

PingAccess®

KCD Site Authenticator v4.0.0

User Guide



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

PingAccess KCD Site Authenticator User Guide
Version 4.0.0
May 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, PingFederate, PingAccess, PingID, PingOne, 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
Configuration	4
Configuring the Managed Service Account	4
Configuring the KCD Site Authenticator	7
Configuring the sample krb5.ini file	9
Test	9
Logging	13

Purpose

This user guide is intended for use by PingAccess clients, with the need to use the Kerberos Constrained Delegation (KCD) Site Authenticator.

Prerequisites

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

- A functional PingAccess and PingFederate environment, version 8.1+
- JDK version 8+

Installation

1. From *pa-kcd-site-authenticator-4.0.0-distro-assembly.zip*, copy the noted files to the corresponding PingAccess directory:

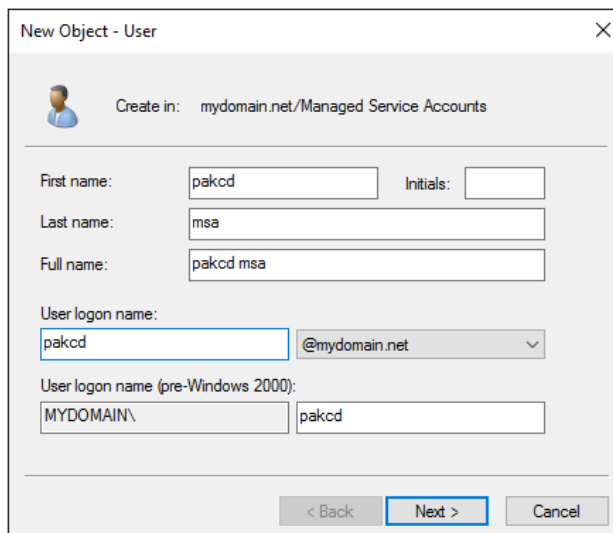
From	To
dist/pa-kcd-site-authenticator-4.0.0.jar	<PingAccessInstall>/lib
config/krb5.ini	<PingAccessInstall>/conf

2. Repeat step 1 on other clustered engine nodes.
3. Start or restart PingAccess.

Configuration

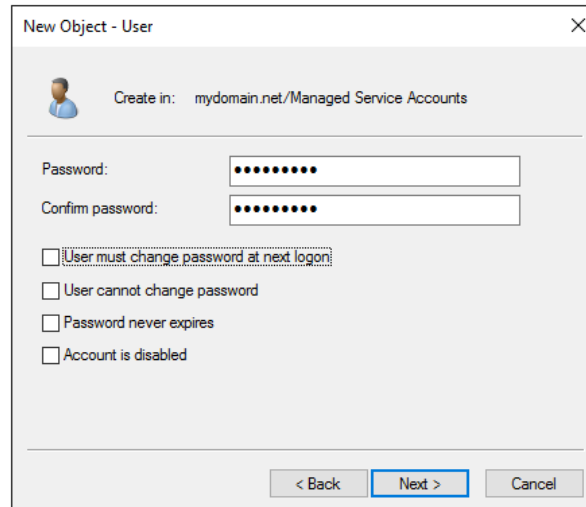
Configuring the Managed Service Account

1. In Windows Server, open *Active Directory Users and Computers*.
2. Under **User Managed Service Accounts**, add a new user.



