# pd-pwp-user-state-plugin 1.6.13

## *User Guide*

PingDirectory

PingDirectory pd-pwp-user-state-plugin User Guide
Version 1.6.13
April 2025

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

# 1. Purpose/Requirements

This extension provides support for managing the user account password policy state with simple LDAP operations. To facilitate compatibility with legacy systems, it allows the attribute names to be configured.

# 2. Prerequisites

This document assumes that you already have the following installed and configured:

- PingDirectory, version 9.2.0.0 or later.
- JDK version 11

# 3. Installation

1. Install the pd-pwp-user-state-plugin into PingDirectory using the `manage-extension` utility:

```
$ <pingdirectory>/bin/manage-extension --no-prompt --install pd-pwp-user-state-plugin-v1.6.13-runtime.zip
```

2. Start or restart PingDirectory.
3. Repeat steps 1 and 2 on other PingDirectory servers.

# 4. PingDirectory Configuration

Configuration below is mostly for illustrative purposes. Configuration will be unique to each environment.

## 4.1. Basic Plugin Configuration

The simplest configuration of the pd-pwp-user-state-plugin uses the default names of the attributes. This represents a minimal configuration that works in a new installation. Client applications that rely on specific attribute names for password management in the directory may require modification to use the default attribute names.

1. Configure the pd-pwp-user-state-plugin:

```
dsconfig create-plugin \
    --plugin-name 'Password Policy User State'  \
    --type third-party  \
    --set enabled:true  \
    --set plugin-type:postoperationadd  \
    --set plugin-type:preparseadd  \
    --set plugin-type:preparsemodify  \
    --set plugin-type:preparsesearch  \
    --set plugin-type:searchresultentry  \
    --set invoke-for-internal-operations:false  \
    --set extension-class:com.pingidentity.ps.pd.plugin.PwpUserState
```

## 4.2. Advanced Plugin Configuration

When using the pd-pwp-user-state-plugin in a deployment that replaces an LDAP directory, there may be existing applications that rely on certain attributes for password and account management. The attribute names in the pd-pwp-user-state-plugin can be specified to match the attribute names used in the previous LDAP directory, possibly reducing code changes in client applications. See Appendix A for full documentation of the extension arguments.

1. Configure the pd-pwp-user-state-plugin:

```
dsconfig create-plugin \
    --plugin-name 'Password Policy User State'  \
    --type third-party  \
    --set enabled:true  \
    --set plugin-type:postoperationadd  \
    --set plugin-type:preparseadd  \
    --set plugin-type:preparsemodify  \
    --set plugin-type:preparsesearch  \
    --set plugin-type:searchresultentry  \
    --set invoke-for-internal-operations:false  \
    --set extension-class:com.pingidentity.ps.pd.plugin.PwpUserState  \
    --set extension-argument:failure-lockout-time=failureLockoutTime  \
    --set extension-argument:account-disabled=loginDisabled
```

This example sets the name of the `ds-pwp-user-state-failure-lockout-time` attribute name to `failureLockoutTime` and the name of the `ds-pwp-user-state-account-disabled` attribute name to `loginDisabled`. Note that if the supplied attribute names match any attribute name that appears in the LDAP schema, manipulating the attribute with the name conflict will lead to unpredictable and strange behavior. Please ensure that the attribute names selected in the plugin configuration do not match the name of any attribute specified in the LDAP schema.

## 4.3. Create Time Configuration

The pd-pwp-user-state-pluginn allows modifications (add and replace) to the createTimestamp attribute. Unlike other attributes used by this plugin, createTimestamp is **not** a Password Policy State attribute. The plugin performs modifies on the attribute via a Modify Request that use the Ignore No User Modification control. createTimestamp must be enabled to use the Ignore No User Modification control.

1. Configure createTimestamp to be modifiable with the ignore no user modification control:

```
dsconfig set-global-configuration-prop \
--set attributes-modifiable-with-ignore-no-user-modification-request-
control:createTimestamp
```

## 4.4. Request Criteria Considerations

The pd-pwp-user-state-plugin can be configured with request criteria to specify which request the plugin should process. The example configuration below will result in the plugin only processing operations made by the sync user with a DN of `cn=Sync User,dc=example,dc=com`.

