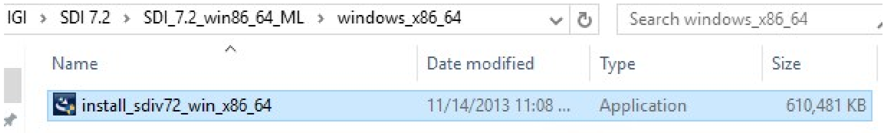
Installing Security Directory Integrator 7.2

You can install Security Directory Integrator 7.2. using the **Security Directory Integrator** wizard. IBM IGI uses Security Directory Integrator to communicate with various managed resources.

To install Security Directory Integrator 7.2:

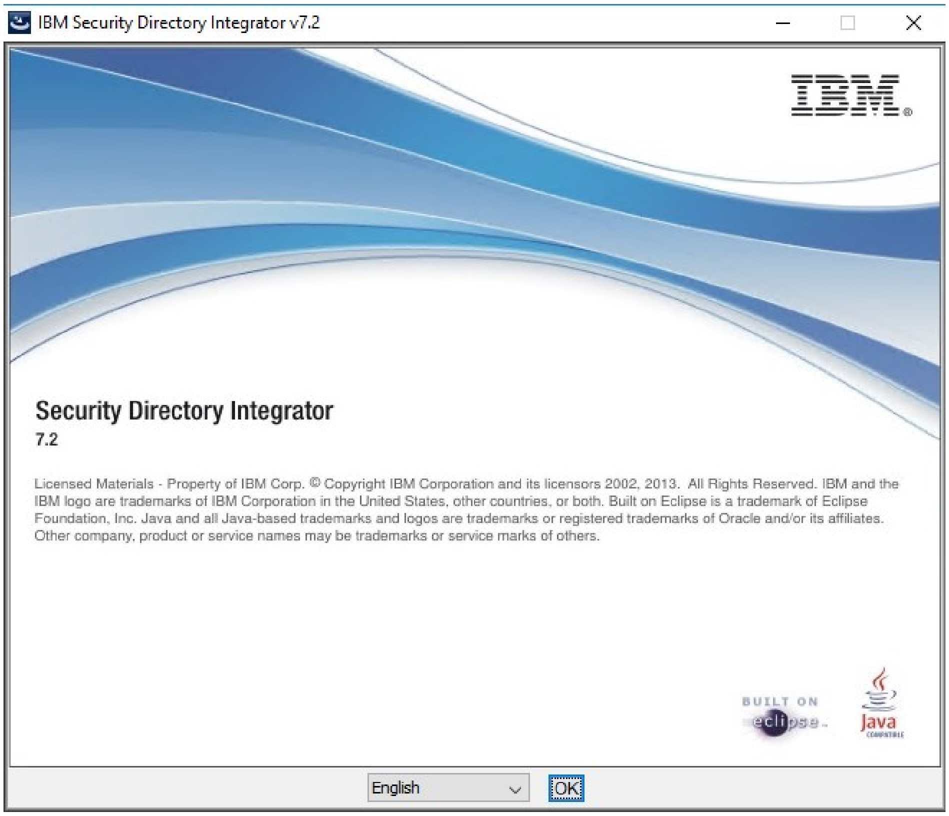
1. Go to the Security Directory Integrator 7.2 folder that you have downloaded from the IBM website.
2. Double-click the windows_x86_64 folder.



IGI > SDI 7.2 > SDI_7.2_win86_64_ML > windows_x86_64

Name	Date modified	Type	Size
install_sdiv72_win_x86_64	11/14/2013 11:08 ...	Application	610,481 KB

3. Run as administrator. The **User Account Control** dialog box appears.
4. Click **Yes** to run the setup. The **Security Directory Integrator wizard** appears.



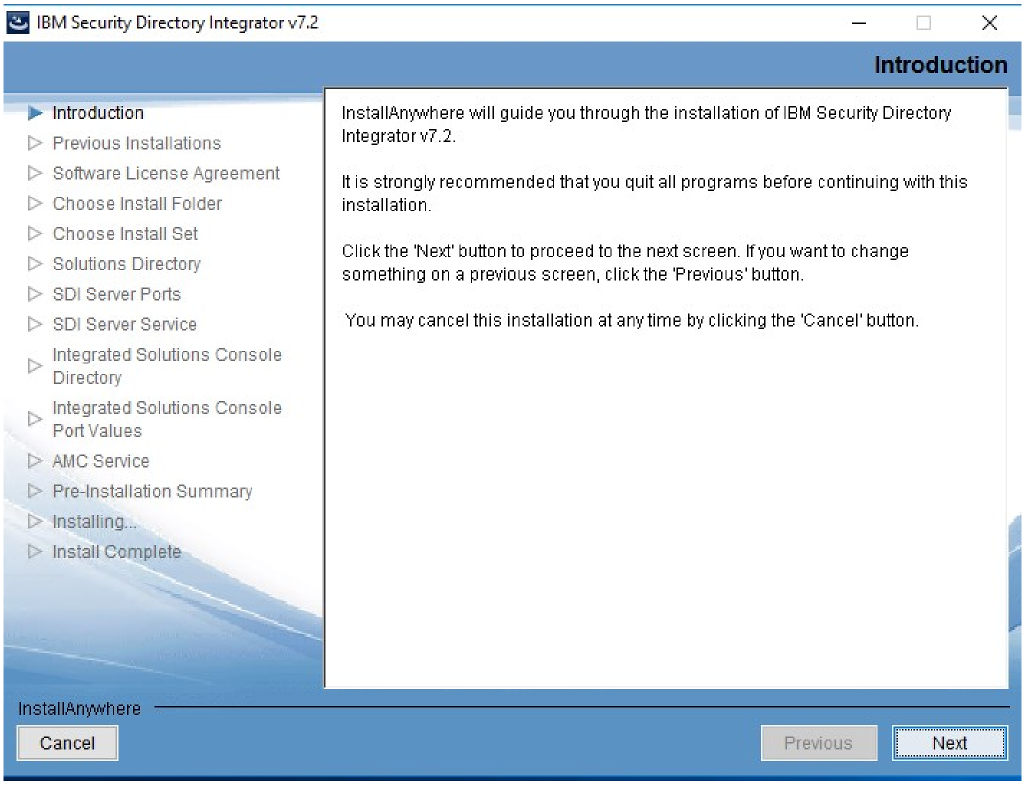
IBM Security Directory Integrator v7.2

Security Directory Integrator

7.2

Licensed Materials - Property of IBM Corp. © Copyright IBM Corporation and its licensors 2002, 2013. All Rights Reserved. IBM and the IBM logo are trademarks of IBM Corporation in the United States, other countries, or both. Built on Eclipse is a trademark of Eclipse Foundation, Inc. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates. Other company, product or service names may be trademarks or service marks of others.

5. Click **OK**.
6. The **Introduction** panel appears.



InstallAnywhere will guide you through the installation of IBM Security Directory Integrator v7.2.

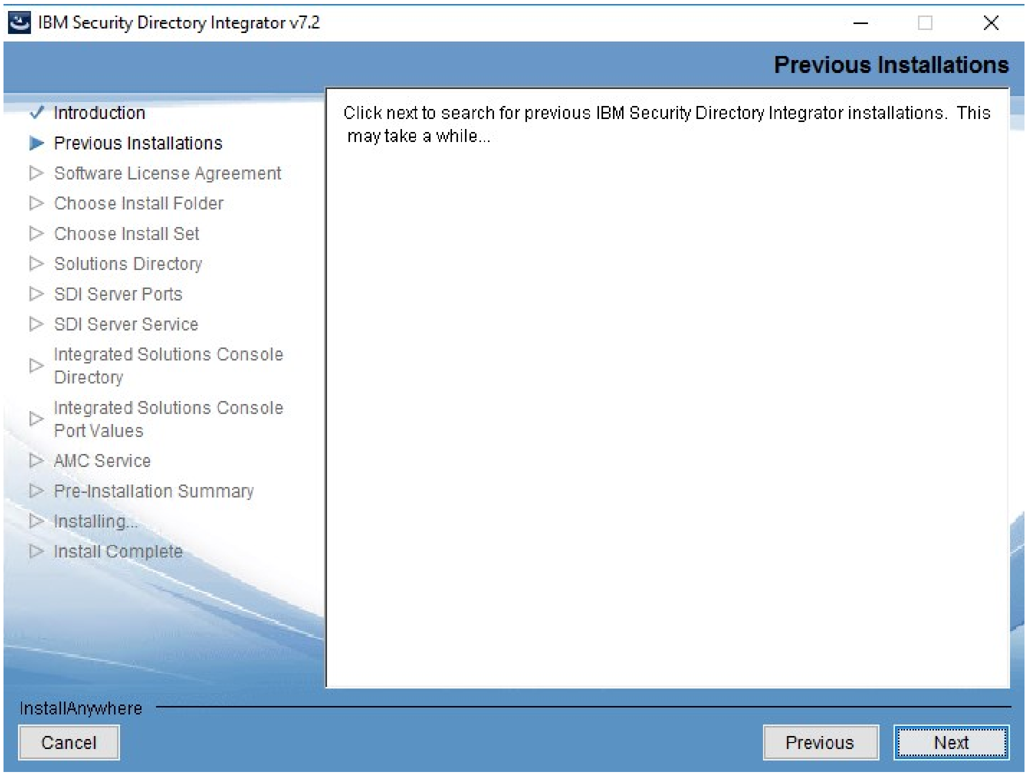
It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

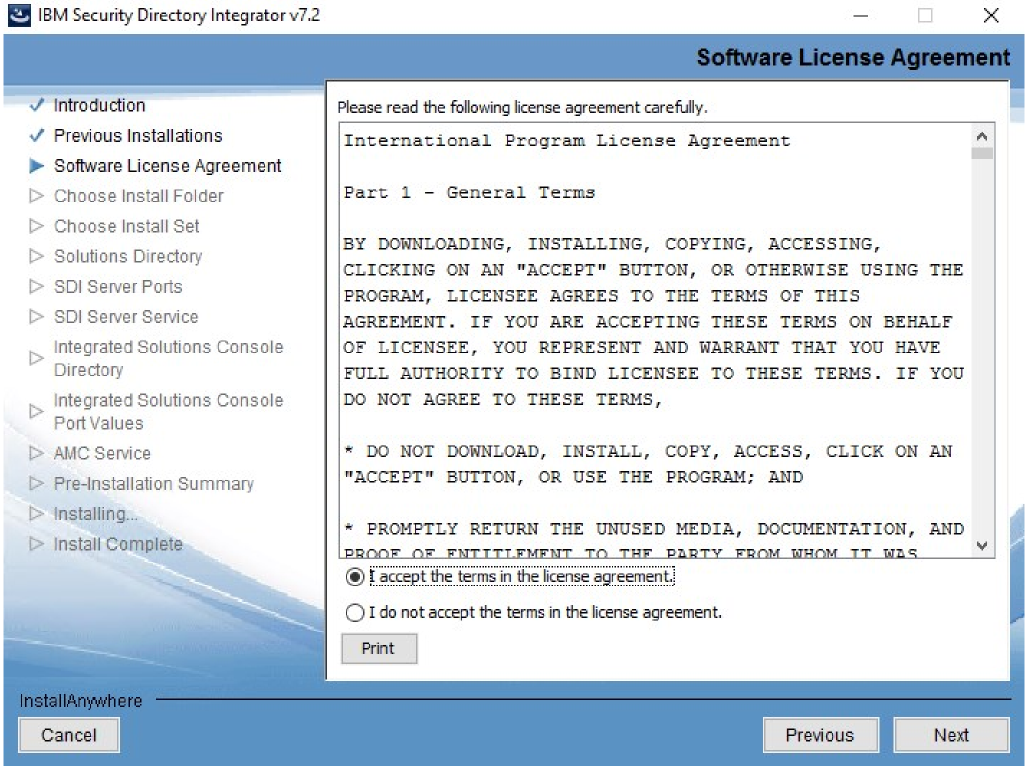
7. Click **Next**.

8. The **Previous Installations** panel appears.



Click next to search for previous IBM Security Directory Integrator installations. This may take a while...

9. Click **Next**.



Please read the following license agreement carefully.

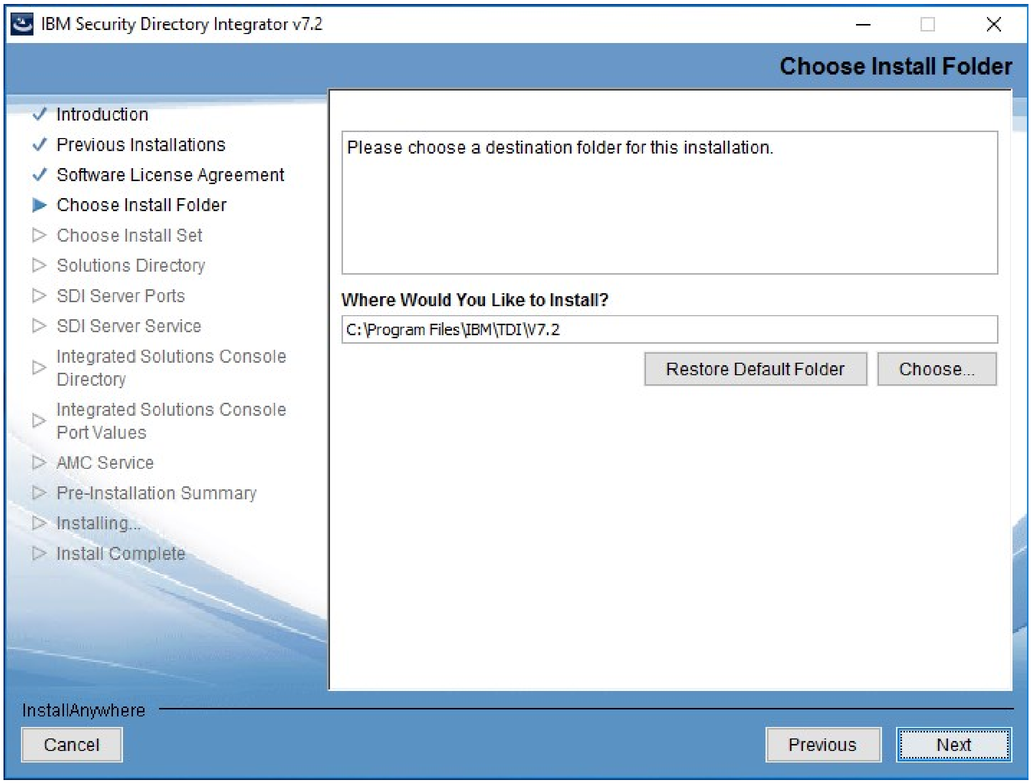
```
International Program License Agreement

Part 1 - General Terms

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING,
CLICKING ON AN "ACCEPT" BUTTON, OR OTHERWISE USING THE
PROGRAM, LICENSEE AGREES TO THE TERMS OF THIS
AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF
OF LICENSEE, YOU REPRESENT AND WARRANT THAT YOU HAVE
FULL AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU
DO NOT AGREE TO THESE TERMS,

* DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN
"ACCEPT" BUTTON, OR USE THE PROGRAM; AND

* PROMPTLY RETURN THE UNUSED MEDIA, DOCUMENTATION, AND
PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM IT WAS
```

● I accept the terms in the license agreement.

○ I do not accept the terms in the license agreement.

10. Select **I accept the terms in the license agreement**.

11. Click **Next**.



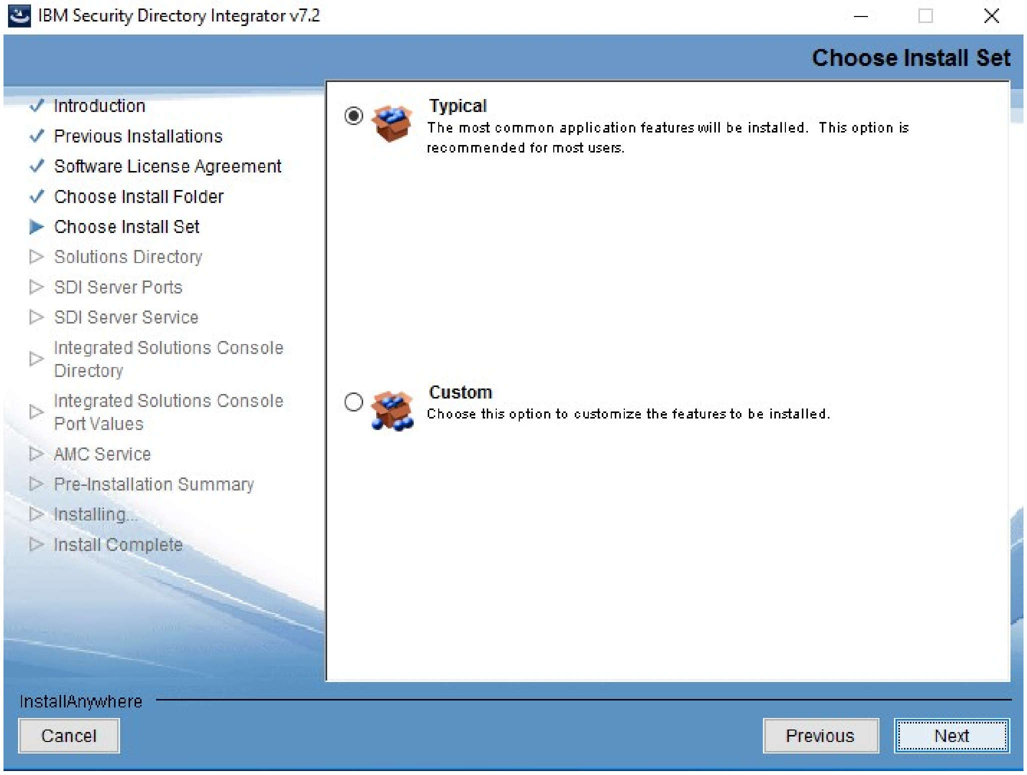
Please choose a destination folder for this installation.

Where Would You Like to Install?

C:\Program Files\IBM\TDI\V7.2

12. In the **Choose Install Folder**, the folder where Security Directory Integrator 7.2 is installed appears. Click **Choose** to change the folder where you want to install Security Directory Integrator 7.2.

13. After installing Security Directory Integrator 7.2, in the **Choose Install Folder**, click **Next**. The **Choose Install Set** panel appears.



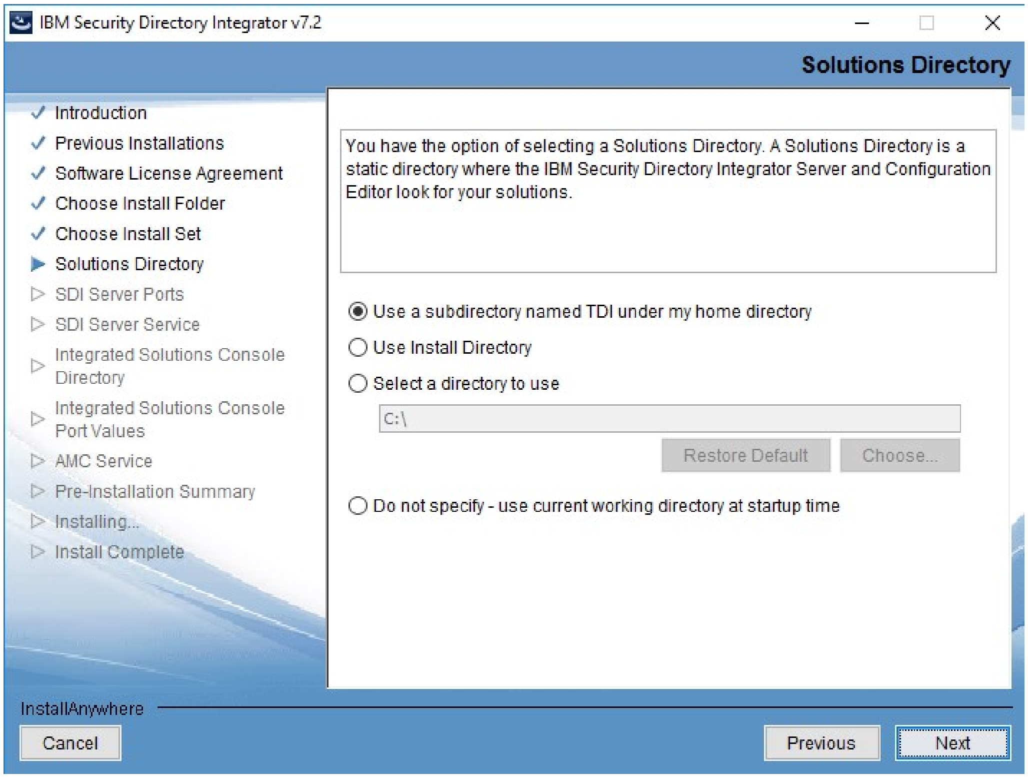
IBM Security Directory Integrator v7.2

Choose Install Set

● **Typical**
The most common application features will be installed. This option is recommended for most users.

○ **Custom**
Choose this option to customize the features to be installed.

14. Select **Typical** and click **Next**.



IBM Security Directory Integrator v7.2

Solutions Directory

You have the option of selecting a Solutions Directory. A Solutions Directory is a static directory where the IBM Security Directory Integrator Server and Configuration Editor look for your solutions.

● Use a subdirectory named TDI under my home directory

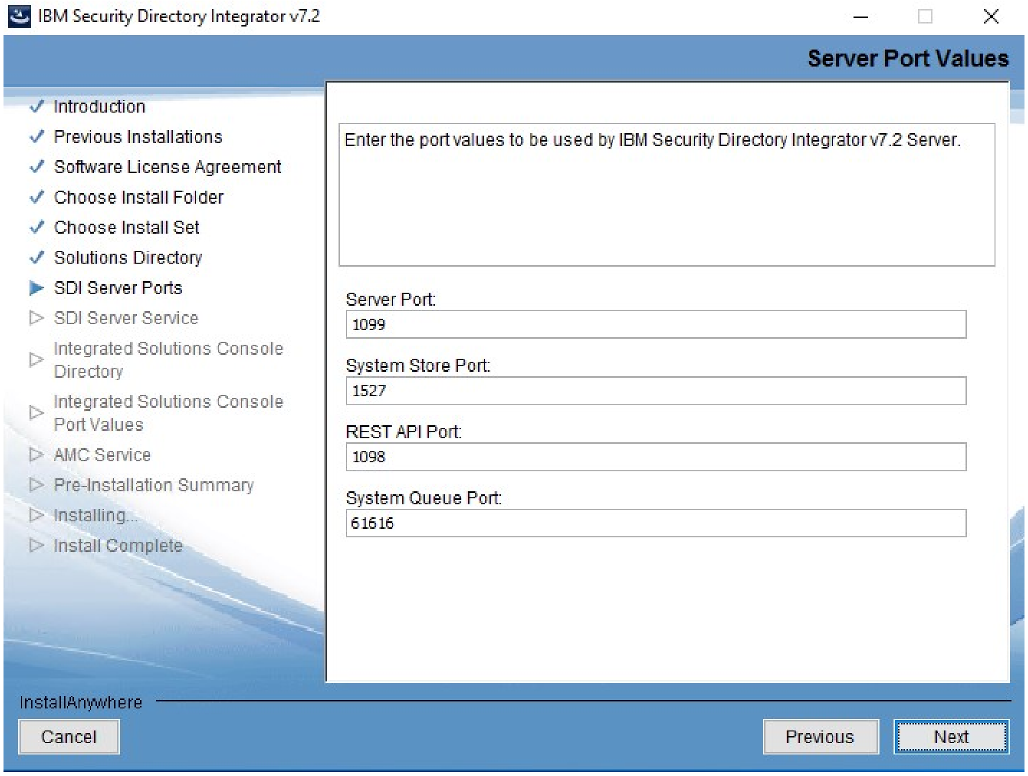
○ Use Install Directory

○ Select a directory to use

C:\

○ Do not specify - use current working directory at startup time

15. Click **Next**. The **Server Ports Values** panel appears.



Enter the port values to be used by IBM Security Directory Integrator v7.2 Server.

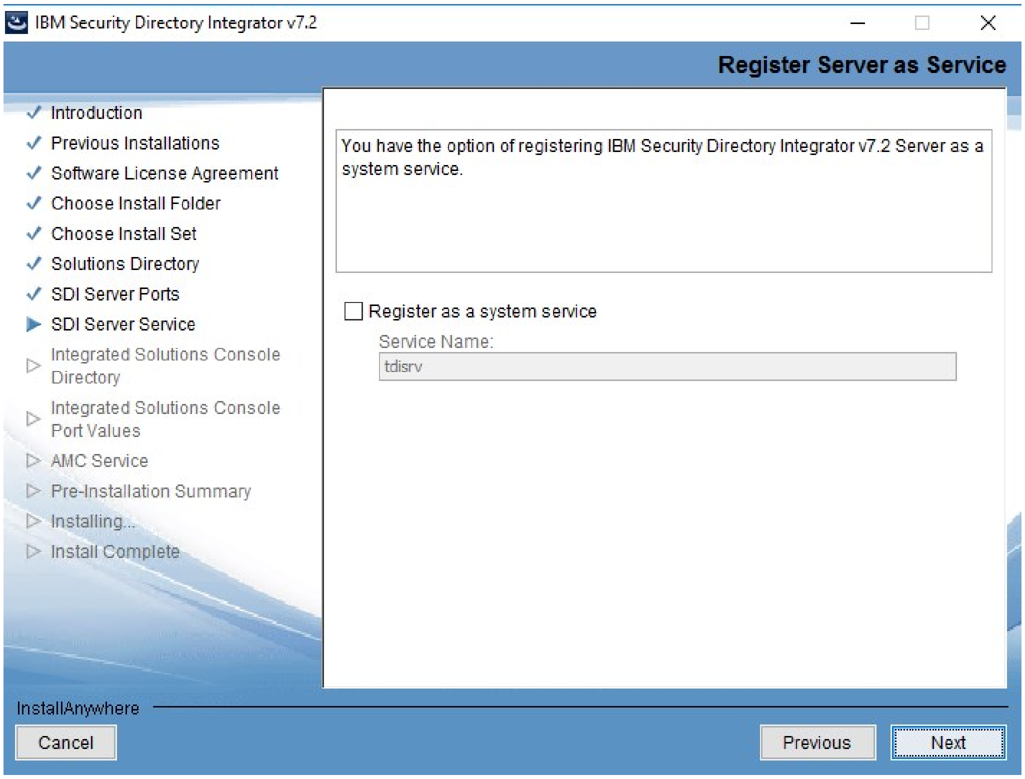
Server Port: 1099

System Store Port: 1527

REST API Port: 1098

System Queue Port: 61616

16. Click **Next**. The **Register Server as Service** panel appears.

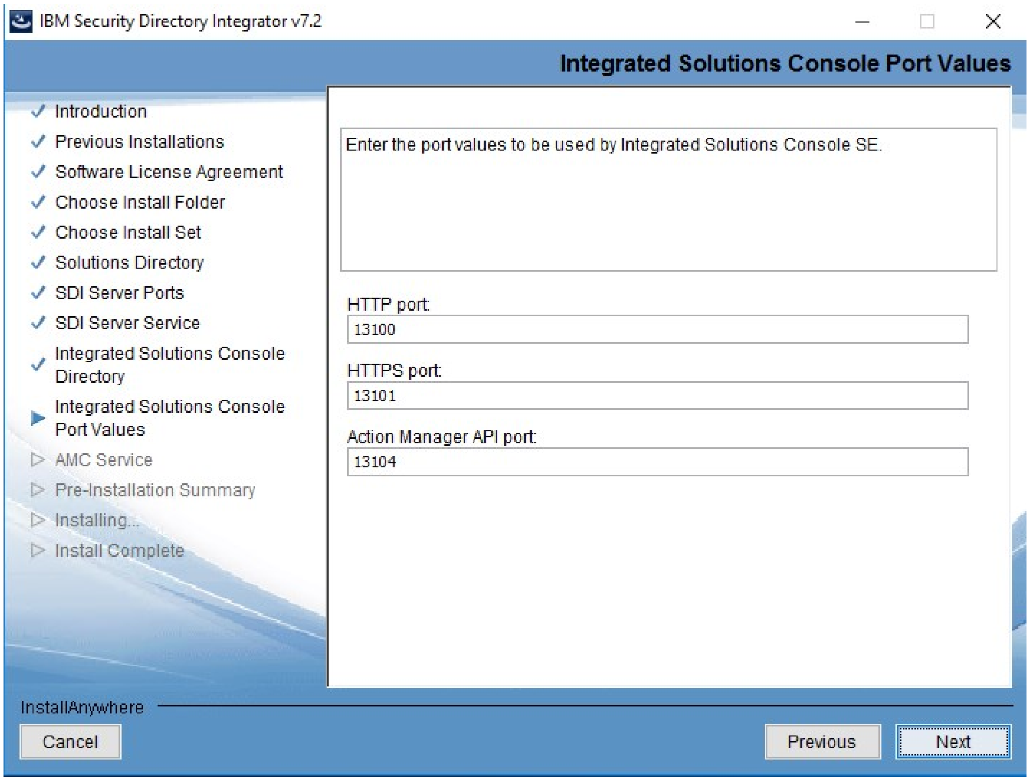


You have the option of registering IBM Security Directory Integrator v7.2 Server as a system service.

□ Register as a system service

Service Name: tdisrv

17. Click **Next**. The **Integrated Solutions Console Port Values** panel appears.



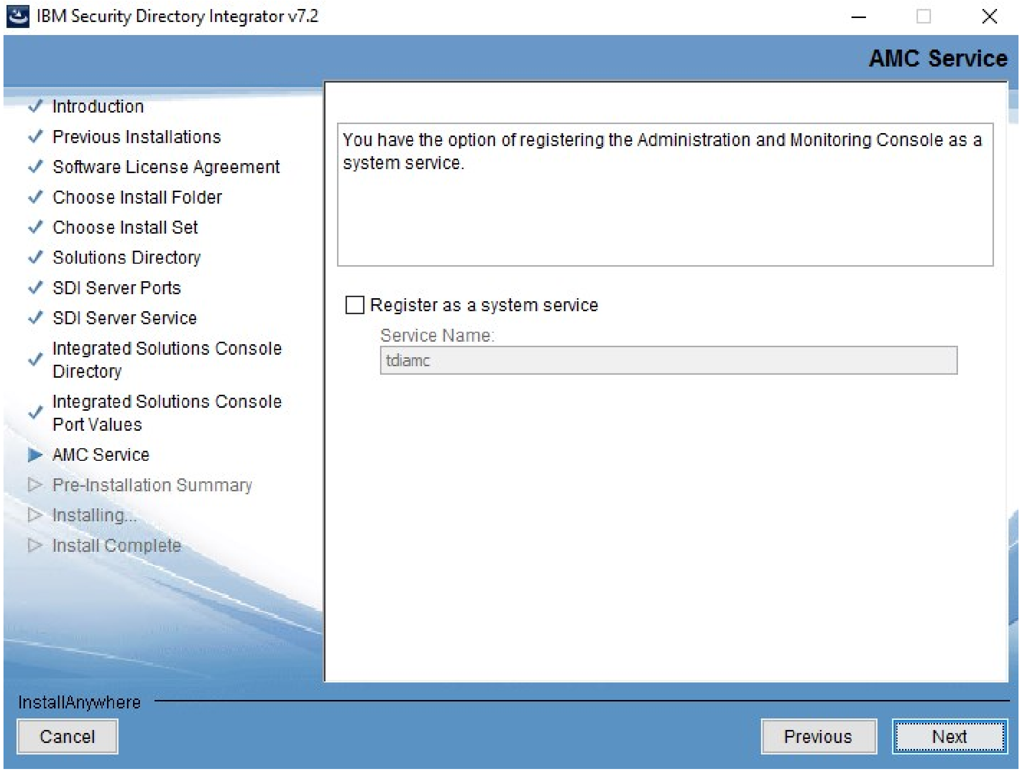
Enter the port values to be used by Integrated Solutions Console SE.

HTTP port: 13100

HTTPS port: 13101

Action Manager API port: 13104

18. Click **Next**. The **AMC Service** panel appears.

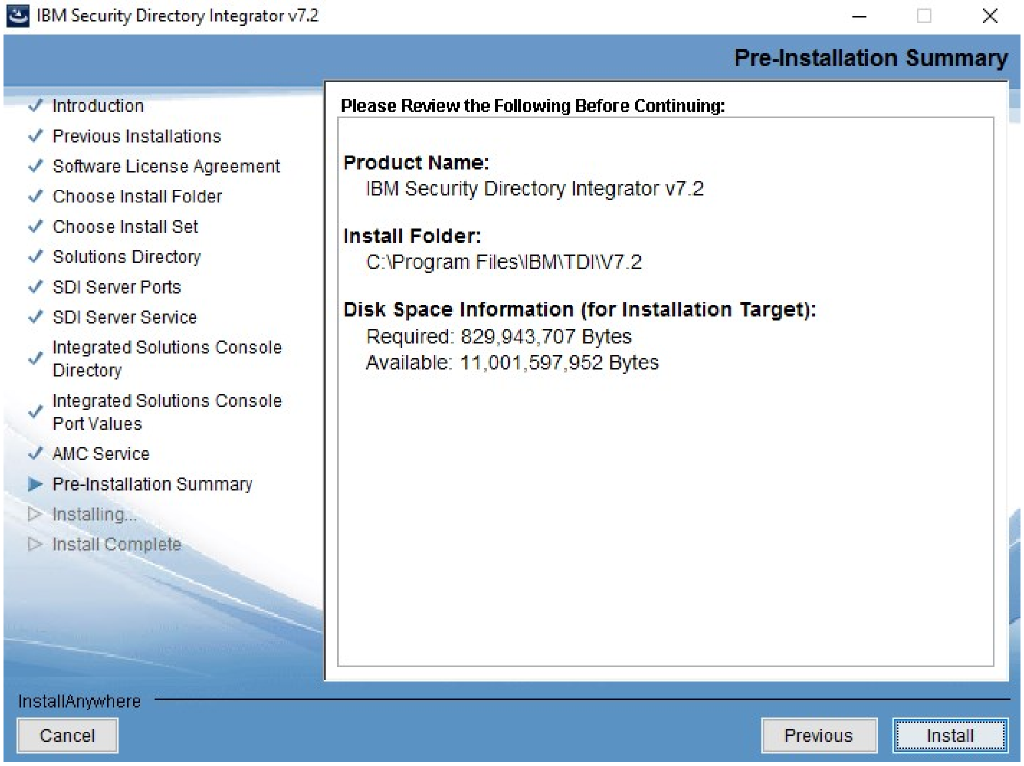


You have the option of registering the Administration and Monitoring Console as a system service.

□ Register as a system service

Service Name:
tdiamc

19. Click **Next**. The **Pre-Installation Summary** panel appears.



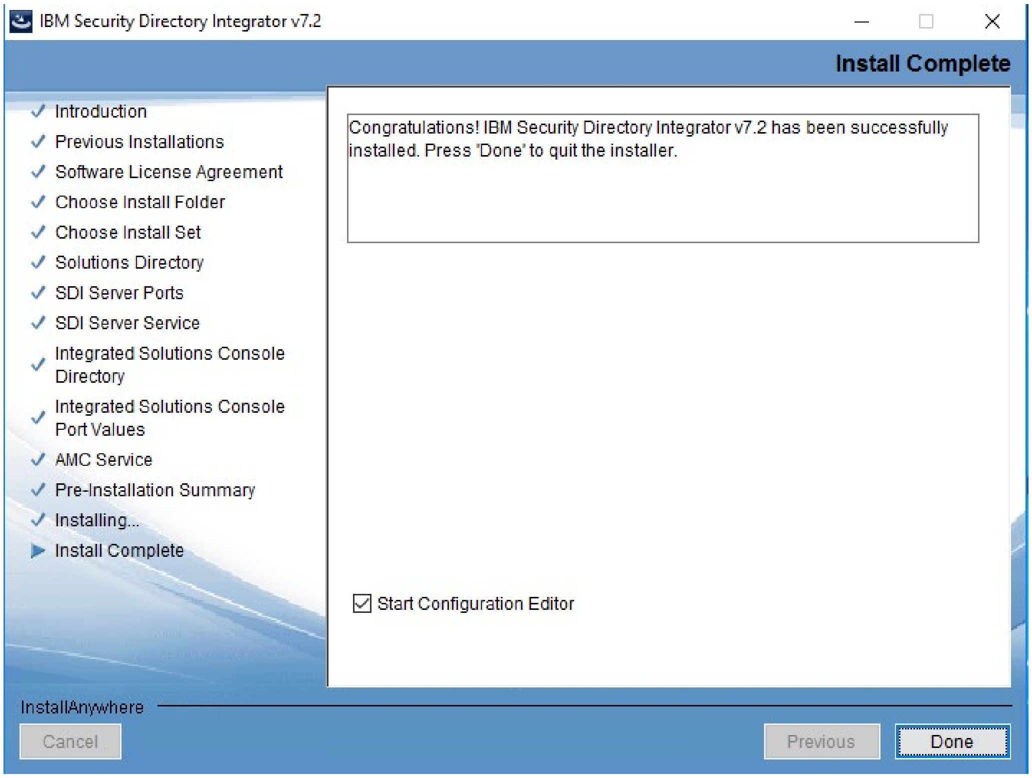
Please Review the Following Before Continuing:

Product Name:
IBM Security Directory Integrator v7.2

Install Folder:
C:\Program Files\IBM\TDI\V7.2

Disk Space Information (for Installation Target):
Required: 829,943,707 Bytes
Available: 11,001,597,952 Bytes

20. Click **Install**. The **Install Complete** panel appears.



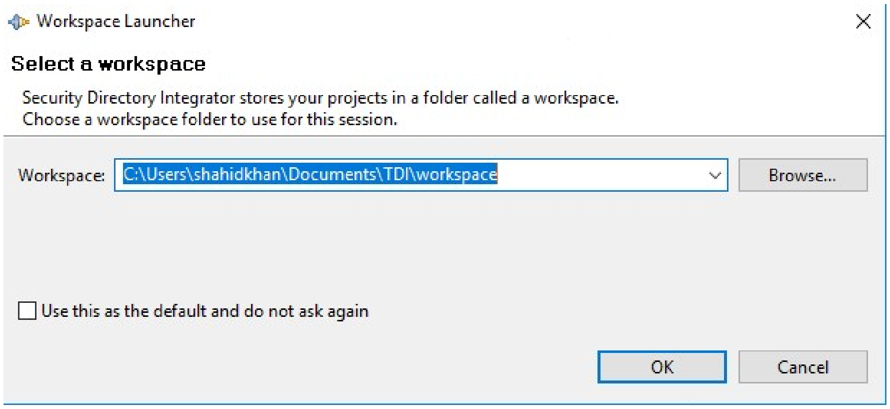
IBM Security Directory Integrator v7.2

Install Complete

Congratulations! IBM Security Directory Integrator v7.2 has been successfully installed. Press 'Done' to quit the installer.