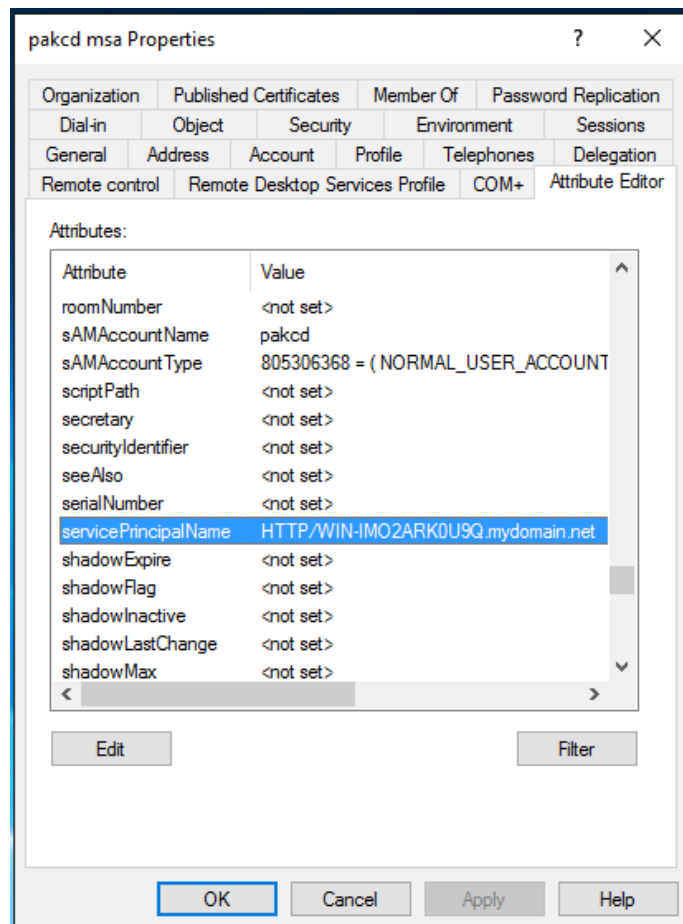
The screenshot shows the 'New Object - User' dialog box in Active Directory Users and Computers. The 'Create in' field is set to 'mydomain.net/Managed Service Accounts'. The 'First name' field contains 'pakcd', the 'Last name' field contains 'msa', and the 'Full name' field contains 'pakcd msa'. The 'User logon name' field contains 'pakcd' and the domain dropdown is set to '@mydomain.net'. The 'User logon name (pre-Windows 2000)' field contains 'MYDOMAIN\pakcd'. The 'Next >' button is highlighted.

3. Select **Next**, enter a password and unselect “User must change password at next login”.



The 'New Object - User' dialog box shows the 'Create in' field set to 'mydomain.net/Managed Service Accounts'. The 'Password' and 'Confirm password' fields are filled with dots. The checkbox 'User must change password at next login' is unselected. Other checkboxes for 'User cannot change password', 'Password never expires', and 'Account is disabled' are also unselected. The 'Next >' button is highlighted.

4. Click **Next** and then **Finish** to create the new account.
5. In order to enable delegation on the service account, it needs the *servicePrincipalName* to be set. Right click on the new user account, select *Properties* and in the *Attribute Editor* tab, enter the *servicePrincipalName* as “HTTP/<FQDN>”. The FQDN will be server where the application that needs to be protected by PingAccess is running. In this example, the application is running on “WIN-IMO2ARK0U9Q.mydomain.net”.



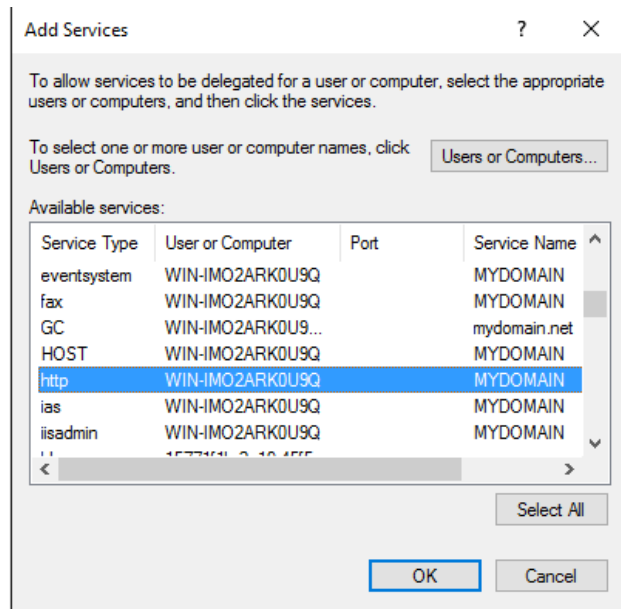
The 'pakcd msa Properties' dialog box shows the 'Attribute Editor' tab. The 'servicePrincipalName' attribute is highlighted with the value 'HTTP/WIN-IMO2ARK0U9Q.mydomain.net'. Other attributes like 'roomNumber', 'sAMAccountName', 'sAMAccountType', 'scriptPath', 'secretary', 'securityIdentifier', 'seeAlso', 'serialNumber', 'shadowExpire', 'shadowFlag', 'shadowInactive', 'shadowLastChange', and 'shadowMax' are all set to '<not set>'. The 'OK' button is highlighted.