1. Configure a connection criteria:

```
dsconfig create-connection-criteria \
--criteria-name "PDS User"  \
--type simple  \
--set included-user-base-dn: cn=Sync User,dc=example,dc=com
```

2. Configure a request criteria:

```
dsconfig create-request-criteria \
    --criteria-name "PDS User Request"  \
    --type simple  \
    --set "connection-criteria:PDS User"
```

3. Set the request criteria for the plugin:

```
dsconfig set-plugin-prop \
    --plugin-name "pwp-reset"  \
    --set "request-criteria:PDS User Request"
```

# 5. Usage

## 5.1. Basic

The following examples are based off the Basic Configuration as described in 4.1.

### 5.1.1. Get all user attributes and password policy attributes

Executing an LDAP search operation with no attributes specified retrieves all user attributes and password policy attributes.

```
<PingDirectory>/bin/ldapsearch --suppressPropertiesFileComment --terse --baseDN
"dc=example,dc=com" --searchScope sub "(uid=user.0)"

dn: uid=user.0,ou=People,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
mail: user.0@example.com
initials: AOR
homePhone: +1 295 940 2750
pager: +1 604 109 3407
givenName: Anetta
employeeNumber: 0
telephoneNumber: +1 594 307 3495
mobile: +1 164 286 4924
sn: Rhew
cn: Anetta Rhew
userPassword: {SSHA256}j4MQNJt83f1lbHSfOqi5kNmEPAogqEejpv8dRyjM32kpEz24xA9DdQ==
description: This is the description for Anetta Rhew.
street: 22411 Birch Street
st: PA
postalAddress: Anetta Rhew$22411 Birch Street$Rhinelander, PA  98160
uid: user.0
l: Rhinelander
postalCode: 98160
ds-pwp-user-state-pwp-dn: cn=Default Password Policy,cn=Password Policies,cn=config
ds-pwp-user-state-account-usable: false
ds-pwp-user-state-account-usability-error::
Y29kZT0xCW5hbWU9YWNjb3VudC1kaXNhYmxlZAltZXNzYWdlPVRoZSBhY2NvdW50IGhhcyBiZWVuIGR
 pc2FibGVkIGJ5IGFuIGFkbWluaXN0cmF0b3I=
# Non-base64-encoded representation of the above value: code=1{TAB}name=account-
disabled{TAB}message=The account has been
#  disabled by an administrator
ds-pwp-user-state-pw-changed-time: 19700101000000.000Z
ds-pwp-user-state-account-disabled: true
ds-pwp-user-state-account-not-active-yet: false
ds-pwp-user-state-account-expired: false
```

```
ds-pwp-user-state-pw-expired: false
ds-pwp-user-state-account-failure-locked: false
ds-pwp-user-state-failure-lockout-time: 20250401161907.522Z
ds-pwp-user-state-pw-reset: false
ds-pwp-user-state-account-reset-locked: false
ds-pwp-user-state-account-idle-locked: false
ds-pwp-user-state-pw-history-count: 0
ds-pwp-user-state-remaining-grace-login-count: 0
ds-pwp-user-state-has-retired-password: false
ds-pwp-user-state-available-sasl-mechanism: EXTERNAL
ds-pwp-user-state-available-sasl-mechanism: PLAIN
ds-pwp-user-state-available-sasl-mechanism: UNBOUNDID-CERTIFICATE-PLUS-PASSWORD
ds-pwp-user-state-available-sasl-mechanism: UNBOUNDID-EXTERNALLY-PROCESSED-
AUTHENTICATION
ds-pwp-user-state-has-totp-shared-secret: false
ds-pwp-user-state-account-is-validation-locked: false
ds-pwp-user-state-recent-login-history: { "successful-attempts":[ ], "failed-
attempts":[ ] }
```

