Using Username and Password for pxGrid Client
# Table of Contents

About this Document .................................................................................................................. 3
Why Username and Password? ................................................................................................. 4
Enabling pxGrid .......................................................................................................................... 5
Creating pxGrid client trusted jks store for initial account creation using ISE with self-signed certs .......... 7
Enabling Username and Password ............................................................................................ 10
Using pxGrid Sample Scripts ................................................................................................... 11
Creating pxGrid client trusted jks store for initial account creation using ISE with CA-signed certs .......... 15
Using pxGrid Sample Scripts ................................................................................................... 17
References ................................................................................................................................. 20
About this Document

This document is for pxGrid ecosystem partners looking to integrate their solution with the Cisco platform exchange grid (pxGrid) using pre-shared keys. This document discusses the details of this integration with Cisco Identity Services Engine (ISE) 2.1 in a stand-alone environment with pxGrid enabled. This document uses a MacBook Pro as the pxGrid client. Using pre-shared keys is available with ISE 2.1 and higher.

Why Username and Password?

Cisco Platform Exchange Grid (pxGrid) clients require an easier way of connecting and authenticating to the ISE pxGrid controller. Normally, CA (certificate authority) signed certificates or self-signed certificates are implemented on the pxGrid client or the ISE pxGrid node establish trust and ensure a successful integration. Certificates are deemed as being difficult to deploy. As an alternative method, a username password based client authentication mechanism was developed. This feature enables a client to create and setup a connection with the pxGrid controller and authenticate itself using a username and password in place of using these certificates.

- A pxGrid client will be able to register itself providing a username with the pxGrid controller via a REST API.
- A pxGrid client will be able to setup a new connection with the pxGrid controller over XMPP by providing the appropriate user credentials, username and password, as generated by the ISE pxGrid node.
- The ISE admin will have the ability to approve/deny the pxGrid client’s username and password request.
Enabling pxGrid

ISE will be configured to use either CA-signed or self-signed certificates. If using CA-signed certificates, please ensure the CA root certificate has been installed in the trusted certificate store and the CA-signed ISE certificate has been bound to the initial CSR request and uploaded to the system certificates store.

**Step 1** Select **Administration->System->Deployment** and edit the node

**Step 2** Enable pxGrid
Step 3  Select Save

Step 4  Select Administration->pxGrid Services, you should see the ISE published nodes

**Note:** This may take a few minutes to come up

Step 5  You should see the following:
Creating pxGrid client trusted jks store for initial account creation using ISE with self-signed certs

The trusted jks store for pxGrid client will be created, and the ISE pxGrid node certificate will be imported into the pxGrid client’s trust store. No certificates need to be created for the pxGrid client.

**Step 1** Export the ISE self signed certificate and import this certificate into the pxGrid client. Note this will be in PEM format. You can rename the file to make it easier to read. In this example, the file was renamed to ise21self.

Select Administration->System->Certificates->Certificate Management->System Certificates, select the certificate and Export

**Note:** Select Export Certificate Only

**Step 2** Select Export

**Step 3** Save the file locally
Step 4  Select OK
Step 5  Rename the file to make it easier to work with. In the example below the defaultsignedservercerti.pem file was renamed to ise21self.pem
Step 6  Convert the .PEM file to a .DER format

Note: In a Distributed ISE Environment, Certificate-Authority (CA-Signed) certs will be used. In this case both the ISE Mnt Node certificate and the CA-root certificates will be downloaded

```
openssl x509 -outform der -in ise21self.pem -out ise21self.der
```

Step 7  Convert the .PEM file to a .DER format
Step 8  Import the ISE self-signed certificate in .DER format (i.e. 201self.der) into the trusted root keystore (i.e. root1jks). This will serve as the root truststore filename and root trust store password for the pxGrid scripts.

```
keytool -import -alias ise21root -keystore root1.jks -file ise21self.der
```