Attribute	Value
roomNumber	<not set>
sAMAccountName	pakcd
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
scriptPath	<not set>
secretary	<not set>
securityIdentifier	<not set>
seeAlso	<not set>
serialNumber	<not set>
servicePrincipalName	HTTP/WIN-IMO2ARK0U9Q.mydomain.net
shadowExpire	<not set>
shadowFlag	<not set>
shadowInactive	<not set>
shadowLastChange	<not set>
shadowMax	<not set>

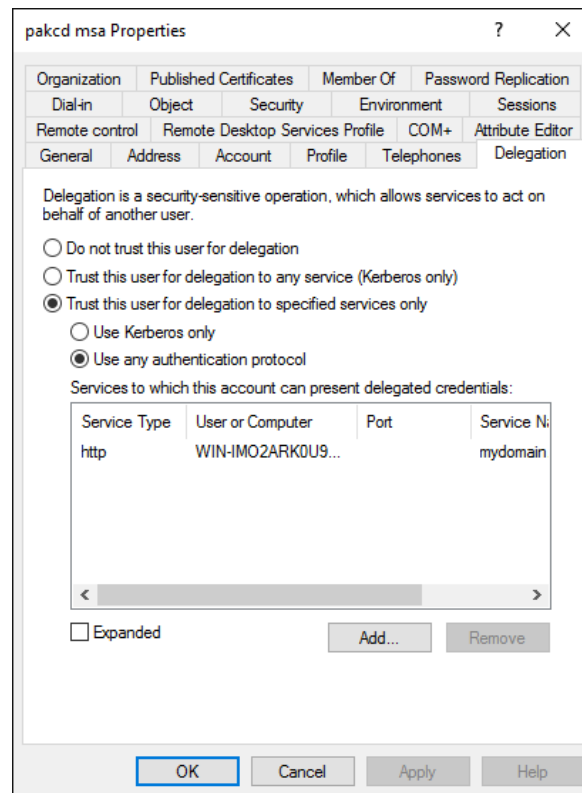
6. Click **Ok** to save the changes to the user and enable the **Delegation** tab.
7. Right click on the account, select *Properties*, then *Delegation*. Click on “Trust this user for delegation to specified services only” and then click on “Use any authentication protocol”.

8. Click **Add** then click on **Users or Computers** and enter the name of the server that is running the application and click **Ok**.

9. Select the appropriate HTTP service and click **Ok**. Note that the protocol must be HTTP.



10. Click **Ok** to finish configuring the service account.



Configuring the KCD Site Authenticator

1. Log into the *PingAccess* admin console and click **Sites | Site Authenticators**.
2. Click **Add Site Authenticator**.
3. Enter a name and select type "Kerberos Constrained Delegation Site Authenticator".
4. Configure the Site Authenticator as follows:

Field	Description
Kerberos Configuration File	Enter the path to the krb5.ini that was installed in the previous step.
Kerberos Service Principal Name	Fully qualified domain name identifier for the Kerberos Service Account. This is the value that was entered in step 5 of “Configuring the Managed Service Account”.
Kerberos Service Account	Name of the Kerberos Service Account. This is the logon name of the managed service account that was created in “Configuring the Managed Service Account”.
Kerberos Service Account Password	Password for the Kerberos Service Account created in “Configuring the Managed Service Account”.