### 5.1.2. Get all password policy attributes only

Executing an LDAP search operation with the special attribute `ds-pwp-user-state-get-all` retrieves only the password policy attributes.

```
<PingDirectory>/bin/ldapsearch --suppressPropertiesFileComment --terse --baseDN
"dc=example,dc=com" --searchScope sub "(uid=user.0)" ds-pwp-user-state-get-all

dn: uid=user.0,ou=People,dc=example,dc=com
ds-pwp-user-state-pwp-dn: cn=Default Password Policy,cn=Password Policies,cn=config
ds-pwp-user-state-account-usable: false
ds-pwp-user-state-account-usability-error::
Y29kZT0xCW5hbWU9YWNjb3VudC1kaXNhYmxlZAltZXNzYWdlPVRoZSBhY2NvdW50IGhhcyBiZWVuIGR
 pc2FibGVkIGJ5IGFuIGFkbWluaXN0cmF0b3I=
# Non-base64-encoded representation of the above value: code=1{TAB}name=account-
disabled{TAB}message=The account has been
#  disabled by an administrator
ds-pwp-user-state-pw-changed-time: 19700101000000.000Z
ds-pwp-user-state-account-disabled: true
ds-pwp-user-state-account-not-active-yet: false
ds-pwp-user-state-account-expired: false
ds-pwp-user-state-pw-expired: false
ds-pwp-user-state-account-failure-locked: false
ds-pwp-user-state-failure-lockout-time: 20250401161907.522Z
ds-pwp-user-state-pw-reset: false
ds-pwp-user-state-account-reset-locked: false
ds-pwp-user-state-account-idle-locked: false
ds-pwp-user-state-pw-history-count: 0
ds-pwp-user-state-remaining-grace-login-count: 0
ds-pwp-user-state-has-retired-password: false
```

```
ds-pwp-user-state-available-sasl-mechanism: EXTERNAL
ds-pwp-user-state-available-sasl-mechanism: PLAIN
ds-pwp-user-state-available-sasl-mechanism: UNBOUNDID-CERTIFICATE-PLUS-PASSWORD
ds-pwp-user-state-available-sasl-mechanism: UNBOUNDID-EXTERNALLY-PROCESSED-
AUTHENTICATION
ds-pwp-user-state-has-totp-shared-secret: false
ds-pwp-user-state-account-is-validation-locked: false
ds-pwp-user-state-recent-login-history: { "successful-attempts":[ ], "failed-
attempts":[ ] }
```

### 5.1.3. Get specific password policy attributes

Executing an LDAP search operation with specific attributes will retrieve only those attributes.

```
<PingDirectory>/bin/ldapsearch --suppressPropertiesFileComment --terse --baseDN
"dc=example,dc=com" --searchScope sub "(uid=user.0)" ds-pwp-user-state-account-
disabled cn

dn: uid=user.0,ou=People,dc=example,dc=com
cn: Anetta Rhew
ds-pwp-user-state-account-disabled: true
```

### 5.1.4. Modify a password policy attribute

Any password policy attribute that supports modification can be modified with an LDAP modify operation.

```
<PingDirectory>/bin/ldapsearch --suppressPropertiesFileComment --terse --baseDN
"dc=example,dc=com" --searchScope sub "(uid=user.0)" ds-pwp-user-state-account-
disabled

dn: uid=user.0,ou=People,dc=example,dc=com
ds-pwp-user-state-account-disabled: true

echo $ldifFile

dn: uid=user.0,ou=People,dc=example,dc=com
changetype: modify
replace: ds-pwp-user-state-account-disabled
ds-pwp-user-state-account-disabled: false

<PingDirectory>/bin/ldapmodify --suppressPropertiesFileComment --script-friendly
--ldifFile "$ldifFile"

<PingDirectory>/bin/ldapsearch --suppressPropertiesFileComment --terse --baseDN
"dc=example,dc=com" --searchScope sub "(uid=user.0)" ds-pwp-user-state-account-
disabled
```

```
dn: uid=user.0,ou=People,dc=example,dc=com
ds-pwp-user-state-account-disabled: false
```

# 5.2. Advanced

The following examples are based off the Advanced Configuration as described in 4.2.

In the examples below, notice how the attributes `ds-pwp-user-state-failure-lockout-time` and `ds-pwp-user-state-account-disabled` have been renamed to `failureLockoutTime` and `loginDisabled`, respectively.

