

PingAccess[®]

KCD Site Authenticator v5.1

User Guide



© 2005-2024 Ping Identity ® Corporation. All rights reserved.

PingAccess KCD Site Authenticator User Guide
July 2024

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

Requirements 4

Prerequisites 4

Installation 4

Configuration..... 5

Configuring the Managed Service Account 5

Configuring the KCD Site Authenticator 9

Configuring the sample krb5.ini file 11

Test..... 12

Logging..... 16

Purpose

A PingAccess Kerberos Site Authenticator that provides the users the ability to authenticate into a client app using Kerberos.

Requirements

- The Site Authenticator will make a call to Kerberos to get a TGT.
- The configuration will allow the TGT to be cached in the user session and re-used until it expires.
- The Site Authenticator will make a call using the TGT to obtain a Service Ticket for the user.
- The Service Ticket is included in the request header. Example:
`Authorization: Negotiate 89a8742aa8729a8b028`

Prerequisites

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

- PingAccess 6.3+
- PingFederate 8.1+
- JDK version 11+

Installation

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

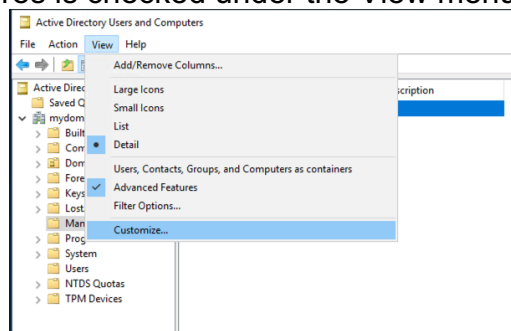
From	To
lib/pa-kcd-site-authenticator.jar	<PingAccessInstall>/deploy
conf/krb5.ini	<PingAccessInstall>/conf

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. Make sure **Advanced Features** is checked under the **View** menu.



3. Under **User Managed Service Accounts**, add a new user.

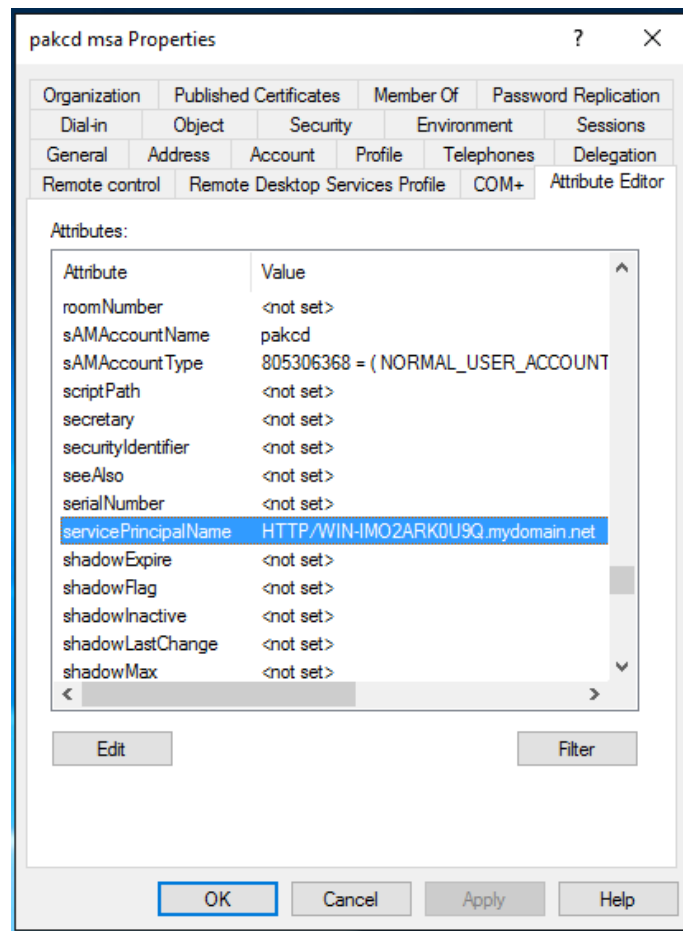
A screenshot of the 'New Object - User' dialog box. The 'Create in' field shows 'mydomain.net/Managed Service Accounts'. The 'First name' field contains 'pakcd', 'Last name' contains 'msa', and 'Full name' shows 'pakcd msa'. The 'User logon name' field contains 'pakcd' and the domain dropdown is '@mydomain.net'. The 'User logon name (pre-Windows 2000)' field shows 'MYDOMAIN\pakcd'. At the bottom are '< Back', 'Next >', and 'Cancel' buttons. The 'Next >' button is highlighted.