MAIN ^

- Applications
- Sites**
- Agents
- Rules

SETTINGS ^

- Access
- Networking
- Security
- System

New Site Authenticator

NAME

TYPE

Kerberos Constrained Delegation Site ... v

KERBEROS CONFIGURATION FILE (FULL PATH)

KERBEROS SERVICE PRINCIPAL NAME

KERBEROS SERVICE ACCOUNT

KERBEROS SERVICE ACCOUNT PASSWORD

Copyright © 2003-2018
Ping Identity Corporation
All rights reserved

Cancel Save

5. Click **Save**.

Configuring the sample krb5.ini file

This file should contain the default_realm, kdc, admin_server and default_domain relevant to your implementation.

```
[libdefaults]
default_tkt_enctypes = RC4-HMAC
default_tgs_enctypes = RC4-HMAC
default_realm = MYDOMAIN.NET
forwardable = true

[realms]
MYDOMAIN.NET = {
    kdc = WIN-IM02ARK0U9Q.mydomain.net
    admin_server = WIN-IM02ARK0U9Q.mydomain.net
    default_domain = MYDOMAIN.NET
}
```

Test

In this example, the KCD Site Authenticator is tested using the PingAccess Quickstart Application. However, the KCD Site Authenticator can be tested with any application that is currently protected by PingAccess.

1. Configure PingAccess and PingFederate with the PingAccess Quickstart Application following the user guide that is included in the PingAccess QuickStart Application.
2. Add the KCD Site Authenticator to the QuickStart application and click **Save**.

Ping PingAccess

MAIN ^

- Applications
- Sites**
- Agents
- Rules

SETTINGS ^

- Access
- Networking
- Security
- System

[< To Site List](#)

QuickStart

This site is used by 2 Applications. [View on the applications page](#)

NAME

QuickStart

TARGETS ⓘ

localhost:9031

[+ ADD TARGET](#)

SECURE ⓘ

☐ No ☒ Yes

TRUSTED CERTIFICATE GROUP ⓘ

PingFederate Trusted Group

SITE AUTHENTICATORS ⓘ [+ Create](#)

Please Choose...

KCD

[+ Create Site Authenticator](#)

[Show Advanced](#)


3. Point your web browser to the QuickStart application and select *Web Access Management*.

Browser address bar: <https://localhost:3000/PingAccessQuickStart/home/>

Navigation bar: Most Visited, Getting Started, PingOne, Mail, Google Apps, SDKs, Ping, UnboundID, Ping Federate, Ping Access, ClientServiceArchitect..., JIRA Kanban Board, My WebEx Room, Scalr

Welcome to the PingAccess Quick-Start


Use this interactive Quick-Start application to explore how the PingAccess solution can work for your organization.



Web Access Management

Centralize the authorization and session management of your protected web applications. Using the OpenID Connect protocol, PingAccess leverages a PingFederate server for authentication and attribute resolution. Session management at the application level is handled via a cookie using an open standard format called JSON Web Token (JWT). Run a test request to get a demonstration of basic web resource protection.

[Try It Now](#)



API Access Management

Paired with PingFederate, PingAccess provides a secure method of controlling access to APIs while integrating them with existing identity management infrastructure. PingFederate acts as an OAuth Authorization Server to manage application clients and API token lifecycles, while PingAccess acts as the OAuth Resource Server to validate tokens and apply policies. To get a demonstration of a complete OAuth client interaction, try it now.

[Try It Now](#)

© 2003-2017 Ping Identity Corporation

- Log in using an account that exist on the domain controller and that can be delegated (default setting for AD accounts). For this example, the username "joe" is defined in the PingFederate Simple PCV so a Windows account was created with the same username in the same domain where the Kerberos service account exists.

Sign On

USERNAME

PASSWORD

☐ Remember my username

[Sign On](#)

5. Confirm that a Kerberos ticket has been issued.




Quick-Start

Web Access Management

Your PingAccess test request was received successfully.