☑ Start Configuration Editor

21. Click **Done**. The Security Directory Integrator 7.2 is installed successfully. The **Workspace Launcher** dialog box appears.



Workspace Launcher

Select a workspace

Security Directory Integrator stores your projects in a folder called a workspace.
Choose a workspace folder to use for this session.

Workspace: C:\Users\shahidkhan\Documents\TDI\workspace

□ Use this as the default and do not ask again

22. Click **Cancel**.

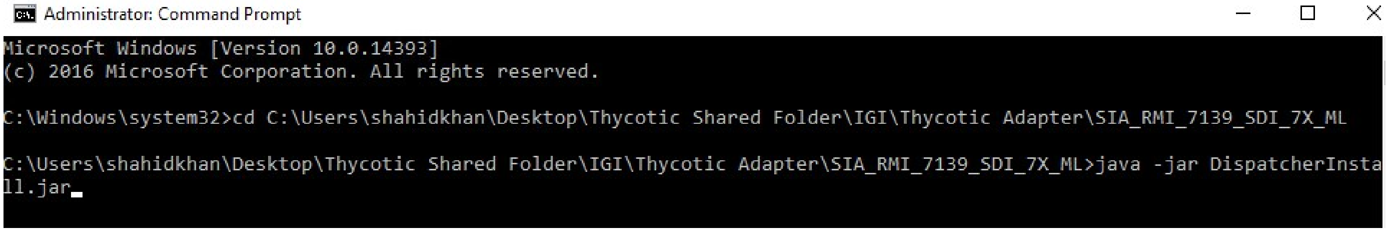
23. Go to C:\Program Files\IBM\TDI\V7.2. This is the **Security Directory Integrator 7.2** folder.

Installing Tivoli Dispatcher

You must install the Tivoli Dispatcher using the **IBM Security Identity Adapter** wizard. The Tivoli Dispatcher is a Security Directory Integrator component that enables the IGI to communicate with IBM Security Directory Integrator.

To install Tivoli Dispatcher:

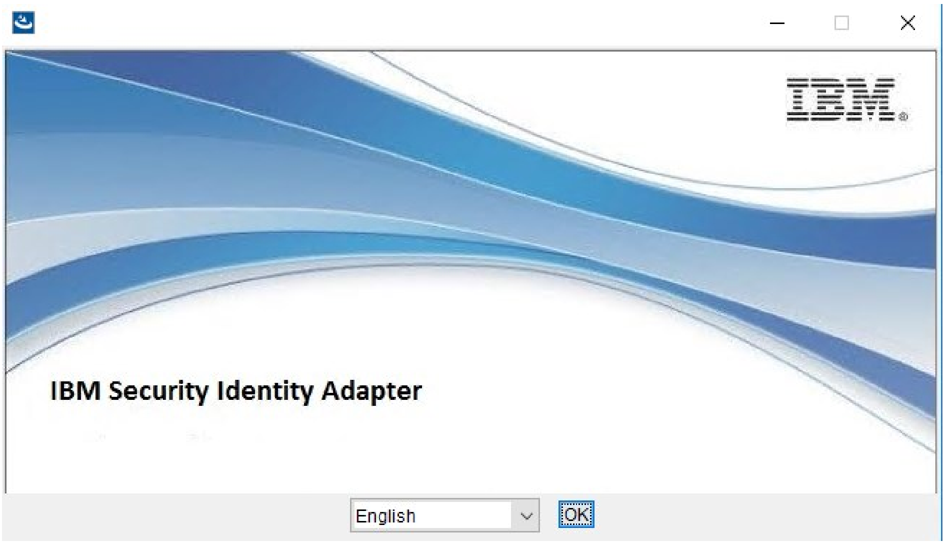
1. Go to the **Thycotic Shared Folder** > **IGI** > **Thycotic Adapter** > **SIA_RMI_7139_SDI_7X_ML**.
2. In the **Widnows Search** box type cmd. The results are auto-populated. Right-click **Command Prompt** and click **Run as administrator**.
3. In the **User Account Control** dialog box, click **Yes**.



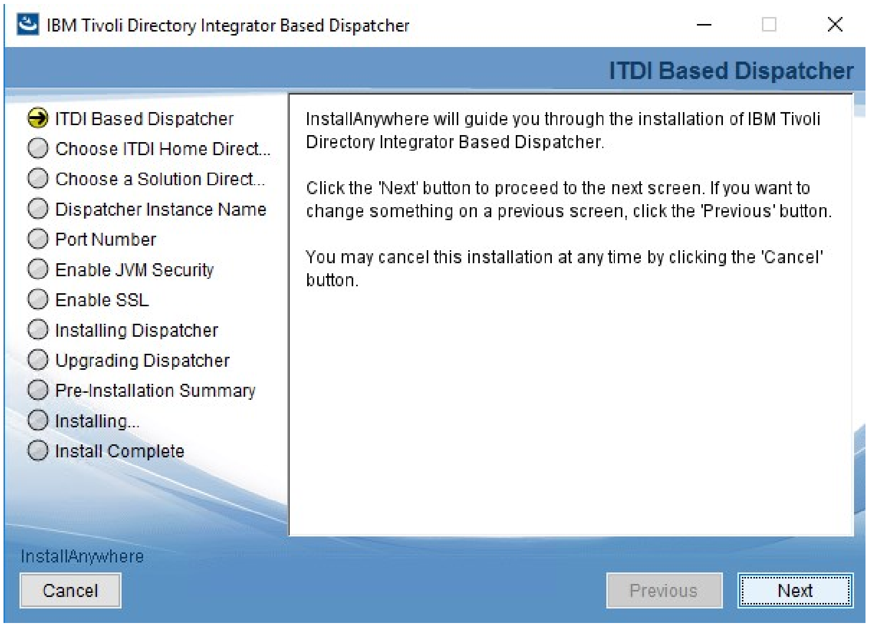
Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\shahidkhan\Desktop\Thycotic Shared Folder\IGI\Thycotic Adapter\SIA_RMI_7139_SDI_7X_ML

C:\Users\shahidkhan\Desktop\Thycotic Shared Folder\IGI\Thycotic Adapter\SIA_RMI_7139_SDI_7X_ML>java -jar DispatcherInsta
ll.jar_
```

4. In the **Command Prompt** type the following: cd <path where the DispatcherInstall is located> and press **Enter**.
5. In the **Command Prompt** then type the following: Java -jar DispatcherInstall.jar
   and press **Enter**. The **IBM Security Identity Adapter** wizard appears.



6. Click **OK**. The **ITDI Based Dispatcher** panel appears.

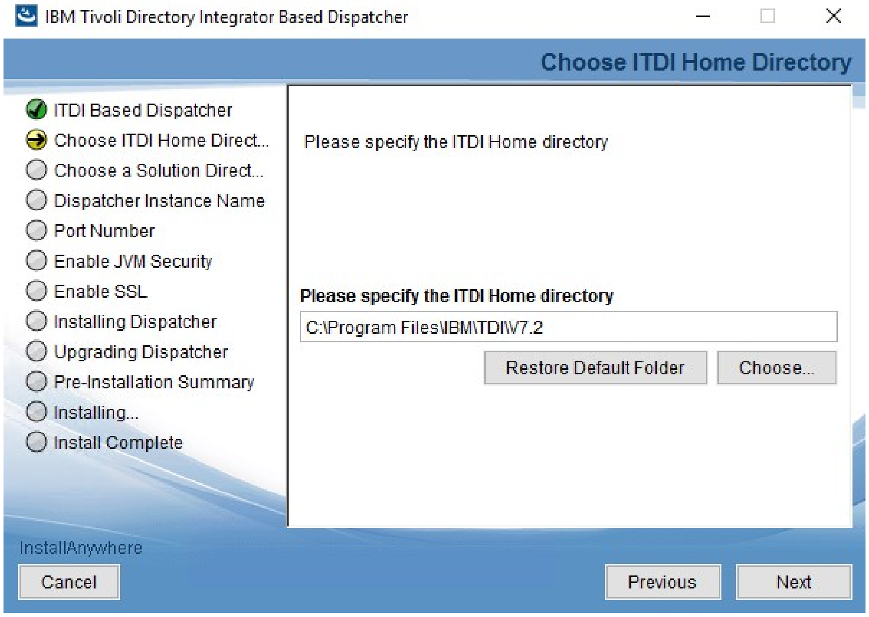


InstallAnywhere will guide you through the installation of IBM Tivoli Directory Integrator Based Dispatcher.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

7. Click **Next**. The **Choose ITDI Home Directory** panel appears.

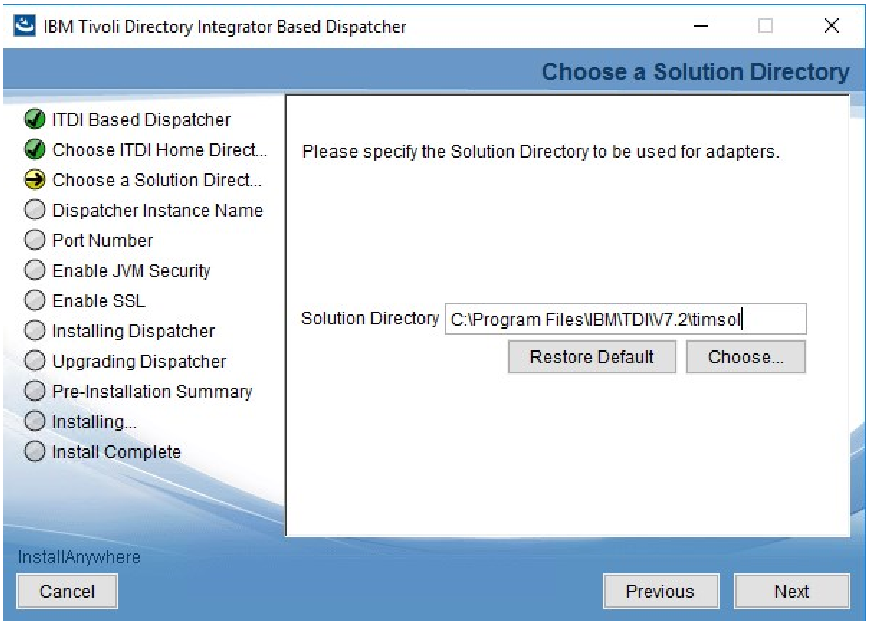


Please specify the ITDI Home directory

Please specify the ITDI Home directory

C:\Program Files\IBM\TDI\V7.2

8. Click **Choose** to select Security Directory Integrator path and click **Next**. The **Choose a Solution Directory** panel appears.

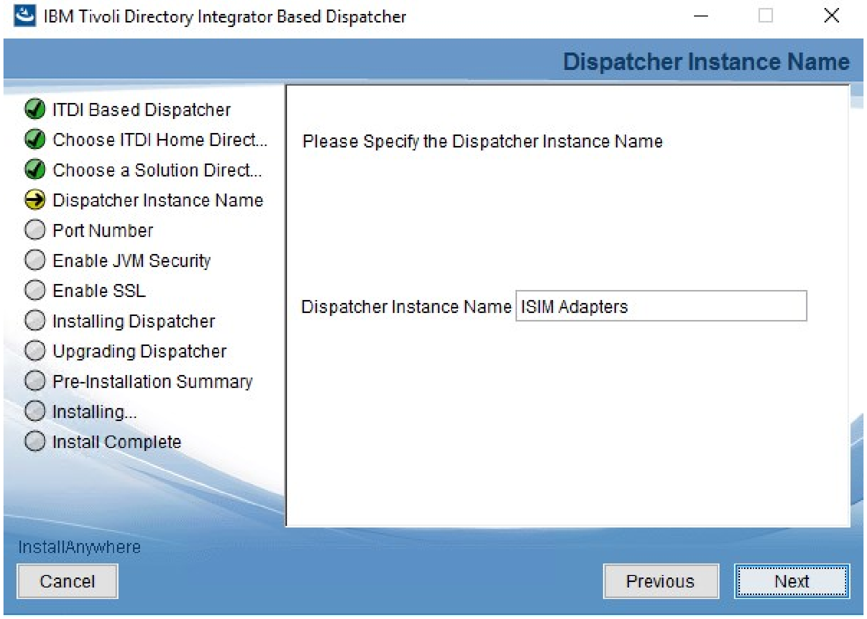


Please specify the Solution Directory to be used for adapters.

Solution Directory: C:\Program Files\IBM\TDI\V7.2\timsol

9. Add \timsol to the ITDI Home Directory and click **Next**. The **Dispatcher Instance Name** panel appears.

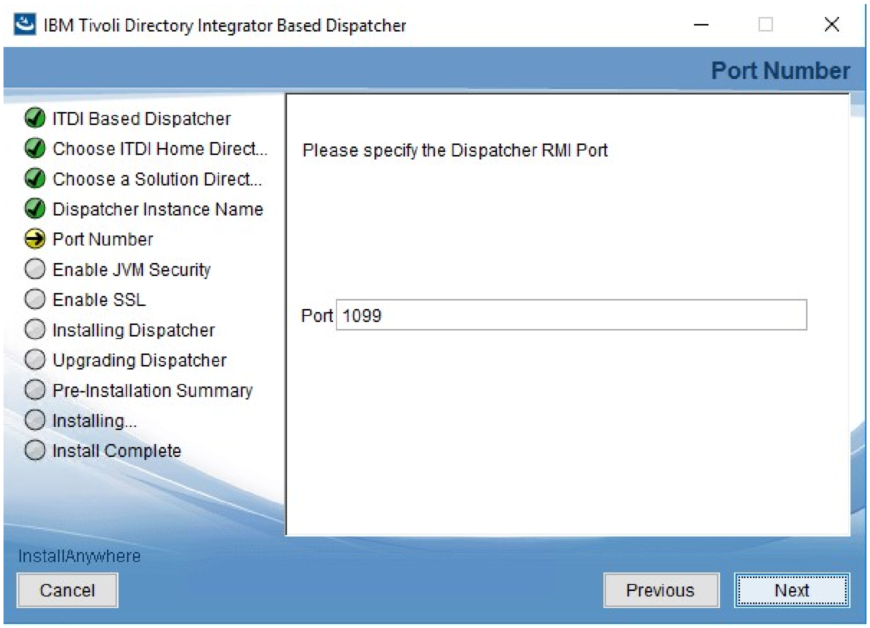
   Note: Timsol is the folder where all the Tivoli directory integrator based dispatcher file is placed.



Please Specify the Dispatcher Instance Name

Dispatcher Instance Name: ISIM Adapters

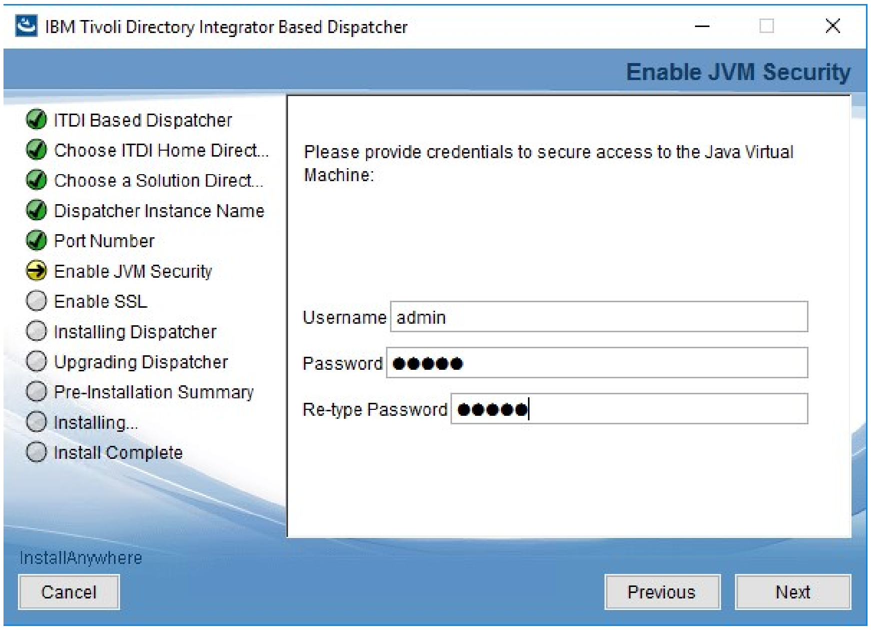
10. Click **Next**. The **Port Number** panel appears.



Please specify the Dispatcher RMI Port

Port 1099

11. Click **Next**. The **Enable JVM Security** panel appears.



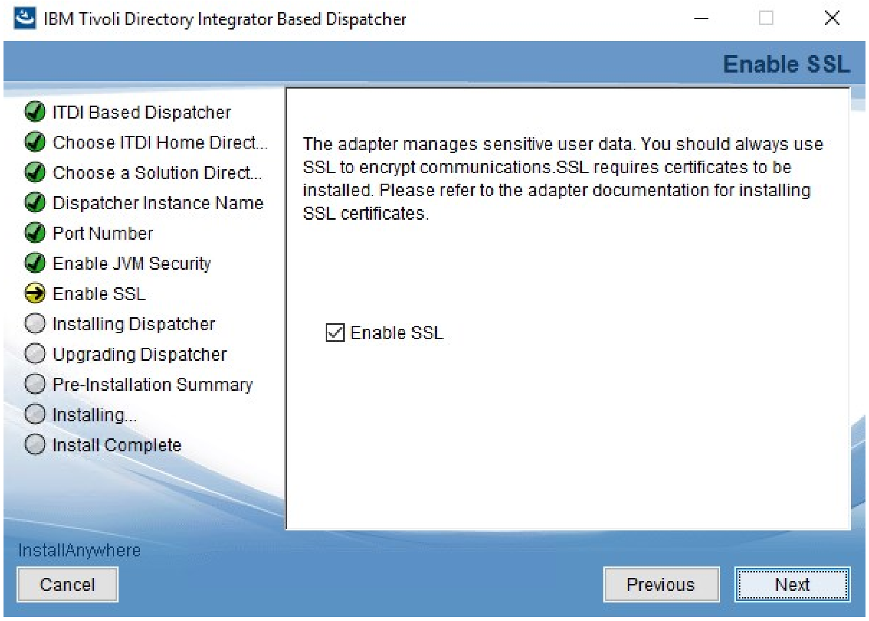
Please provide credentials to secure access to the Java Virtual Machine:

Username admin

Password ●●●●●

Re-type Password ●●●●●

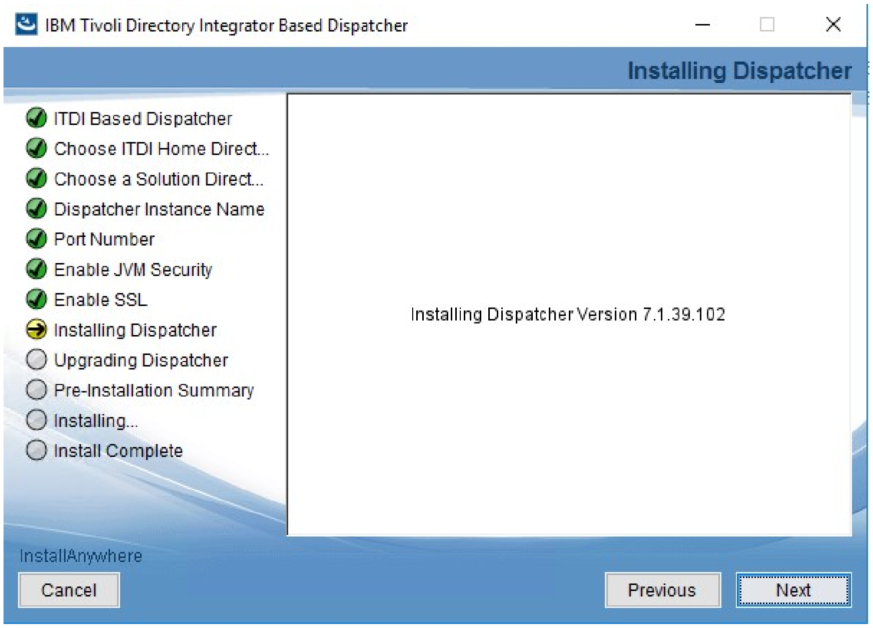
12. Type username, password, re-type password and click **Next**. The **Enable SSL** panel appears.



The adapter manages sensitive user data. You should always use SSL to encrypt communications.SSL requires certificates to be installed. Please refer to the adapter documentation for installing SSL certificates.

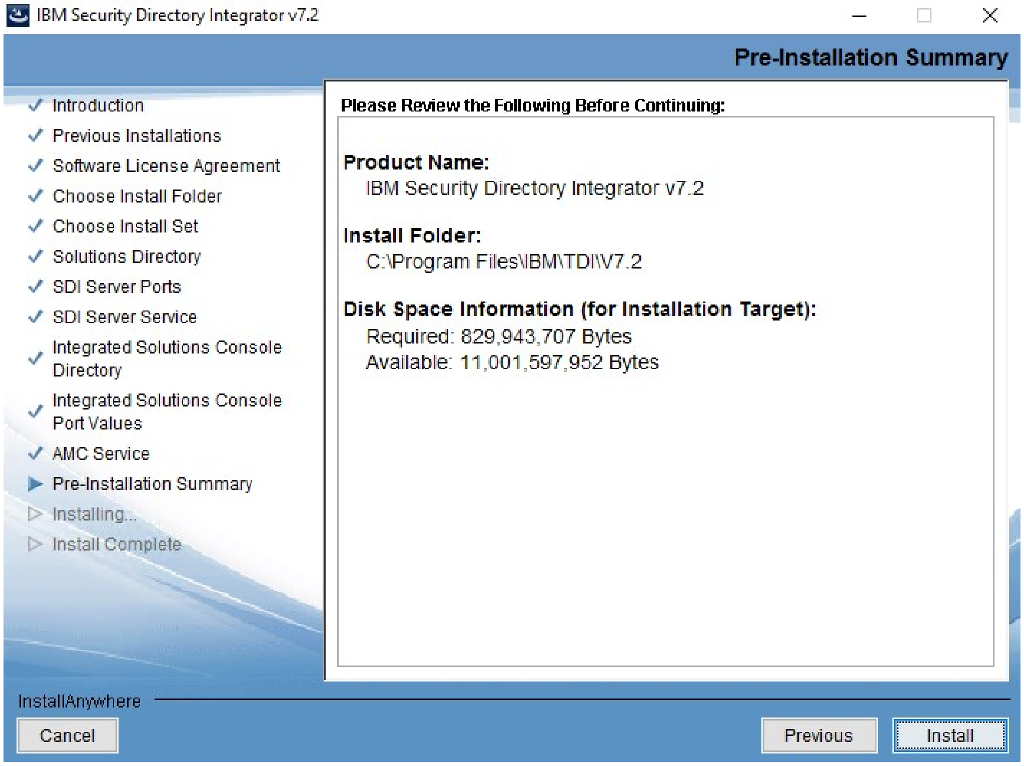
☑ Enable SSL

13. Click **Next**. The **Installing Dispatcher** panel appears.



Installing Dispatcher Version 7.1.39.102

14. Click **Next**. The **Pre-Installation Summary** panel appears.



IBM Security Directory Integrator v7.2

Pre-Installation Summary

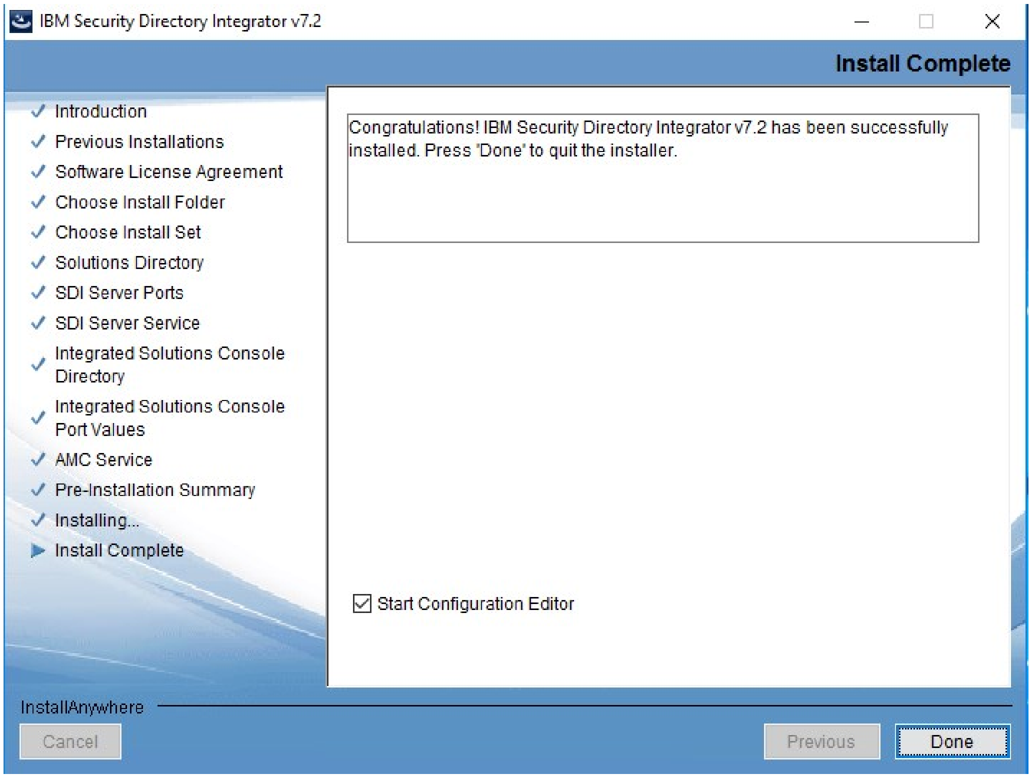
Please Review the Following Before Continuing:

Product Name:
IBM Security Directory Integrator v7.2

Install Folder:
C:\Program Files\IBM\TDI\V7.2

Disk Space Information (for Installation Target):
Required: 829,943,707 Bytes
Available: 11,001,597,952 Bytes

15. Click **Install**.



IBM Security Directory Integrator v7.2

Install Complete

Congratulations! IBM Security Directory Integrator v7.2 has been successfully installed. Press 'Done' to quit the installer.

☑ Start Configuration Editor

16. In the **Install Complete** panel, click **Done**. The Security Directory Integrator is installed.

17. To verify the installation, go to C:\Program Files\IBM\TDI\V7.2 and verify if the timsol folder is created.

18. In the **Search** box type services. The results are auto-populated.

19. Click Services. Verify if the **IBM Security Directory Integrator (ISIM Adapters)** service is running.

Configuration

The following are steps to integrate IBM IGI with Secret Server, please follow the steps in the following order to configure IBM IGI for Secret Server.

1. Configuring IBM IGI GUI and Dispatcher Folder to Access Admin Console.
2. Check the validity of the Tivoli Directory Integrator certificate.
3. Manage Host file.
4. Integrate Secret Server with IBM IGI Admin Console.
5. Configure the connector.
6. Update user details in Secret Server through IBM IGI.
7. Verifying the Integration.

Configuring IBM IGI GUI and Dispatcher Folder to Access Admin Console

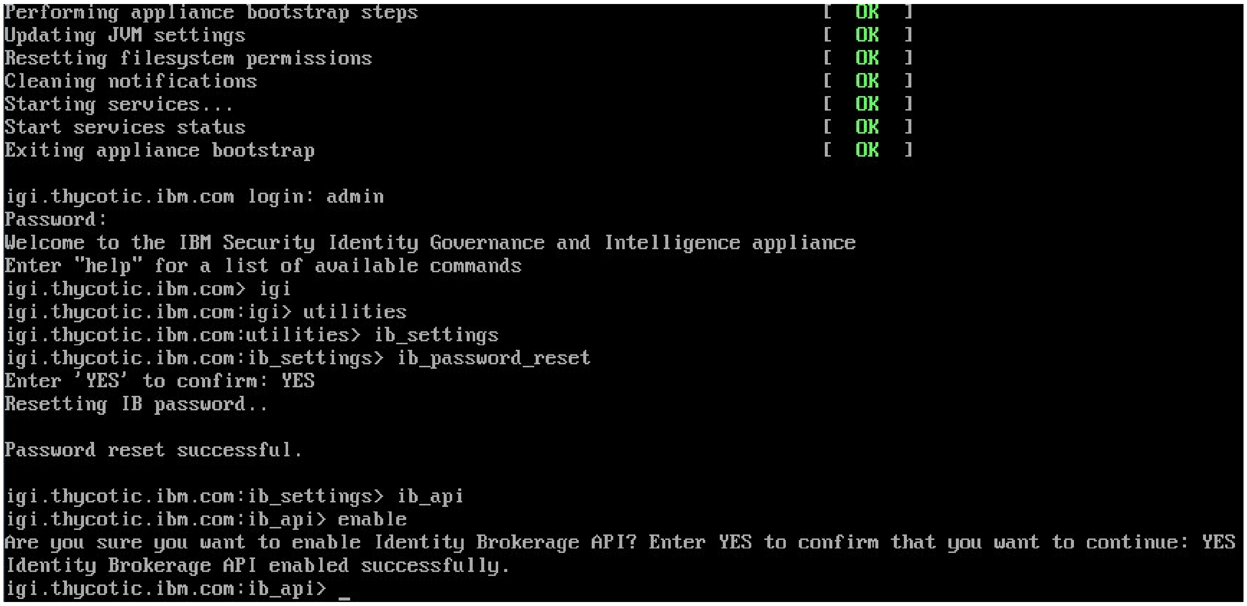
You need to configure IBM IGI GUI and Timsol to establish connection with Secret Server.

Update files in folders

You have to update the files in folders such as Connectors, Axix2, Others, and Timsol.

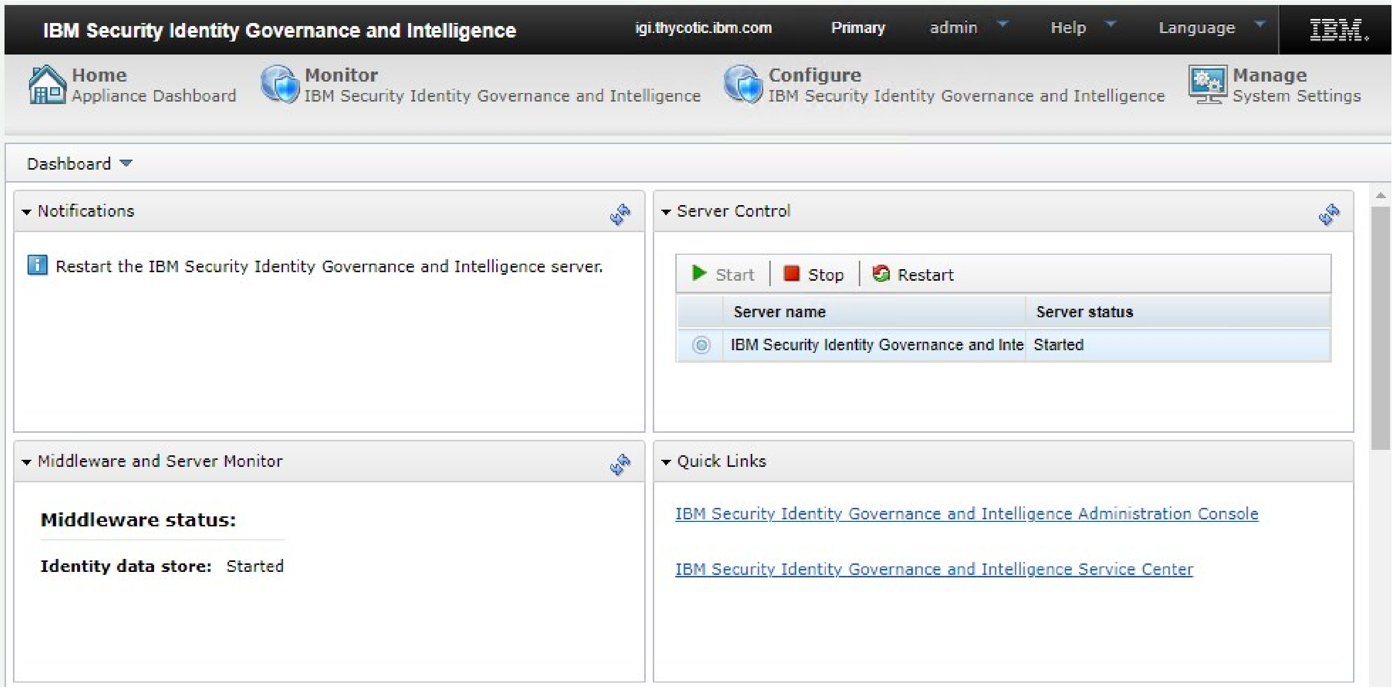
To update the files in folders:

1. Go to the virtual appliance.



```
Performing appliance bootstrap steps                                  [  OK  ]
Updating JVM settings                                                 [  OK  ]
Resetting filesystem permissions                                      [  OK  ]
Cleaning notifications                                                [  OK  ]
Starting services...                                                  [  OK  ]
Start services status                                                 [  OK  ]
Exiting appliance bootstrap                                           [  OK  ]

igi.thycotic.ibm.com login: admin
Password:
Welcome to the IBM Security Identity Governance and Intelligence appliance
Enter "help" for a list of available commands
igi.thycotic.ibm.com> igi
igi.thycotic.ibm.com:igi> utilities
igi.thycotic.ibm.com:utilities> ib_settings
igi.thycotic.ibm.com:ib_settings> ib_password_reset
Enter 'YES' to confirm: YES
Resetting IB password..