## 5.2.1. Get all user attributes and password policy attributes

Executing an LDAP search operation with no attributes specified retrieves all user attributes and password policy attributes.

```
<PingDirectory>/bin/ldapsearch --suppressPropertiesFileComment --terse --baseDN
"dc=example,dc=com" --searchScope sub "(uid=user.0)"

dn: uid=user.0,ou=People,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
mail: user.0@example.com
initials: AOR
homePhone: +1 295 940 2750
pager: +1 604 109 3407
givenName: Anetta
employeeNumber: 0
telephoneNumber: +1 594 307 3495
mobile: +1 164 286 4924
sn: Rhew
cn: Anetta Rhew
userPassword: {SSHA256}j4MQNJt83f1lbHSfOqi5kNmEPAogqEejpv8dRyjM32kpEz24xA9DdQ==
description: This is the description for Anetta Rhew.
street: 22411 Birch Street
st: PA
postalAddress: Anetta Rhew$22411 Birch Street$Rhinelander, PA  98160
uid: user.0
l: Rhinelander
postalCode: 98160
ds-pwp-user-state-pwp-dn: cn=Default Password Policy,cn=Password Policies,cn=config
ds-pwp-user-state-account-usable: false
ds-pwp-user-state-account-usability-error::
Y29kZT0xCW5hbWU9YWNjb3VudC1kaXNhYmxlZAltZXNzYWdlPVRoZSBhY2NvdW50IGhhcyBiZWVuIGR
 pc2FibGVkIGJ5IGFuIGFkbWluaXN0cmF0b3I=
# Non-base64-encoded representation of the above value: code=1{TAB}name=account-
disabled{TAB}message=The account has been
```

```
#  disabled by an administrator
ds-pwp-user-state-pw-changed-time: 19700101000000.000Z
loginDisabled: true
ds-pwp-user-state-account-not-active-yet: false
ds-pwp-user-state-account-expired: false
ds-pwp-user-state-pw-expired: false
ds-pwp-user-state-account-failure-locked: false
failureLockoutTime: 20250401161907.522Z
ds-pwp-user-state-pw-reset: false
ds-pwp-user-state-account-reset-locked: false
ds-pwp-user-state-account-idle-locked: false
ds-pwp-user-state-pw-history-count: 0
ds-pwp-user-state-remaining-grace-login-count: 0
ds-pwp-user-state-has-retired-password: false
ds-pwp-user-state-available-sasl-mechanism: EXTERNAL
ds-pwp-user-state-available-sasl-mechanism: PLAIN
ds-pwp-user-state-available-sasl-mechanism: UNBOUNDID-CERTIFICATE-PLUS-PASSWORD
ds-pwp-user-state-available-sasl-mechanism: UNBOUNDID-EXTERNALLY-PROCESSED-
AUTHENTICATION
ds-pwp-user-state-has-totp-shared-secret: false
ds-pwp-user-state-account-is-validation-locked: false
ds-pwp-user-state-recent-login-history: { "successful-attempts":[ ], "failed-
attempts":[ ] }
```

### 5.2.2. Get all password policy attributes only

Executing an LDAP search operation with the special attribute `ds-pwp-user-state-get-all` retrieves only the password policy attributes.

```
<PingDirectory>/bin/ldapsearch --suppressPropertiesFileComment --terse --baseDN
"dc=example,dc=com" --searchScope sub "(uid=user.0)" ds-pwp-user-state-get-all

dn: uid=user.0,ou=People,dc=example,dc=com
ds-pwp-user-state-pwp-dn: cn=Default Password Policy,cn=Password Policies,cn=config
ds-pwp-user-state-account-usable: false
ds-pwp-user-state-account-usability-error::
Y29kZT0xCW5hbWU9YWNjb3VudC1kaXNhYmxlZAltZXNzYWdlPVRoZSBhY2NvdW50IGhhcyBiZWVuIGR
pc2FibGVkIGJ5IGFuIGFkbWluaXN0cmF0b3I=
# Non-base64-encoded representation of the above value: code=1{TAB}name=account-
disabled{TAB}message=The account has been
#  disabled by an administrator
ds-pwp-user-state-pw-changed-time: 19700101000000.000Z
loginDisabled: true
ds-pwp-user-state-account-not-active-yet: false
ds-pwp-user-state-account-expired: false
ds-pwp-user-state-pw-expired: false
ds-pwp-user-state-account-failure-locked: false
failureLockoutTime: 20250401161907.522Z
ds-pwp-user-state-pw-reset: false
```

```
ds-pwp-user-state-account-reset-locked: false
ds-pwp-user-state-account-idle-locked: false
ds-pwp-user-state-pw-history-count: 0
ds-pwp-user-state-remaining-grace-login-count: 0
ds-pwp-user-state-has-retired-password: false
ds-pwp-user-state-available-sasl-mechanism: EXTERNAL
ds-pwp-user-state-available-sasl-mechanism: PLAIN
ds-pwp-user-state-available-sasl-mechanism: UNBOUNDID-CERTIFICATE-PLUS-PASSWORD
ds-pwp-user-state-available-sasl-mechanism: UNBOUNDID-EXTERNALLY-PROCESSED-
AUTHENTICATION
ds-pwp-user-state-has-totp-shared-secret: false
ds-pwp-user-state-account-is-validation-locked: false
ds-pwp-user-state-recent-login-history: { "successful-attempts":[ ], "failed-
attempts":[ ] }
```