Enter keystore password: cisco123
Re-enter new password: cisco123
Owner: CN=ise21self.lab10.com
Issuer: CN=ise21self.lab10.com
Serial number: 5776cb4300000000f9401fa2c193400d
Certificate fingerprints:
  SHA256:
Signature algorithm name: SHA1withRSA
Version: 3

Extensions:
#1: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:
CA: true
PathLen: 2147483647

#2: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Non_repudiation
  Key_Encipherment
  Key_Agreement
  Key_CertSign
]

#4: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
  SSL server
]

#5: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
  KeyIdentifier [
    0000: 6A E7 D9 9E A5 C7 88 92 15 E6 BF C6 7A 39 AB FD j...........z9..
    0010: 12 B8 E8 9A                                        ....
  ]
]

Trust this certificate? [no]: yes
Certificate was added to keystore
Enabling Username and Password

Here we enable the username and based option in the ISE pxGrid node.

**Step 1** Select Administration->pxGrid Services->Settings->Under pxGrid settings, enable Allow password based on account creation

**Note:** You can also enable automatically approved new accounts, if you desire to have the pxGrid client automatically register to the ISE pxGrid node without administrator intervention.

**Step 2** Select Save
Using pxGrid Sample Scripts

Here we step through some sample scripts. The `create account` script was added in ISE 2.1 and will generate the password provided from the initial pxGrid client certificate. The `session_subscribe` script provides the pxGrid client with real-time 802.1X notification when subscribed to the Session Directory topic. The `session download` script provides the pxGrid client with active bulk download user sessions.

Note the `–w` option specifies the generated password.

**Step 1**  Create Account and obtain password

```bash
./create_account.sh -a ise12self.lab10.com -u mac -t maccertroot.jks -q cisco123
```

```properties
version=1.0.3.37
hostnames=ise12self.lab10.com
username=mac
password=
group=Session
description=null
keystoreFilename=/Applications/iseself/pxGrid-sdk-1.0.3.37/samples/certs/clientsample1.jks
keystorePassword=cisco123
truststoreFilename=maccertroot.jks
truststorePassword=cisco123
```

HTTP status=OK
password: O3yt1cKDE89OBIT1

**Step 2**  Subscribe to session

```bash
./session_subscribe.sh -a ise12self.lab10.com -u mac -t maccertroot.jks -q cisco123 -w O3yt1cKDE89OBIT1
```

```properties
version=1.0.3.37
hostnames=ise12self.lab10.com
username=mac
password=O3yt1cKDE89OBIT1
group=Session
description=null
keystoreFilename=/Applications/iseself/pxGrid-sdk-1.0.3.37/samples/certs/clientsample1.jks
keystorePassword=cisco123
truststoreFilename=maccertroot.jks
truststorePassword=cisco123
```

Connecting...

**Step 3**  View in ISE

**Step 4**  Select `mac` -> Approve -> Yes, when prompted to approve the selected client
Step 5  You should now see the pxGrid client subscribed to the session

Step 6  Run session_subscribe

```bash
./session_subscribe.sh -a ise12self.lab10.com -u mac -t maccertroot.jks -q cisco123 -w O3yt1cKDE89OBIT1
------- properties -------
version=1.0.3.37
hostnames=ise12self.lab10.com
username=mac
password=O3yt1cKDE89OBIT1
group=Session
description=null
keystoreFilename=/Applications/iseself/pxGrid-sdk-1.0.3.37/samples/certs/clientsample1.jks
truststoreFilename=maccertroot.jks
truststorePassword=cisco123
--------------------------
```

