReminder/Source/Rule/Samples/ | Sample Password Expiration Rule to determine whether an Active Directory account has an expiring password. Provided as an example - not deployed automatically. |
| Sample_DS_Password_Expiration_Rule.xml | config/SSF_Tools/PasswordExpirationReminder/Source/Rule/Samples/ | Sample Password Expiration Rule to determine whether an account for a custom application has an expiring password. Provided as an example - not deployed automatically. |
| Password_Expiration_Reminder_Workflow.xml | config/SSF_Tools/PasswordExpirationReminder/Source/Workflow/ | Password Expiration Reminder Workflow to send emails to identities whose passwords are due to expire. |
| Expired_Password_Workflow.xml | config/SSF_Tools/PasswordExpirationReminder/Source/Workflow/ | Expired Password Workflow to define any actions that should be taken when a Policy Violation is generated due to an expired password. Takes no action by default. |
| Password_Expiration_Reminder_Email.xml | config/SSF_Tools/PasswordExpirationReminder/Source/EmailTemplate/ | An Email Template to define the content of the email sent to identities whose passwords are due to expire. |

# Deployment and Configuration

To deploy and configure the Password Expiration Reminder solution, follow the instructions below. If you are using the SSD Deployer tool, step 1 will be completed for you if you selected the option to deploy Password Expiration Reminder. Refer to the SSD Deployer User Guide for more information.

1. In the SSB build.properties file, set the 'deployPasswordExpirationReminder' property to 'true'.

2. Edit the 'Password Expiration Configuration' Custom object:

```
<Custom name="Password Expiration Configuration">
  <Attributes>
    <Map>
      <entry key="Active Directory" value="Sample AD Password Expiration Rule"/>
      <entry key="Directory Server" value="Sample DS Password Expiration Rule"/>
    </Map>
  </Attributes>
</Custom>
```

   The *key* for each attribute is the name of an IdentityIQ Application, and the *value* contains the name of a custom Rule, containing the password expiration logic for that Application. Thus, in the above example, there are two Application ("Active Directory" and "Directory Server") password expiration rules configured.

3. For each configured Application, write a corresponding Rule that returns an integer, representing the number of days before the account password expires. If no notification should be sent, return null. If a number less than zero (0) is returned, it will signify that the password has expired and a policy violation will be generated (see below). Note that the Rules referenced in the above configuration example are provided as samples and can be used with Active Directory and certain supported LDAP servers (respectively). Use these sample rules as templates, but place the finished rules directly in the 'Rule' folder; any rules under the 'Rule/Samples' folder will not be deployed by the build process.

4. Optionally, review the provided Workflow named "Expired Password Workflow", which will be launched when a password has expired. Currently no action is taken by the Workflow, but it can be customized as needed.

5. Run and deploy the build (refer to the Services Standard Build User Guide for more information).

A daily Identity Refresh Task needs to be configured with the "Check active policies" option enabled (see screenshot below). This is required to evaluate the password expiration logic and send out notifications accordingly. If policies are not checked on a daily schedule, notifications may be missed.

## Notes

The password expiration reminder schedule is handled as part of the logic within the Rules specified for each configured Application (see example above). In the provided sample Rules, this is stored as a String variable containing a comma-separated list of days before expiration that a reminder notification should be sent. This configuration may be moved into a Custom object if desired.

Currently the notification message is constructed via a combination of text returned by the Advanced Policy (via the “Password Expiration Policy Rule” Rule) and the provided EmailTemplate (named “Password Expiration Reminder Template”). As a result, customization and internationalization is not easily supported. This may be rectified in a future release.