Ping Identity™

PingDirectory®

Password Policy User State v1.0.0

User Guide

PingDirectory Password Policy User State User Guide
Version 1.0.0
February 2018

Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
USA

Phone: 877.898.2905 (+1 303.468.2882 outside North America)
Fax: 303.468.2909 E-mail: info@pingidentity.com
Web Site: http://www.pingidentity.com

Trademarks

Disclaimer
This document is proprietary and not for general publication. It may be provided ad hoc for informational purposes only, and the information herein is subject to change without notice. Ping Identity does not provide any warranties and specifically disclaims any liability in connection with this document.

Note that Ping Identity may not provide support for any sample configurations provided in this document. The variability inherent among security environments prevents full testing and support for all possible platform configurations. If you need special assistance or would like to inquire about implementation or support programs, please contact Ping Identity Global Client Services (http://support.pingidentity.com).

Table of Contents

Purpose

The “Password Policy User State” Plugin provides the ability to manage user account password policy state with regular LDAP modify operations and to check a user account password policy state with a simple LDAP search operation

Prerequisites

This document assumes that a functional PingDirectory, Version 6.*, has already been installed and configured.

Installation

1. Copy the included zip file to a temporary location on the server that is running PingDirectory.
2. Open a terminal window.
3. Change directories to the installation path of the target PingDirectory server.
4. Execute the “`manage-extension`” command in the bin directory of the installation path to install the zip file and follow any prompts to continue and restart the server:

   ```
   bin/manage-extension --install <path to the zip file>
   ```

5. Execute the “`dsconfig`” command in the bin directory of the installation path to configure the plugin and press “`f`” at the prompt to finish the configuration of the plugin:

   ```
   bin/dsconfig create-plugin --plugin-name "Password Policy User State Plugin" \
     --type third-party \
     --set enabled:true \
     --set plugin-type:preparsemodify \
     --set plugin-type:searchresultentry \
     --set extension-class:com.pingidentity.ds.plugin.PwpUserState
     --set extension-argument:time-format=<time-format>
   ```

   ‘`time-format`’ is an optional argument and specifies the pattern for formatting date and time values per the Java SDK SimpleDateFormat formatting rules. The default value is: `yyyyMMddHHmmss.SSS'Z'`

6. *Optional*: To enable Server Extension debug messages, execute the following command:

   ```
   bin/dsconfig set-log-publisher-prop \
         --publisher-name "Server SDK Extension Debug Logger" \
         --set enabled:true
   ```

7. *Optional*: To delete the plugin, execute the following command:

   ```
   bin/dsconfig delete-plugin --plugin-name "Password Policy User State Plugin"
   ```

Using the extension

Reading user account state

Simply add the `ds-pwp-user-state-get-all` attribute with an LDAP search request to retrieve all the password policy state information available.

To find an individual attribute, the following can be used:

- account-activation-time
- account-disabled
- account-expiration-time
- account-expired
- account-failure-locked
- account-idle-locked
- account-not-active-yet
- account-reset-locked
- account-usability-error
- account-usability-notice
- account-usability-warning
- account-usable
- auth-failure-time
- available-sasl-mechanism
- available-totp-delivery-mechanism
- failure-lockout-time
- grace-login-use-time
- idle-lockout-time
- last-login-ip-address
- last-login-time
- pw-changed-by-required-time
- pw-changed-time
- pw-expiration-time
- pw-expiration-warned-time
- pw-expired
- pw-history
- pw-history-count
- pw-reset
- pw-retired-time
- pwp-dn
- remaining-auth-failure-count
- remaining-grace-login-count
- reset-lockout-time
- has-retired-password
- retired-password-expiration-time
- seconds-until-account-activation
- seconds-until-account-expiration
- seconds-until-auth-failure-unlock
- seconds-until-idle-lockout
- seconds-until-pw-expiration
- seconds-until-pw-expiration-warning

- seconds-until-pw-reset-lockout
- seconds-until-required-changed-time

Setting user account state

Setting password policy state attribute values can be accomplished thru the LDAP modify request. The examples below show how invoking the LDAP modify request with an LDIF can make changes to a user's password policy state.

Disabling an account

Use the replace modification to the 'ds-pwp-user-state-account-disabled' attribute to true:

```
changetype: modify
replace: ds-pwp-user-state-account-disabled
ds-pwp-user-state-account-disabled: true
```

Enabling an account

There are two options, by replacing the value of the 'ds-pwp-user-state-account-disabled' attribute to false, similar to the previous example:

```
changetype: modify
replace: ds-pwp-user-state-account-disabled
ds-pwp-user-state-account-disabled: false
```

Alternatively, one could simply delete the 'ds-pwp-user-state-account-disabled' attribute from the entry altogether:

```
changetype: modify
delete: ds-pwp-user-state-account-disabled
```

Unlocking a user out

This is a very popular request, especially from access manager middle-tiers that cannot use extended operations.

To unlock an account that has been locked due to exceeding the authentication failure limit set in password policy, clear the history of authentication failure times, which can be accomplished by deleting the 'ds-pwp-user-state-auth-failure-time' attribute:

```
changetype: modify
delete: ds-pwp-user-state-auth-failure-time
```

or by using the replace modification:

```
changetype: modify
replace: ds-pwp-user-state-auth-failure-time
```