Password reset successful.

igi.thycotic.ibm.com:ib_settings> ib_api
igi.thycotic.ibm.com:ib_api> enable
Are you sure you want to enable Identity Brokerage API? Enter YES to confirm that you want to continue: YES
Identity Brokerage API enabled successfully.
igi.thycotic.ibm.com:ib_api> _
```

2. Login using the **login** and **Password**.
3. Type the command igi and press **Enter**.
4. Type the command utilities and press **Enter**.
5. Type the command ib_settings and press **Enter**.
6. Type the command ib_password_reset and press **Enter**.
7. Type YES to confirm password reset and press **Enter**. The password reset is successful.
8. Type the command ib_api and press **Enter**.
9. Type the command enable and press **Enter**
10. Type YES if you are sure you want to enable Identity Brokerage API.
11. Go to **IBM Security Identity Governance and Intelligence Appliance** dashboard.


IBM Security Identity Governance and Intelligence
igi.thycotic.ibm.com
Primary
admin
Help
Language
IBM.
Home
Appliance Dashboard
Monitor
IBM Security Identity Governance and Intelligence
Configure
IBM Security Identity Governance and Intelligence
Manage
System Settings
Dashboard
Notifications
Server Control
Start
Stop
Restart
Middleware and Server Monitor
Quick Links

Restart the IBM Security Identity Governance and Intelligence server.

Server name	Server status
IBM Security Identity Governance and Inte	Started

Middleware status:

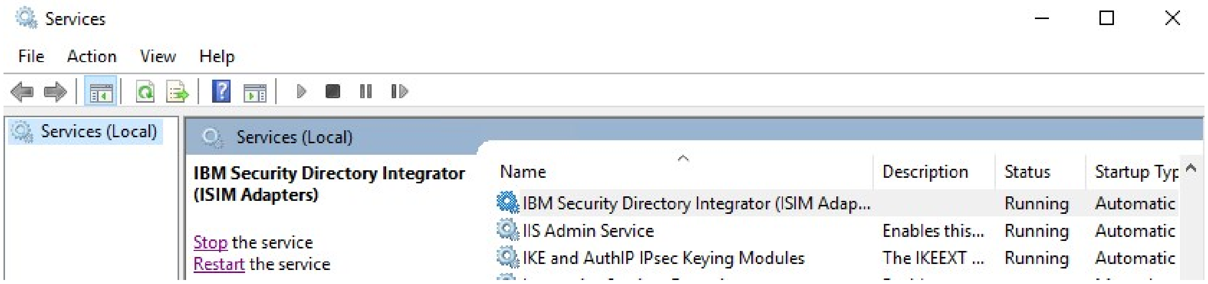
Identity data store: Started

IBM Security Identity Governance and Intelligence Administration Console

IBM Security Identity Governance and Intelligence Service Center

12. In the **Server Control** area, select the server and click **Restart**.

13. In the **Windows Search** box type services. The results are auto-populated. Click **Services**. The **Services** window appears.



IBM Security Directory Integrator (ISIM Adapters)

Stop the service
Restart the service

Name	Description	Status	Startup Typ
IBM Security Directory Integrator (ISIM Adap...		Running	Automatic
IIS Admin Service	Enables this...	Running	Automatic
IKE and AuthIP IPsec Keying Modules	The IKEEXT ...	Running	Automatic

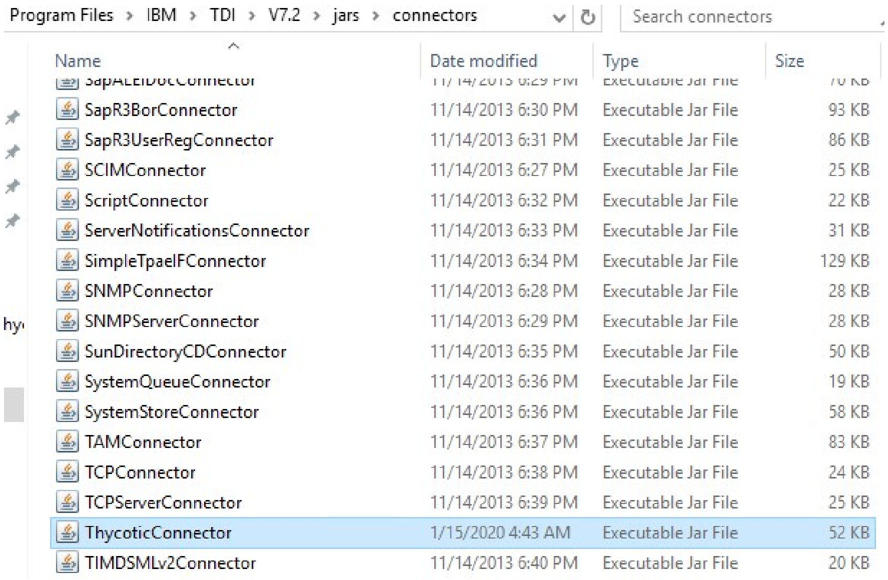
14. Verify if the **IBM Security Directory Integrator (ISIM Adapters)** service is running.

15. Open the Thycotic Adapter integration files and navigate to **Thycotic Adapter | SIA_V7.1.5_SSS_Thycotic_Sec_Serv**.

16. Copy the ThycoticConnector file.

17. On the server hosting IGI navigate to C:\Program Files\IBM\TDI\V7.2\jars\connectors and paste the ThycoticConnector file.

    Note: Stop the **IBM Security Directory Integrator** service before pasting the file.



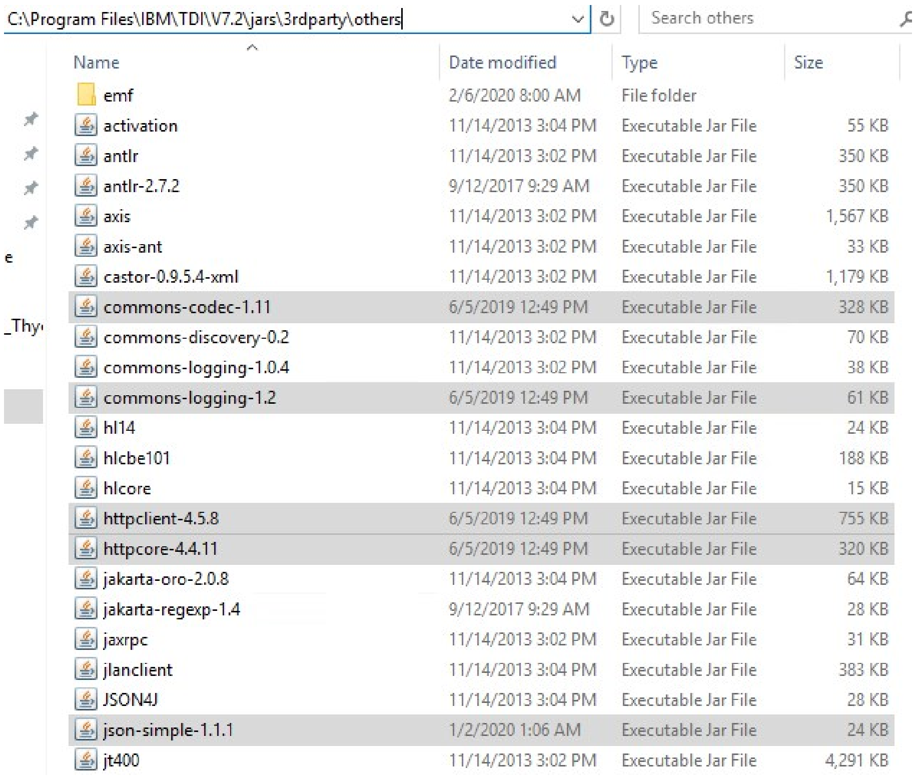
Name	Date modified	Type	Size
SapALEIDocConnector	11/14/2013 6:29 PM	Executable Jar File	70 KB
SapR3BorConnector	11/14/2013 6:30 PM	Executable Jar File	93 KB
SapR3UserRegConnector	11/14/2013 6:31 PM	Executable Jar File	86 KB
SCIMConnector	11/14/2013 6:27 PM	Executable Jar File	25 KB
ScriptConnector	11/14/2013 6:32 PM	Executable Jar File	22 KB
ServerNotificationsConnector	11/14/2013 6:33 PM	Executable Jar File	31 KB
SimpleTpaelFConnector	11/14/2013 6:34 PM	Executable Jar File	129 KB
SNMPConnector	11/14/2013 6:28 PM	Executable Jar File	28 KB
SNMPServerConnector	11/14/2013 6:29 PM	Executable Jar File	28 KB
SunDirectoryCDConnector	11/14/2013 6:35 PM	Executable Jar File	50 KB
SystemQueueConnector	11/14/2013 6:36 PM	Executable Jar File	19 KB
SystemStoreConnector	11/14/2013 6:36 PM	Executable Jar File	58 KB
TAMConnector	11/14/2013 6:37 PM	Executable Jar File	83 KB
TCPConnector	11/14/2013 6:38 PM	Executable Jar File	24 KB
TCPServerConnector	11/14/2013 6:39 PM	Executable Jar File	25 KB
ThycoticConnector	1/15/2020 4:43 AM	Executable Jar File	52 KB
TIMDSMLv2Connector	11/14/2013 6:40 PM	Executable Jar File	20 KB

18. Download the following files:

    - Commons Codec: http://commons.apache.org/proper/commons-codec/
    - Commons Logging: http://commons.apache.org/proper/commons-logging/
    - Http Client: https://hc.apache.org/downloads.cgi
    - Http Core: https://hc.apache.org/downloads.cgi
    - Json Simple: https://mvnrepository.com/artifact/com.googlecode.json-simple/json-simple/1.1.1

19. Go to C:\Program Files\IBM\TDI\V7.2\jars\3rdparty\others and paste the following files here:

    - commons-codec-1.11
    - commons-logging-1.2
    - httpclient-4.5.8
    - httpcore-4.4.11
    - json-simple-1.1.1



C:\Program Files\IBM\TDI\V7.2\jars\3rdparty\others

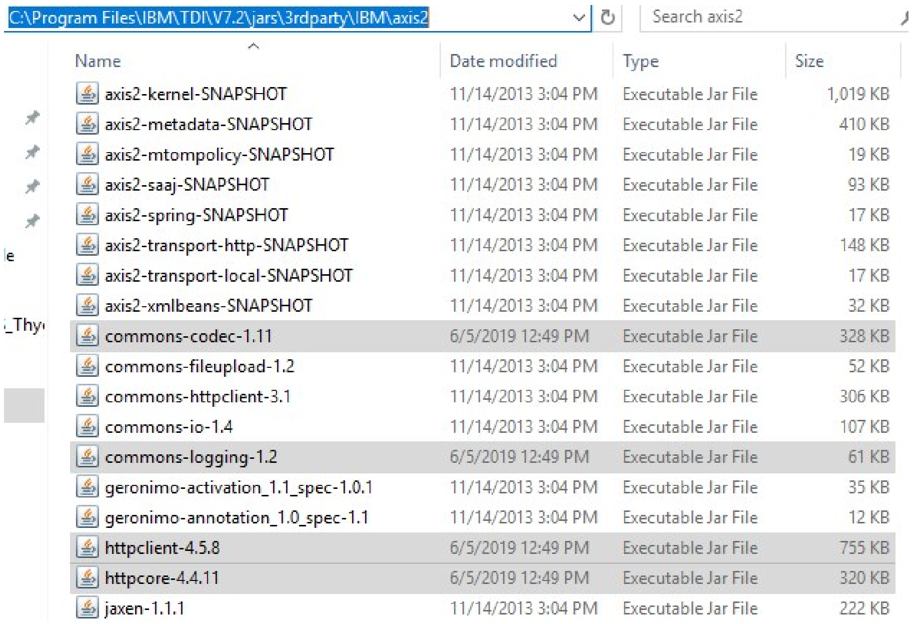
Name	Date modified	Type	Size
emf	2/6/2020 8:00 AM	File folder	
activation	11/14/2013 3:04 PM	Executable Jar File	55 KB
antlr	11/14/2013 3:02 PM	Executable Jar File	350 KB
antlr-2.7.2	9/12/2017 9:29 AM	Executable Jar File	350 KB
axis	11/14/2013 3:02 PM	Executable Jar File	1,567 KB
axis-ant	11/14/2013 3:02 PM	Executable Jar File	33 KB
castor-0.9.5.4-xml	11/14/2013 3:02 PM	Executable Jar File	1,179 KB
commons-codec-1.11	6/5/2019 12:49 PM	Executable Jar File	328 KB
commons-discovery-0.2	11/14/2013 3:02 PM	Executable Jar File	70 KB
commons-logging-1.0.4	11/14/2013 3:02 PM	Executable Jar File	38 KB
commons-logging-1.2	6/5/2019 12:49 PM	Executable Jar File	61 KB
hl14	11/14/2013 3:04 PM	Executable Jar File	24 KB
hlcbe101	11/14/2013 3:04 PM	Executable Jar File	188 KB
hlcore	11/14/2013 3:04 PM	Executable Jar File	15 KB
httpclient-4.5.8	6/5/2019 12:49 PM	Executable Jar File	755 KB
httpcore-4.4.11	6/5/2019 12:49 PM	Executable Jar File	320 KB
jakarta-oro-2.0.8	11/14/2013 3:04 PM	Executable Jar File	64 KB
jakarta-regexp-1.4	9/12/2017 9:29 AM	Executable Jar File	28 KB
jaxrpc	11/14/2013 3:02 PM	Executable Jar File	31 KB
jlanclient	11/14/2013 3:04 PM	Executable Jar File	383 KB
JSON4J	11/14/2013 3:04 PM	Executable Jar File	28 KB
json-simple-1.1.1	1/2/2020 1:06 AM	Executable Jar File	24 KB
jt400	11/14/2013 3:02 PM	Executable Jar File	4,291 KB

20. Go to C:\Program Files\IBM\TDI\V7.2\jars\3rdparty\IBM\axis2 and delete the existing version of the following files:

- commons-codec
- commons-logging
- httpclient
- httpcore

and paste the latest version of the following files:

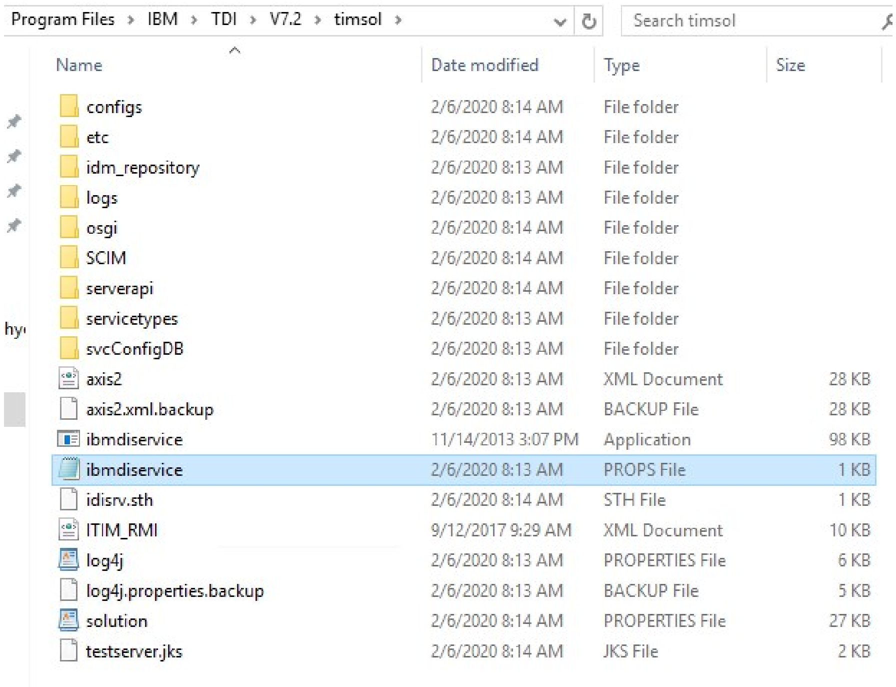
- commons-codec-1.11
- commons-logging-1.2
- httpclient-4.5.8
- httpcore-4.4.11



C:\Program Files\IBM\TDI\V7.2\jars\3rdparty\IBM\axis2

Name	Date modified	Type	Size
axis2-kernel-SNAPSHOT	11/14/2013 3:04 PM	Executable Jar File	1,019 KB
axis2-metadata-SNAPSHOT	11/14/2013 3:04 PM	Executable Jar File	410 KB
axis2-mtompolicy-SNAPSHOT	11/14/2013 3:04 PM	Executable Jar File	19 KB
axis2-saaj-SNAPSHOT	11/14/2013 3:04 PM	Executable Jar File	93 KB
axis2-spring-SNAPSHOT	11/14/2013 3:04 PM	Executable Jar File	17 KB
axis2-transport-http-SNAPSHOT	11/14/2013 3:04 PM	Executable Jar File	148 KB
axis2-transport-local-SNAPSHOT	11/14/2013 3:04 PM	Executable Jar File	17 KB
axis2-xmlbeans-SNAPSHOT	11/14/2013 3:04 PM	Executable Jar File	32 KB
commons-codec-1.11	6/5/2019 12:49 PM	Executable Jar File	328 KB
commons-fileupload-1.2	11/14/2013 3:04 PM	Executable Jar File	52 KB
commons-httpclient-3.1	11/14/2013 3:04 PM	Executable Jar File	306 KB
commons-io-1.4	11/14/2013 3:04 PM	Executable Jar File	107 KB
commons-logging-1.2	6/5/2019 12:49 PM	Executable Jar File	61 KB
geronimo-activation_1.1_spec-1.0.1	11/14/2013 3:04 PM	Executable Jar File	35 KB
geronimo-annotation_1.0_spec-1.1	11/14/2013 3:04 PM	Executable Jar File	12 KB
httpclient-4.5.8	6/5/2019 12:49 PM	Executable Jar File	755 KB
httpcore-4.4.11	6/5/2019 12:49 PM	Executable Jar File	320 KB
jaxen-1.1.1	11/14/2013 3:04 PM	Executable Jar File	222 KB

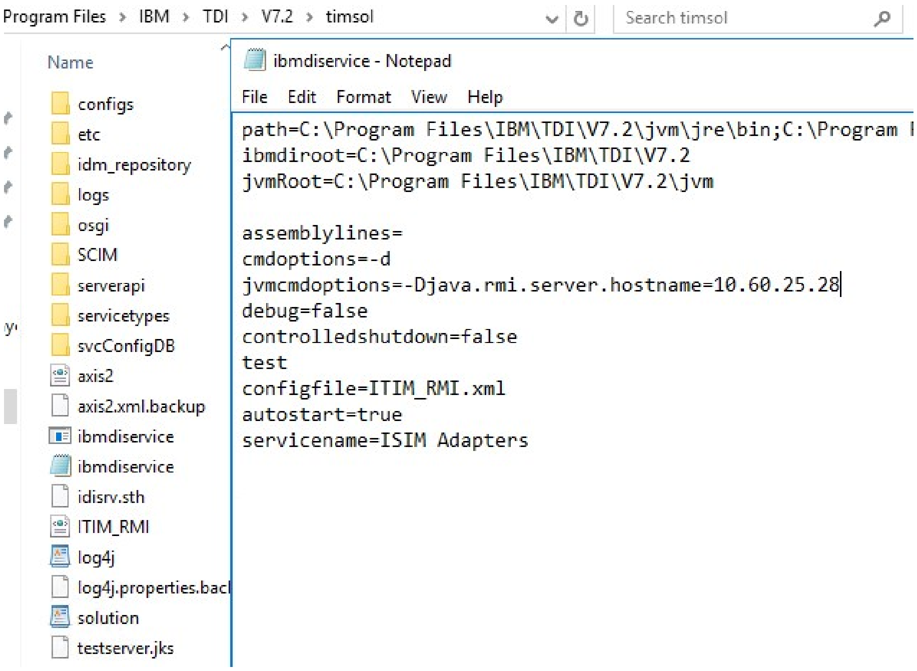
21. Go to C:\Program Files\IBM\TDI\V7.2\timsol.



Program Files › IBM › TDI › V7.2 › timsol ›

Name	Date modified	Type	Size
configs	2/6/2020 8:14 AM	File folder	
etc	2/6/2020 8:14 AM	File folder	
idm_repository	2/6/2020 8:13 AM	File folder	
logs	2/6/2020 8:13 AM	File folder	
osgi	2/6/2020 8:14 AM	File folder	
SCIM	2/6/2020 8:14 AM	File folder	
serverapi	2/6/2020 8:14 AM	File folder	
servicetypes	2/6/2020 8:13 AM	File folder	
svcConfigDB	2/6/2020 8:13 AM	File folder	
axis2	2/6/2020 8:13 AM	XML Document	28 KB
axis2.xml.backup	2/6/2020 8:13 AM	BACKUP File	28 KB
ibmdiservice	11/14/2013 3:07 PM	Application	98 KB
ibmdiservice	2/6/2020 8:13 AM	PROPS File	1 KB
idisrv.sth	2/6/2020 8:14 AM	STH File	1 KB
ITIM_RMI	9/12/2017 9:29 AM	XML Document	10 KB
log4j	2/6/2020 8:13 AM	PROPERTIES File	6 KB
log4j.properties.backup	2/6/2020 8:13 AM	BACKUP File	5 KB
solution	2/6/2020 8:14 AM	PROPERTIES File	27 KB
testserver.jks	2/6/2020 8:14 AM	JKS File	2 KB

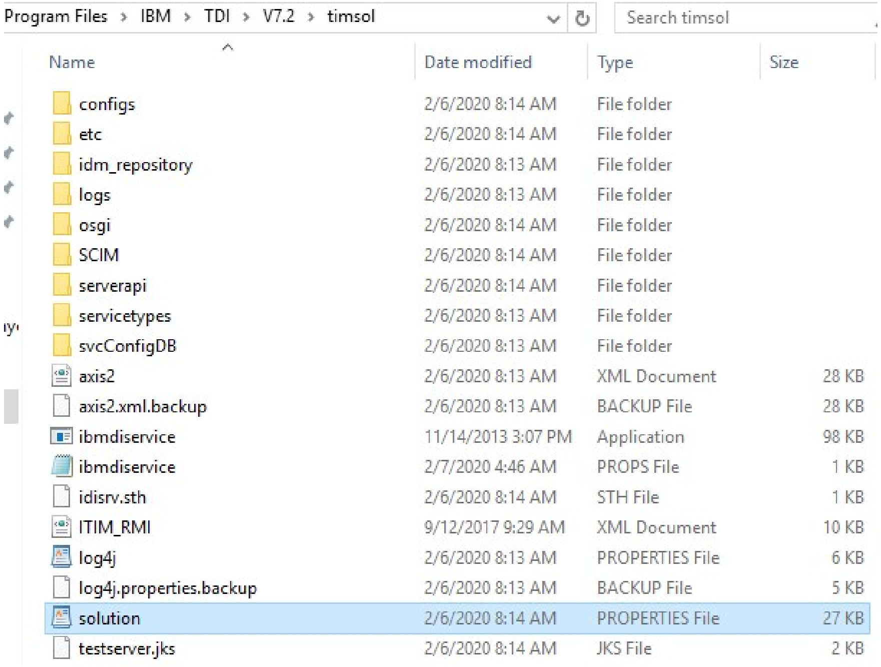
22. Select the ibmdiservice file and open it in Notepad in administrative mode.



```
path=C:\Program Files\IBM\TDI\V7.2\jvm\jre\bin;C:\Program I
ibmdiroot=C:\Program Files\IBM\TDI\V7.2
jvmRoot=C:\Program Files\IBM\TDI\V7.2\jvm

assemblylines=
cmdoptions=-d
jvmcmdoptions=-Djava.rmi.server.hostname=10.60.25.28
debug=false
controlledshutdown=false
test
configfile=ITIM_RMI.xml
autostart=true
servicename=ISIM Adapters
```

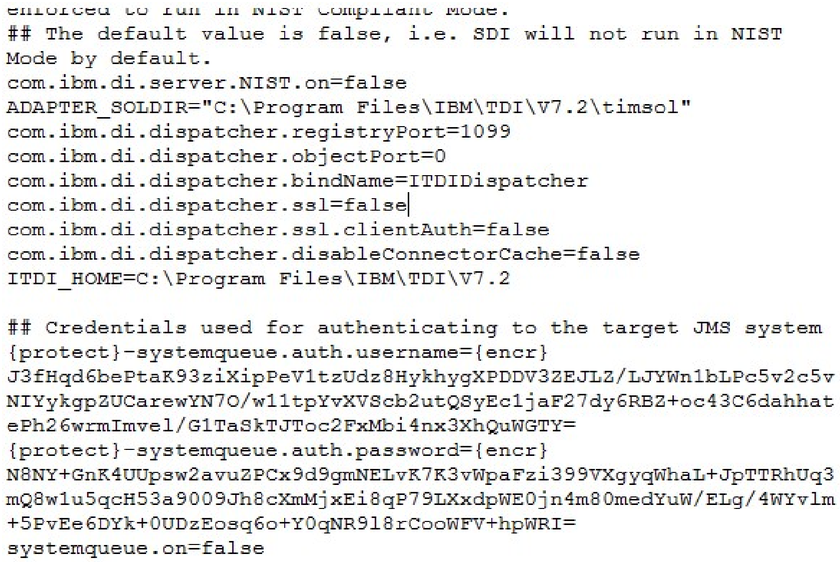
23. In the jvmcmdoptions, type -Djava.rmi.server.hostname= <server hostname where Tivoli directory installer is installed and security directory integrator is installed> and save the file.

24. In the Timsol folder, select the solution file and open it Wordpad in administrative mode.



Name	Date modified	Type	Size
configs	2/6/2020 8:14 AM	File folder	
etc	2/6/2020 8:14 AM	File folder	
idm_repository	2/6/2020 8:13 AM	File folder	
logs	2/6/2020 8:13 AM	File folder	
osgi	2/6/2020 8:14 AM	File folder	
SCIM	2/6/2020 8:14 AM	File folder	
serverapi	2/6/2020 8:14 AM	File folder	
servicetypes	2/6/2020 8:13 AM	File folder	
svcConfigDB	2/6/2020 8:13 AM	File folder	
axis2	2/6/2020 8:13 AM	XML Document	28 KB
axis2.xml.backup	2/6/2020 8:13 AM	BACKUP File	28 KB
ibmdiservice	11/14/2013 3:07 PM	Application	98 KB
ibmdiservice	2/7/2020 4:46 AM	PROPS File	1 KB
idisrv.sth	2/6/2020 8:14 AM	STH File	1 KB
ITIM_RMI	9/12/2017 9:29 AM	XML Document	10 KB
log4j	2/6/2020 8:13 AM	PROPERTIES File	6 KB
log4j.properties.backup	2/6/2020 8:13 AM	BACKUP File	5 KB
solution	2/6/2020 8:14 AM	PROPERTIES File	27 KB
testserver.jks	2/6/2020 8:14 AM	JKS File	2 KB

25. In the com.ibm.di.dispatcher.ssl, delete true and type false and save the file.

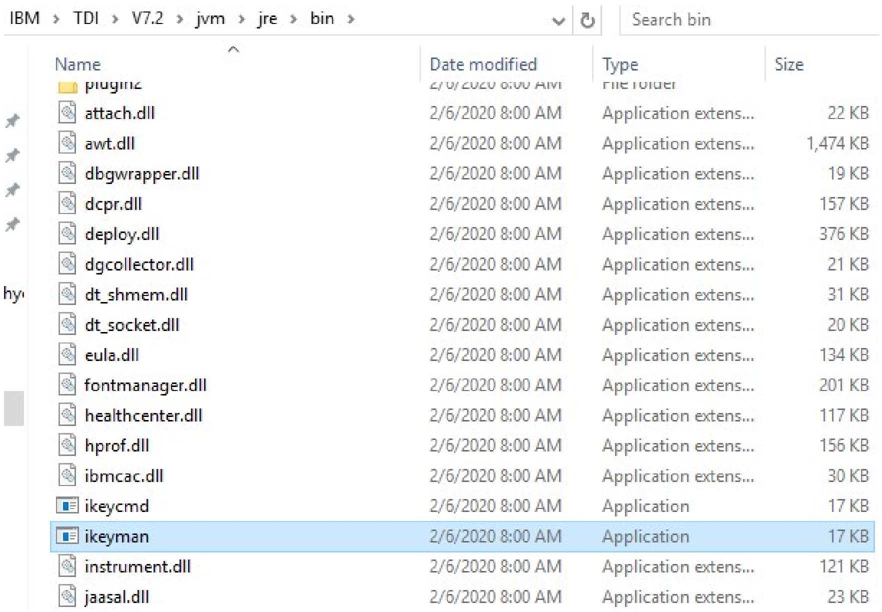


```
enforced to run in NIST compliant mode.
## The default value is false, i.e. SDI will not run in NIST
Mode by default.
com.ibm.di.server.NIST.on=false
ADAPTER_SOLDIR="C:\Program Files\IBM\TDI\V7.2\timsol"
com.ibm.di.dispatcher.registryPort=1099
com.ibm.di.dispatcher.objectPort=0
com.ibm.di.dispatcher.bindName=ITDIDispatcher
com.ibm.di.dispatcher.ssl=false
com.ibm.di.dispatcher.ssl.clientAuth=false
com.ibm.di.dispatcher.disableConnectorCache=false
ITDI_HOME=C:\Program Files\IBM\TDI\V7.2