Connecting...
Account enabled
Connected
Filters (ex. '1.0.0.0/255.0.0.0,1234::/16,...' or <enter> for no filter): 18:54:24.518 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Step 7  Verify authenticated users, login using 802.1X or with RADIUSsimulator you should see the following:

```
./session_subscribe.sh -a ise12self.lab10.com -u mac -t maccertroot.jks -q cisco123 -w O3yt1cKDE89OBIT1
------- properties -------
version=1.0.3.37
hostnames=ise12self.lab10.com
username=mac
password=O3yt1cKDE89OBIT1
group=Session
description=null
keystoreFilename=/Applications/iseself/pxGrid-sdk-1.0.3.37/samples/certs/clientsample1.jks
truststoreFilename=maccertroot.jks
truststorePassword=cisco123

--------------------------
Connecting...
Account enabled
Connected
Filters (ex. '1.0.0.0/255.0.0.0,1234::/16,...' or <enter> for no filter): 18:54:24.518 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
press <enter> to disconnect...Session={ip=[192.168.1.9], Audit Session Id=0A0000010000002F01FE4A9C, User Name=host/jeppich-PC.lab10.com, AD User DNS Domain=null, AD Host DNS Domain=lab10.com, AD User NetBIOS Name=null, AD Host NetBIOS Name=LAB10, Calling station id=00:0C:29:CF:07:17, Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint Profile=Microsoft-Workstation, MEM Endpoint MAC Address=null, MDM Operating System=null, MDM Compliance Status=null, MDM Encryption=null, MDM Pin Lock=null, MDM Jail Broken=null, MDM Model=null, MDM Manufacturer=null, MDM IMEI=null, MDM MEID=null, MDM UDID=null, MDM Serial Number=null, MDM Device Manager=null, MDM Last Sync Up Time=null, NAS IP=192.168.1.3, NAS Port=GigabitEthernet1/0/11, RADIUSAVPairs=[ Acct-Session-Id=00000037], Posture Status=null, Posture Timestamp=, Session Last Update Time=Sat Jul 02 19:21:17 EDT 2016, Session attributeName=Authorization_Profiles, Session attributeValue=PermitAccess}
```

Step 8  Verify 802.1x authentications in the Radius Live Logs

Select Operations->RADIUS->Live Logs
Step 9   Verify the pxGrid client has subscribed to the SessionDirectory
Select Administration->pxGrid Services

Step 10  Run session_download script

```
./session_download.sh -a ise12self.lab10.com -u mac -t maccertroot.jks -q cisco123 -w O3yt1cKDE89OBIT1
------- properties -------
version=1.0.3.37
hostnames=ise12self.lab10.com
username=mac
password=O3yt1cKDE89OBIT1
group=Session
description=null
keystoreFilename=/Applications/iseself/pxGrid-sdk-1.0.3.37/samples/certs/clientsample1.jks
keystorePassword=cisco123
truststoreFilename=maccertroot.jks
truststorePassword=cisco123
--------------------------
Connecting...
Connected
Filters (ex. '1.0.0.0/255.0.0.0,1234::/16...' or <enter> for no filter):
Start time (ex. '2015-01-31 13:00:00' or <enter> for no start time):
End time (ex. '2015-01-31 13:00:00' or <enter> for no end time):
pxGrid controller version=1.0.3.32
Session={ip=[192.168.1.9], Audit Session Id=0A0000010000002F01FE4A9C, User Name=host/jeppich-PC.lab10.com, AD User DNS Domain=null, AD Host DNS Domain=lab10.com, AD User NetBIOS Name=null, AD Host NETBIOS Name=LAB10, Calling station id=00:0C:29:CF:07:17, Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint Profile=Microsoft-Workstation, MDM Endpoint MAC Address=null, MDM Operating System=null, MDM Registration Status=null, MDM Compliance Status=null, MDM Disk Encryption=null, MDM Pin Lock=null, MDM Jail Broken=null, MDM Model=null, MDM Manufacturer=null, MDM IMEI=null, MDM MEID=null, MDM UDID=null, MDM Serial Number=null, MDM Location=null, MDM Device Manager=null, MDM Last Sync Up Time=null, NAS IP=192.168.1.3, NAS Port=GigabitEthernet1/0/11, RADIUSAVPairs=[ Acct-Session-Id=00000037], Posture Status=null, Posture Timestamp=', Session Last Update Time=Sat Jul 02 19:21:17 EDT 2016, Session attributeName=Authorization_Profiles, Session attributeValue=PermitAccess} Session count=1
Connection closed
```
Creating pxGrid client trusted jks store for initial account creation using ISE with CA-signed certs

We create the pxGrid client trusted jks store. The CA-signed root certificate from ISE will be imported into the pxGrid client certificate store.