Here is the full set of HTTP request headers received by the protected application:

HTTP Header	Value
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding	gzip, deflate, br
Accept-Language	en-US,en;q=0.5
Authorization	Negotiate YlIFkAYJKoZlhcSAQICAQBuggV/MIIFe6ADAgEFoQMCAQ6iBwMF ACAAAACjggSoYYIEpDCCBKCGAwIBBAEOGwXNWURPTUFTJt5OR VSiljAggAMCAQChGTAXGwRodHRwGw9XSU4tSU1PMkFSSzBV0V GjggRjMlIEY6ADAgEoQMCAQOigRRBIIETbiSp4ejZOaXctV7X2t nmXQgkDAfaNA50VSugRTa0k8iULkkoUNLiD16wwwVxQ1SdgplKuC N1e5EZzW9Eq0PiJEKB29VkrBn9vLvhkLRarPvrsW2nnqK++SgrfoXC /GDwFVM2rPBK8cJfAdOmF+Kbr+0lZBZ32f6Z /1uSQ9wQn0e4Vz4oOykG9NnmUqdbv0VxAKjz4xgAXT6D56CouG8+ Zb7EBY9VfjArVgCypRuP7dzKWOChJ2yyt7edYv6z86l7xexTx56WdY cLhxG5WugpBFN /mz9B38XxOOBcXONwHyAb5QEHPR4o4A98fsXeHW3Ukd0zPq75 ARhsUXyhLGYaXi/dlxe6PV9xDCU9tvQAfhSAwtjojkAd/LdFsA /GcXqaHEWIr44TCHh/6voZUdW/Y1+XFZNBhn /15b3QscJZJ4+xVBIKoc+MoUPkNwo76CyEwSb5iwrUBfL04cJT5aw CKtFmmkcJZlRjKWsDSrlonfqgGR1JzfrjYl86RJBZs /CkVIEmyuFCp1cbJl7wX7jp7f4ONRC0ppjS9hYunt+48LDyU13Yr4Knp WeYCc3cJw0W4htdjeeEgYH+G99xAE97s65lxaZj5LKOeHRPIMm3 F5CZMiRbuSjUe6356V0uVLGameHHbUMMjWYyY5 /VQOWRiAp6ZSUIMBDQijzb8p7X91GQ2z5gWkRidfnZ73UUEKok87 w+VeQBekoGvdaP2s8Z1z85Tk9EChTQMaa5WFM /td0MLKpmrDVDQqFWggtfBRgGz+0fnHfq7XzTNnXyM6MoB61XnlPv VW2LmOgXAJnQFbBa5PAUOyi9bP1PkQklmtaLIXmMaX /XBgd6jrzwT8HyhfsW1ZQvUH9m86x1keCXNelDcZFxbt74xCuBWKdr4 32zG0kNNwvhghC3eDh5UgDCjbdlytcyqpiwdYNuC9gmRvmJJaQPkO RflsJxyKnrBPE7R2P6Psg95Cteq2P9y+go /qRHqLBI4PwdyTC2MYyqUqwlq1aiYHkG6Q2Y /4P1win+TDwnm662iCXlvhyJpiJTES119EFnmCZQ8eEAGl0soC7Va1v SWEm46vaQdm+JG7YEBhuY/ojXSORldZ41o /ZmnY8f+IGlhTyB71MrRnS+V6qJceePhrCL5XLju+p/LsFcoEqAex /NDjGqoBO4j5watN+U08BW06N9qF512 /9KLYn3YPH3LjH32goyGrC9VU85v57YMERH+LVqQbqTxv9fZl8nKmin PlsekeTpE6t9YAsCOvd6mhvmlO8eQCXm8yNnEmZUw73RzE12XJW/i nLzVzpryqx3HukgrzEGNNabm9B+BV3Ed+Pz1Xanlw4dL8TGBZ5sUc5 slhLDFloDmlQKWPNsxxRmcCFkjZ5AFivxPZuMbwsJiAkvH0Aat1yrl6 rO6YbMdB/ZcPp4wcGVlxnSazpQJpETPHjx+jWAW3st /X/NKSBUtCBtqADAgEXooGuBGr3VGSeRZ++hMUys+IEkxJldgvlb0j uvGcvAqbyNZ9OjDMKnF8DfEk5X9883bv7WqBLm3dlrX9KwSzwWY V5csYJne4ozZgyOLyg+47LGWxemaOtrmGcJMOF7EL1GaGeT6P2 VQwX+ffX9s5Vzjrcf mTVvXzmhF5T5sfcTaT /GcaCnUlhwppoxZHpcEVnSoDQf0JzaAbyHr220QISFQhGe2UJ /0pQfSBemjqn1