4. Select **Next**, enter a password and unselect "User must change password at next logon".

A screenshot of the 'New Object - User' dialog box, showing the password and account options section. The 'Password' and 'Confirm password' fields are filled with dots. Below these are four checkboxes: 'User must change password at next logon' (unchecked), 'User cannot change password' (unchecked), 'Password never expires' (unchecked), and 'Account is disabled' (unchecked). At the bottom are '< Back', 'Next >', and 'Cancel' buttons. The 'Next >' button is highlighted.

5. Click **Next** and then **Finish** to create the new account.

6. 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”.



7. Click Ok to save the changes to the user and enable the Delegation tab.
8. 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”.

Organization Published Certificates Member Of Password Replication
Dial-in Object Security Environment Sessions
Remote control Remote Desktop Services Profile COM+ Attribute Editor
General Address Account Profile Telephones Delegation

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

☐ Do not trust this user for delegation
☐ Trust this user for delegation to any service (Kerberos only)
☒ Trust this user for delegation to specified services only

☐ Use Kerberos only
☒ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service Name

☐ Expanded Add... Remove

OK Cancel Apply Help

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

Select Users or Computers

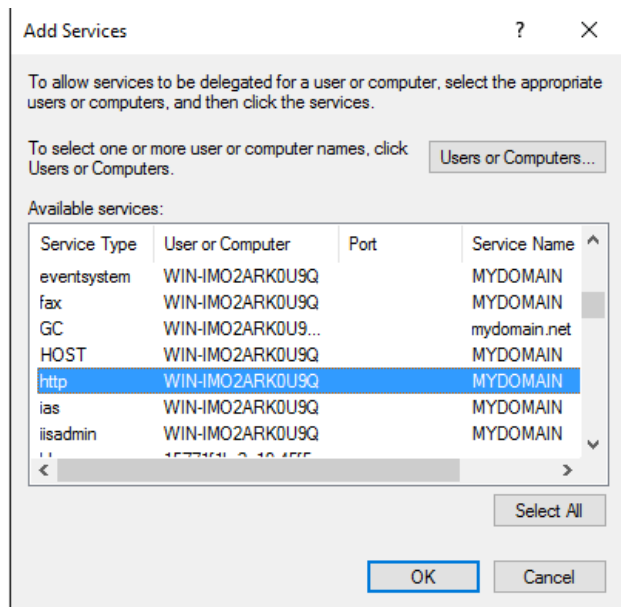
Select this object type:
Users, Computers, Built-in security principals, or Other objects Object Types...

From this location:
mydomain.net Locations...

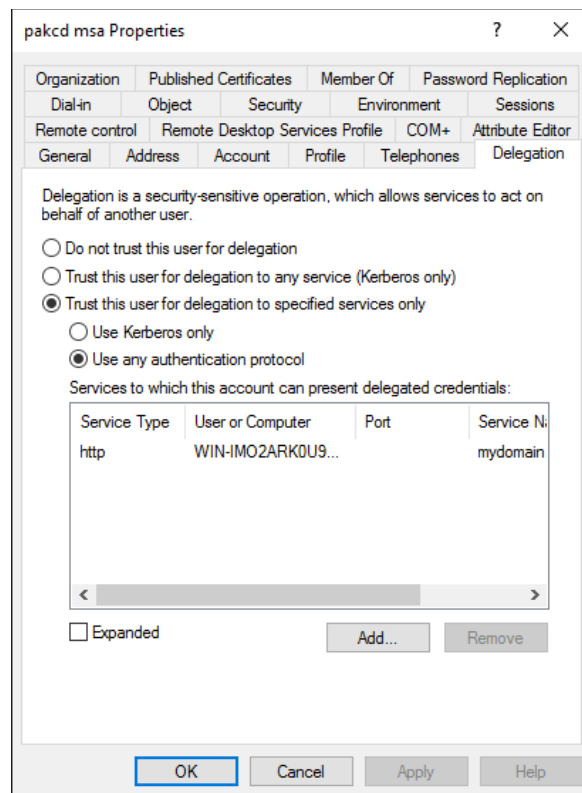
Enter the object names to select (examples):
WIN-IMO2ARK0U9Q Check Names