Please see http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-89-CA_signed_pxGridISEnode_CAsigned_pxGridclient.pdf on deploying ISE using CA-signed certificates if you are not familiar with deploying ISE pxGrid node in a CA-signed environment.

Step 1  Convert the CA root.cer file to DER format

openssl x509 -outform der -in root.cer -out root.der

Step 2  Import the CA root certificate in DER format into the trusted root store (i.e. preshareroot.jks)

keytool -import -alias ise21prodca10 -keystore preshareroot.jks -file root.der

Enter keystore password:
Owner: CN=lab10-WIN-N3OR1A7H9KL-CA, DC=lab10, DC=com
Issuer: CN=lab10-WIN-N3OR1A7H9KL-CA, DC=lab10, DC=com
Serial number: 6f0fce547462b29a4e86e88536eb829d
Certificate fingerprints:
  Signature algorithm name: SHA256withRSA
  Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
   0000: 02 01 00 ...

#2: ObjectId: 2.5.29.19 Criticality=true
   BasicConstraints: [CA:true, PathLen:2147483647]

#3: ObjectId: 2.5.29.15 Criticality=false
   KeyUsage: [DigitalSignature, Key_CertSign, Crl_Sign]

#4: ObjectId: 2.5.29.14 Criticality=false
   SubjectKeyIdentifier: [KeyIdentifier: 0000: 16 EB 8F 72 43 0F 41 9B 68 16 F9 12 10 7E 86 73 ...r.C.A.h.......
   Owner: 0010: 3F 01 1B E1]

Trust this certificate? [no]: yes
Certificate was added to keystore
Using pxGrid Sample Scripts

Here we step through some sample scripts. The ./create account script was added in ISE 2.1 and will generate the password provided from the initial pxGrid client certificate. The ./session_subscribe script provides the pxGrid client with real-time 802.1X notification when subscribed to the Session Directory topic. The ./session download script provides the pxGrid client with active bulk download user sessions.

Note the –w option specifies the generated password.

Step 1  Create Account and obtain password

```
./create_account.sh -a ise21ca.lab10.com -u mac -t preshareroot.jks -q cisco123
------- properties -------
version=1.0.3.37
hostnames=ise21ca.lab10.com
username=mac
password=
group=Session
description=null
keystoreFilename=/Applications/ise21caprod/pxGrid-sdk-1.0.3.37/samples/certs/clientsample1.jks
keystorePassword=cisco123
truststoreFilename=preshareroot.jks
truststorePassword=cisco123
--------------------------
HTTP status=OK
password: 9EppjFWdSUBhiGTR
```

