



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.

© Copyright 2017 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 photocopied, reproduced, 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 reexport 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 reexport 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 Entities List; a party prohibited from participation in export or reexport 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.

Trademark Notices. Copyright © 2017 SailPoint Technologies, Inc. All rights reserved. SailPoint, the SailPoint logo, SailPoint IdentityIQ, and SailPoint Identity Analyzer are trademarks of SailPoint Technologies, Inc. and may not 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

Introduction.....	4
Components	4
Deployment and Configuration	5
Notes	6

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.

Check active policies



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.