Advanced... OK Cancel

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



11. 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”.
Kerberos TGT Session Enable	Enables the storing of the TGT in the user session for re-use until it expires.

PingAccess® APPLICATIONS ACCESS SECURITY SETTINGS

APPLICATIONS

- Applications
- Sites
- Sites
- Site Authenticators**
- Third-Party Services
- Agents
- Sideband Clients

kerberos

< To Site Authenticator List

NAME:

TYPE:

KERBEROS CONFIGURATION FILE (FULL PATH):

KERBEROS SERVICE PRINCIPAL NAME:

KERBEROS SERVICE ACCOUNT:

KERBEROS SERVICE ACCOUNT PASSWORD:

KERBEROS TGT SESSION ENABLE: ☒

5. Click **Save**.

kerberos
Kerberos Constrained Delegation Site Authenticator

KERBEROS CONFIGURATION FILE (FULL PATH): C:/ping/pingaccess/pingaccess-6.3.1/conf/krb5.ini

KERBEROS SERVICE PRINCIPAL NAME: http/EC2AMAZ-9PN3FQE.mydomain.net

KERBEROS SERVICE ACCOUNT: pakcd

KERBEROS SERVICE ACCOUNT PASSWORD: *****

KERBEROS TGT SESSION ENABLE: true

Configuring the sample krb5.ini file

This file should contain the default_realm, kdc, admin_server and default_domain relevant to your implementation. Use UPPER CASE for the realm name.

```
[libdefaults]
default_realm = MYDOMAIN.NET
forwardable = true

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

The default port used by Kerberos is port 88 for the KDC.

If the ports in your environment are different, for example 111 for the KDC you can specify it in the file as follows:

```
kdc = WIN-IM02ARK0U9Q.mydomain.net:111
```

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**.

The screenshot shows the PingAccess web interface. On the left is a sidebar with a 'MAIN' section containing 'Applications', 'Sites' (selected), 'Agents', and 'Rules', and a 'SETTINGS' section containing 'Access', 'Networking', 'Security', and 'System'. The main content area is titled 'QuickStart' and includes a link '< To Site List'. Below the title, it states 'This site is used by 2 Applications. View on the applications page'. The 'NAME' field contains 'QuickStart'. The 'TARGETS' section shows 'localhost:9031' with a '+ ADD TARGET' link. The 'SECURE' section has radio buttons for 'No' and 'Yes', with 'Yes' selected. The 'TRUSTED CERTIFICATE GROUP' dropdown is set to 'PingFederate Trusted Group'. The 'SITE AUTHENTICATORS' section has a '+ Create' link and a dropdown menu currently showing 'Please Choose...'. Below the dropdown, 'KCD' is listed as an option, followed by a '+ Create Site Authenticator' link. At the bottom, there is a 'Show Advanced' link with a downward arrow.

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


← → ↻ 🏠 <https://localhost:3000/PingAccessQuickStart/home/> 110% ⋮ 🔒 ⭐

⚙️ Most Visited 🌐 Getting Started 📧 PingOne 📧 Mail 📧 Google Apps 📧 SDKs 📧 Ping 📧 UnboundID 📧 Ping Federate 📧 Ping Access 📧 ClientServiceArchitect... 📧 JIRA Kanban Board 🌐 My WebEx Room 📊 Scalr

Ping PingAccess

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

4. 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.


PingAccess

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 YIIIFkAYJKoZlhcSAQICAQBuggV/MIIFe6ADAgEFoQMCAQ6iBwMF ACAAAAAAGggSoYYIEpDCCBKCgAwIBBAEOGwXNWURPTUFTJi5OR VSiljAgoAMCAQChGTAXGwRodHRwGw9XSU4tSU1PMkFSSzBV0V GjggRjMIIEEX6ADAgEoQMCAQOigRRBIIETbiSp4ejZoaXctWzV7X2t nmXQgkDAfaNA50VSuqRTa0k8iULkkoUNLiD16wwwVxQ1SdgplKuCN 1e5EZzW9Eq0PiJEKB29VkrXbN9vLvhklRarPvrsW2nnqK++SgrfoXC /GDwFVIM2rPBK8cJfAdOmF+Kbr+0IZBZ332f6Z /1uSQ9wQn0e4Vz4oOykG9NomUqdbv0VxAKjz4xgAXT6D56CouG8+ Zb7EBY9VfArVgCypRuP7dzKWOChJ2yyt7edYv6z86l7xexTx56WdY cLhxG5WugpBFN /mz9By38XxOObCxxONwHyAb5QEHPR4o4A98fsXeHW3Ukd0zPq75 ARhsUXyhLGYaXi/dlxe6PV9xDCU9tvQAfhSawtjokAd/LdFsA /GcXqaHEW44TCHh/6voZUdW/Y1+XFZNUJBhn /15b3OscJZJ4+xBVKoc+MoUPkNwo76CyEwSb5iwrUBfL04cJT5aw CktFmmkcJZ1RjKWsDSrlonfgGR1JzfrjY86RUBZs /CKViEmyuFCp1cbJl7wX7jp7f4ONRC0ppjS9hYunt+48LDyU13Yr4Knp WeYcC3cJw0W4htdjeeEqYH+C99xAE97s65lxaZj5LKOeHRPIMm3 