## Credentials used for authenticating to the target JMS system
{protect}-systemqueue.auth.username={encr}
J3fHqd6bePtaK93ziXipPeV1tzUdz8HykhygXPDDV3ZEJLZ/LJYWn1bLPc5v2c5v
NIYykgpZUCarewYN7O/w11tpYvXVScb2utQSyEc1jaF27dy6RBZ+oc43C6dahhat
ePh26wrmImvel/G1TaSkTJToc2FxMbi4nx3XhQuWGTY=
{protect}-systemqueue.auth.password={encr}
N8NY+GnK4UUpsw2avuZPCx9d9gmNELvK7K3vWpaFzi399VXgyqWhaL+JpTTRhUq3
mQ8w1u5qcH53a9009Jh8cXmMjxEi8qP79LXxdpWE0jn4m80medYuW/ELg/4WYvlm
+5PvEe6DYk+0UDzEosq6o+Y0qNR9l8rCooWFV+hpWRI=
systemqueue.on=false
```

The folders are updated successfully. Now, you need to verify the validity of the certificate.

Check the validity of the Tivoli Directory Integrator certificate

1. Go to C:\Program Files\IBM\TDI\V7.2\jvm\jre\bin.



IBM › TDI › V7.2 › jvm › jre › bin ›

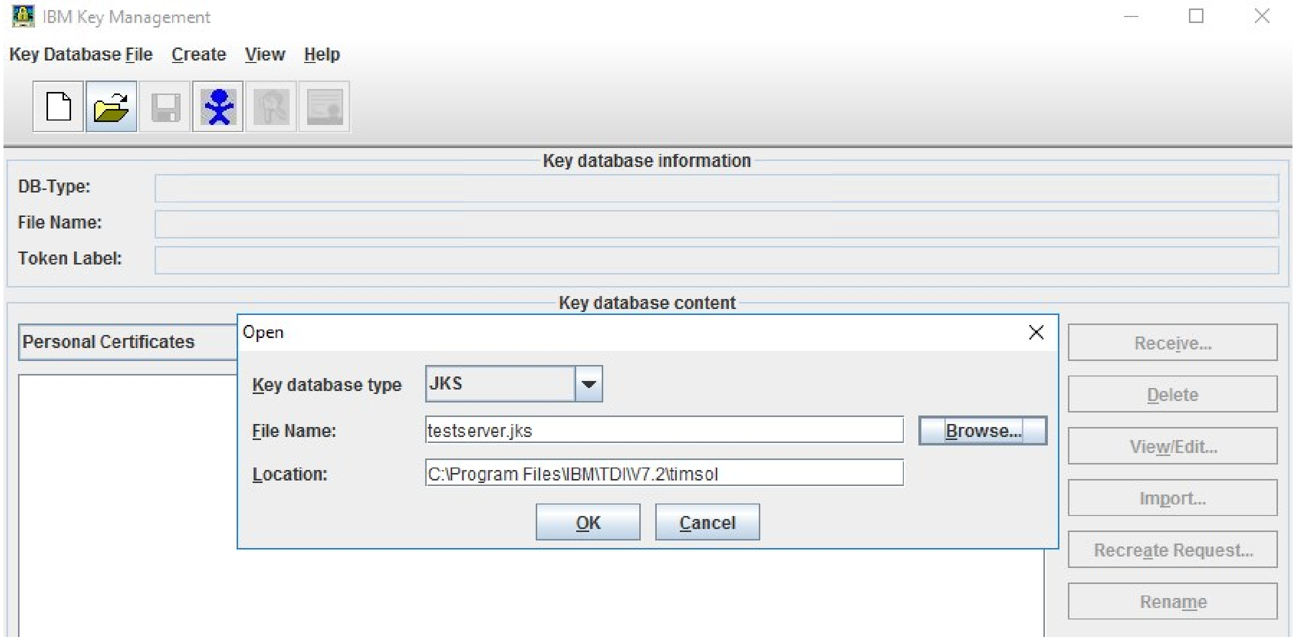
Search bin

Name	Date modified	Type	Size
plugin2	2/6/2020 8:00 AM	File folder	
attach.dll	2/6/2020 8:00 AM	Application extens...	22 KB
awt.dll	2/6/2020 8:00 AM	Application extens...	1,474 KB
dbgwrapper.dll	2/6/2020 8:00 AM	Application extens...	19 KB
dcpr.dll	2/6/2020 8:00 AM	Application extens...	157 KB
deploy.dll	2/6/2020 8:00 AM	Application extens...	376 KB
dgcollector.dll	2/6/2020 8:00 AM	Application extens...	21 KB
dt_shmem.dll	2/6/2020 8:00 AM	Application extens...	31 KB
dt_socket.dll	2/6/2020 8:00 AM	Application extens...	20 KB
eula.dll	2/6/2020 8:00 AM	Application extens...	134 KB
fontmanager.dll	2/6/2020 8:00 AM	Application extens...	201 KB
healthcenter.dll	2/6/2020 8:00 AM	Application extens...	117 KB
hprof.dll	2/6/2020 8:00 AM	Application extens...	156 KB
ibmcac.dll	2/6/2020 8:00 AM	Application extens...	30 KB
ikeycmd	2/6/2020 8:00 AM	Application	17 KB
ikeyman	2/6/2020 8:00 AM	Application	17 KB
instrument.dll	2/6/2020 8:00 AM	Application extens...	121 KB
jaasal.dll	2/6/2020 8:00 AM	Application extens...	23 KB

2. Select ikeyman file, right-click the file and click **Run as administrator**.

3. In the **User Account Control** dialog box, click **Yes**. The **IBM Key Management** dialog box appears.

4. Click **Open** icon. The **Open** dialog box appears.



Key database information

DB-Type:

File Name:

Token Label:

Key database content

Personal Certificates

Open

Key database type: JKS

File Name: testserver.jks

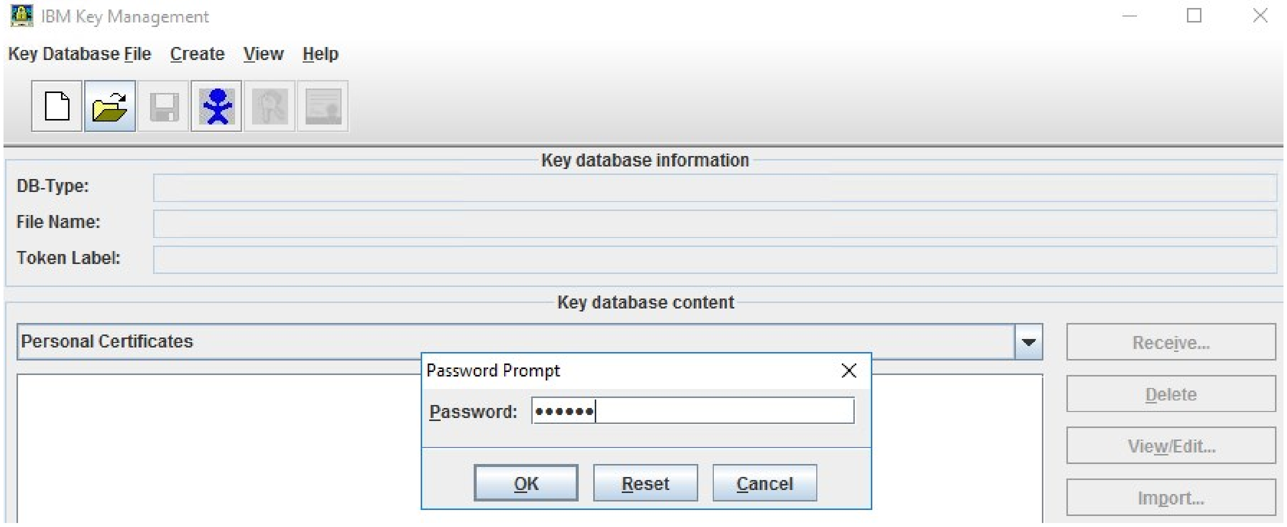
Location: C:\Program Files\IBM\TDI\V7.2\timsol

Browse...

OK Cancel

5. Click **Browse** and navigate to the timsol folder which is located at C:\Program Files\IBM\TDI\V7.2\timsol.

6. In the timsol folder, select the testserver.jks and click **OK**. The **Password Prompt** dialog box appears.

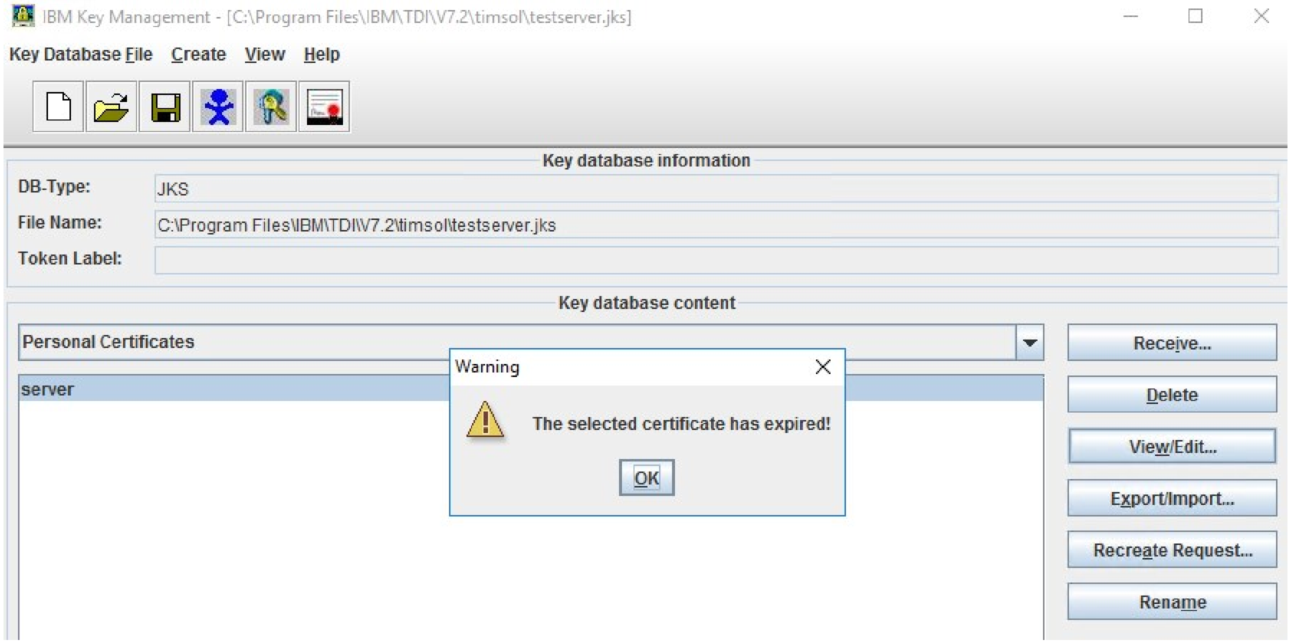


Password: ••••••

7. In the **Password** text box, type the password, and click **OK**.

   **Note:: The default password of testserver.jks is server.

8. On the right-hand side, click **View/Edit**. A Warning '**The selected certificate has expired!**' might appear.



DB-Type: JKS

File Name: C:\Program Files\IBM\TDI\V7.2\timsol\testserver.jks

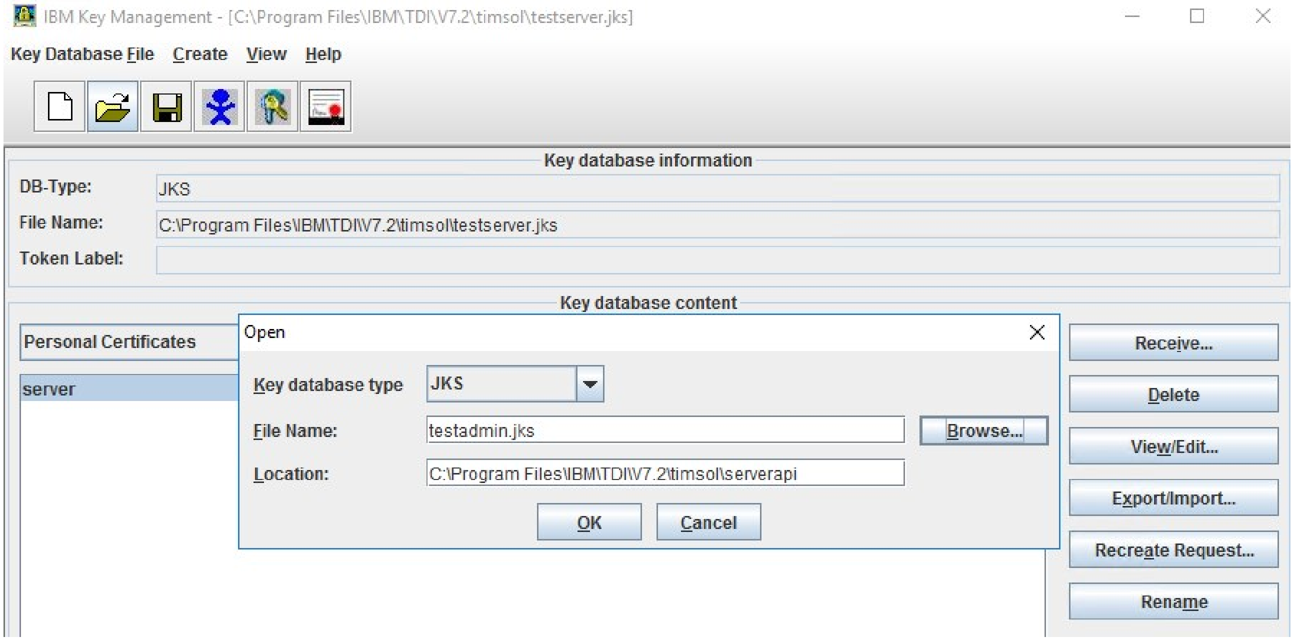
Token Label:

The selected certificate has expired!

9. Click **OK**. The certificate details appear.

10. Click **Open** icon. The **Open** dialog box appears.

11. Navigate to the serverapi folder which is located at C:\Program Files\IBM\TDI\V7.2\timsol\serverapi.



IBM Key Management - [C:\Program Files\IBM\TDI\V7.2\timsol\testserver.jks]

Key database information

DB-Type: JKS

File Name: C:\Program Files\IBM\TDI\V7.2\timsol\testserver.jks

Token Label:

Key database content

Personal Certificates

server

Open

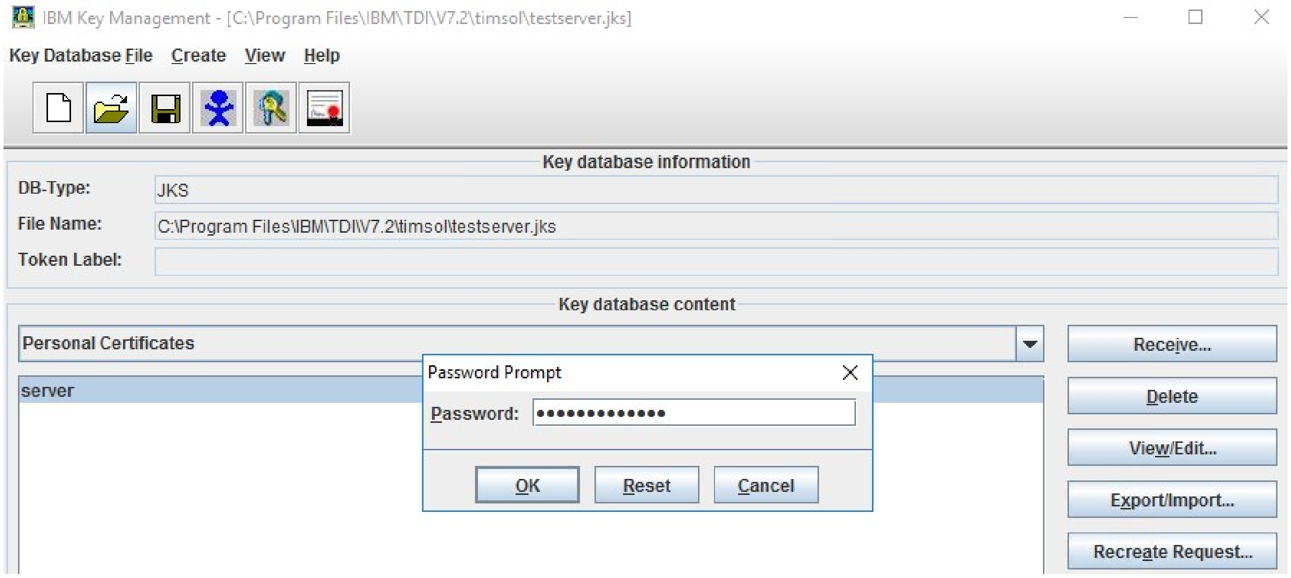
Key database type: JKS

File Name: testadmin.jks

Location: C:\Program Files\IBM\TDI\V7.2\timsol\serverapi

12. Select testadmin.jks and click **Open**.

13. In the **Open dialog** box, click **OK**. The **Password Prompt** dialog box appears.



IBM Key Management - [C:\Program Files\IBM\TDI\V7.2\timsol\testserver.jks]

Key database information

DB-Type: JKS

File Name: C:\Program Files\IBM\TDI\V7.2\timsol\testserver.jks

Token Label:

Key database content

Personal Certificates

server

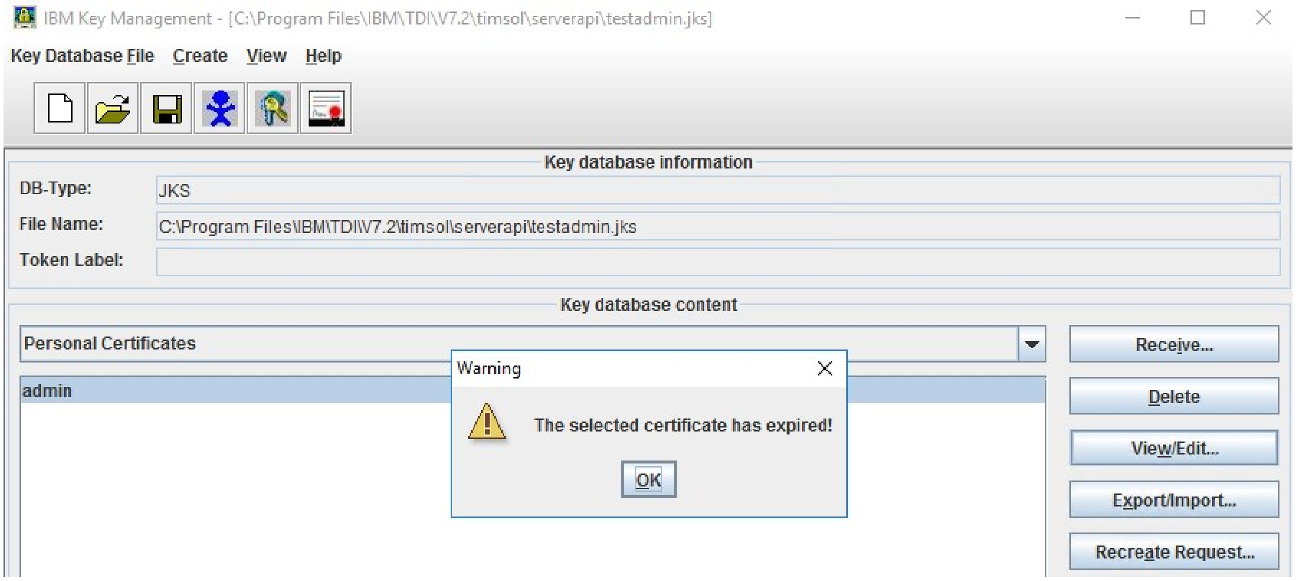
Password Prompt

Password: •••••••••••••

14. In the **Password** text box, type the password, and click **OK**.

    Note: The default password of testserver.jks is administrator.

15. On the right-hand side, click **View/Edit**. A Warning '**The selected certificate has expired!**' might appear. If so, please see further steps for extending the certificate in Troubleshooting



DB-Type: JKS

File Name: C:\Program Files\IBM\TDI\V7.2\timsol\serverapi\testadmin.jks

Token Label:

Personal Certificates

admin

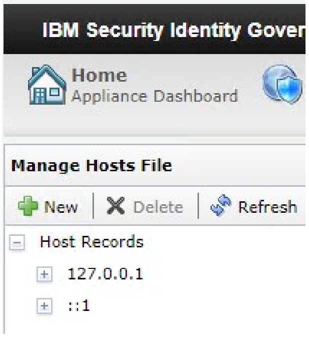
The selected certificate has expired!

Manage Host file

You will need to add the details of the host file for communication between Secret Server and Dispatcher.

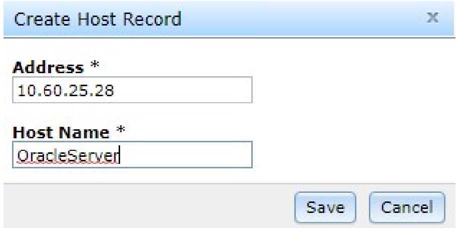
To manage host file:

1. Go to **IBM Security Identity Governance and Intelligence** user interface.
2. Click **Manage System Settings I Network Settings I Hosts File**. The **Manage Hosts File** page appears.



Host Records
- 127.0.0.1
- ::1

3. Click **New** New icon. The **Create Host Record** dialog box appears.

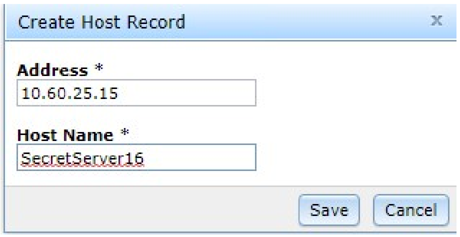


Address *
10.60.25.28

Host Name *
OracleServer

Note: Fields marked with asterisk (*) are mandatory.

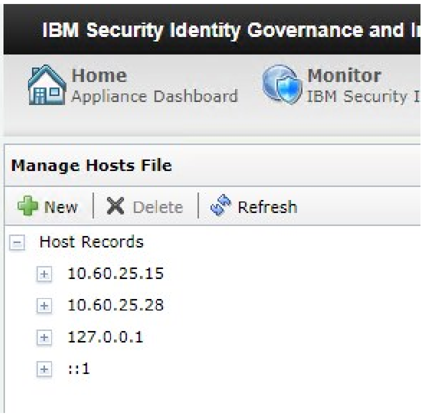
4. **Address:** Type the IP address where the Dispatcher is installed.
5. **Host Name:** Type the host name.
6. Click **Save**. The record is listed under **Hosts Records** in the **Manage Host File** page.
7. Click **New** New icon. The **Create Host Record** dialog box appears.



Address *
10.60.25.15

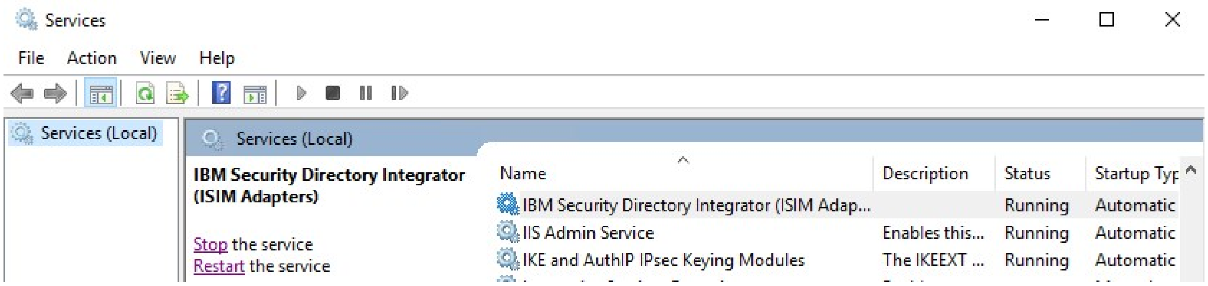
Host Name *
SecretServer16

8. **Address:** Type the IP address where the Secret Server is installed.
9. **Host Name:** Type the host name.
10. Click **Save**.
11. The host record is listed under **Hosts Records**.



Host Records
- 10.60.25.15
- 10.60.25.28
- 127.0.0.1
- ::1

12. Go to **Windows Services** and click **IBM Security Directory Integrator** service.