### 5.2.3. Get specific password policy attributes

Executing an LDAP search operation with specific attributes will retrieve only those attributes.

```
<PingDirectory>/bin/ldapsearch --suppressPropertiesFileComment --terse --baseDN
"dc=example,dc=com" --searchScope sub "(uid=user.0)" loginDisabled cn

dn: uid=user.0,ou=People,dc=example,dc=com
cn: Anetta Rhew
loginDisabled: true
```

### 5.2.4. Modify a password policy attribute

Any password policy attribute that supports modification can be modified with an LDAP modify operation.

```
<PingDirectory>/bin/ldapsearch --suppressPropertiesFileComment --terse --baseDN
"dc=example,dc=com" --searchScope sub "(uid=user.0)" loginDisabled

dn: uid=user.0,ou=People,dc=example,dc=com
loginDisabled: true

echo $ldifFile

dn: uid=user.0,ou=People,dc=example,dc=com
changetype: modify
replace: loginDisabled
loginDisabled: false

<PingDirectory>/bin/ldapmodify --suppressPropertiesFileComment --script-friendly
--ldifFile "$ldifFile"

<PingDirectory>/bin/ldapsearch --suppressPropertiesFileComment --terse --baseDN
```

```
"dc=example,dc=com" --searchScope sub "(uid=user.0)" loginDisabled

dn: uid=user.0,ou=People,dc=example,dc=com
loginDisabled: false
```

# Appendix A: Configuration Arguments

| Argument | Default Value | Modifiable | Description |
|---|---|---|---|
| account-activation-time | ds-pwp-user-state-account-activation-time | true | The operation type that may be used to get the time that the user’s account will become active. |
| account-disabled | ds-pwp-user-state-account-disabled | true | The operation type that may be used to determine whether the user account is disabled. |
| account-expiration-time | ds-pwp-user-state-account-expiration-time | true | The operation type that may be used to get the time that the user’s account will expire. |
| account-expired | ds-pwp-user-state-account-expired | false | The operation type that may be used to determine whether an account is expired (because the account expiration time is in the past). |
| account-failure-locked | ds-pwp-user-state-account-failure-locked | true | The operation type that may be used to determine whether a user’s account is locked because of too many authentication failures. |
| account-idle-locked | ds-pwp-user-state-account-idle-locked | false | The operation type that may be used to determine whether a user’s account is locked because it has been idle for too long. |
| account-is-validation-locked | ds-pwp-user-state-account-is-validation-locked | false | The operation type that may be used to determine whether a user’s account is locked because it contains a password that does not satisfy all of the configured password validators. |
| account-not-active-yet | ds-pwp-user-state-account-not-active-yet | false | The operation type that may be used to determine whether an account is not yet active (because the account activation time is in the future). |
| account-reset-locked | ds-pwp-user-state-account-reset-locked | false | The operation type that may be used to determine whether a user’s account is locked because the user did not change their password in a timely manner after an administrative reset. |
| account-usability-error | ds-pwp-user-state-account-usability-error | false | The operation type that may be used to retrieve a list of structured strings that provide information about errors that may affect the account usability. |