Cookie	JSESSIONID=1gc1ah8pm9saw8jffc7khzybm; pf-directory=oauth; PF=mPsi9Z2nv0zaxOoLZ6Qhs99KBMZwxWayGWDzVdpFi9yo; PA_global=eyJhbGciOiJkaXkiLjIjbmMiOiJBMtI4Q0JDUhTmJlU2liwiaz2 IkjoYSlSlNBPnNyaSl6lkxhUDV5TUIBcmNmVHFVZVdSMzg0LWJtJT 2RURSJ9..TzPHexFnrhugz99xjyCYKw.u k- pzdDB2AuoSP1aklCkajMGsXp0P90z4mJkAGahIVNmellRRUZp5vN8i aDRPSHPiGaZJ4PhVvj6_Glp4R0OWKxY0ikmZlwub2q4j6raJbHDBNb 1ZBrgh8Kl6sUUxtRqHq- lArjSOYCJguoAvXitD8ywsy69RbytsWpZ9wwMAeHdwGj5RwUX2ErE MXnVDGihP56eF7fRVCFteKoufdqjDIV4DHsXlvZkkChFqcGgahWoUUG VL_Q76zmZ9t_osx24zp3DqvtQphvQIRQfbiVX0bS89zFYM2HSioSepI Swsvj3rnoZ_p4fZ33azYfYwbkxFNIGq6b7bkj0ZP- IOfBEpORMO19HRL0ngMjl3jl.X8vHreCWWY4OzDyQU4aLog
Host	localhost:3000
Referer	https://localhost:9031/
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:59.0) Gecko/20100101 Firefox/59.0
X-Forwarded-For	127.0.0.1
X-GROUP	sales
X-USER	joe

```
run.bat
PingAccess running...
14:19:19,847 DEBUG [KCDSiteAuthenticator] Authenticating kerberos service account: pakcd
14:19:19,847 DEBUG [KCDSiteAuthenticator] No identity object in exchange
14:19:20,502 DEBUG [KCDSiteAuthenticator] Authenticating kerberos service account: pakcd
14:19:20,502 DEBUG [KCDSiteAuthenticator] No identity object in exchange
14:19:21,205 DEBUG [KCDSiteAuthenticator] Authenticating kerberos service account: pakcd
14:19:21,205 DEBUG [KCDSiteAuthenticator] No identity object in exchange
Listening for transport dt_socket at address: 8787
14:25:47,391 DEBUG [KCDSiteAuthenticator] Authenticating kerberos service account: pakcd
14:25:47,610 DEBUG [KCDSiteAuthenticator] Creating delegated credential for user : joe
14:25:47,750 DEBUG [KCDSiteAuthenticator] Getting the service ticket for: http/WIN-IM02ARK0U9Q
14:25:47,750 DEBUG [KerberosContext] pakcd as joe call initSecContext
14:25:47,860 DEBUG [KCDSiteAuthenticator] Delegated ticket : YIIFkAYJKoZIhvcSAQICAQBuggV/MIIFe6ADAgEFoQMCAQ6iBwMFACAAAA
CjggSoYYIEpDCCBKCGAwIBBAEOGwNURPTUFJTi5ORVSiIjAgoAMCAQChGTAXGwRodHRwGw9XSU4tSU1PMkFSSzBV0VGjggRjMIIEX6ADAgEXoQMCAQOig
gRRBIITBtSp4ejZ0aXctWzV7X2tnmXQgkDAfANA50VSuqRTa0k8iULkkoUNLiD16vvwWxQ1Sdgp1KuCN1e5EZzW9Eq0PiJEKB29VkrXbN9vLivhklRanPv