IBM Security Directory Integrator (ISIM Adapters)

Stop the service
Restart the service

Name	Description	Status	Startup Typ
IBM Security Directory Integrator (ISIM Adap...		Running	Automatic
IIS Admin Service	Enables this...	Running	Automatic
IKE and AuthIP IPsec Keying Modules	The IKEEXT ...	Running	Automatic

13. Click **Restart**.

14. Go to the **Windows Firewall**.

15. Add port **1099** to the Inbound Rule and Outbound Rule.

    Note: This step is mandatory for a successful connection between Secret Server and IBM IGI.

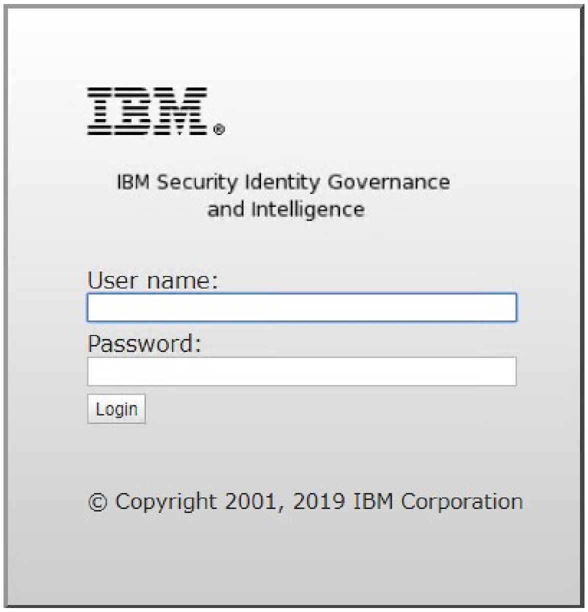
Integrate Secret Server with IBM IGI Admin Console

The integration of Secret Server is done with IBM IGI Admin Console to fetch Secret Server data into IBM IGI Admin Console.

Import attribute mapping file

You can import the attribute mapping files using the IBM IGI Administration Console.

1. Go to **IBM Security Identity Governance and Intelligence** administrative UI.



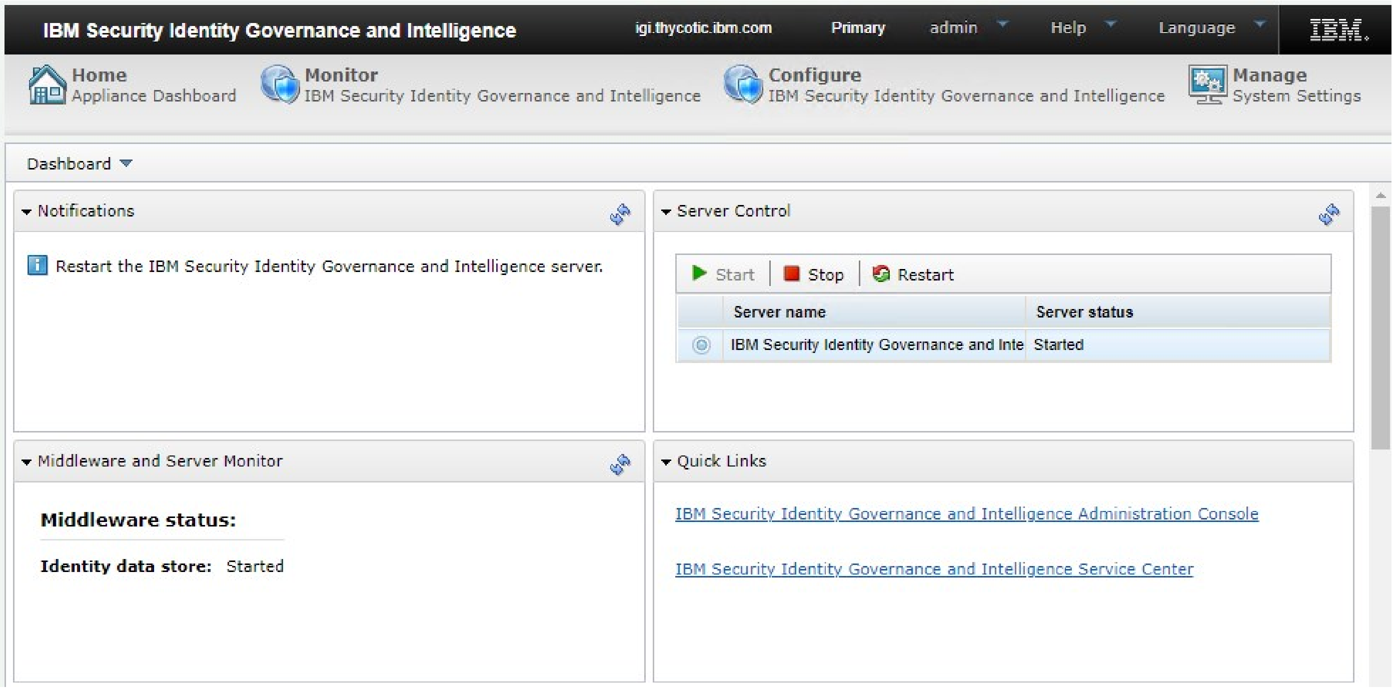
IBM Security Identity Governance and Intelligence

User name:

Password:

© Copyright 2001, 2019 IBM Corporation

2. Fill in the required information, such as user name, password, and click **Login**. The **IBM IGI Administration Console** dashboard appears.


IBM Security Identity Governance and Intelligence
igi.thycotic.ibm.com
Primary
admin
Help
Language
IBM.
Home
Appliance Dashboard
Monitor
IBM Security Identity Governance and Intelligence
Configure
IBM Security Identity Governance and Intelligence
Manage
System Settings
Dashboard
Notifications
Server Control
Start
Stop
Restart
Middleware and Server Monitor
Quick Links

Restart the IBM Security Identity Governance and Intelligence server.

	Server name	Server status
○	IBM Security Identity Governance and Inte	Started

Middleware status:

Identity data store: Started

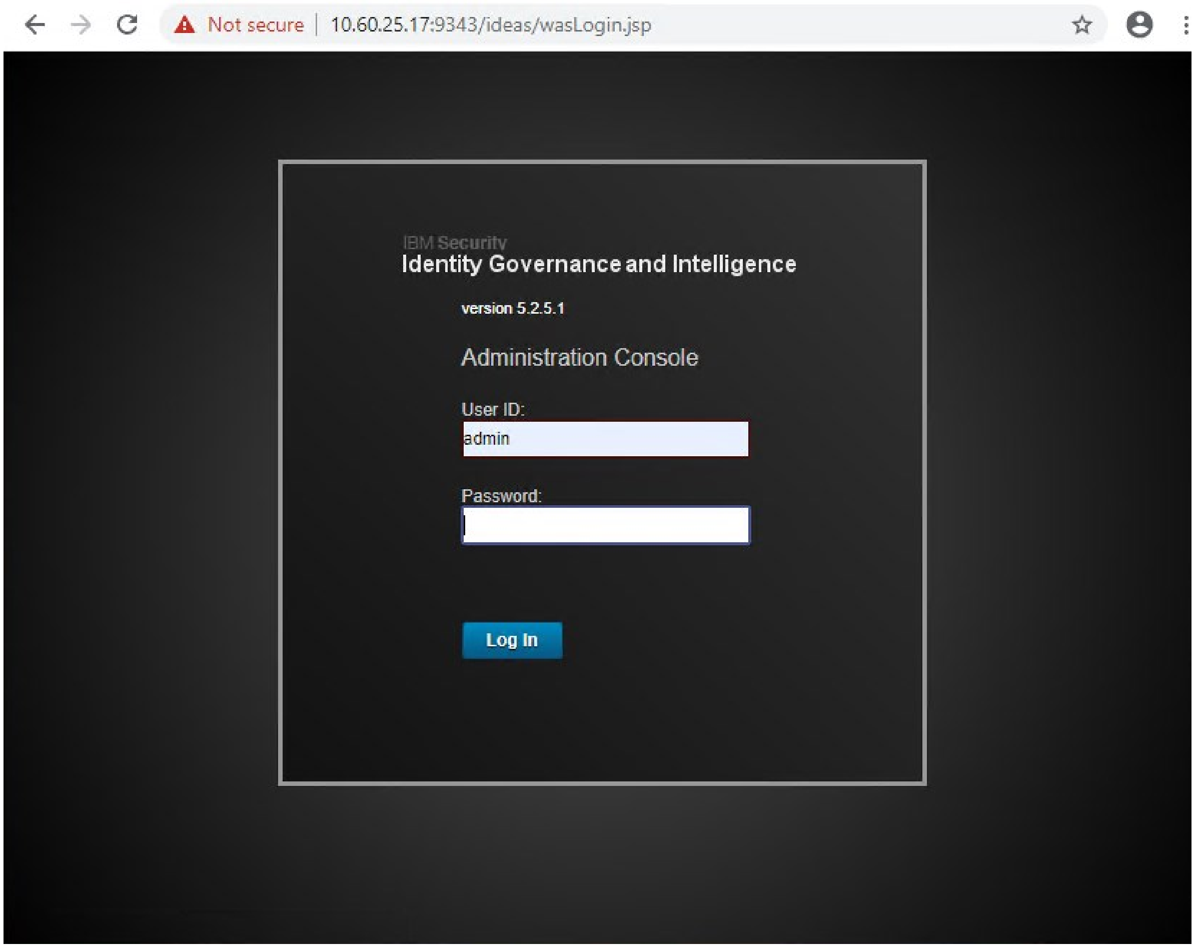
IBM Security Identity Governance and Intelligence Administration Console

IBM Security Identity Governance and Intelligence Service Center

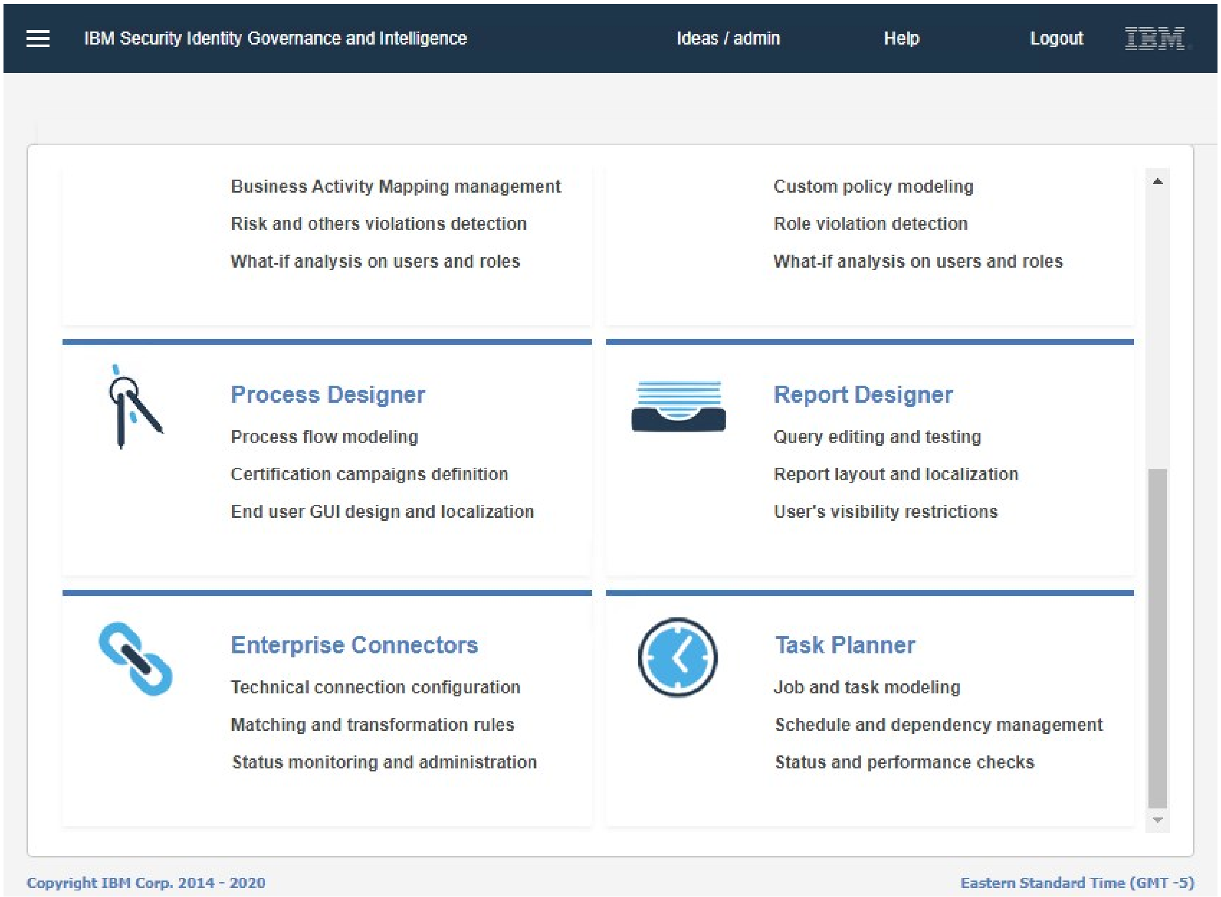
3. In the **Quick Links** section, click **IBM Security Identity Governance and Intelligence Administration Console**.

   Note: If you have a self-signed certificate, you may get a 'site can't be reached' message in that case you need to use the IP Address instead of domain name.

4. The **IBM IGI Administration Console** login page appears.



5. Fill in the required information, such as user ID, password, and click **Login**. The **IBM IGI Administration Console** UI appears.



IBM Security Identity Governance and Intelligence

Business Activity Mapping management
Risk and others violations detection
What-if analysis on users and roles

Custom policy modeling
Role violation detection
What-if analysis on users and roles

Process Designer
Process flow modeling
Certification campaigns definition
End user GUI design and localization

Report Designer
Query editing and testing
Report layout and localization
User's visibility restrictions

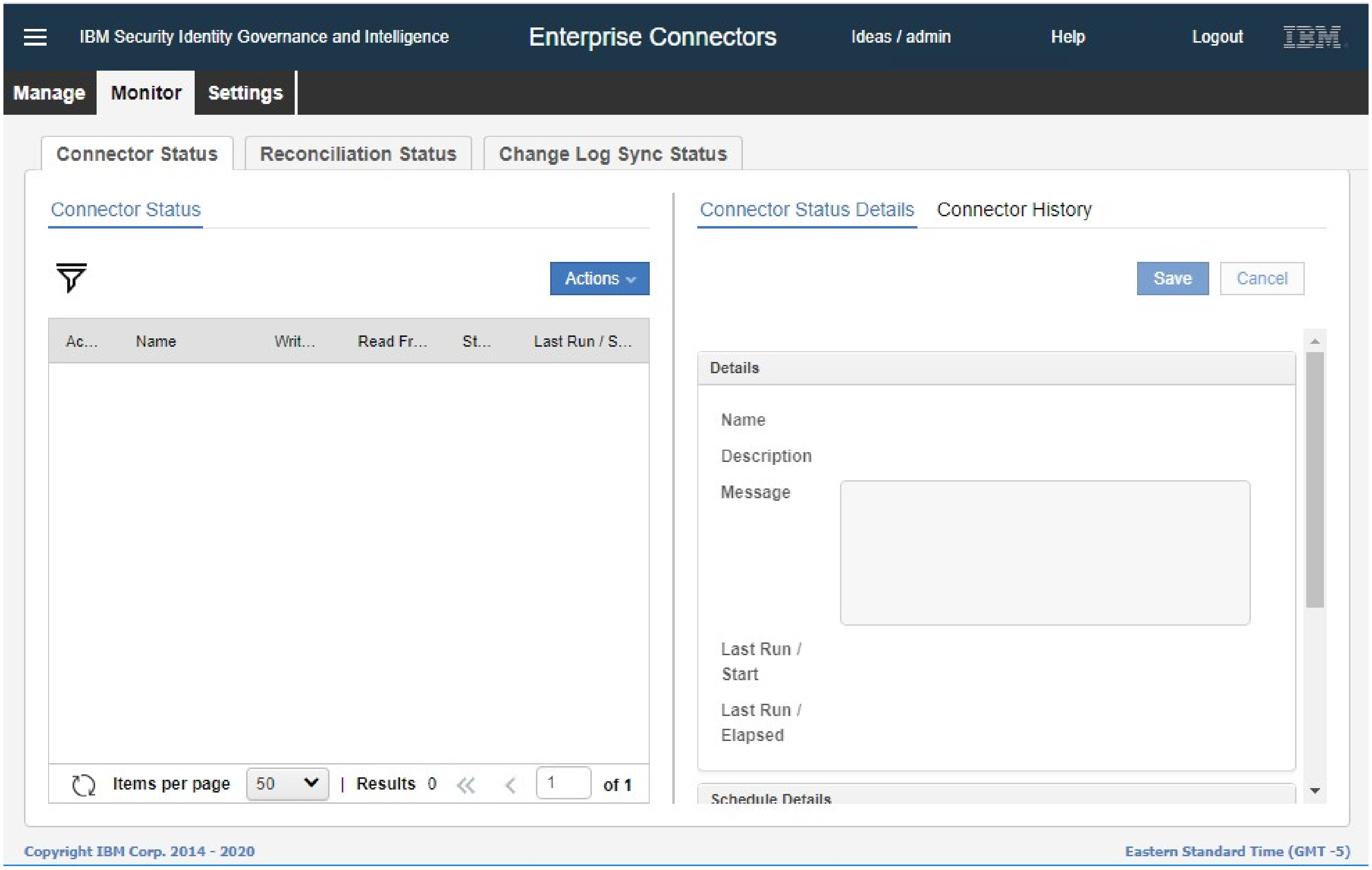
Enterprise Connectors
Technical connection configuration
Matching and transformation rules
Status monitoring and administration

Task Planner
Job and task modeling
Schedule and dependency management
Status and performance checks

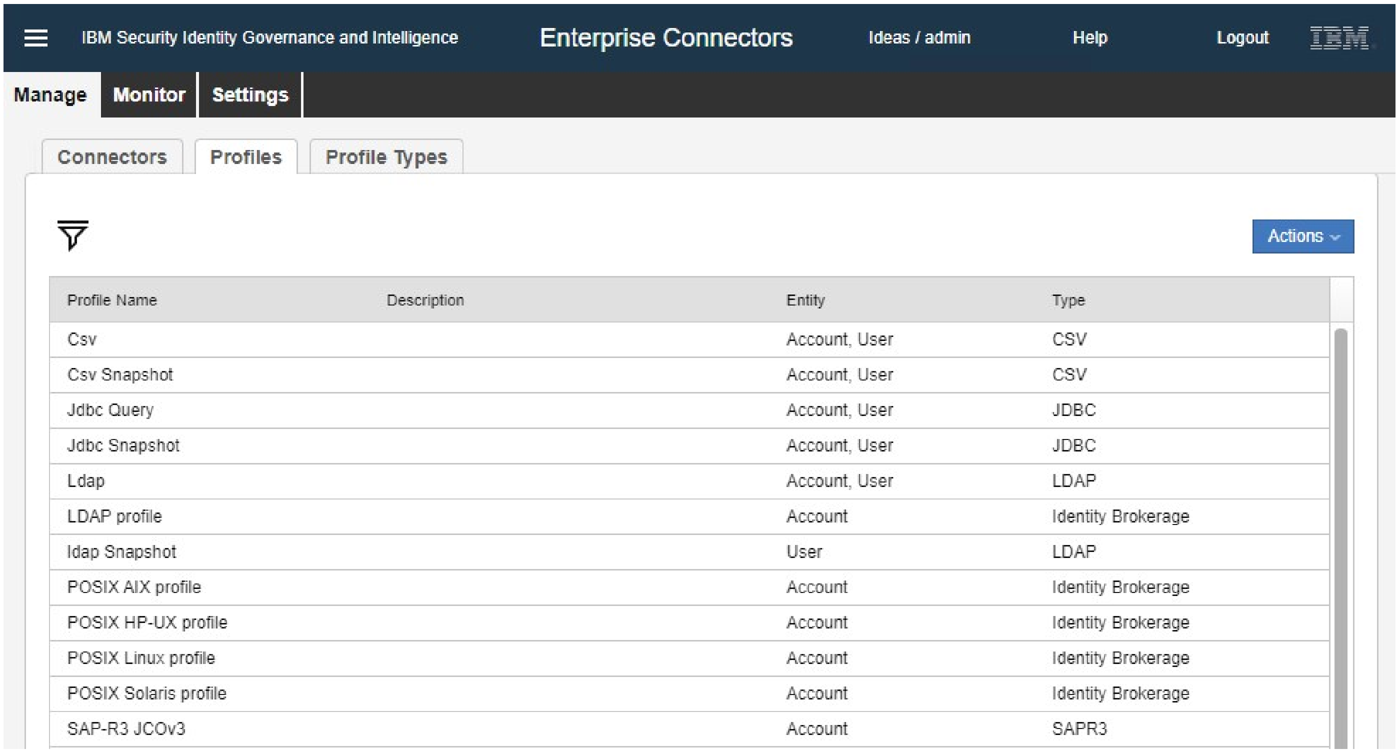
Copyright IBM Corp. 2014 - 2020

Eastern Standard Time (GMT -5)

6. Click **Enterprise Connectors**. The **Enterprise Connectors** page with the **Monitor** tab selected appears.

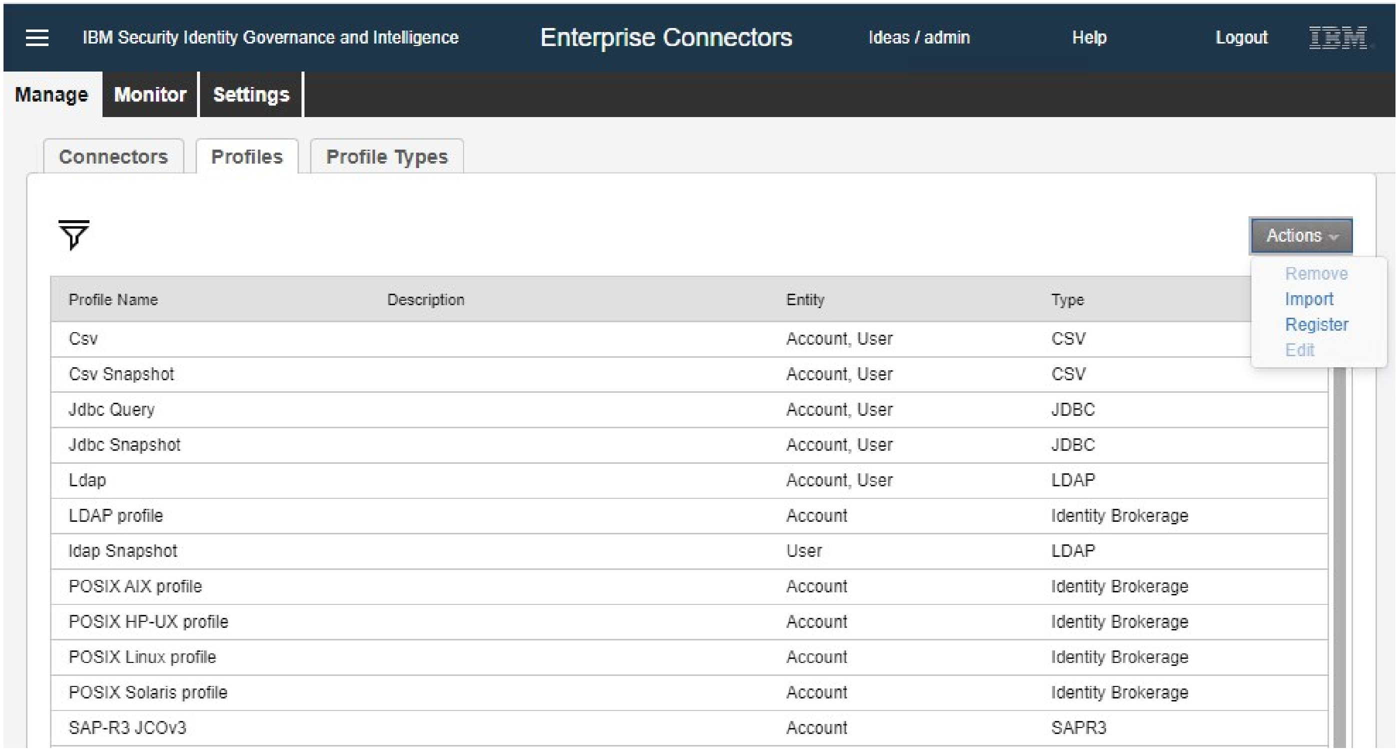


7. Click **Manage | Profiles**.



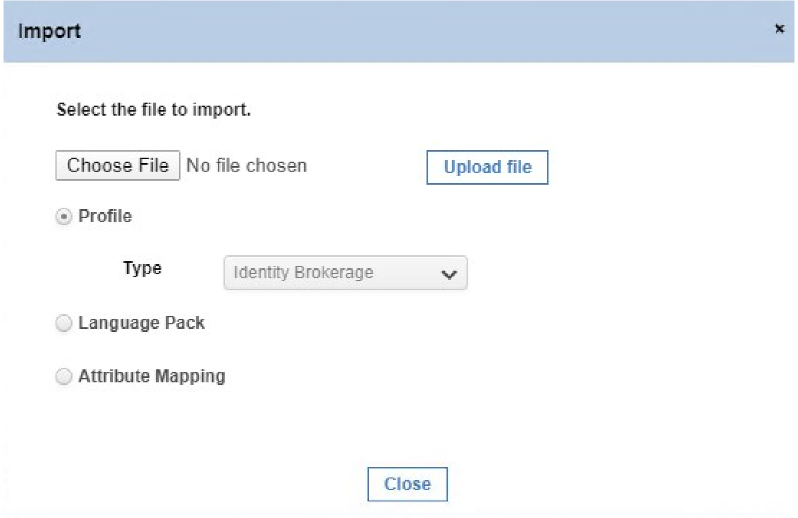
Profile Name	Description	Entity	Type
Csv		Account, User	CSV
Csv Snapshot		Account, User	CSV
Jdbc Query		Account, User	JDBC
Jdbc Snapshot		Account, User	JDBC
Ldap		Account, User	LDAP
LDAP profile		Account	Identity Brokerage
ldap Snapshot		User	LDAP
POSIX AIX profile		Account	Identity Brokerage
POSIX HP-UX profile		Account	Identity Brokerage
POSIX Linux profile		Account	Identity Brokerage
POSIX Solaris profile		Account	Identity Brokerage
SAP-R3 JCOv3		Account	SAPR3

8. In the **Actions** list, click **Import**.



Profile Name	Description	Entity	Type
Csv		Account, User	CSV
Csv Snapshot		Account, User	CSV
Jdbc Query		Account, User	JDBC
Jdbc Snapshot		Account, User	JDBC
Ldap		Account, User	LDAP
LDAP profile		Account	Identity Brokerage
ldap Snapshot		User	LDAP
POSIX AIX profile		Account	Identity Brokerage
POSIX HP-UX profile		Account	Identity Brokerage
POSIX Linux profile		Account	Identity Brokerage
POSIX Solaris profile		Account	Identity Brokerage
SAP-R3 JCOv3		Account	SAPR3

9. The **Import** dialog box appears.



Select the file to import.

No file chosen

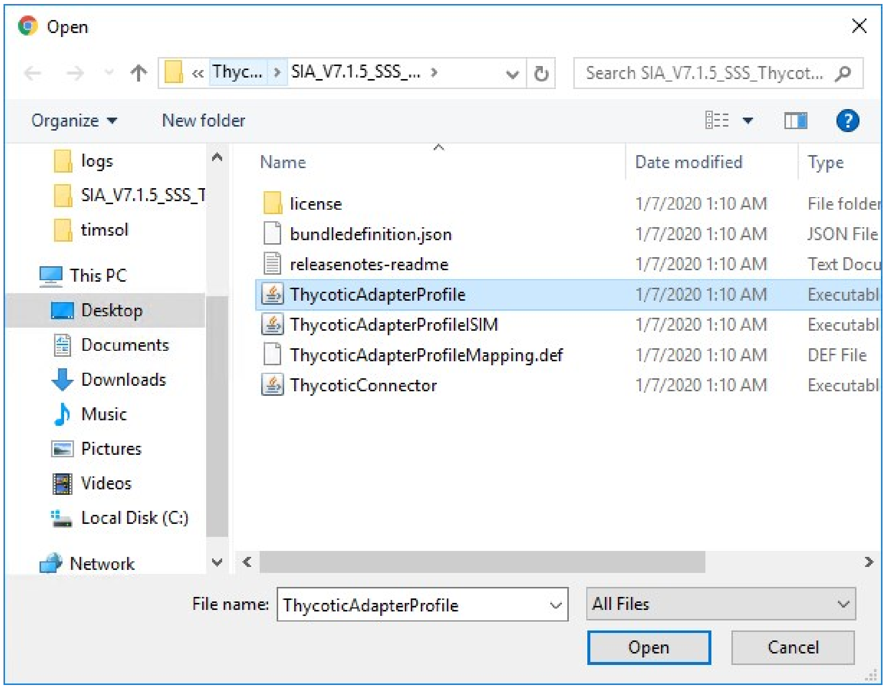
● Profile

Type: Identity Brokerage

○ Language Pack

○ Attribute Mapping

10. Click **Choose File**. The **Open** dialog box appears.

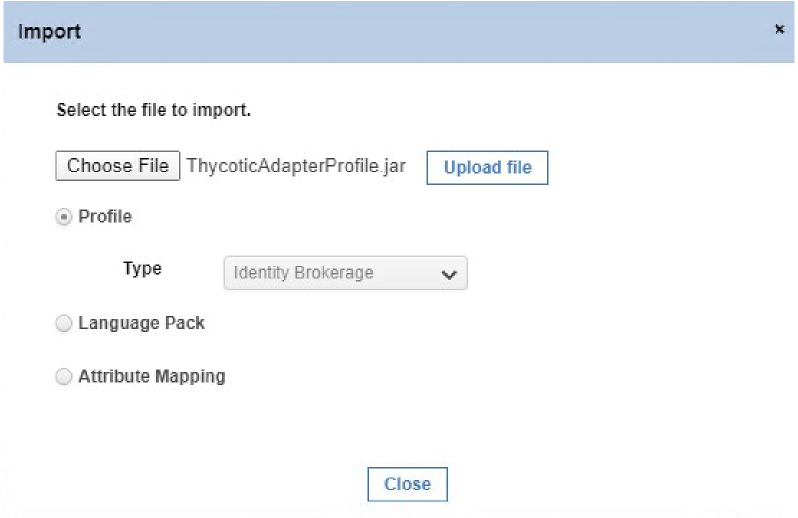


Name	Date modified	Type
license	1/7/2020 1:10 AM	File folder
bundledefinition.json	1/7/2020 1:10 AM	JSON File
releasenotes-readme	1/7/2020 1:10 AM	Text Docu
ThycoticAdapterProfile	1/7/2020 1:10 AM	Executabl
ThycoticAdapterProfileISIM	1/7/2020 1:10 AM	Executabl
ThycoticAdapterProfileMapping.def	1/7/2020 1:10 AM	DEF File
ThycoticConnector	1/7/2020 1:10 AM	Executabl

File name: ThycoticAdapterProfile

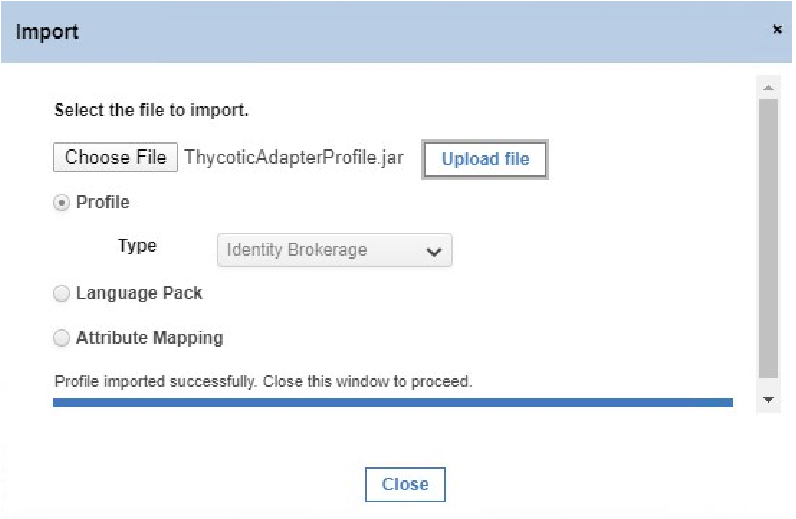
All Files

11. Navigate to the ThycoticAdapterProfile file and click **Open**.



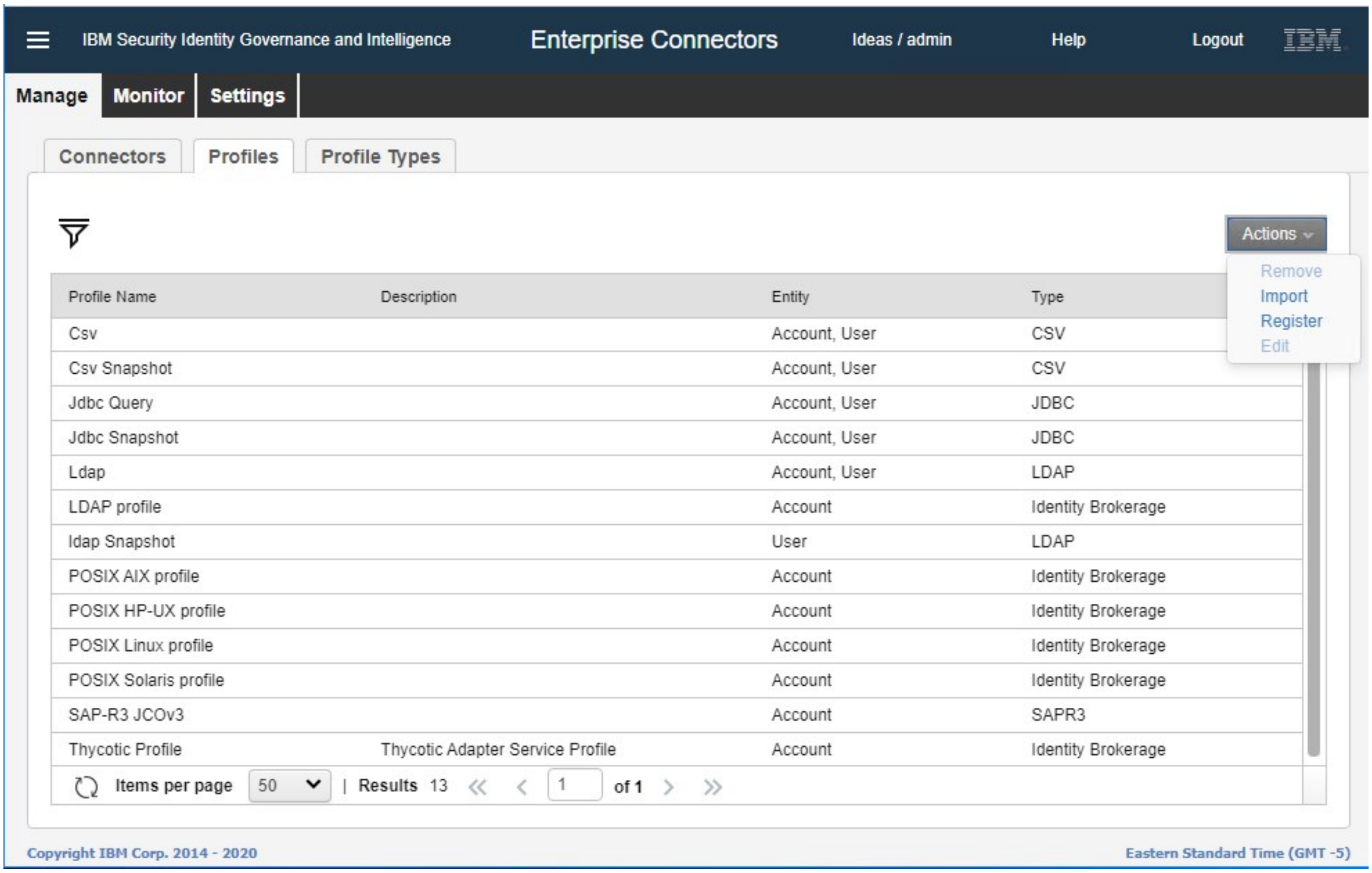
12. Click **Upload file**. A message, '**Profile imported successfully. Close this window to proceed.**' appears.

13. Click **Close**.



Profile imported successfully. Close this window to proceed.

14. In the **Enterprise Connectors** page, Click **Manage | Profiles**.

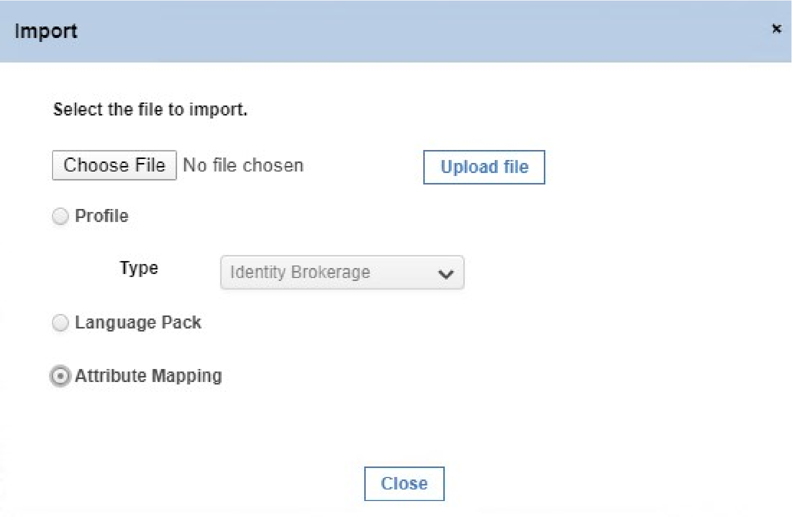


Profile Name	Description	Entity	Type
Csv		Account, User	CSV
Csv Snapshot		Account, User	CSV
Jdbc Query		Account, User	JDBC
Jdbc Snapshot		Account, User	JDBC
Ldap		Account, User	LDAP
LDAP profile		Account	Identity Brokerage
ldap Snapshot		User	LDAP
