

# Credential Cycling in IdentityIQ with CyberArk

---

Back to the IdentityIQ 7.3 overview: [What's New in IdentityIQ 7.3](#)

- [Overview](#) on page 1
  - [About Credential Cycling](#) on page 1
  - [How Credential Cycling Works in IdentityIQ](#) on page 1
- [Working with the Credential Configuration Template](#) on page 2
  - [Template General Guidelines](#) on page 2
  - [Working with the CyberArk Template](#) on page 2
- [Credential Cycling in an Application](#) on page 4

## Overview

IdentityIQ version 7.3 continues to build out a robust Privileged Access Management (PAM) solution, by adding **credential cycling** to IdentityIQ's support for PAM.

The [Identity University](#) eLearning course on IdentityIQ 7.3 New Features includes a detailed lesson on enabling credential cycling.

## About Credential Cycling

At a high level, credential cycling is a feature that allows applications which require credentials (such as username and password) to obtain that information directly from a PAM source, such as CyberArk . Previously, these credentials had to be set up in the application definition manually, and if any information changed in the PAM solution, those changes had to be made manually in IdentityIQ by an administrator. With IdentityIQ 7.3, the credential cycling feature lets credentials be pulled directly from the PAM vault at runtime, with no manual intervention (other than initial configuration) by the IdentityIQ administrator, adding both security and convenience.

## How Credential Cycling Works in IdentityIQ

With version 7.3, you can manage credentials solely within your PAM solution. Essentially, an administrator defines which applications will use credential cycling, which PAM solution provides those credentials, and how each of the applications will contact the PAM vault to retrieve the credentials. This is done via a configuration file that is imported into IdentityIQ as an object.

Here is a brief summary of how credential cycling is configured in IdentityIQ. A more detailed look at the template and the configuration options is provided in a later section.

- Your applications should already be set up in IdentityIQ (**Applications > Application Definition**)

- In some cases the discovery options in an application can be disabled when credential cycling is enabled, so perform any necessary discovery operations before enabling credential cycling for the application.
- A template file is provided in your IdentityIQ installation, which you use as a model for setting up your own configuration. The template file is

*[IdentityIQ installation directory]\WEB-INF\config\credentialConfigurationTemplate.xml*

- You edit this file to define your PAM source values. The template includes models for **CyberArk**.
- You also include information in the file about which of your applications in IdentityIQ will use credential cycling, and how the PAM-provided values map to your application fields for authentication.
- You import the edited XML file into IdentityIQ (using **gear > Global Configuration > Import File**)
- Importing the file creates a new object in IdentityIQ: **Credential Configuration**
- If you need to update your credential cycling configuration, you can modify and re-import the credential configuration XML. You can also edit the Credential Configuration object directly in the Debug pages.

## Working with the Credential Configuration Template

The credentialConfigurationTemplate.xml is located in the WEB-INF\config directory of your IdentityIQ installation. The file is fully commented, to provide guidance as you insert your configuration settings.

### Template General Guidelines

- Remove the sections that you will not use before importing the template. For example, if you want to implement just a CyberArk solution, remove all other template sections.
- Each solution option has a section for mapping **Credential Source** details, which manage the connection to your PAM solution, and a **Credential Association** section, which handles the association of the secure credentials in your PAM solution to your applications in IdentityIQ.
- As always when working with templates, the best practice is to make a **copy** of this template to hold your specific configuration values, rather than modifying the original template file.

### Working with the CyberArk Template

Here are some key points to observe when you work with the CyberArk portion of the template. In the **Credential Source** section, you configure

- The name of your CyberArk safe - this information comes from CyberArk.
- The folder where your secure credentials are stored. Use "root" here if you do not use folders.
- An AppID, which is a unique identifier, used for authorization, which the CyberArk Credential Provider creates when it's installed on a host

In the **Credential Association** section, you configure

- The name(s) of your IdentityIQ applications that will use credential cycling
- The attributes for your application's username, and the corresponding CyberArk username that provides the secure username credential to the application at runtime.

- A CyberArk object, which is CyberArk's representation of a collection of attributes which store password and user name information
- Any application-specific overrides to the overall CyberArk settings

```
<CredentialSource credentialClass="sailpoint.pam.credential.CyberArkCredentialManager"
name="cyberark">
    <!-- The attributes in this map are used mainly to communicate with
CyberArk.
    Any values here can be overridden by values of the same name in the
attributes
    map of each credential association. Required attributes must either
be configured
    here or in every credential source. Attributes:
    Required: safe
    Required: folder
    Required: appId
    Required: object
    -->
    <Attributes>
    <Map>
        <entry key="safe" value="cyber_ark_safe_name"/>
        <entry key="folder" value="cyber_ark_folder_name"/>
        <entry key="appId" value="cyber_ark_app_ID"/>
    </Map>
    </Attributes>

    <!-- *** Application Configuration -->
    <CredentialAssociation applicationName="application_name"
        attributeName="application_username_attribute"
credentialAttributeName="CyberArk_username_attribute">
        <!-- *** Attribute values go here. These attributes can be used to
override values from
        *** above, or can be left out if not needed -->
        <Attributes>
        <Map>
            <entry key="object" value="object_value"/>
        </Map>
        </Attributes>
    </CredentialAssociation>
</CredentialSource>
```

## Credential Cycling in an Application

When credential cycling is configured for an application, the Application Definition UI shows a message to indicate this. Although the relevant credential fields (in this example, **Connection User** and **Connection Password**) are still marked as requiring values, these fields are not validated when credential cycling is enabled, and so can be left blank, or can include dummy values.

### Edit Application JDBCDirectDemoData

Details **Configuration** Correlation Accounts Risk Activity Data Sources Rules Password Policy

Settings Schema Provisioning Policies

Credential Cycling is enabled for this application. Required field validation will not be performed.

Add Object Type

Object Type: account

Settings Merging Iteration Partitioning Delta Aggregation

JDBC Connection Settings

\* Connection User ?

Connection Password ?

\* Database URL ?

jdbc:mysql:[REDACTED]jdbcdirectdemodata

\* JDBC Driver ?

com.mysql.jdbc.Driver

Query Settings