F5CZMiRbuSjUe635bV0uVLGameHHbUMMjWVY5 /VQOWRiAp6ZSUIMBDQijzb8p7X91GQ2z5gWkRidfnZ73UUEKok87 w+VeQBekoGvdaP2s8Z1z85Tk9EChtQMaa5WFM /td0MLKpmrDVDQQFwgtfIBRgGz+0fnHfq7XzTNnXyM6MoB61XnIPV VW2LMogXAJnQFbrBa5PAUOyi9bP1PkQklmaLXmMax /XBgd6jrzwT8HyhfsW1ZQvUH9m86x1keCXNelDcZFxbt74xCuBWKdr4 32zG0kNNwvhghC3eDh5UGDcjbldtscyqpiwYNUc9gmRvmJJaQPkO RfIsJxyKnrBPE7R2P6Psg95Cteq2P9y+go /qRHqLBI4PwdyTC2MYyqUqwlq1aiYHkG6Q2Y /4P1win+TDwnm662iCXlvhyJpiJTES119EFnmCZQ8eEAGl0soC7Va1v SWEm46vaQdm+JG7YEBhuY/ojXSONldZ41o /ZmnY8t+IGlhTyB71MrRnS+V6qJceePhRCL5XLju+p/LsFcvEqAex /NDJGqoBO4j5watN+U08BW06N9qF512 /9KLYn3YPH3LH32goyGrC9VU85v5YMERH+LVqQbqTxv9fZl8nKmin PlsekeTpE6t9YAsCOvd6mhvmlO8eQCXm8yNnEmZUw73RzE12XJWi rxLvZpryqx3HukgrzEGNNabm9B+BV3Ed+Pz1Xanlw4dL8TGBZ5sUc5 slhLDFloDMLQKWPNsxxRmcCFkjZ5AFivxPZuMbwsJiAkvH0Aat1Ylr6 rO6YbMdBl/ZcPp4wcGVlxnSazpQJpETPHix+jWAW3st /X/NKSBUtCBtgADAgEXooGuBilGr3VGSeRZ++hMUys+IEkxJldgvlb0j uvGcvAqbyNZ9OjDMKnF8DIEk5X9883bv7WqBLm3dlrX9KwSzwWV V5csYJne4ozZgyOLyg+47LGWxemaOtrmGJCJMOf7EL1GaGeT6P2 VQwX+Fx9s5Vzjrcf mTVvXzmhF5T5sfTaT /GcaCnUlhwppoxZHpceVnSoDQf0JzaAbyHr220QISFQhGe2UJ /0pQfSBemjqn1
Cookie	JSESSIONID=1gc1ah8pm9saw8jffc7khzybm; pf-directory=oauth; PF=mPsi9Z2nv0zaxOoLZ6Qhs99KBMZwxWayGWDzVdpFi9yo; PA_global=eyJhbGciOiJIUzI1NiIsInR5bGEiOiJ1bmMiOiJBMj04Q0JDLUhTMjU2Iiwia2 lkjoIYSlSnBpLnNyaSI6IkhxUDV5TUJcmNmVHFVZVdSMzgwLWtJT 2RURSJ9..TzPHexFnrhugz99xyCYKw.u_k- pzdDB2AuoSP1aklCkajMGsXp0P90z4mJKaGahIVNmeIIRRUZp5vN8i aDRPSHPiGaZJ4PhVvj6_Glp4R0OWKxY0ikmZlwub2q4j6raJbHDBNb 1ZBrfgh8Kl6sUuxtRqIHQ- lArjSOYCJguoAvXitD8ywsy69RbytswPZ9wwMAeHdwGj5RwUX2ErE MXnvDGihP56eF7fRVCFteKoufdqjDIV4DhsXlvZkkChFqcGgahWoUUG VL_Q76zmZ9t_oxs24zp3DqvtQphvQIRQfbiVX0bS89zFYM2HSioSepl Swsvj3rmoZ_p4fZ33azYFywbkxFNIGq6b7bkj0ZP- IOBEpORmO19HRL0ngMjl3jl.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 [KCDSSiteAuthenticator] Authenticating kerberos service account: pakcd
14:19:19,847 DEBUG [KCDSSiteAuthenticator] No identity object in exchange
14:19:20,502 DEBUG [KCDSSiteAuthenticator] Authenticating kerberos service account: pakcd
14:19:20,502 DEBUG [KCDSSiteAuthenticator] No identity object in exchange
14:19:21,205 DEBUG [KCDSSiteAuthenticator] Authenticating kerberos service account: pakcd
14:19:21,205 DEBUG [KCDSSiteAuthenticator] No identity object in exchange
Listening for transport dt_socket at address: 8787
14:25:47,391 DEBUG [KCDSSiteAuthenticator] Authenticating kerberos service account: pakcd