POSIX AIX profile		Account	Identity Brokerage
POSIX HP-UX profile		Account	Identity Brokerage
POSIX Linux profile		Account	Identity Brokerage
POSIX Solaris profile		Account	Identity Brokerage
SAP-R3 JCOv3		Account	SAPR3
Thycotic Profile	Thycotic Adapter Service Profile	Account	Identity Brokerage

Items per page 50 | Results 13 « ‹ 1 of 1 › »

Copyright IBM Corp. 2014 - 2020 Eastern Standard Time (GMT -5)

15. In the **Actions** list, click **Import**. The **Import** dialog box appears.



Select the file to import.

No file chosen

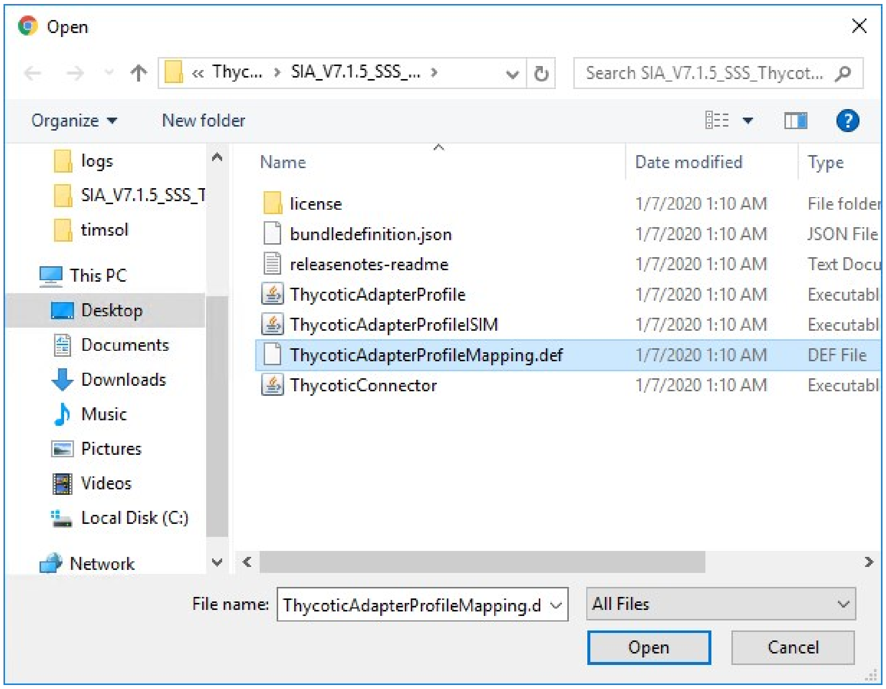
○ Profile

Type: Identity Brokerage

○ Language Pack

● Attribute Mapping

16. Select **Attribute Mapping** option and click **Choose File**. The **Open** dialog box appears.

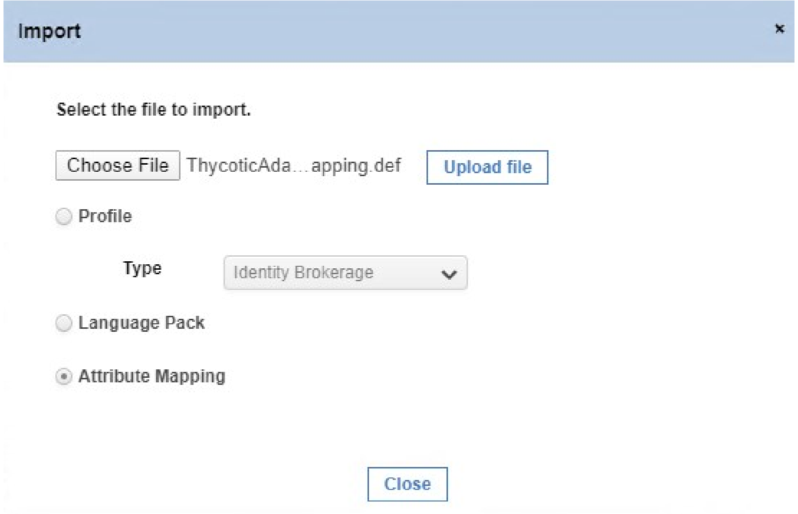


Name	Date modified	Type
license	1/7/2020 1:10 AM	File folder
bundledefinition.json	1/7/2020 1:10 AM	JSON File
releasenotes-readme	1/7/2020 1:10 AM	Text Docu
ThycoticAdapterProfile	1/7/2020 1:10 AM	Executabl
ThycoticAdapterProfileISIM	1/7/2020 1:10 AM	Executabl
ThycoticAdapterProfileMapping.def	1/7/2020 1:10 AM	DEF File
ThycoticConnector	1/7/2020 1:10 AM	Executabl

File name: ThycoticAdapterProfileMapping.d

All Files

17. Navigate to the ThycoticAdapterProfileMapping.def file, and click **Open**.



Select the file to import.

ThycoticAda…apping.def

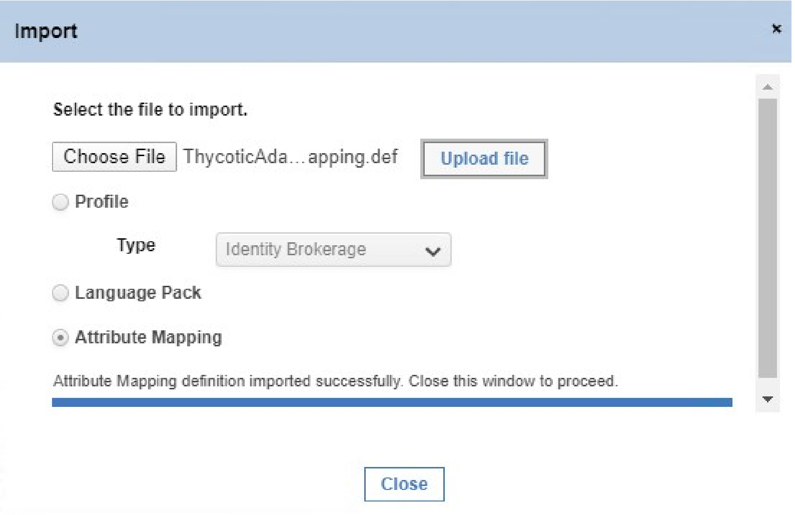
○ Profile

Type: Identity Brokerage

○ Language Pack

● Attribute Mapping

18. Click **Upload file**. A message, '**Attribute Mapping defining imported successfully. Close this window to proceed.**' appears.



Attribute Mapping definition imported successfully. Close this window to proceed.

19. Click **Close**.

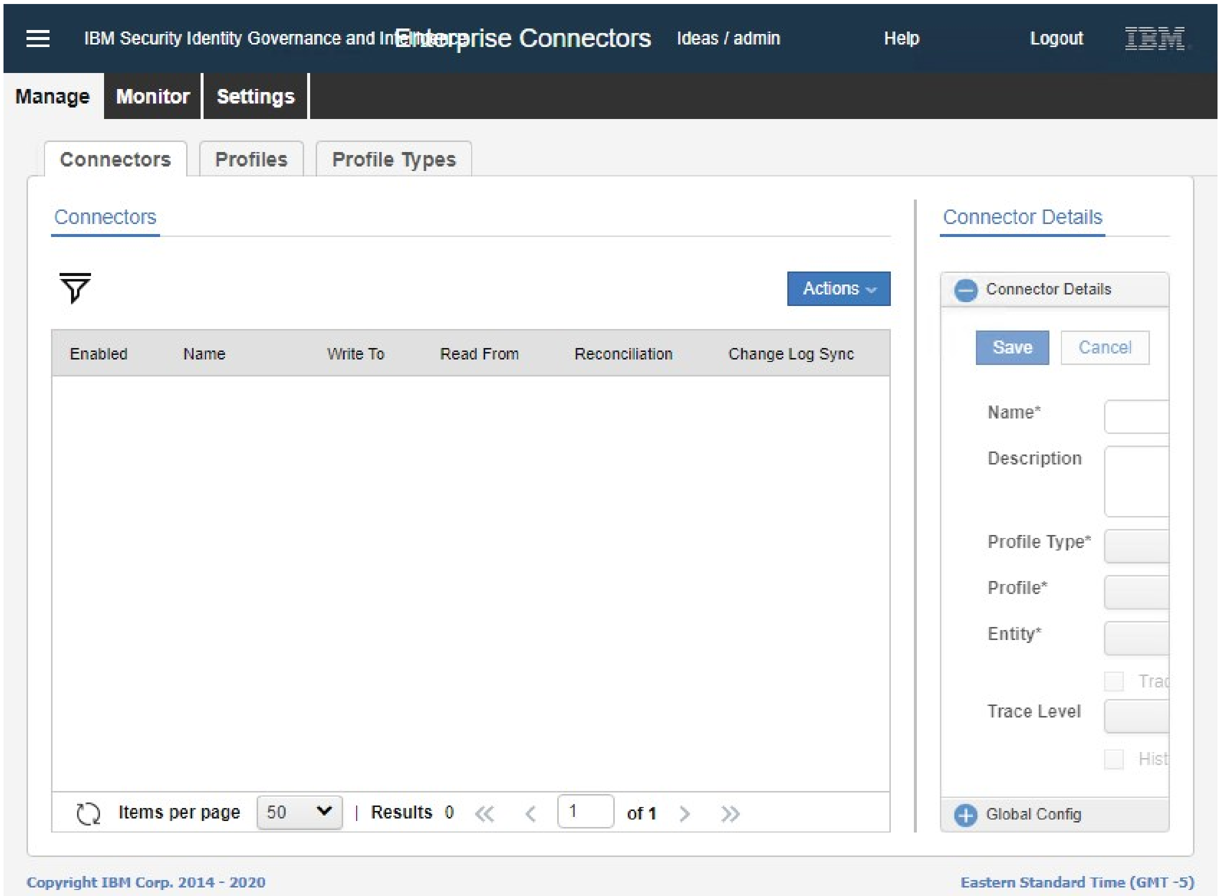
The attribute mapping definition is imported successfully.

Configure the connector

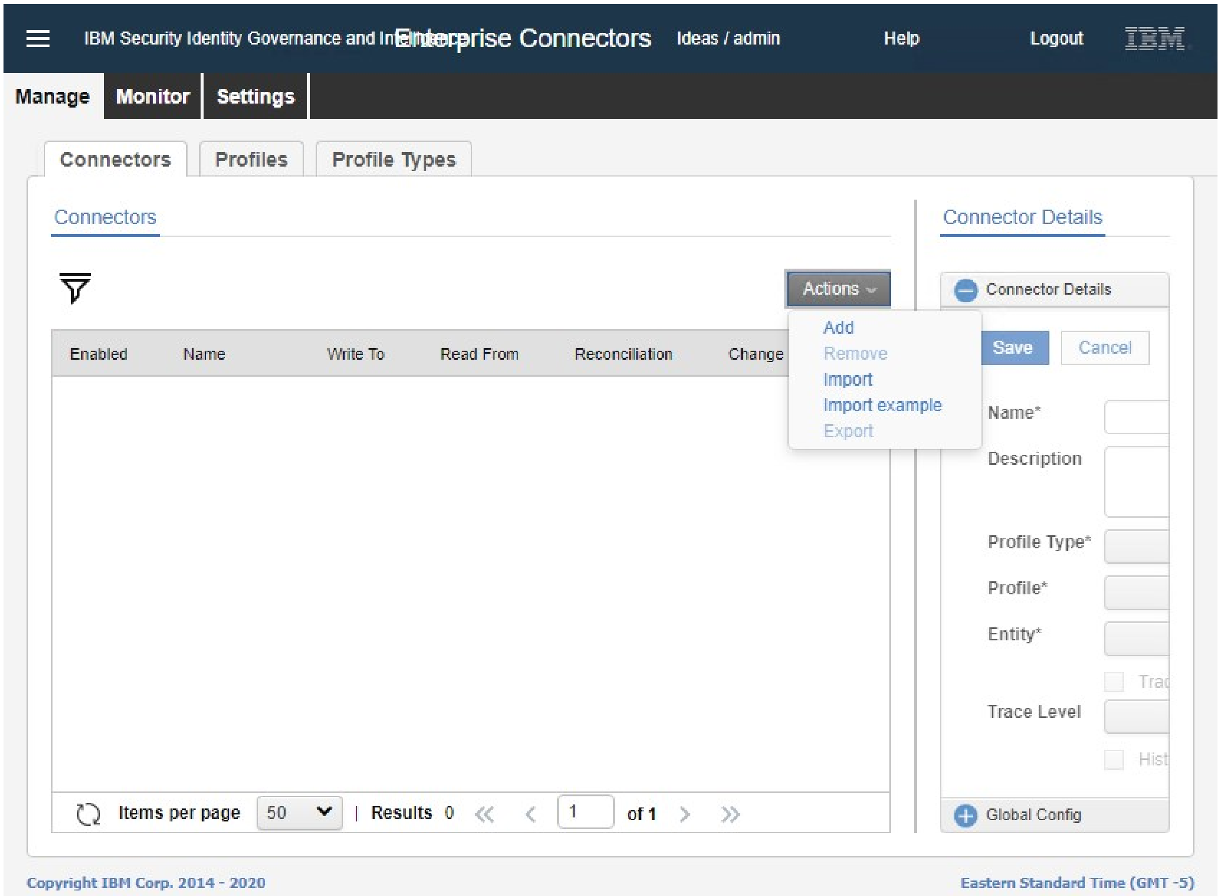
The next step is to configure the connector.

To configure the Connector:

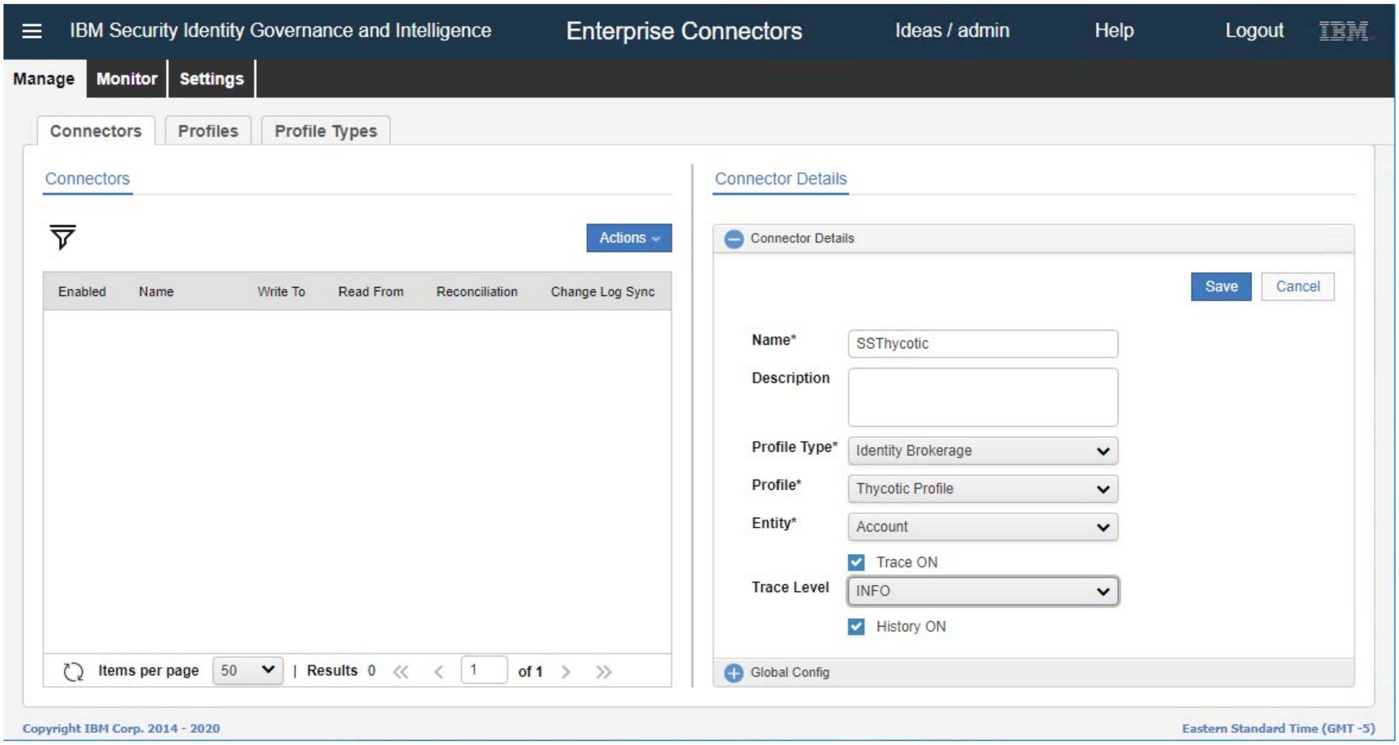
1. Click **Manage** | **Connectors**.



2. In the **Actions** list, click **Add**.



3. In the **Connector Details** section, fill in the required information.



Enabled	Name	Write To	Read From	Reconciliation	Change Log Sync

Name* SSThycotic

Description

Profile Type* Identity Brokerage

Profile* Thycotic Profile

Entity* Account

☑ Trace ON

Trace Level INFO

☑ History ON

a. **Name** - Type the name of the connector.

b. **Profile Type** - Select Identity Brokerage.

c. **Profile** - Select Thycotic Profile.

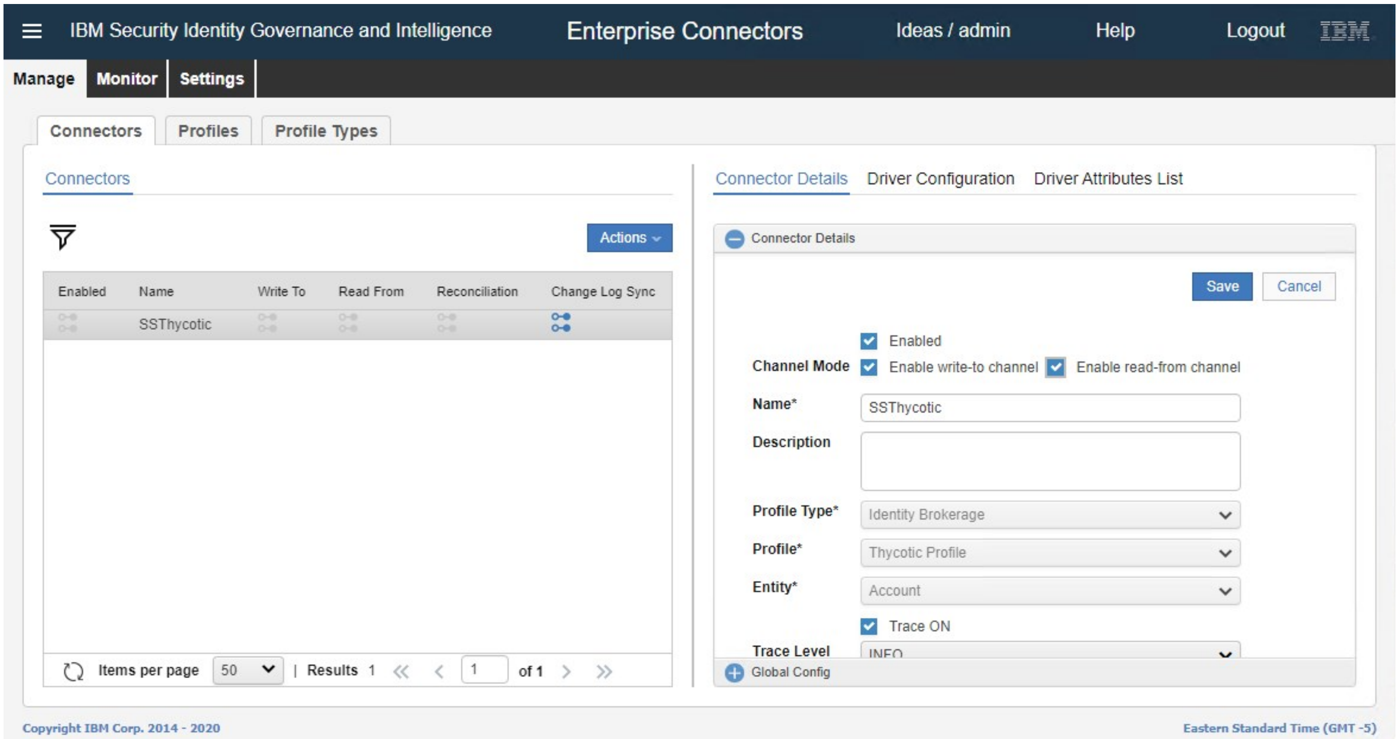
d. **Entity** - Select Account.

e. **Trace ON** - Select the check box.

f. **Trace Level** - Select INFO.

g. **History ON** - Select the check box

4. Click **Save**. More options are available for selection.



IBM Security Identity Governance and Intelligence | Enterprise Connectors | Ideas / admin | Help | Logout

Manage | Monitor | Settings

Connectors | Profiles | Profile Types

Connectors

Actions

Enabled	Name	Write To	Read From	Reconciliation	Change Log Sync
	SSThycotic				

Items per page 50 | Results 1 | 1 of 1

Connector Details | Driver Configuration | Driver Attributes List

Connector Details

Save | Cancel

☑ Enabled

Channel Mode ☑ Enable write-to channel ☑ Enable read-from channel

Name* SSThycotic

Description

Profile Type* Identity Brokerage

Profile* Thycotic Profile

Entity* Account

☑ Trace ON

Trace Level INFO

Global Config

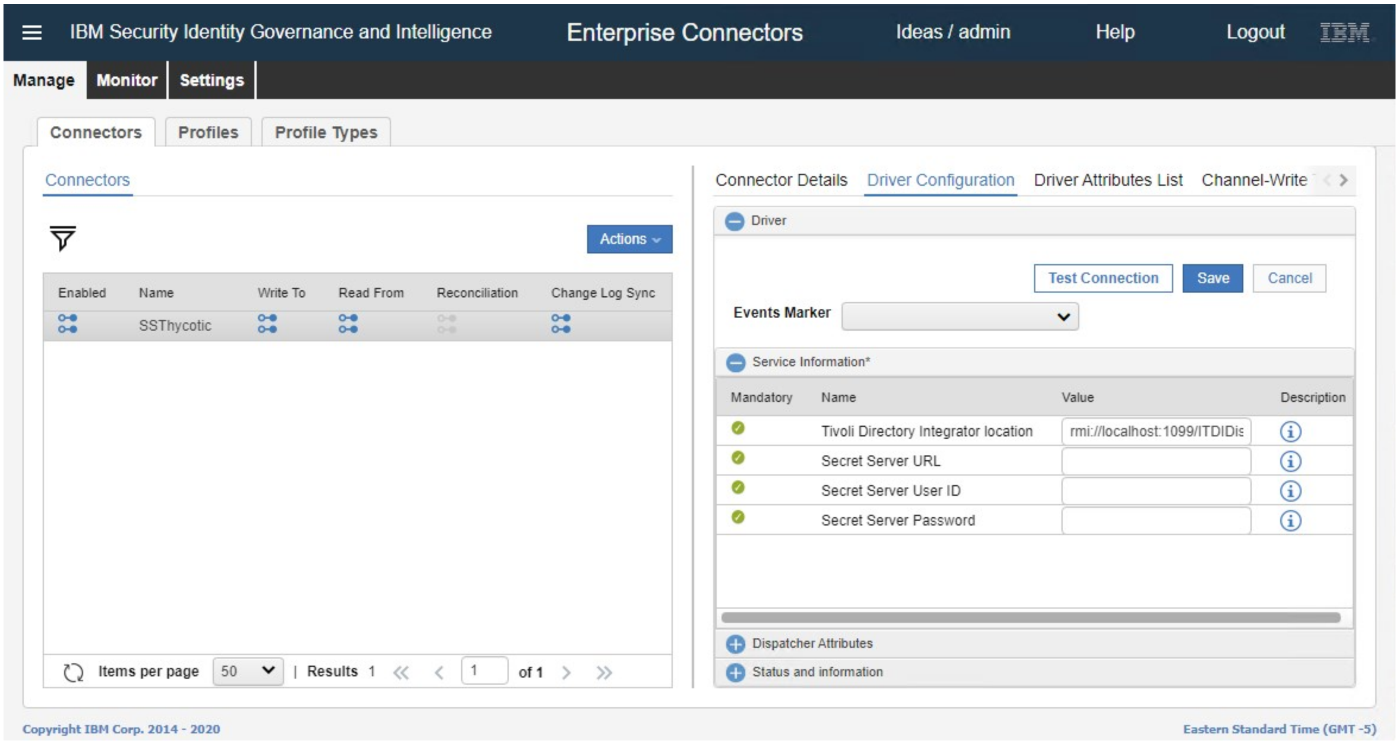
Copyright IBM Corp. 2014 - 2020

Eastern Standard Time (GMT -5)

5. Select the check boxes: **Enabled**, **Enable write-to channel**, and **Enable read-from channel**.

6. click **Save**.

7. Click **Driver Configuration** tab and fill in the required details.



IBM Security Identity Governance and Intelligence | Enterprise Connectors | Ideas / admin | Help | Logout

Manage | Monitor | Settings

Connectors | Profiles | Profile Types

Connectors

Actions

Enabled	Name	Write To	Read From	Reconciliation	Change Log Sync
	SSThycotic				

Items per page 50 | Results 1 | 1 of 1

Connector Details | Driver Configuration | Driver Attributes List | Channel-Write

Driver

Test Connection | Save | Cancel

Events Marker

Service Information*

Mandatory	Name	Value	Description
✓	Tivoli Directory Integrator location	rmi://localhost:1099/ITDIDis	ⓘ
✓	Secret Server URL		ⓘ
✓	Secret Server User ID		ⓘ
✓	Secret Server Password		ⓘ

Dispatcher Attributes

Status and information

Copyright IBM Corp. 2014 - 2020

Eastern Standard Time (GMT -5)

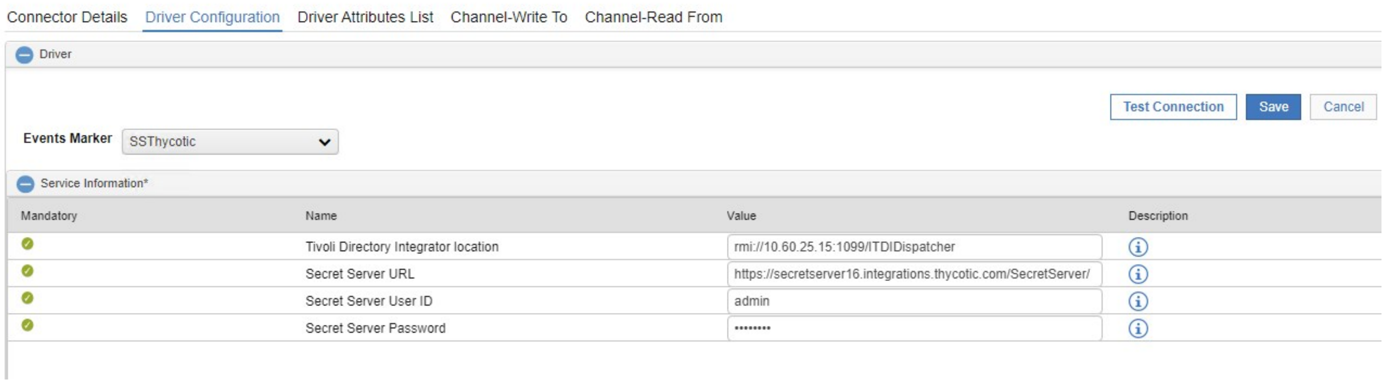
a. **Tivoli Directory Integration location** - Type the IP Address of the Dispatcher where the Dispatcher is installed.

b. **Secret Server URL** - Type the secret server URL

c. **Secret Server User ID** - Type the secret server user ID.

d. **Secret Server Password** - Type the password.

8. Click **Save**.



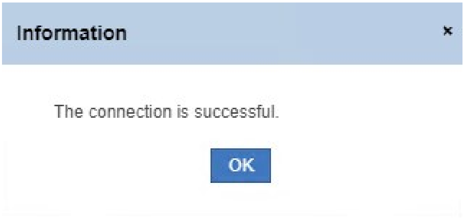
Events Marker: SSThycotic

Service Information*

Mandatory	Name	Value	Description
✓	Tivoli Directory Integrator location	rmi://10.60.25.15:1099/ITDIDispatcher	ⓘ
✓	Secret Server URL	https://secretserver16.integrations.thycotic.com/SecretServer/	ⓘ
✓	Secret Server User ID	admin	ⓘ
✓	Secret Server Password	••••••••	ⓘ

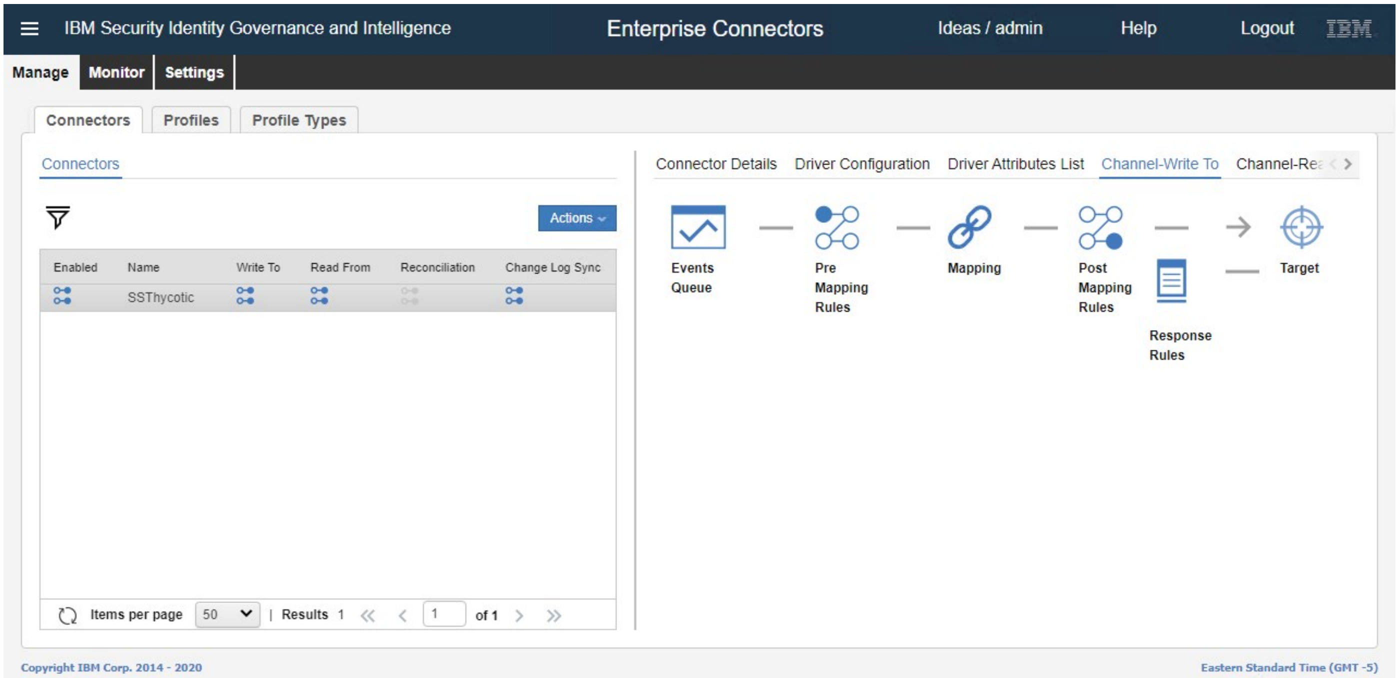
9. In the **Driver** section, on the upper-right click **Save**.

10. Click **Test Connection**. If the connection is successful, a message, '**The connection is successful.**' appears. Click **Ok**.



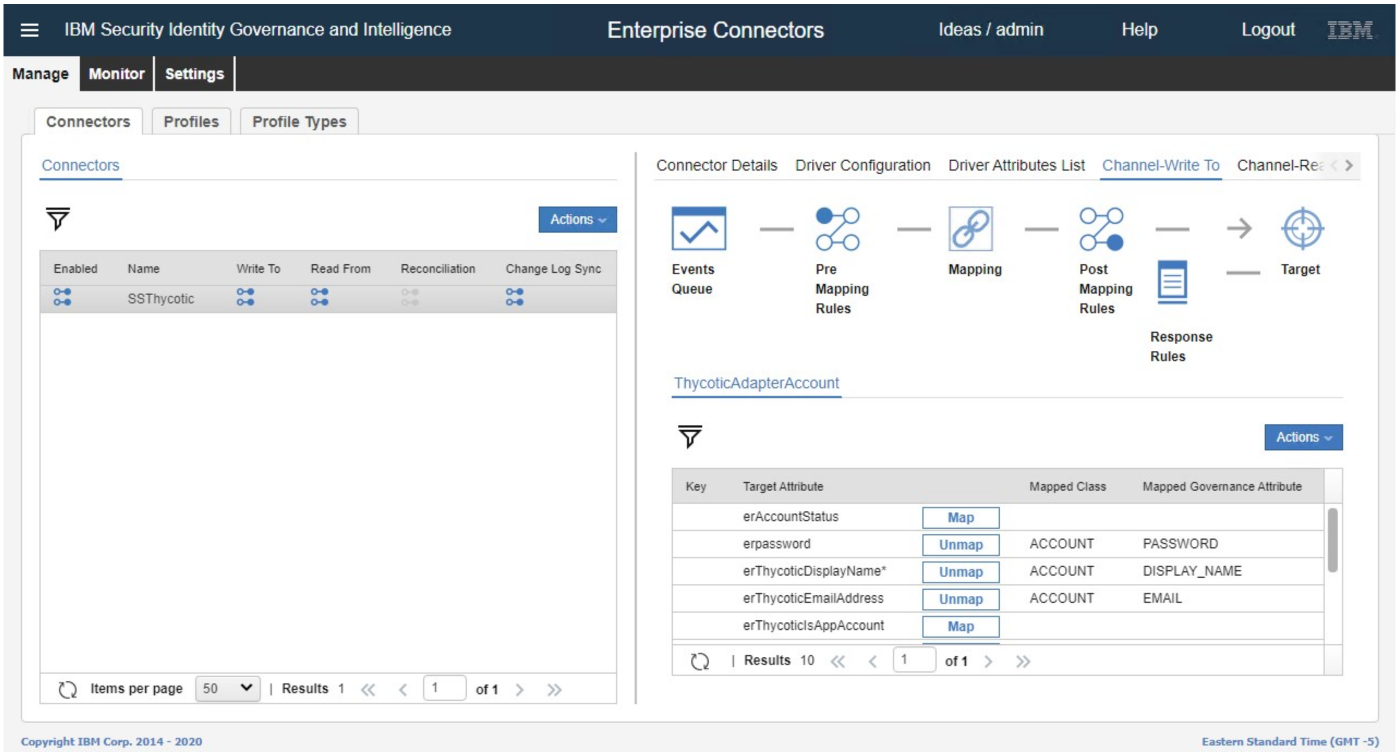
The connection is successful.

11. Click **Channel-Write To** tab | **Mapping**.



Enabled	Name	Write To	Read From	Reconciliation	Change Log Sync
●	SSThycotic	●	●	○	●

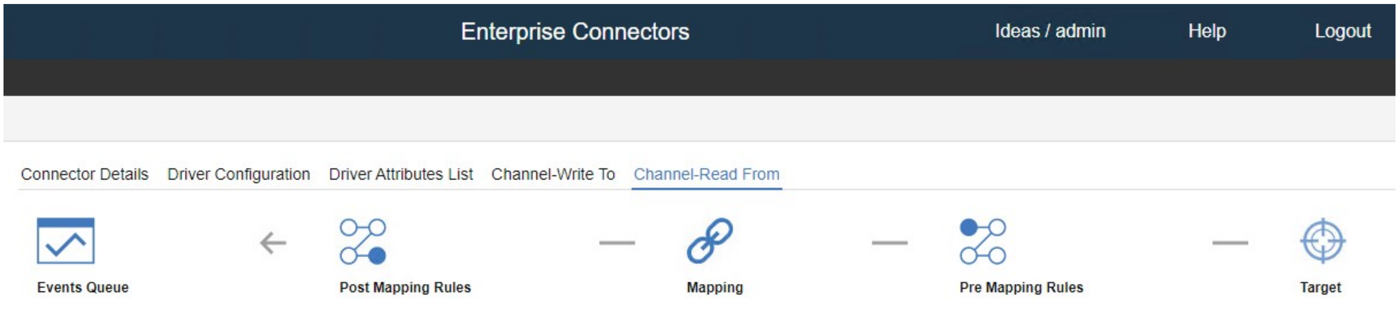
12. Verify the presence of the mapping files.



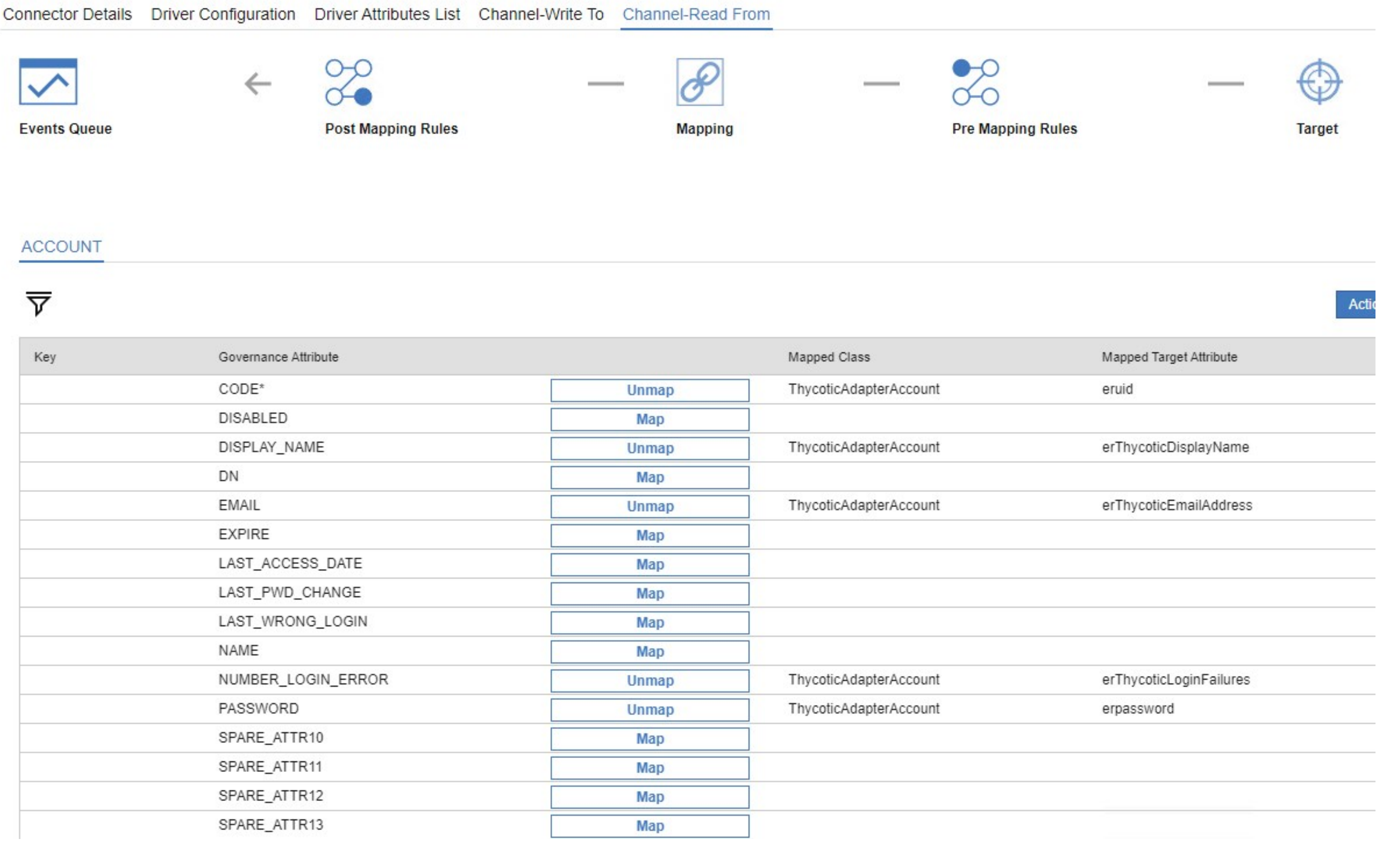
Enabled	Name	Write To	Read From	Reconciliation	Change Log Sync
●	SSThycotic	●	●	○	●

Key	Target Attribute		Mapped Class	Mapped Governance Attribute
	erAccountStatus	Map		
	erpassword	Unmap	ACCOUNT	PASSWORD
	erThycoticDisplayName*	Unmap	ACCOUNT	DISPLAY_NAME
	erThycoticEmailAddress	Unmap	ACCOUNT	EMAIL