| Argument | Default Value | Modifiable | Description |
|---|---|---|---|
| account-usability-notice | ds-pwp-user-state-account-usability-notice | false | The operation type that may be used to retrieve a list of structured strings that provide information about notices pertaining to account usability. |
| account-usability-warning | ds-pwp-user-state-account-usability-warning | false | The operation type that may be used to retrieve a list of structured strings that provide information about warnings that may affect the account usability. |
| account-usable | ds-pwp-user-state-account-usable | false | The operation type that may be used to determine whether an account is usable (i.e., the account may authenticate or be used as an alternate authorization identity). |
| auth-failure-time | ds-pwp-user-state-auth-failure-time | true | The operation type that may be used to get the set of times that the user has unsuccessfully tried to authenticate since the last successful attempt. |
| available-sasl-mechanism | ds-pwp-user-state-available-sasl-mechanism | false | The operation type that may be used to retrieve a list of the SASL mechanisms that are available for a user. |
| available-totp-delivery-mechanism | ds-pwp-user-state-available-totp-delivery-mechanism | false | The operation type that may be used to retrieve a list of the one-time password delivery mechanisms that are available for a user. |
| create-time | N/A | true | The operation type that may be used to set the 'createTimestamp'. This attribute is not part of the PasswordPolicyStateOperation. |
| failure-lockout-time | ds-pwp-user-state-failure-lockout-time | true | The operation type that may be used to determine the failure lockout time for a user account. |
| grace-login-use-time | ds-pwp-user-state-grace-login-use-time | true | The operation type that may be used to retrieve the times that the user has authenticated using a grace login after his/her password has expired. |
| has-retired-password | ds-pwp-user-state-has-retired-password | true | The operation type that may be used to determine whether a user has a valid retired password. |
| has-totp-shared-secret | ds-pwp-user-state-has-totp-shared-secret | false | The operation type that may be used to determine whether a user has one or more TOTP shared secrets. |

| Argument | Default Value | Modifiable | Description |
|---|---|---|---|
| idle-lockout-time | ds-pwp-user-state-idle-lockout-time | false | The operation type that may be used to determine the idle lockout time for a user account. |
| last-bind-password-validation-time | ds-pwp-user-state-last-bind-password-validation-time | false | The operation type that may be used to retrieve the time that the server last invoked password validation during a bind operation for a user. |
| last-login-ip-address | ds-pwp-user-state-last-login-ip-address | true | The operation type that may be used to retrieve the IP address from which the user last authenticated to the server. |
| last-login-time | ds-pwp-user-state-last-login-time | true | The operation type that may be used to retrieve the time that the user last authenticated to the server. |
| pw-changed-by-required-time | ds-pwp-user-state-pw-changed-by-required-time | false | The operation type that may be used to retrieve the last time that the user's password was changed during a required change period. |
| pw-changed-time | ds-pwp-user-state-pw-changed-time | true | The operation type that may be used to get the time that the user's password was last changed. |
| pw-expiration-time | ds-pwp-user-state-pw-expiration-time | false | The operation type that may be used to determine when a user's password will expire |
| pw-expiration-warned-time | ds-pwp-user-state-pw-expiration-warned-time | true | The operation type that may be used to get the time that the user was first sent a password expiration warning. |
| pw-expired | ds-pwp-user-state-pw-expired | false | The operation type that may be used to determine whether a user's password is expired. |
| pw-history | ds-pwp-user-state-pw-history | true | The operation type that may be used to retrieve the stored password history values for a user. Deprecated: This operation type has been deprecated in favor of the OP_TYPE_GET_PW_HISTORY_COUNT operation type. |
| pw-history-count | ds-pwp-user-state-pw-history-count | false | The operation type that may be used to retrieve the password history count for a user. |