Step 2  Subscribe to session

```
./session_subscribe.sh -a ise21ca.lab10.com -u mac -t preshareroot.jks -q cisco123 -w 9EppjFWdSUBhiGTR
------- properties -------
version=1.0.3.37
hostnames=ise21ca.lab10.com
username=mac
password=9EppjFWdSUBhiGTR
group=Session
description=null
keystoreFilename=/Applications/ise21caprod/pxGrid-sdk-1.0.3.37/samples/certs/clientsample1.jks
keystorePassword=cisco123
truststoreFilename=preshareroot.jks
truststorePassword=cisco123
--------------------------
Connecting...
Filters {ex. '1.0.0.0/255.0.0.0,1234::/16,...' or <enter> for no filter}: 21:43:21.211 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
press <enter> to disconnect...Session=[ip=[192.168.1.10], Audit Session Id=0A000010000002A01A2CAB3, User Name=LAB10\jeppich, AD User DNS Domain=lab10.com, AD Host DNS Domain=null, AD User NetBIOS Name=LAB10, AD Host NetBIOS Name=null, Calling station id=00:0C:29:CF:07:17, Session state=DISCONNECTED, ANCstatus=null, Security Group=null, Endpoint Profile=Microsoft-Workstation, MDM Endpoint MAC Address=null, MDM Operating System=null, MDM Registration Status=null, MDM Compliance Status=null, MDM Disk Encryption=null, MDM Pin Lock=null, MDM Jail Broken=null, MDM Model=null, MDM Manufacturer=null, MDM IMEI=null, MDM MEID=null, MDM UDID=null, MDM Serial Number=null, MDM Location=null, MDM Device Manager=null, MDM Last Sync Up Time=null, NAS IP=192.168.1.3, NAS Port=GigabitEthernet1/0/11, RADIUSAVPairs=[ Acct-Session-Id=0000002E], Posture Status=null, Posture Timestamp=, Session Last Update Time=Sun Jul 03 21:43:41 EDT 2016, Session attributeName=Authorization Profiles, Session attributeValue=PermitAccess}
Connection closed
```
Step 3 Run session_download script

```
./session_download.sh -a ise21ca.lab10.com -u mac -t preshareroot.jks -q cisco123 -w 9EppjF WD SUB h i G T R
```

```properties
version=1.0.3.37
hostnames=ise21ca.lab10.com
username=mac
password=9EppjF WD SUB h i G T R
group=Session
description=null
keyStoreFilename=/Applications/ise21caprod/pxGrid-sdk-1.0.3.37/samples/certs/clientsample1.jks
keyStorePassword=cisco123
trustStoreFilename=preshareroot.jks
trustStorePassword=cisco123
```

Connecting...

End time (ex. '2015-01-31 13:00:00' or <enter> for no end time):
```
pxGrid controller version=1.0.3.32
Session={ip=[192.168.1.30], Audit Session Id=0A000001000000270165C960, User Name=00:0C:29:CA:73:9F, AD User DNS Domain=null, AD Host DNS Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station id=00:0C:29:CA:73:9F, Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint Profile=VMware-Device, MDM Endpoint MAC Address=null, MDM Operating System=null, MDM Registration Status=null, MDM Compliance Status=null, MDM Disk Encryption=null, MDM Pin Lock=null, MDM Jail Broken=null, MDM Model=null, MDM Manufacturer=null, MDM IMEI=null, MDM MEID=null, MDM UDIM null, MDM Serial Number=null, MDM Location=null, MDM Device Manager=null, MDM Last Sync Up Time=null, NAS IP=192.168.1.3, NAS Port=Gi g abit Ethenet1/0/15, RADIUSAVPairs={ Acct-Session-Id=00000028}, Posture Status=null, Posture Timestamp=, Session Last Update Time=Sun Jul 03 17:16:34 EDT 2016, Session attributeName=Authorization_Profiles, Session attributeValue=PermitAccess}
```

Session={ip=[192.168.1.30], Audit Session Id=0A000001000000270165C960, User Name=00:0C:29:CA:73:9F, AD User DNS Domain=null, AD Host DNS Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station id=00:0C:29:CA:73:9F, Session state=STARTED, ANCstatus=null, Security Group=null, Endpoint Profile=Microsoft-Workstation, MDM Endpoint MAC Address=null, MDM Operating System=null, MDM Registration Status=null, MDM Compliance Status=null, MDM Disk Encryption=null, MDM Pin Lock=null, MDM Jail Broken=null, MDM Model=null, MDM Manufacturer=null, MDM IMEI=null, MDM MEID=null, MDM UDIM null, MDM Serial Number=null, MDM Location=null, MDM Device Manager=null, MDM Last Sync Up Time=null, NAS IP=192.168.1.3, NAS Port=Gi g abit Ethenet1/0/11, RADIUSAVPairs={ Acct-Session-Id=00000032}, Posture Status=null, Posture Timestamp=, Session Last Update Time=Sun Jul 03 17:16:34 EDT 2016, Session attributeName=Authorization_Profiles, Session attributeValue=PermitAccess}
```
```
Stoppi ng...
```

Step 3 Run session_download script
References