	erThycoticIsAppAccount	Map		

13. Click **Channel-Read From** tab I **Mapping**.

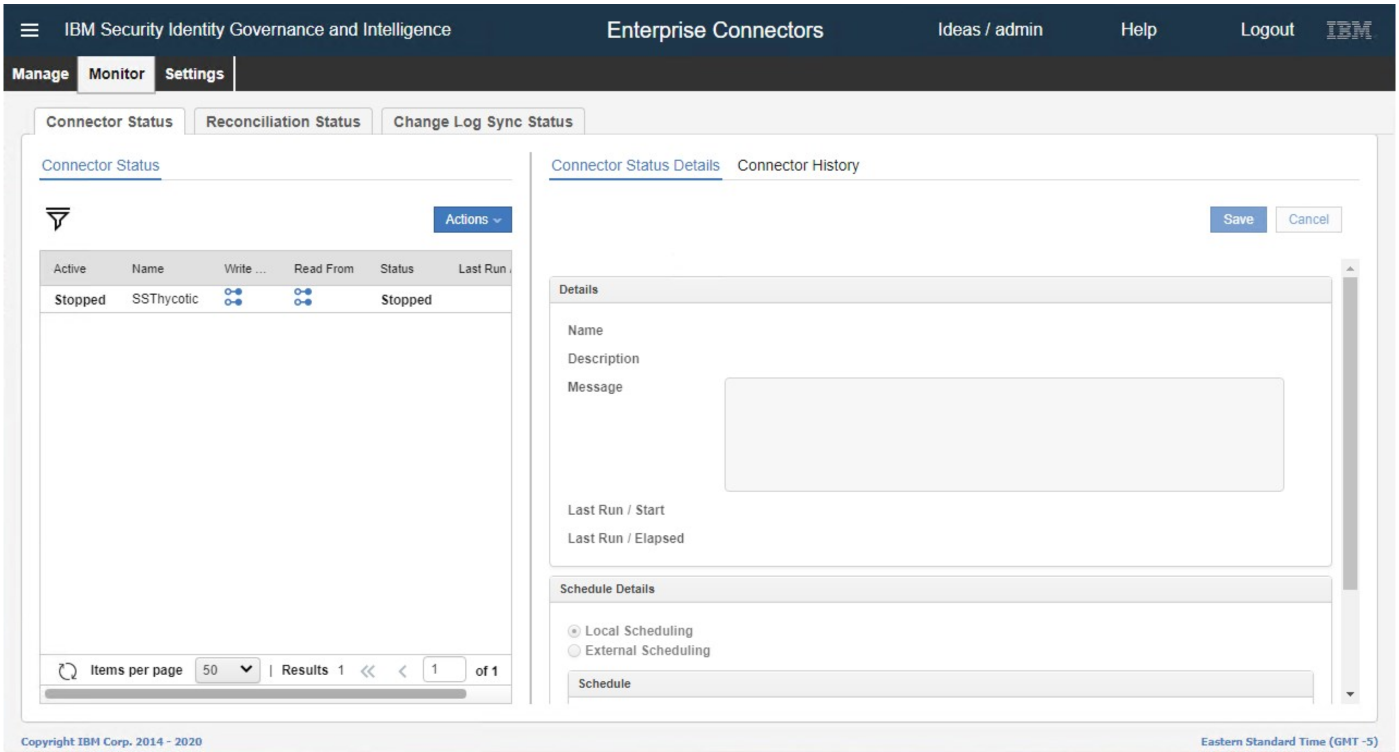


14. Verify the presence of the mapping files.



Key	Governance Attribute		Mapped Class	Mapped Target Attribute
	CODE*	Unmap	ThycoticAdapterAccount	eruid
	DISABLED	Map		
	DISPLAY_NAME	Unmap	ThycoticAdapterAccount	erThycoticDisplayName
	DN	Map		
	EMAIL	Unmap	ThycoticAdapterAccount	erThycoticEmailAddress
	EXPIRE	Map		
	LAST_ACCESS_DATE	Map		
	LAST_PWD_CHANGE	Map		
	LAST_WRONG_LOGIN	Map		
	NAME	Map		
	NUMBER_LOGIN_ERROR	Unmap	ThycoticAdapterAccount	erThycoticLoginFailures
	PASSWORD	Unmap	ThycoticAdapterAccount	erpassword
	SPARE_ATTR10	Map		
	SPARE_ATTR11	Map		
	SPARE_ATTR12	Map		
	SPARE_ATTR13	Map		

15. Click **Monitor | Connector Status**.



Active	Name	Write ...	Read From	Status	Last Run
Stopped	SSThycotic			Stopped	

Details

Name

Description

Message

Last Run / Start

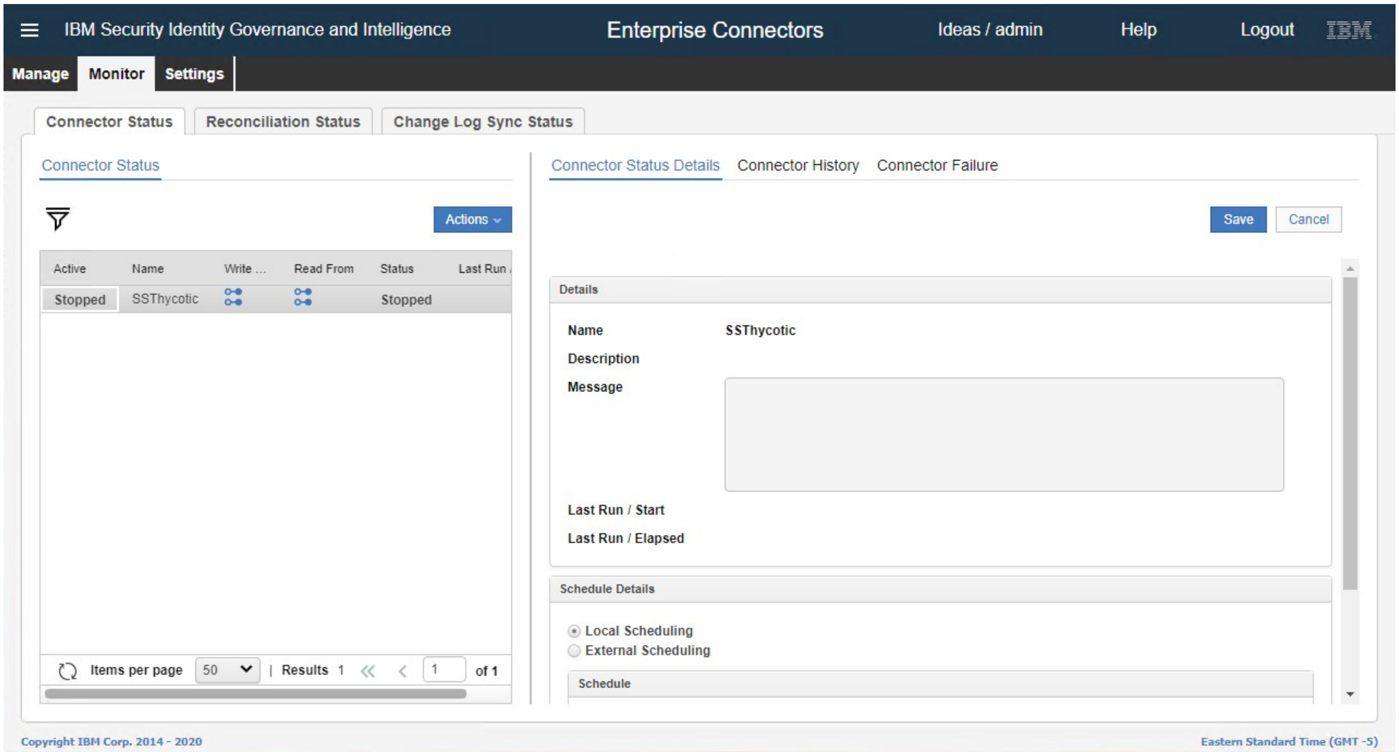
Last Run / Elapsed

Schedule Details

● Local Scheduling
○ External Scheduling

Schedule

16. Select the connector.



Active	Name	Write ...	Read From	Status	Last Run
Stopped	SSThycotic			Stopped	

Details

Name SSThycotic

Description

Message

Last Run / Start

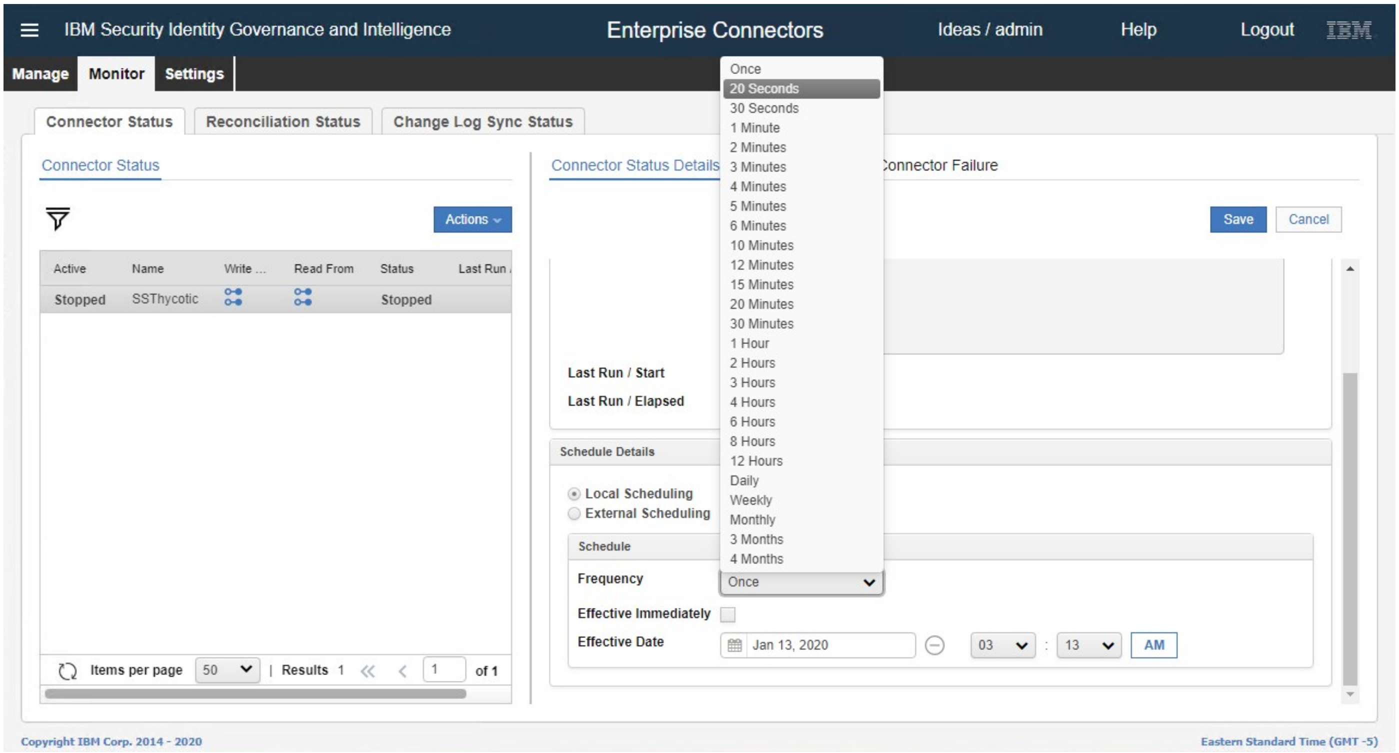
Last Run / Elapsed

Schedule Details

● Local Scheduling
○ External Scheduling

Schedule

17. In the **Schedule Details** I **Frequency** list, select the value as 20 seconds and then select **Effective Immedialtely**.



Active	Name	Write ...	Read From	Status	Last Run
Stopped	SSThycotic			Stopped	

Last Run / Start

Last Run / Elapsed

Schedule Details

● Local Scheduling
○ External Scheduling

Schedule

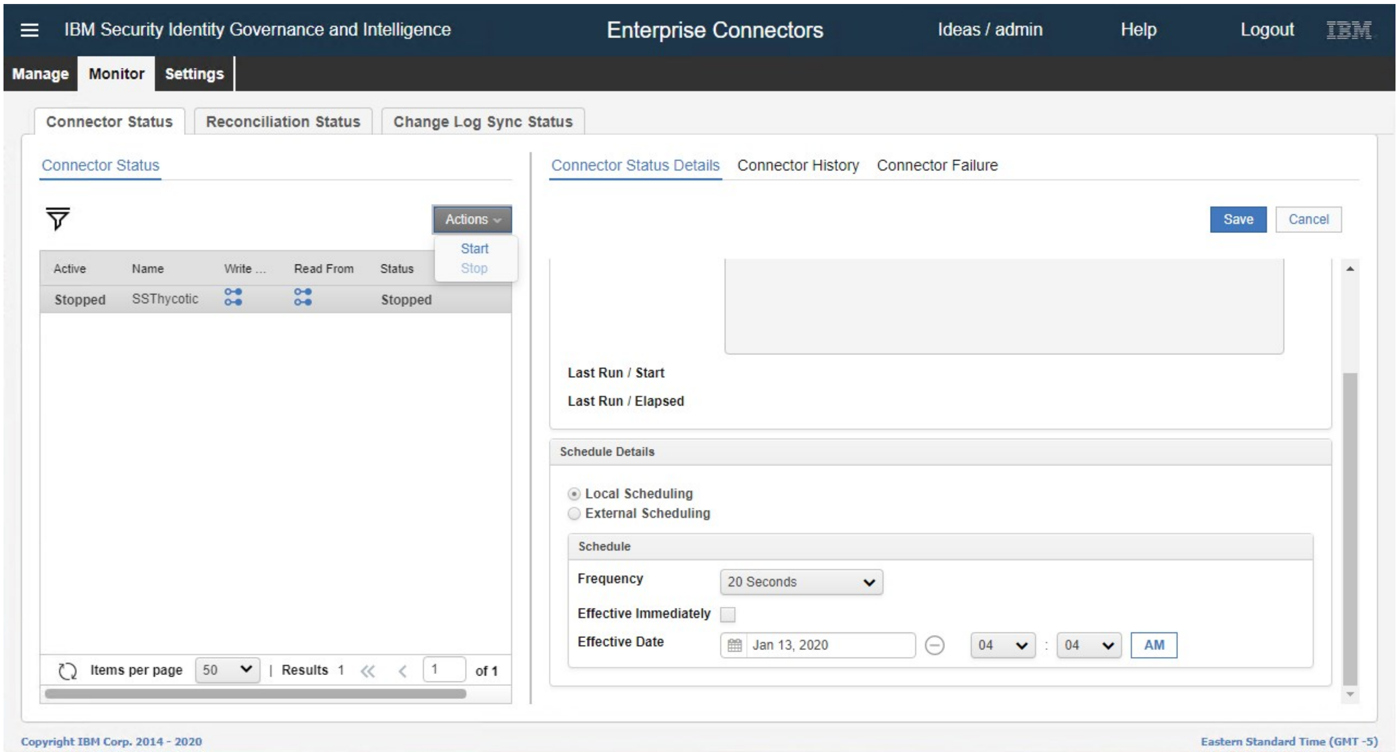
Frequency: Once

Effective Immediately: □

Effective Date: Jan 13, 2020 03 : 13 AM

Items per page 50 | Results 1 1 of 1

18. In the **Actions** list, click Start.



Active	Name	Write ...	Read From	Status
Stopped	SSThycotic			Stopped

Last Run / Start

Last Run / Elapsed

Schedule Details

● Local Scheduling
○ External Scheduling

Schedule

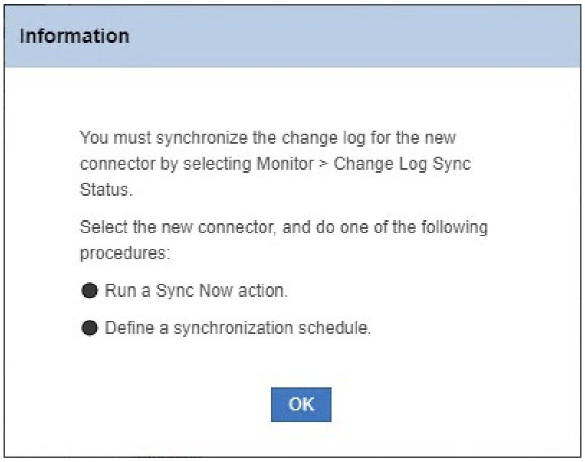
Frequency: 20 Seconds

Effective Immediately: □

Effective Date: Jan 13, 2020 04 : 04 AM

Items per page 50 | Results 1 1 of 1

19. The **Information** dialog box appears. Click **Ok**.



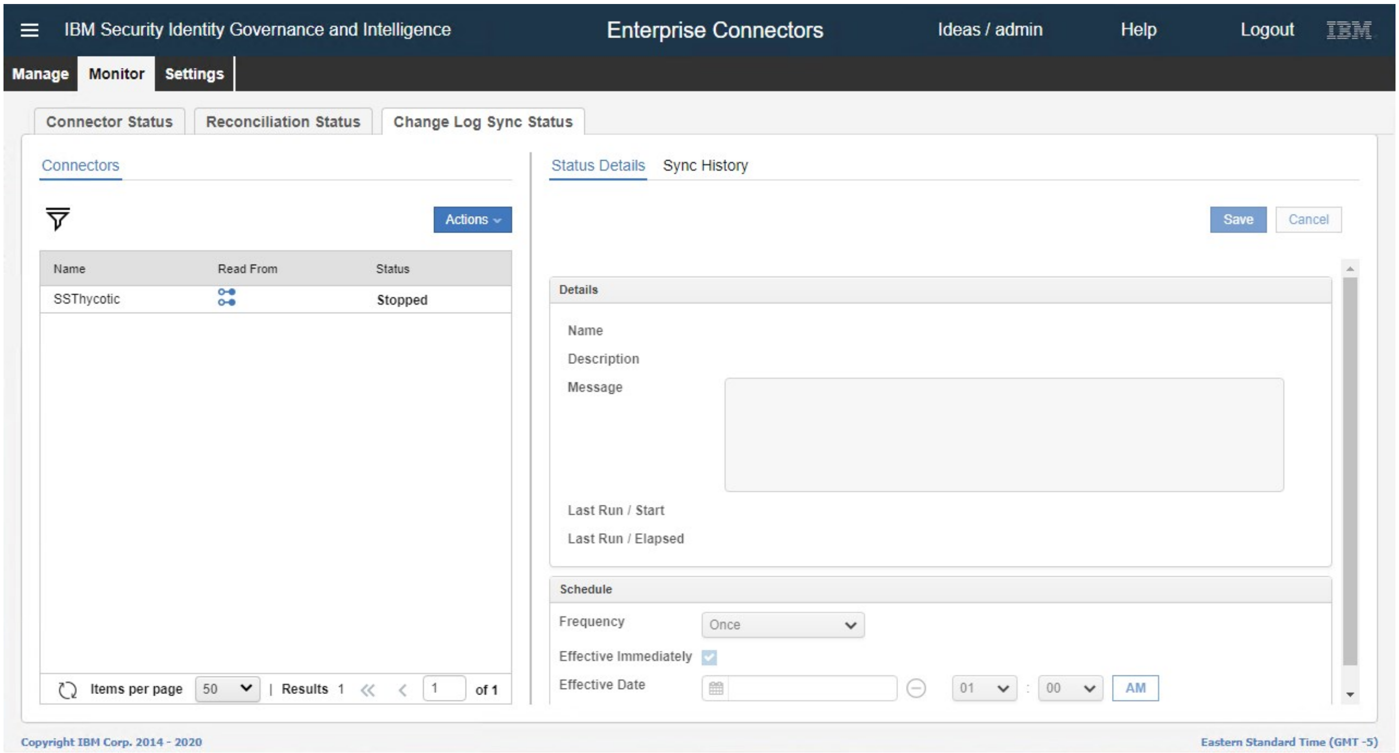
Information

You must synchronize the change log for the new connector by selecting Monitor > Change Log Sync Status.

Select the new connector, and do one of the following procedures:

- Run a Sync Now action.
- Define a synchronization schedule.

20. Click **Monitor | Change Log Sync Status**.



Name	Read From	Status
SSThycotic		Stopped

Items per page 50 | Results 1 | 1 of 1

Details

Name

Description

Message

Last Run / Start

Last Run / Elapsed

Schedule

Frequency: Once

Effective Immediately: ☑

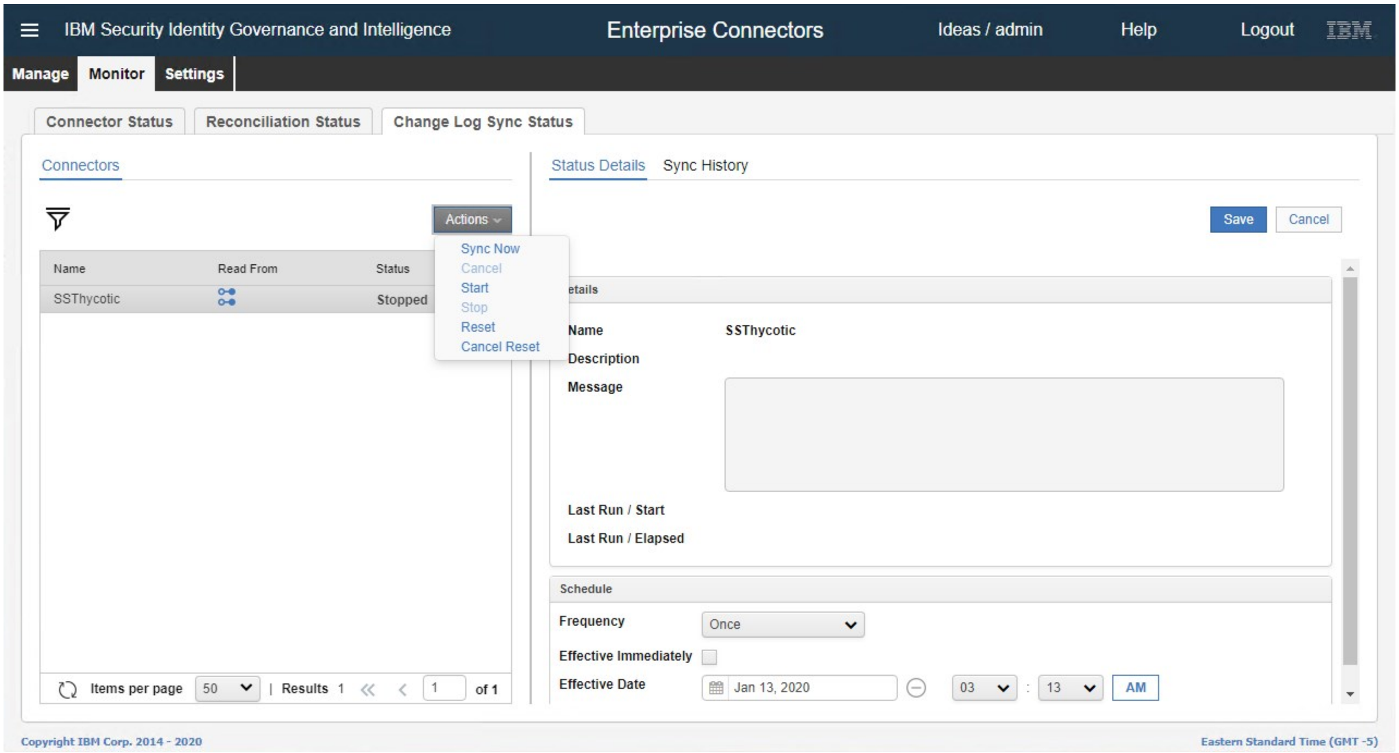
Effective Date: 01 : 00 AM

Copyright IBM Corp. 2014 - 2020

Eastern Standard Time (GMT -5)

21. Select the connector.

22. In the **Actions list**, click **Sync Now**.



Name	Read From	Status
SSThycotic		Stopped

etails

Name SSThycotic

Description

Message

Last Run / Start

Last Run / Elapsed

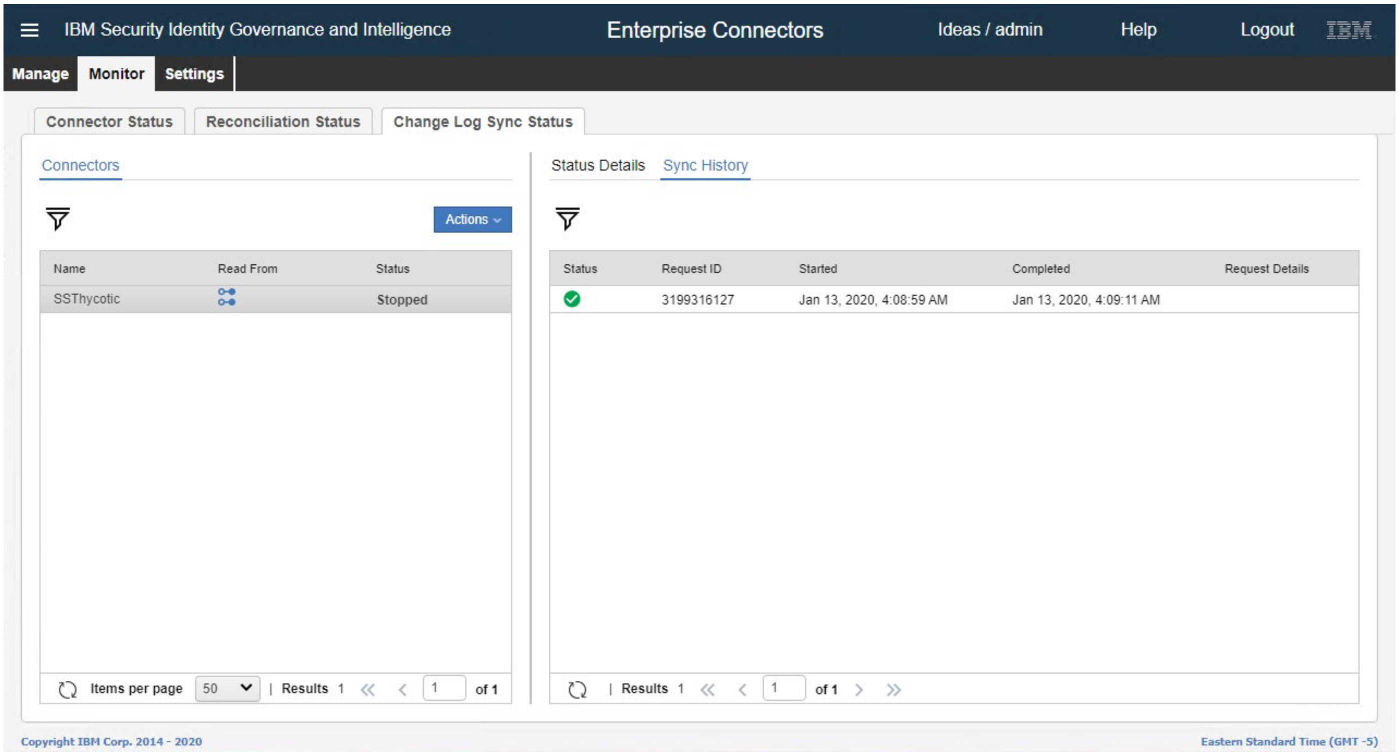
Schedule

Frequency Once

Effective Immediately □

Effective Date Jan 13, 2020 03 : 13 AM

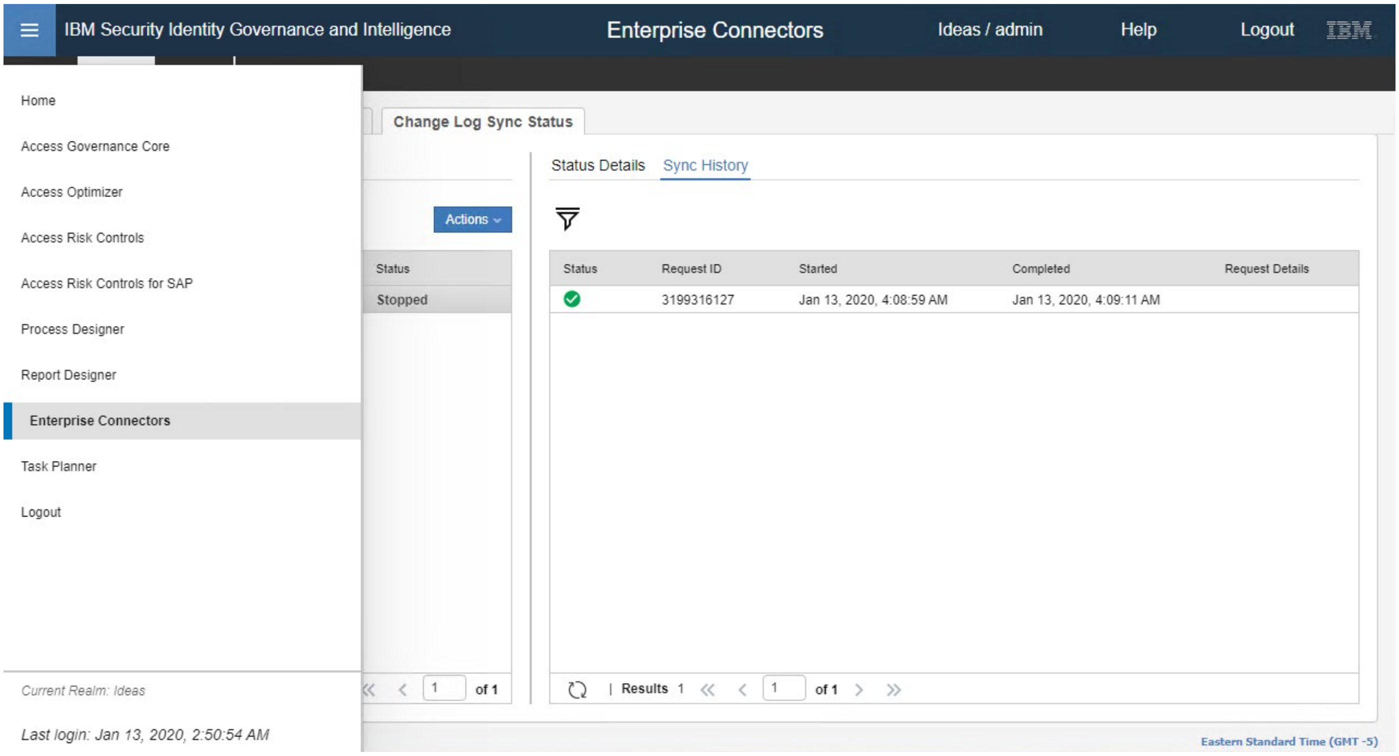
23. To verify the synch, on the right-hand side click **Sync History**. The sync must be completed.



Name	Read From	Status
SSThycotic		Stopped

Status	Request ID	Started	Completed	Request Details
✓	3199316127	Jan 13, 2020, 4:08:59 AM	Jan 13, 2020, 4:09:11 AM	

24. In the menu on the left-hand side, click **Access Governance Core**.



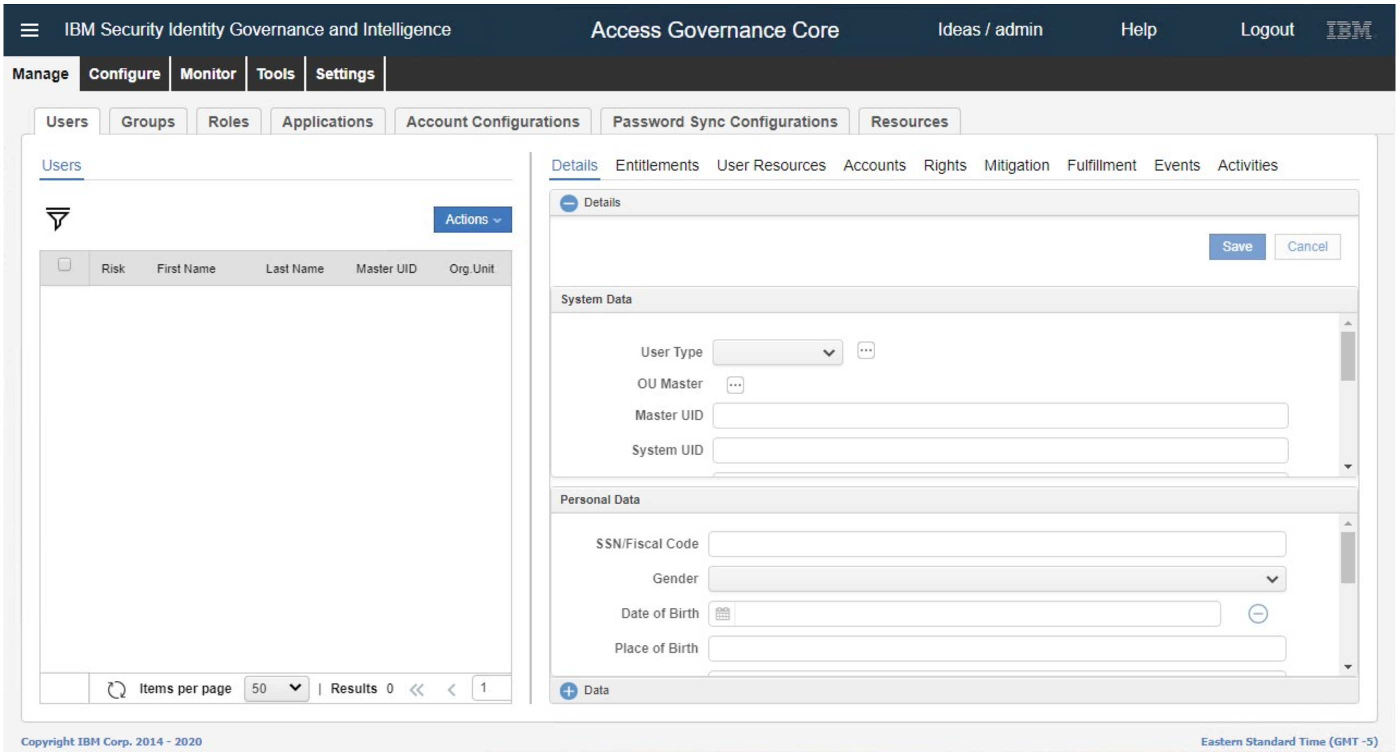
Status	Request ID	Started	Completed	Request Details
✓	3199316127	Jan 13, 2020, 4:08:59 AM	Jan 13, 2020, 4:09:11 AM	

Current Realm: Ideas

Last login: Jan 13, 2020, 2:50:54 AM

Eastern Standard Time (GMT -5)

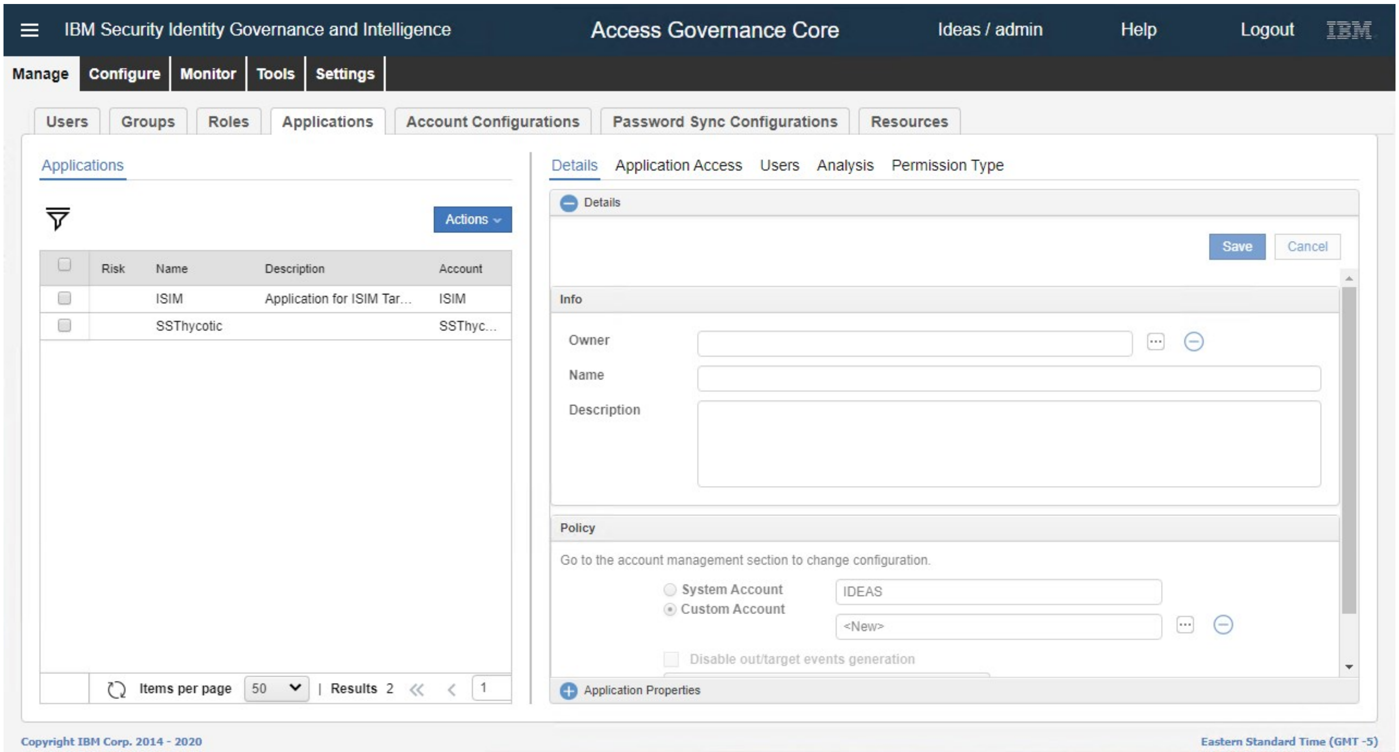
25. The **Access Governance Core** UI appears.



Copyright IBM Corp. 2014 - 2020

Eastern Standard Time (GMT -5)

26. Click **Manage** | **Applications**.



☐	Risk	Name	Description	Account
☐		ISIM	Application for ISIM Tar...	ISIM
☐		SSThycotic		SSThyc...

Items per page 50 | Results 2 | 1

Details

Info

Owner:

Name:

Description:

Policy

Go to the account management section to change configuration.

○ System Account: IDEAS

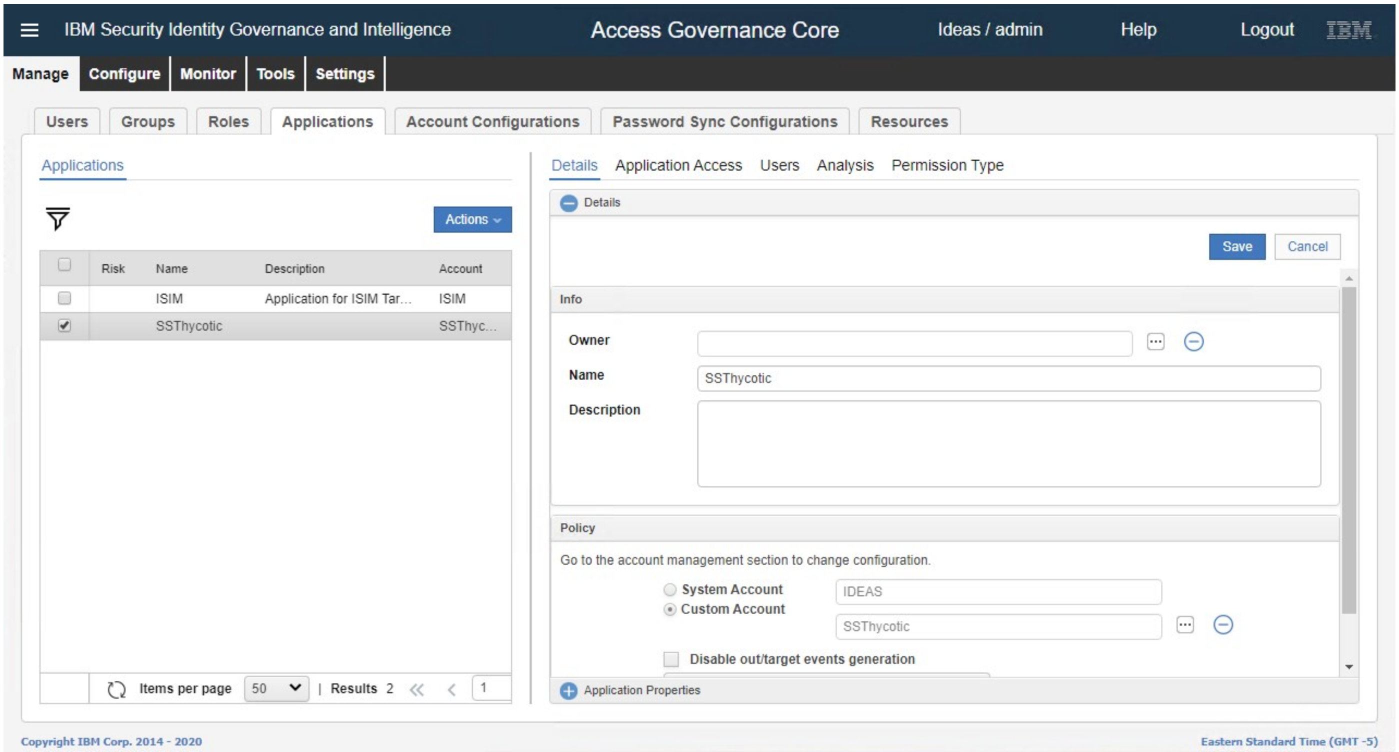
● Custom Account: <New>

☐ Disable out/target events generation

Copyright IBM Corp. 2014 - 2020

Eastern Standard Time (GMT -5)

27. Select the account.



☐	Risk	Name	Description	Account
☐		ISIM	Application for ISIM Tar...	ISIM
☑		SSThycotic		SSThyc...

Items per page 50 | Results 2 | 1

Details

Info

Owner:

Name: SSThycotic

Description:

Policy

Go to the account management section to change configuration.

○ System Account: IDEAS

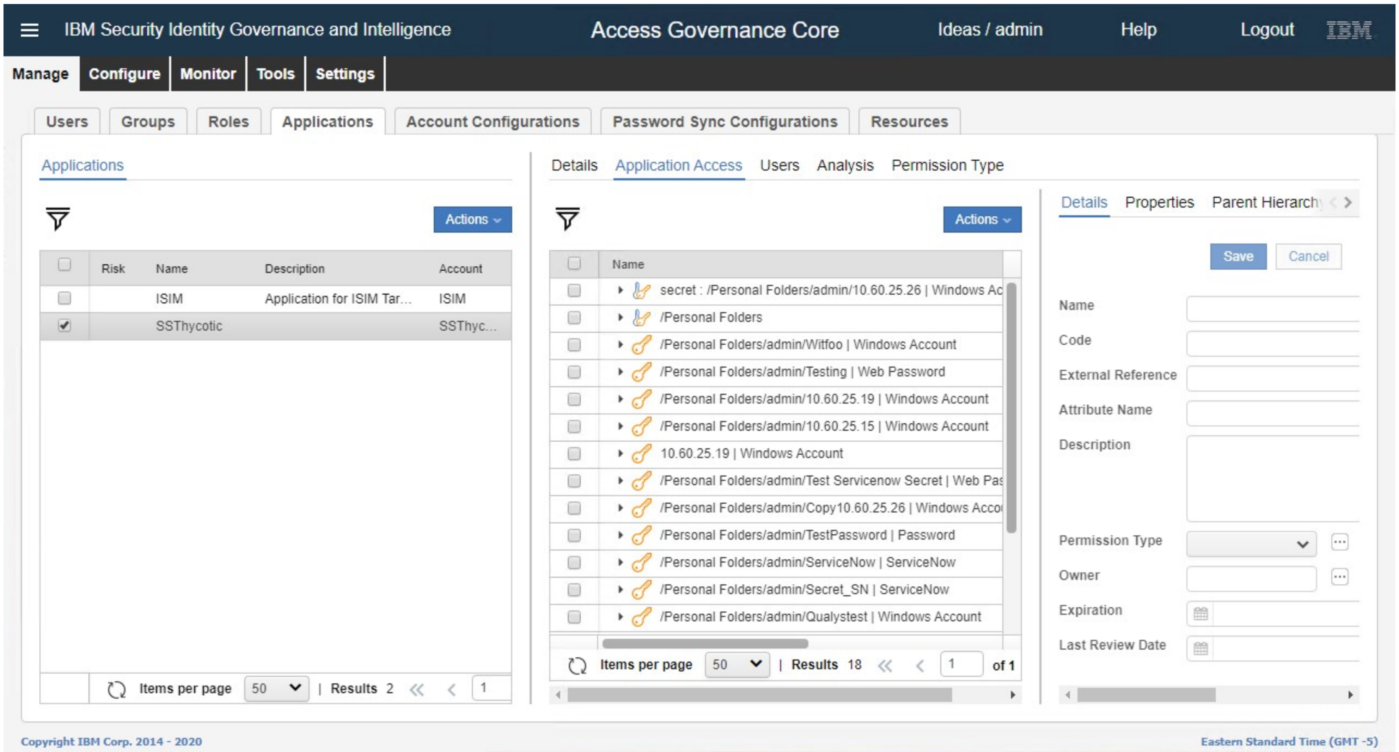
● Custom Account: SSThycotic

☐ Disable out/target events generation

Copyright IBM Corp. 2014 - 2020

Eastern Standard Time (GMT -5)

28. On the right-hand side, click **Application Access**. All the information from Secret Server appears.



	Risk	Name	Description	Account
□		ISIM	Application for ISIM Tar...	ISIM
☑		SSThycotic		SSThyc...

Items per page 50 | Results 2 1

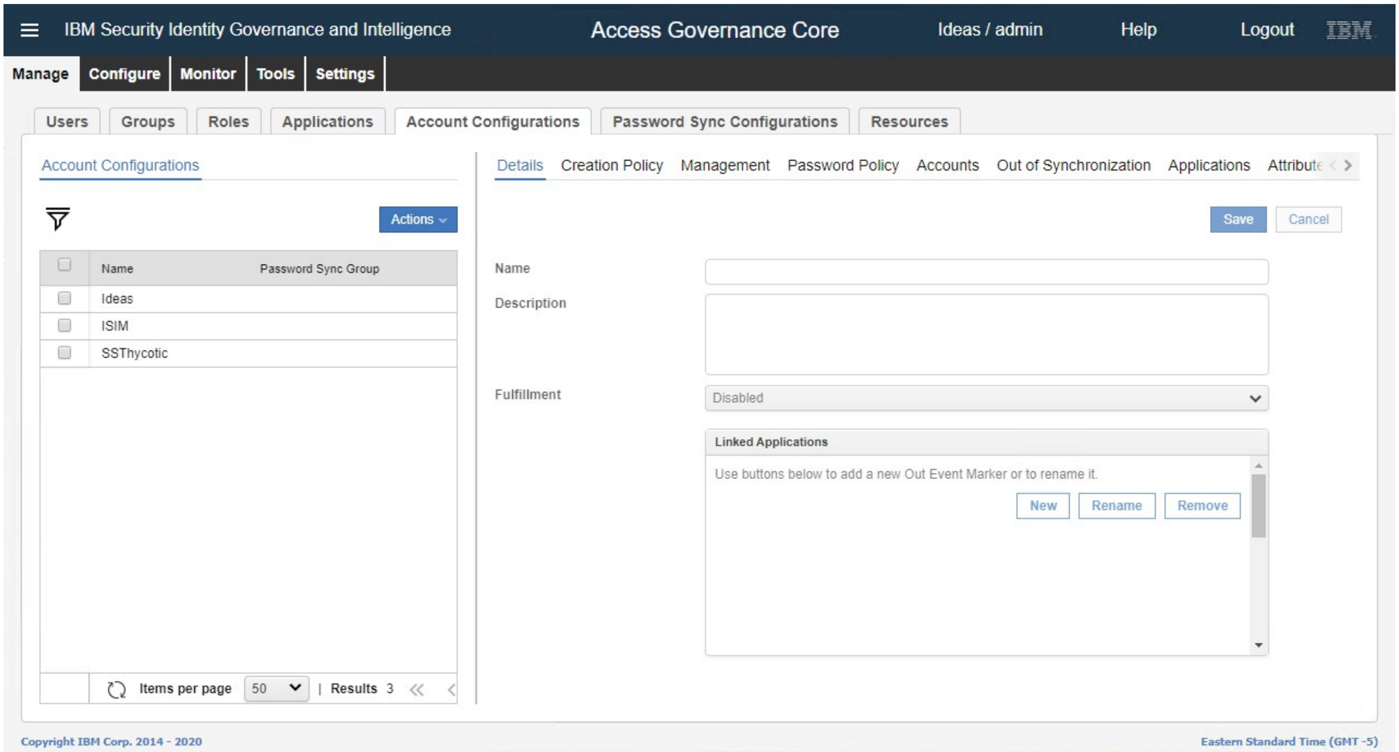
	Name
□	secret : /Personal Folders/admin/10.60.25.26 | Windows Ac
□	/Personal Folders
□	/Personal Folders/admin/Witfoo | Windows Account
□	/Personal Folders/admin/Testing | Web Password
□	/Personal Folders/admin/10.60.25.19 | Windows Account
□	/Personal Folders/admin/10.60.25.15 | Windows Account
□	10.60.25.19 | Windows Account
□	/Personal Folders/admin/Test Servicenow Secret | Web Pas
□	/Personal Folders/admin/Copy10.60.25.26 | Windows Acco
□	/Personal Folders/admin/TestPassword | Password
□	/Personal Folders/admin/ServiceNow | ServiceNow
□	/Personal Folders/admin/Secret_SN | ServiceNow
□	/Personal Folders/admin/Qualystest | Windows Account

Items per page 50 | Results 18 1 of 1

Name
Code
External Reference
Attribute Name
Description
Permission Type