| Argument | Default Value | Modifiable | Description |
|---|---|---|---|
| pw-reset | ds-pwp-user-state-pw-reset | true | The operation type that may be used to determine whether a user’s password has been reset by an administrator and must be changed. |
| pw-retired-time | ds-pwp-user-state-pw-retired-time | false | The operation type that may be used to retrieve the time that the user’s former password was retired. |
| pwp-dn | ds-pwp-user-state-pwp-dn | false | The operation type that may be used to retrieve the DN of the password policy to which the user is subject. |
| recent-login-history | ds-pwp-user-state-recent-login-history | false | The operation type that may be used to retrieve a user’s recent login history. |
| registered-yubikey-public-ids | ds-pwp-user-state-registered-yubikey-public-ids | false | The operation type that may be used to retrieve get the set of public IDs for the registered YubiKey OTP devices for a user. |
| remaining-auth-failure-count | ds-pwp-user-state-remaining-auth-failure-count | false | The operation type that may be used to retrieve the number of failed authentication attempts that the user has before the account is locked. |
| remaining-grace-login-count | ds-pwp-user-state-remaining-grace-login-count | false | The operation type that may be used to retrieve the number of grace logins available for the user. |
| reset-lockout-time | ds-pwp-user-state-reset-lockout-time | false | The operation type that may be used to determine the reset lockout time for a user account. |
| retired-password-expiration-time | ds-pwp-user-state-retired-password-expiration-time | false | The operation type that may be used to retrieve the time that the user’s retired password will expire. |
| seconds-until-account-activation | ds-pwp-user-state-seconds-until-account-activation | false | The operation type that may be used to retrieve the length of time in seconds until the user’s account will become active. |
| seconds-until-account-expiration | ds-pwp-user-state-seconds-until-account-expiration | false | The operation type that may be used to retrieve the length of time in seconds until the user’s account expires. |
| seconds-until-auth-failure-unlock | ds-pwp-user-state-seconds-until-auth-failure-unlock | false | The operation type that may be used to retrieve the length of time in seconds until the user’s account is unlocked. |
| seconds-until-idle-lockout | ds-pwp-user-state-seconds-until-idle-lockout | false | The operation type that may be used to get the length of time in seconds until the user account is locked due to inactivity. |

| Argument | Default Value | Modifiable | Description |
|---|---|---|---|
| seconds-until-pw-expiration | ds-pwp-user-state-seconds-until-pw-expiration | false | The operation type that may be used to get the length of time in seconds until the user’s password expires. |
| seconds-until-pw-expiration-warning | ds-pwp-user-state-seconds-until-pw-expiration-warning | false | The operation type that may be used to get the length of time in seconds until the user will be eligible to receive a password expiration warning. |
| seconds-until-pw-reset-lockout | ds-pwp-user-state-seconds-until-pw-reset-lockout | false | The operation type that may be used to get the length of time in seconds until the user’s account is locked due to failure to change the password after an administrative reset. |
| seconds-until-required-changed-time | ds-pwp-user-state-seconds-until-required-changed-time | false | The operation type that may be used to get the length of time in seconds until the user’s account will be locked due to a failure to change the password by a required time. |
| directoryLogger.debugLoggingEnabled | N/A | N/A | Enable debug logging. By default, debug logging is disabled. |
| directoryLogger.alertsEnabled | N/A | N/A | Enable alerts. By default, alerts are disabled. |

# Appendix B: Changelog

```
1.6.0:
    Updated to latest build process.

1.6.2:
    Updated server sdk to 9.3.0.0.

1.6.3:
    Added password policy attribute pw-expiration-warned-time and non password policy
attribute create-time

1.6.5:
    Added additional logging to help diagnose error with setting attributes.

1.6.6:
    Updated the way that failure-lockout-time is set.

1.6.8:
    Logging overhaul

1.6.9:
    General clean up.

1.6.10:
    Removed log4j2 with new and improved DirectoryLogger.

1.6.11:
    Removed password policy dependency.

1.6.12:
    If no attributes are specified, the plugin should return all user attributes PLUS
password policy attributes.

1.6.13:
    Added 'pwp-dn' to the PwpUserStateOperation enum.
```

# Appendix C: Logging

The pd-pwp-user-state-plugin will log to PingDirectory's `errors` log. To enable debug logging for additional logging:

```
dsconfig set-log-publisher-prop \
    --publisher-name 'File-Based Error Logger'  \
    --add default-severity:debug
```

> ℹ There are performance implications of keeping the debugging running in a Production environment, so bear that in mind when configuring your directory.