

PingDirectory®

AD Password Update Plugin v1.0.0

User Guide



© 2005-2018 Ping Identity ® Corporation. All rights reserved.

PingDirectory AD Password Update Plugin 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

Ping Identity, the Ping Identity logo and PingDirectory are registered trademarks of Ping Identity Corporation ("Ping Identity"). All other trademarks or registered trademarks are the property of their respective owners.

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 4

Prerequisites 4

Installation..... 4

Purpose

The “AD Password Update” Plugin confirms that a proposed password change in PingDirectory meets the requirements for a remote server. The following logic is applied:

- Attempt to change password in AD based on password change request to PingDirectory.
- If successful, complete password change in DS.
- If not successful, return error from AD, and do not change DS password.

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 "AD Password Update Custom Plugin" \  
  --type third-party \  
  --set enabled:true \  
  --set plugin-type:preoperationmodify \  
  --set extension-argument:ad-host=<AD Hostname> \  
  --set extension-argument:ad-port=<AD Port> \  
  --set extension-argument:ad-bind-dn=<AD Bind DN> \  
  --set extension-argument:ad-bind-password=<AD Bind Password> \  
  --set extension-argument:ad-correlation-attribute=<AD user's RDN> \  
  --set extension-argument:local-correlation-attribute=<PD user's RDN> \  
  --set extension-argument:ad-base-dn=<AD Base DN of users> \  
  --set extension-argument:ad-password-attribute=<AD Password Attribute> \  
  --set extension-argument:local-password-attribute=<PD Password Attribute> \  
  --set extension-argument:ssl-trustAll=<True/False> \  
  --set extension-argument:ssl-trustStore-path=<Truststore> \  
  --set extension-argument:connection-min=<Minimum connections> \  
  --set extension-argument:connection-max=<Maximum connections> \  
  --set extension-class:com.pingidentity.ps.ds.plugin.ADPASSWORDUpdate
```

- ‘ad-host’ is a required argument and specifies AD's address, which may be a resolvable name or IP address.

- 'ad-port' is a required argument and specifies the port used for connecting with AD.
- 'ad-bind-dn' is an optional argument and specifies the DN to use to authenticate with AD. Default value is '636'.
- 'ad-bind-password' is a required argument and specifies the password to use to authenticate with AD.
- 'ad-correlation-attribute' is an optional argument and specifies the name of the attribute for user login in AD. Default value is 'sAMAccountName'.
- 'local-correlation-attribute' is a required argument and specifies the name of the attribute to use on the PingDirectory side to correlate to an entry on the target server.
- 'ad-base-dn' is a required argument and specifies the attribute value that will be used to exclude changes.
- 'ad-password-attribute' is an optional argument and specifies the name of the attribute used to store the user password on Active Directory. Default value is 'unicodePwd'.
- 'local-password-attribute' is an optional argument and specifies the name of the attribute used to store the user password the PingDirectory side. Default value is 'userPassword'.
- 'ssl-trustAll' is an optional argument and specifies whether to trust all SSL connections. Default value is 'false'. **This option should only be used for development purposes only and should never be set to 'true' in a production environment.**
- 'ssl-trustStore' is an optional argument and specifies the SSL Truststore file. If 'ssl-trustAll' is 'true', this value is ignored.
- 'connection-min' is an optional argument and specifies the minimum number of connections in the AD connection pool. Default value is '1'.
- 'connection-max' is an optional argument and specifies the maximum number of connections in the AD connection pool. Default value is '8'.

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 "AD Password Update Custom Plugin"
```