rsW2nnqK++SgrFoXC/GDwFVMrPBK8cJJf1AdOmF+Kbr+9IZBZ332f6Z/1uS09wQn0e4Vz4oOykG9NomUqdbv0VxAKjz4xgAXT6D56CouG8+Zb7EBY9VFJA
rVqCypRuP7dzKW0ChJ2yyt7edYv6z8617xexTx56WdYcLhxG5WugpBFN/mz9B38Xx00bCx0NwHyAb5QEHPR4o4A98fsXeHW3Ukd0zPq75ARhsUXyhlGyaX
i/dIxe6PV9xDCU9tvQAFhSAwtjokAd/LdFsA/GcXqAHEwR44TCHh/6voZuUw/Y1+XFZJNBhn/15b30scJZJl4+xVB1Koc+MoUPkNwo76CyEwSb5iwrUBfL
04cJT5awCKtFmmkcJZI1RjKWsDSrIonfqqGR1JzfjrYl86RIJBZs/CkViEmyuFCp1cbJl7wX7jp7f40NRC0ppjS9hYunt+48LDyU13Yr4KnpWeYCC3cJw0W
4htdjceEgYH+C99xAe97s651xaZj5LK0eHRPiMm3F5CZMiRbuSjUe635bV0uVLGameHHBUMMjWjVY5/VQ0WRiAp6ZSUIMBDQijzb8p7X91GQ2z5gWkRidf
nZ73UUEKok87w+VeQBekoGvdaP2s8Z1z85Tk9EChTQMaasWFM/tD0MLKpmrDvDQqFwgqtfIBRgGz+0fnHfQ7XzTnNxyM6MoB61Xn1PvVw2LmOgXAJnQFbrB
a5PAU0y19bP1PkQklmLIXmMaX/XBg6djrzWt8Hyhfsw1ZQvUH9m86x1keCXNeIDcZFxbt74xCuBWKdr432zG0kNNvwhghC3eDh5UgDCjbdIytcyqpiwY
NuC9gmRvmJJaqPkORflsJxyKnrBPE7R2P6Psg95Cteq2P9y+go/qRHqLB14PwdyTC2MYyqUqwiQ1aiYHkG6Q2Y/4P1win+TDwnm662iCXLvhyJpiJTES119
EFnmCZQ8eEAGI0soC7Va1vSWEm46vaQdm+JG7YEBhuY/ojXS0rildZ41o/ZmnY8f+IGlhTyB71MrRnS+V6qJceePHRCL5XLju+p/LsFcvoEqAex/NDjGqoB
04j5watN+U08Bwo6N9qF512/9KLYn3YPH3LjH32goyGrC9VU85v57YMERH+LVqQbqTXv9fZi8nKminPIsekeTpE6t9YAsCOvd6mhvmIO8eQCXm8yNnEmZUw
73RzE12XJWixLvZpryqx3HukgrzEGNNabm9B+BV3Ed+Pz1Xanlw4dL8TGBZ5sUc5slhLDFloDvLIQKWPNsxxRmcCFkjZ5AFiVxPZuMbwsJiAkvh0Aat1y1
r6r0Y6YmDb/ZcPp4wcGV1xnSazpQJpETPHjx+jWAw3st/X/NKSBUtCBtqADAgEXooGuBigr3VGSeRZ++hMUys+1EkxJIdgvlb0juvGcvAqbyNZ90jDMKnF8
DfEk5X9883bv7WqBLm3dIIRX9KwSzvwyWV5csYJne4ozZgyOLyg+47LGWxema0tRmGCJM0F7EL1GaGeT6P2VQwX+FfX9s5VzjrcFmTVvXzmhF5T5sfcTaT/
GcaCnUIhwppoxZHpcEVnSoDQf0JzaAbyHr220Q15FQhGe2UJ/0pQf5Bemjqn1
```

Logging

To enable various logging modes for the KCD Site Authenticator, add the following in the relevant sections in <PingAccessInstall>/conf/log4j2.xml.

```
<AsyncLogger name="com.pingidentity.ps" level="DEBUG" additivity="false"
includeLocation="false">
    <AppenderRef ref="File"/>
    <!--<AppenderRef ref="CONSOLE" />-->
    <!--<AppenderRef ref="SYSLOG" />-->
</AsyncLogger>
```

Where the log level can be one of [DEBUG | INFO | WARN | ERROR].

Detailed training on using Log4j in PingFederate can be found at:

<https://ping.force.com/Support/PingIdentityKnSearchHome?searchText=log4j>