14:25:47,610 DEBUG [KCDSSiteAuthenticator] Creating delegated credential for user : joe
14:25:47,750 DEBUG [KCDSSiteAuthenticator] Getting the service ticket for: http/WIN-IM02ARK0U9Q
14:25:47,750 DEBUG [KerberosContext] pakcd as joe call initSecContext
14:25:47,860 DEBUG [KCDSSiteAuthenticator] Delegated ticket : YIIFkAYJKoZIhvcSAQICAQBuggV/MIIIFe6ADAgEfoQMCAQ6iBwMFACAAAA
CjggSoYYIEpDCCBKCgAwIBBAEOGwXNWURPTUFJTt5ORVSiIjAgoAMCAQChGTAXGwRodHRwGw9XSU4tSU1PMkFSSzBVVGJggRjMIIEX6ADAgEXoQMCAQ0ig
gRRBIIETbiSp4ejZOaXctWzV7X2tnmXQgkDAfaNA50VSuqRTa0k8iULkkoUNLid16vVwWxQ1Sdgp1KuCN1e5EZZW9Eq0PiJEKB29VkrxBn9vLivhklRarPv
rsW2nnqK++SgrfoXC/GDWFMV2rPBK8cJJf1AdOmF+Kbr+0IZBZ332f6Z/1uS09wQn0e4Vz4oOykG9NomUqdbv0VxAkjz4xgAXT6D56CouG8+Zb7EBY9VfjA
rVqCypRuP7dzKW0ChJ2yyt7edYv6z8617xexTx56WdYcLhxG5WugpBFN/mz9By38Xx00bCx0NwHyAb5QEHPR4o4A98fsXeHW3Ukd0zPq75ARhsUXyhLGyaX
i/dIxe6PV9xDcU9tvQAfhSAwtjojkAd/LdFsa/GcXqaHEWr44TCHh/6voZUdW/Y1+XFZNBhn/15b30scJZJl4+xxVBlKoc+MoUPkNwo76CyEwSb5iwrUBfL
04cJT5awCKtFmmkcJZI1RjKWsDSrIonfqqGR1JzfjrYl86RIJBZs/CkViEmyuFCp1cbJl7wX7jp7f40NRC0ppjS9hYunt+48LDyU13Yr4KnpWeYcc3cJw0W
4htdjceEgYH+C99xAE97s651xaZj5LK0eHRPiMm3F5CZMiRbuSjUe635bV0uVLGameHHbUMMjWYVY5/VQ0wRiAp6ZSUIMBDQijzb8p7X91GQ2z5gWkRidf
nZ73UUEKok87w+VeQBekoGvdaP2s8Z1z85Tk9EChTQMaa5WFM/td0MLKpmrDVDQFwqgtfIBRgGz+0fnHfq7XzTNnXyM6MoB61Xn1PvVW2Lm0gXAJnQFbrB
a5PAUOyi9bP1PkQkltmalIXmMaX/XBgd6jrzwt8Hyhfsw1ZQvUH9m86x1keCXNeIDcZFXbt74xCuBWKdr432zG0kNNvwhghC3eDh5UDCjbdIytcyqpiwdY
NuC9gmRvmJJaqPkORflsJxyKnrbPE7R2P6Psg95Cteq2P9y+go/qRHqLB14PwdyTC2MYyQuqWiq1aiYHkG6Q2Y/4P1win+TDwnm662iCXLvhyJpiJTES119
EFnmCZQ8eEAGI0soC7Va1vSWEm46vaQdm+JG7YEBhuy/ojXS0nilDZ41o/ZmnY8f+IG1hTyB71MrRnS+V6qJceePHrCL5XLju+p/LsFcvoEqAex/NDjGqoB
04j5watN+U088W06N9qF512/9KLYn3YPH3LjH32goyGrC9VU85v57YMERH+LVqQbqTXv9fZi8nKminPIsekeTpE6t9YAsCOvd6mhvmI08eQCXm8yNnEmZUw
73RzE12XJWirxLvZpryqx3HukgrzEGNNabm9B+BV3Ed+Pz1Xanlw4dL8TGBZ5sUc51hLDFloDv1IQKWPNsxxRmcCFkjZ5AFiVxPZuMbwsJiAkvH0Aat1y1
r6r06YbMdB/ZcPp4wcGV1xnSazpQJpETPHjx+jWAW3st/X/NKS8uTCBtqADAgEXooGuBigr3VGSeRZ++hMUys+lEkxJIdgvlb0juvGcvAqbyNZ90jDMKnF8
DfEK5X9883bv7WqBLm3dIIrX9KwSzvwyWV5csYJne4ozZgy0Lyg+47LGWXema0tRmGCMOF7EL1GaGeT6P2VQwX+FfX9s5VzjrcFmTVvXzmhF5T5sfctAT/
GcaCnUIhwppoxZHpcEVnSoDQf0JzaAbyHr220Q15FQhGe2UJ/0pQfSBemjqn1
```

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].

More information about using Log4j in PingFederate can be found at:
<https://support.pingidentity.com/s/global-search/%40uri#g=log4j2>