Owner
Expiration
Last Review Date

Copyright IBM Corp. 2014 - 2020
Eastern Standard Time (GMT -5)

29. Click **Manage** | **Account Configurations**.



	Name	Password Sync Group
□	Ideas	
□	ISIM	
□	SSThycotic	

Items per page 50 | Results 3

Name

Description

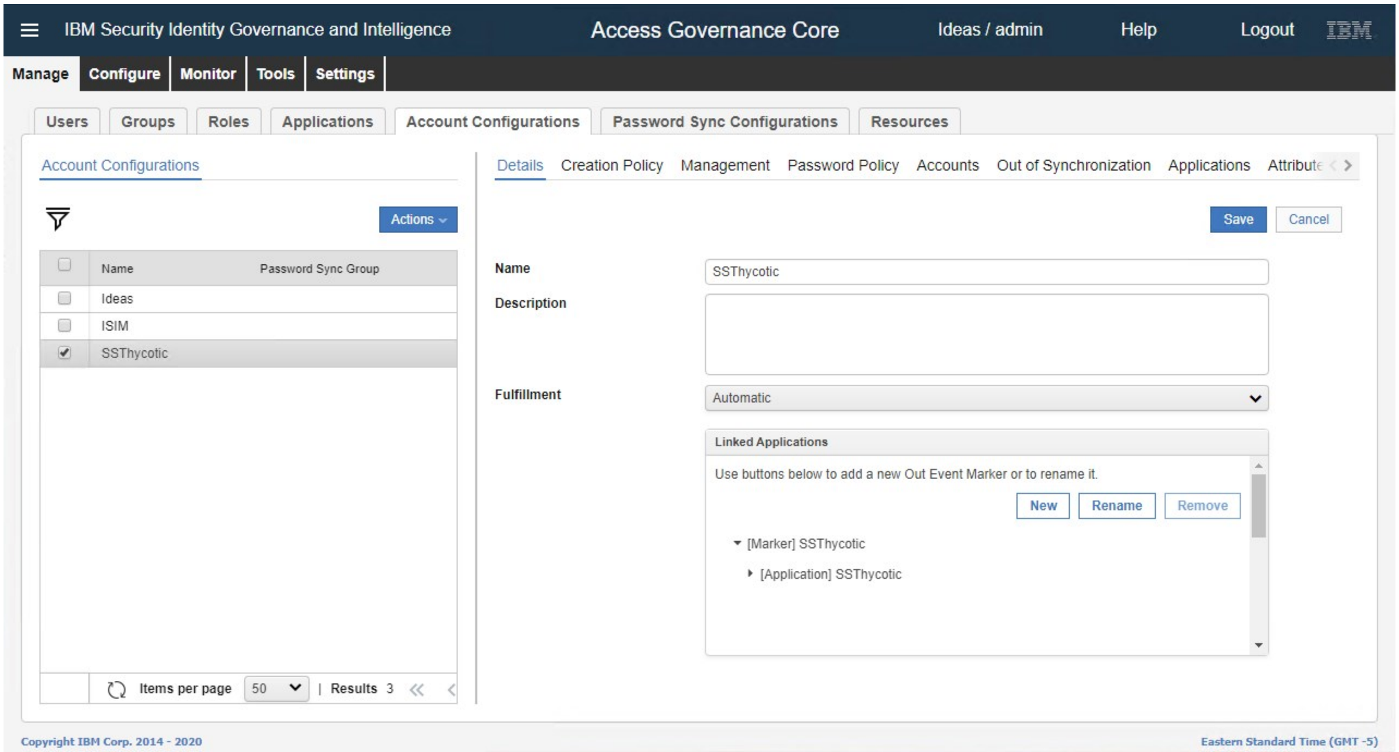
Fulfillment: Disabled

Linked Applications

Use buttons below to add a new Out Event Marker or to rename it.

Copyright IBM Corp. 2014 - 2020
Eastern Standard Time (GMT -5)

30. Select the account.



□	Name	Password Sync Group
□	Ideas	
□	ISIM	
☑	SSThycotic	

Items per page 50 | Results 3

Name: SSThycotic

Description:

Fulfillment: Automatic

Linked Applications

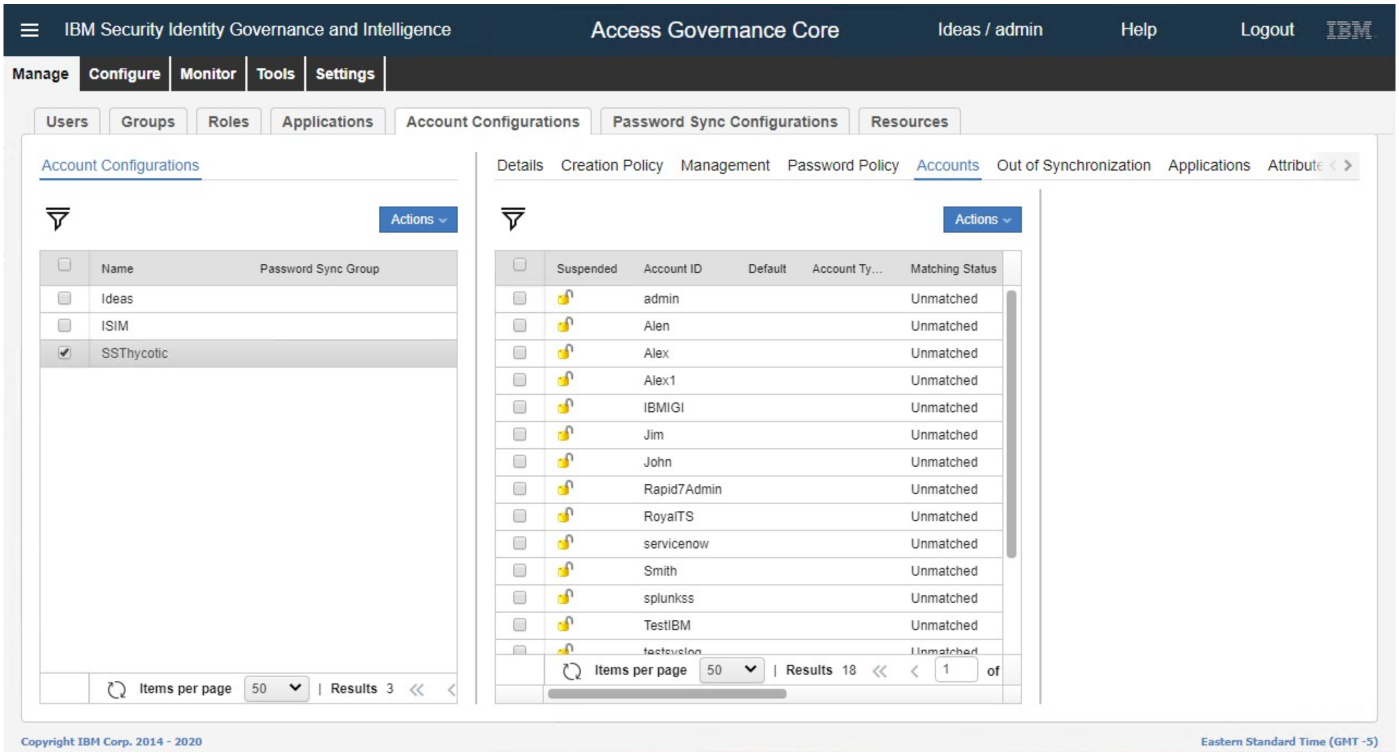
Use buttons below to add a new Out Event Marker or to rename it.

- [Marker] SSThycotic
  - [Application] SSThycotic

Copyright IBM Corp. 2014 - 2020

Eastern Standard Time (GMT -5)

31. On the right-hand side, click **Accounts**. All the users of secret server appear.



□	Name	Password Sync Group
□	Ideas	
□	ISIM	
☑	SSThycotic	

Items per page 50 | Results 3

□	Suspended	Account ID	Default	Account Ty...	Matching Status
□	🔓	admin			Unmatched
□	🔓	Alen			Unmatched
□	🔓	Alex			Unmatched
□	🔓	Alex1			Unmatched
□	🔓	IBMIGI			Unmatched
□	🔓	Jim			Unmatched
□	🔓	John			Unmatched
□	🔓	Rapid7Admin			Unmatched
□	🔓	RoyalTS			Unmatched
□	🔓	servicenow			Unmatched
□	🔓	Smith			Unmatched
□	🔓	splunkss			Unmatched
□	🔓	TestIBM			Unmatched
□	🔓	testsyslog			Unmatched

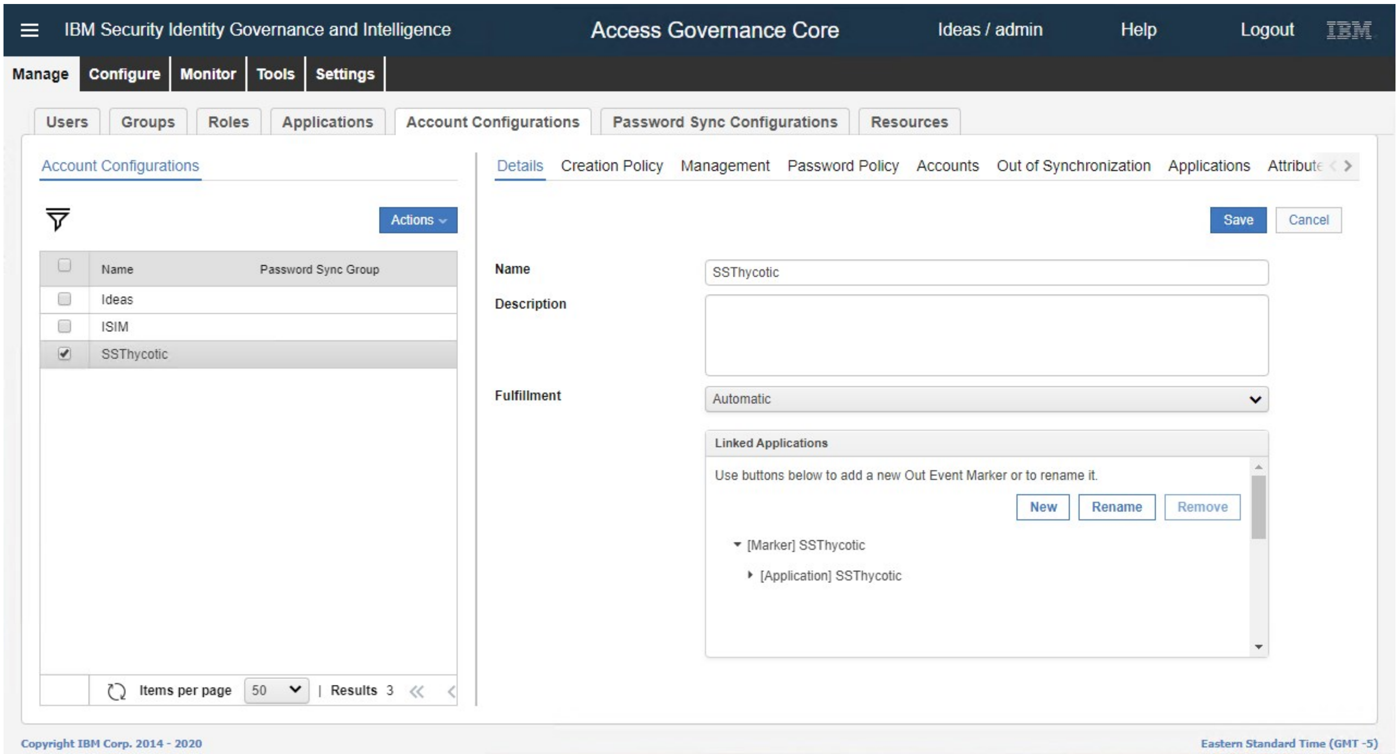
Items per page 50 | Results 18 1 of

Copyright IBM Corp. 2014 - 2020

Eastern Standard Time (GMT -5)

Update user details in Secret Server through IBM IGI

1. Click **Account Configurations**.



☐	Name	Password Sync Group
☐	Ideas	
☐	ISIM	
☑	SSThycotic	

Items per page 50 | Results 3

Name: SSThycotic

Description:

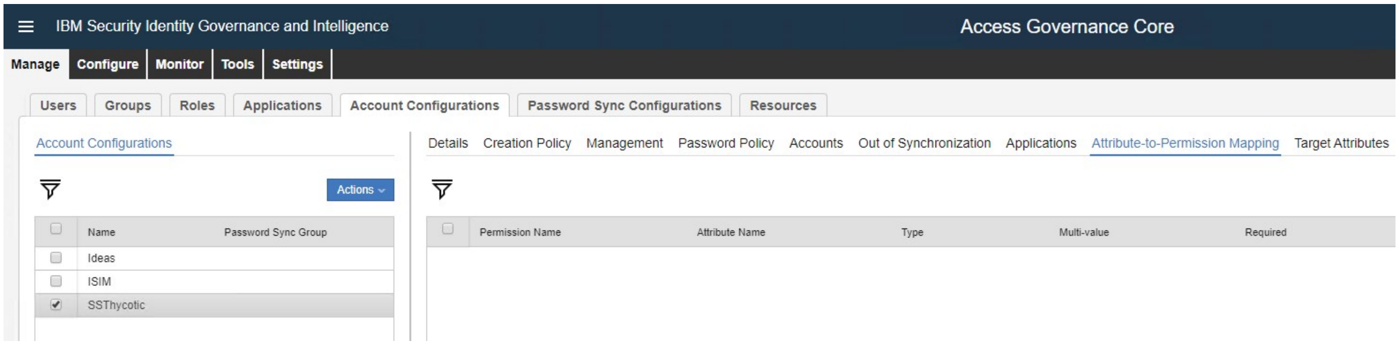
Fulfillment: Automatic

Linked Applications

Use buttons below to add a new Out Event Marker or to rename it.

- [Marker] SSThycotic
  - [Application] SSThycotic

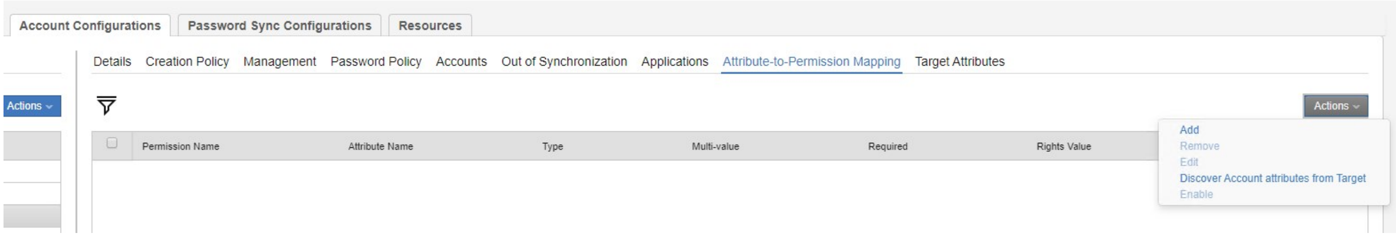
2. Select the account.
3. On the right-hand side, click **Attribute-to-Permission Mapping**.



☐	Name	Password Sync Group
☐	Ideas	
☐	ISIM	
☑	SSThycotic	

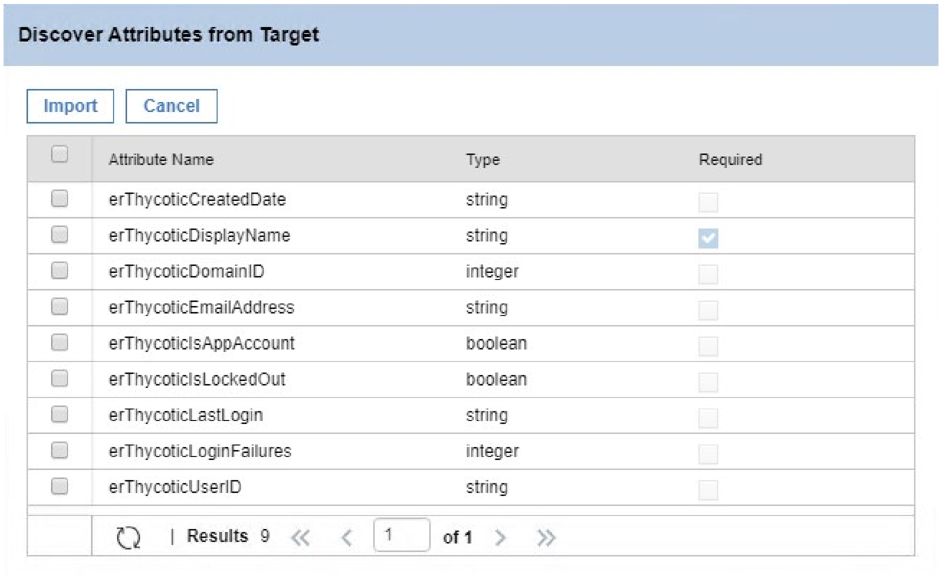
☐	Permission Name	Attribute Name	Type	Multi-value	Required

4. In the **Actions** list, click **Discover Account attributes from Target**.



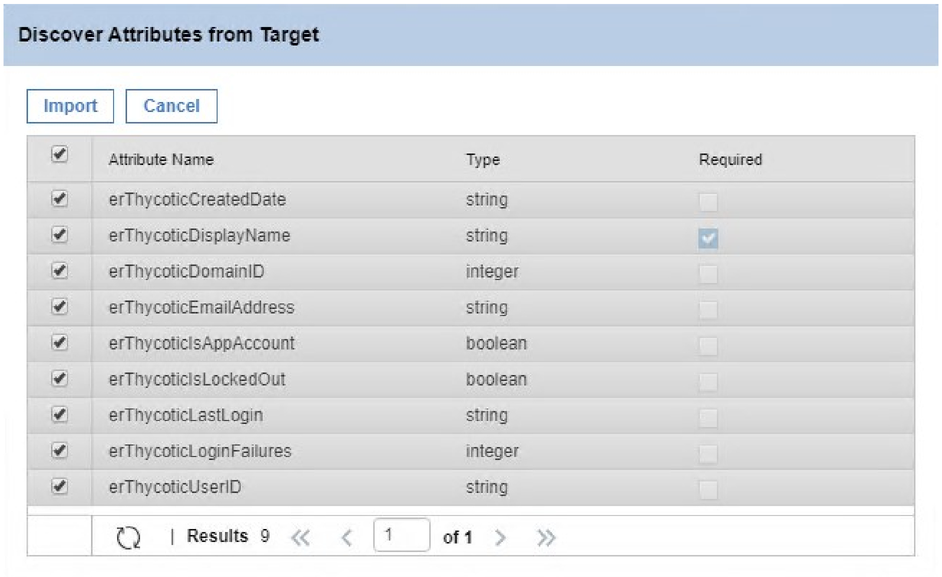
☐	Permission Name	Attribute Name	Type	Multi-value	Required	Rights Value

5. The **Discover Attributes from Target** dialog box appears.



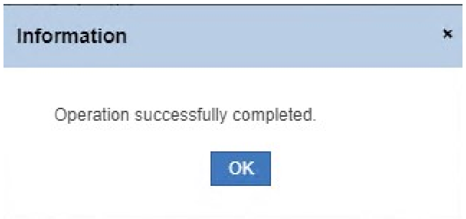
□	Attribute Name	Type	Required
□	erThycoticCreatedDate	string	□
□	erThycoticDisplayName	string	☑
□	erThycoticDomainID	integer	□
□	erThycoticEmailAddress	string	□
□	erThycoticIsAppAccount	boolean	□
□	erThycoticIsLockedOut	boolean	□
□	erThycoticLastLogin	string	□
□	erThycoticLoginFailures	integer	□
□	erThycoticUserID	string	□

6. Select the **Attribute Name** check box in the header.



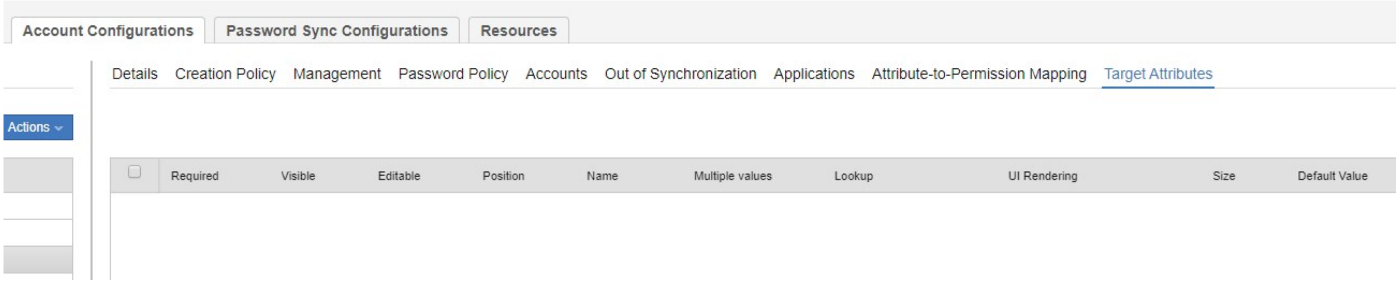
☑	Attribute Name	Type	Required
☑	erThycoticCreatedDate	string	□
☑	erThycoticDisplayName	string	☑
☑	erThycoticDomainID	integer	□
☑	erThycoticEmailAddress	string	□
☑	erThycoticIsAppAccount	boolean	□
☑	erThycoticIsLockedOut	boolean	□
☑	erThycoticLastLogin	string	□
☑	erThycoticLoginFailures	integer	□
☑	erThycoticUserID	string	□

7. Click **Import**. A message, '**Operation successfully completed.**' appears. Click **Ok**.The files are imported.

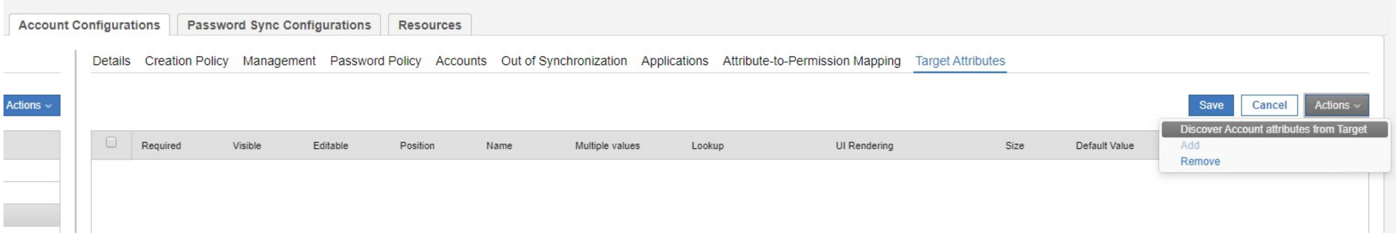


Operation successfully completed.

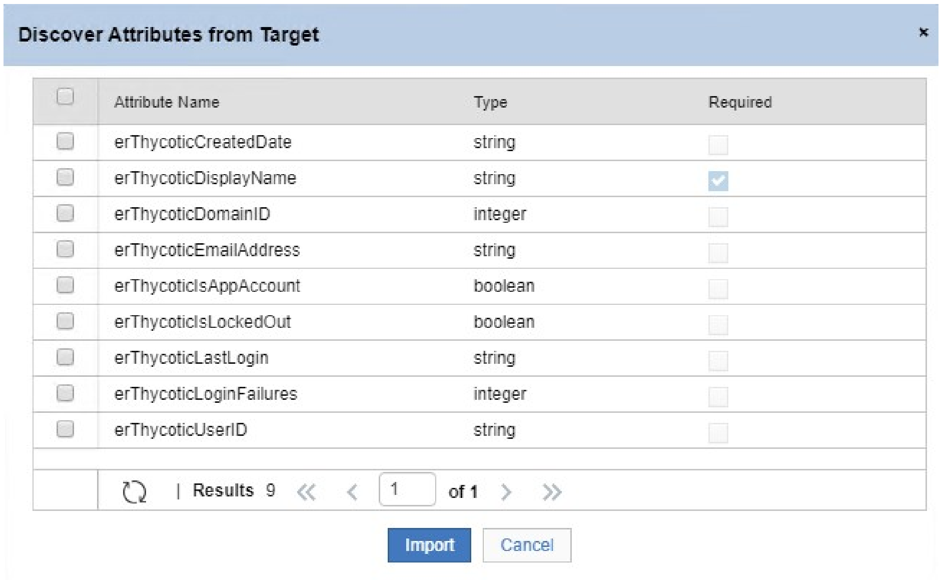
8. On the right-hand side, click **Target Attributes**.



9. In the **Actions** list, click **Discover Account attributes from Target**.

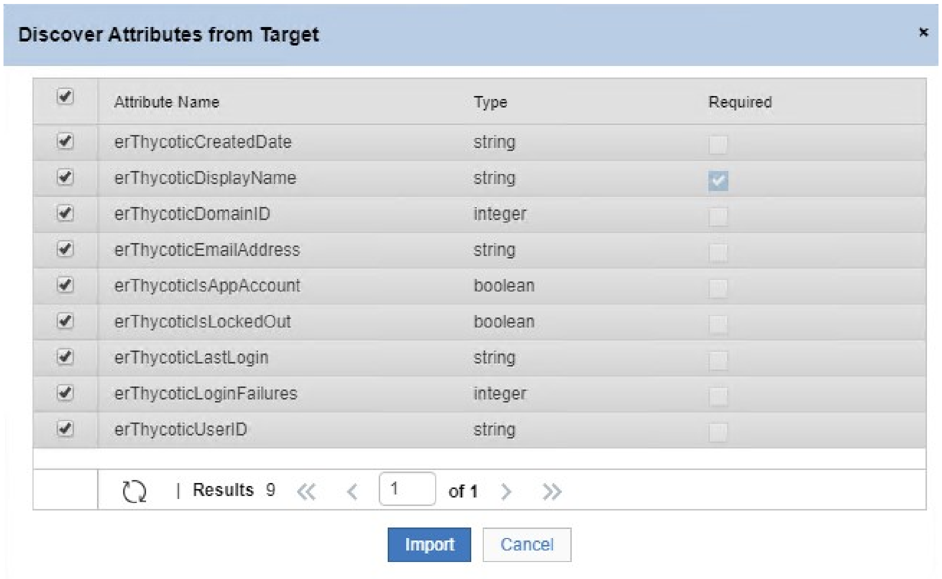


10. The **Discover Attributes from Target** dialog box appears.



□	Attribute Name	Type	Required
□	erThycoticCreatedDate	string	□
□	erThycoticDisplayName	string	☑
□	erThycoticDomainID	integer	□
□	erThycoticEmailAddress	string	□
□	erThycoticIsAppAccount	boolean	□
□	erThycoticIsLockedOut	boolean	□
□	erThycoticLastLogin	string	□
□	erThycoticLoginFailures	integer	□
□	erThycoticUserID	string	□

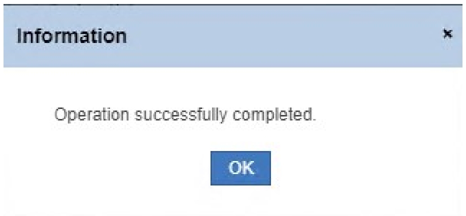
11. Select the **Attribute Name** check box in the header.



Discover Attributes from Target

☑	Attribute Name	Type	Required
☑	erThycoticCreatedDate	string	☐
☑	erThycoticDisplayName	string	☑
☑	erThycoticDomainID	integer	☐
☑	erThycoticEmailAddress	string	☐
☑	erThycoticIsAppAccount	boolean	☐
☑	erThycoticIsLockedOut	boolean	☐
☑	erThycoticLastLogin	string	☐
☑	erThycoticLoginFailures	integer	☐
☑	erThycoticUserID	string	☐

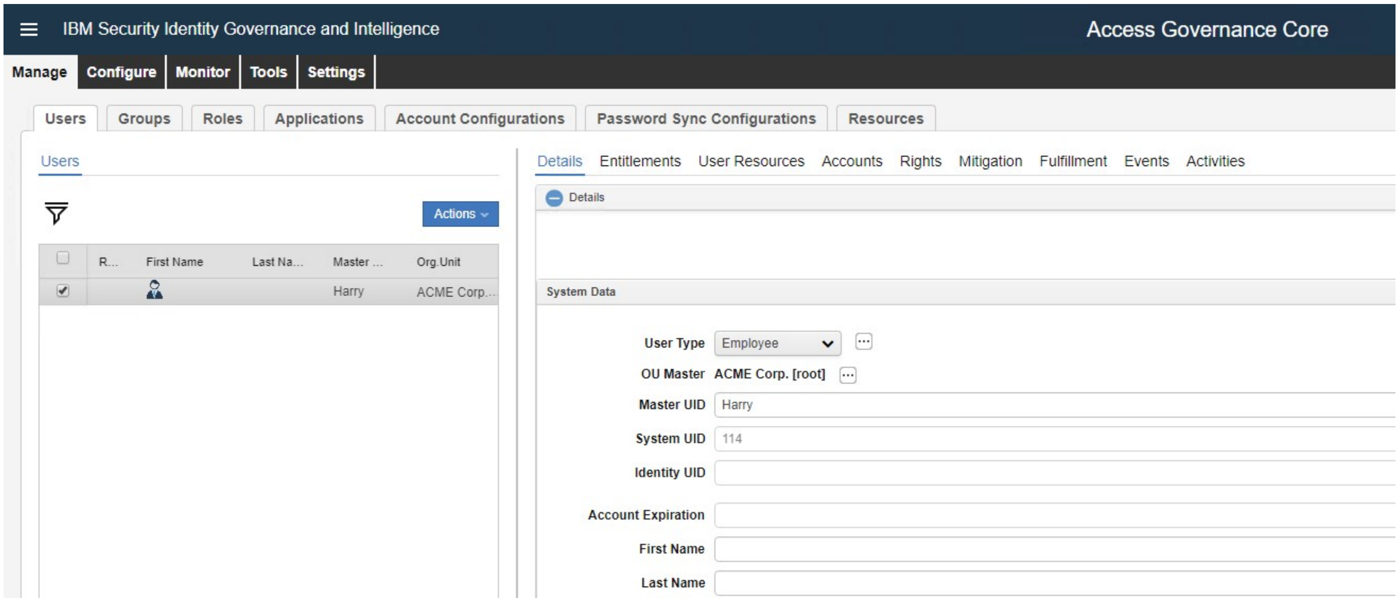
12. Click **Import**. A message, ‘**Operation successfully completed.**’ appears. Click **Ok**. The files are imported.



Information

Operation successfully completed.

13. On the left-hand side, select the **Users** tab.



☐	R...	First Name	Last Na...	Master ...	Org.Unit
☑				Harry	ACME Corp...

User Type: Employee

OU Master: ACME Corp. [root]

Master UID: Harry

System UID: 114

Identity UID:

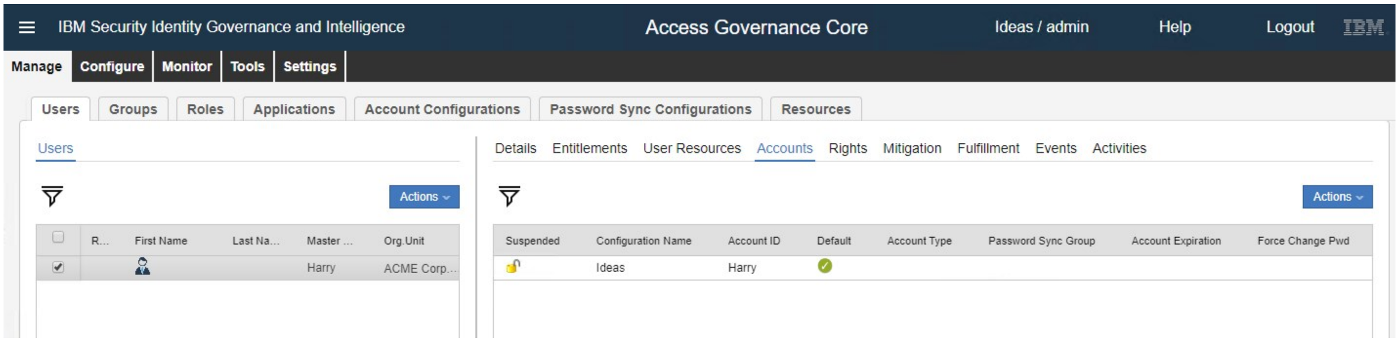
Account Expiration:

First Name:

Last Name:

14. Select the user.

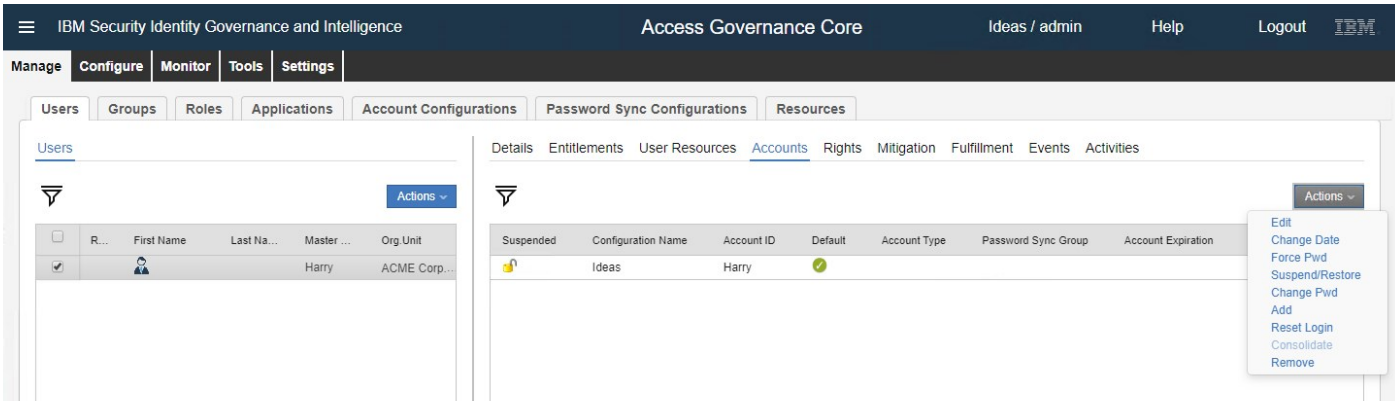
15. On the right-hand side, click **Accounts**. The master account is listed.



□	R...	First Name	Last Na...	Master ...	Org.Unit
☑				Harry	ACME Corp...

Suspended	Configuration Name	Account ID	Default	Account Type	Password Sync Group	Account Expiration	Force Change Pwd
	Ideas	Harry	✓				

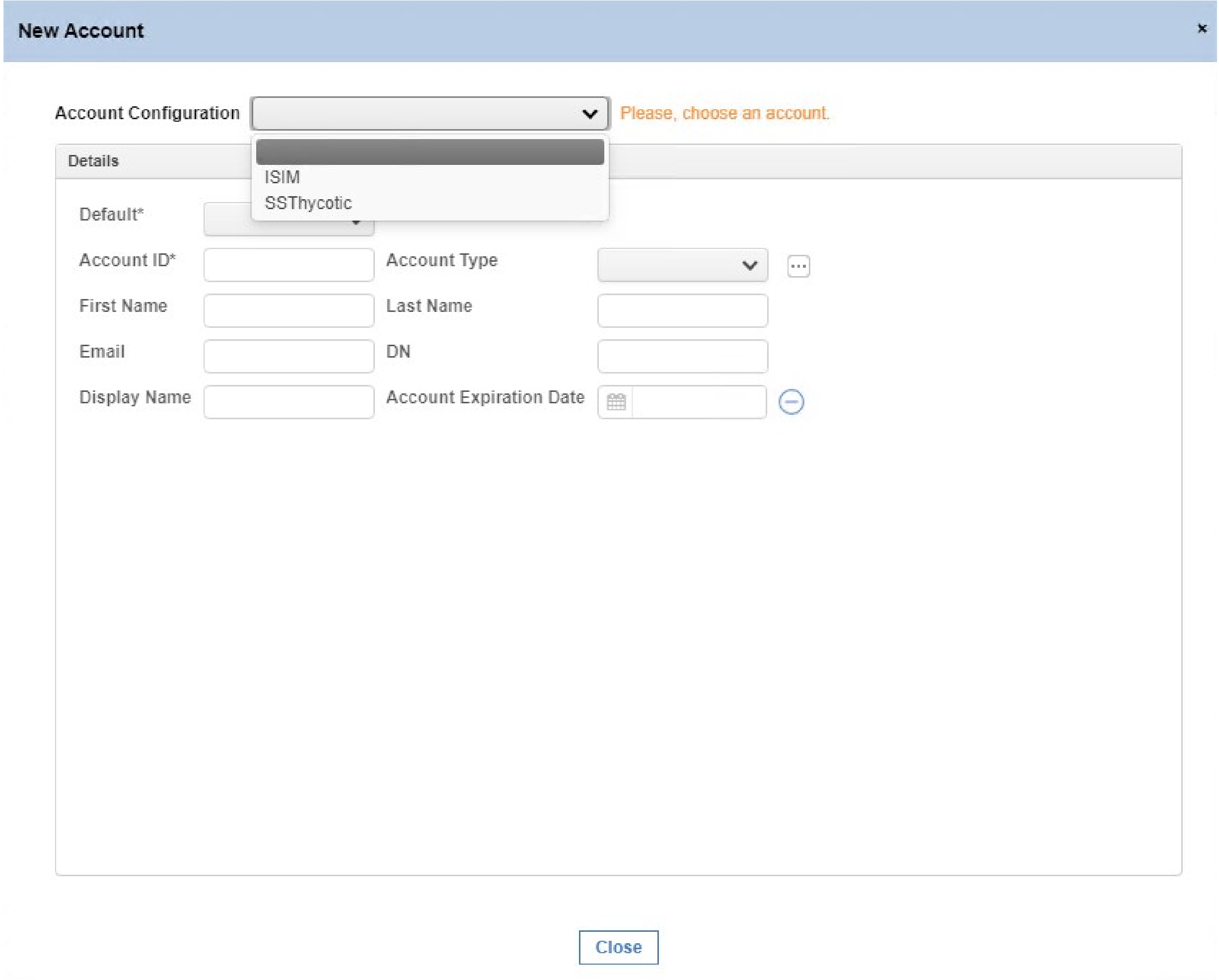
16. In the **Actions** list, click **Add**.



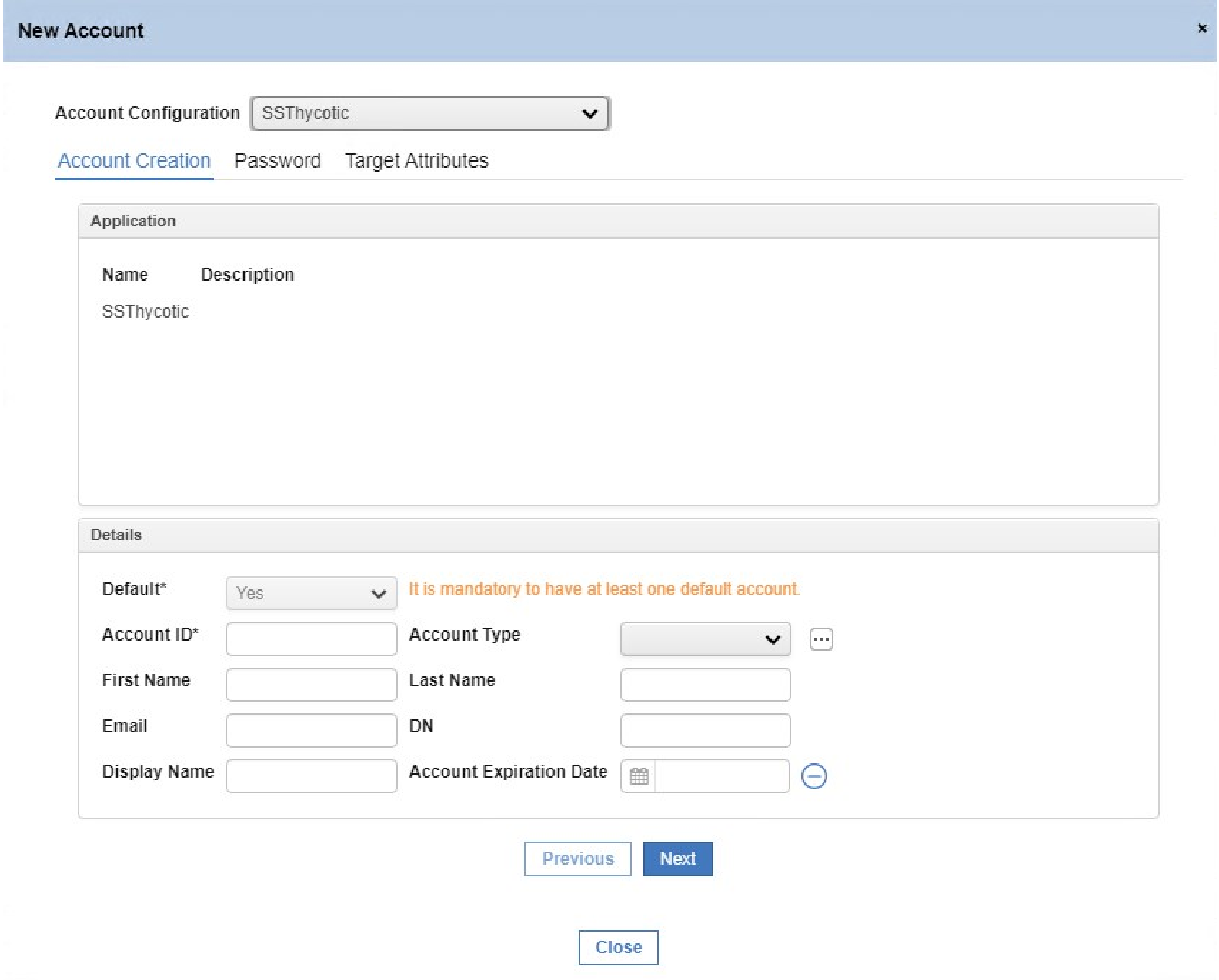
□	R...	First Name	Last Na...	Master ...	Org.Unit
☑				Harry	ACME Corp...

Suspended	Configuration Name	Account ID	Default	Account Type	Password Sync Group	Account Expiration
	Ideas	Harry	✓			

17. The **New Account** dialog box appears.



18. In the **Account Configuration** list, select the Secret Server account. The **Account Creation** tab is selected.



New Account

Account Configuration: SSThycotic

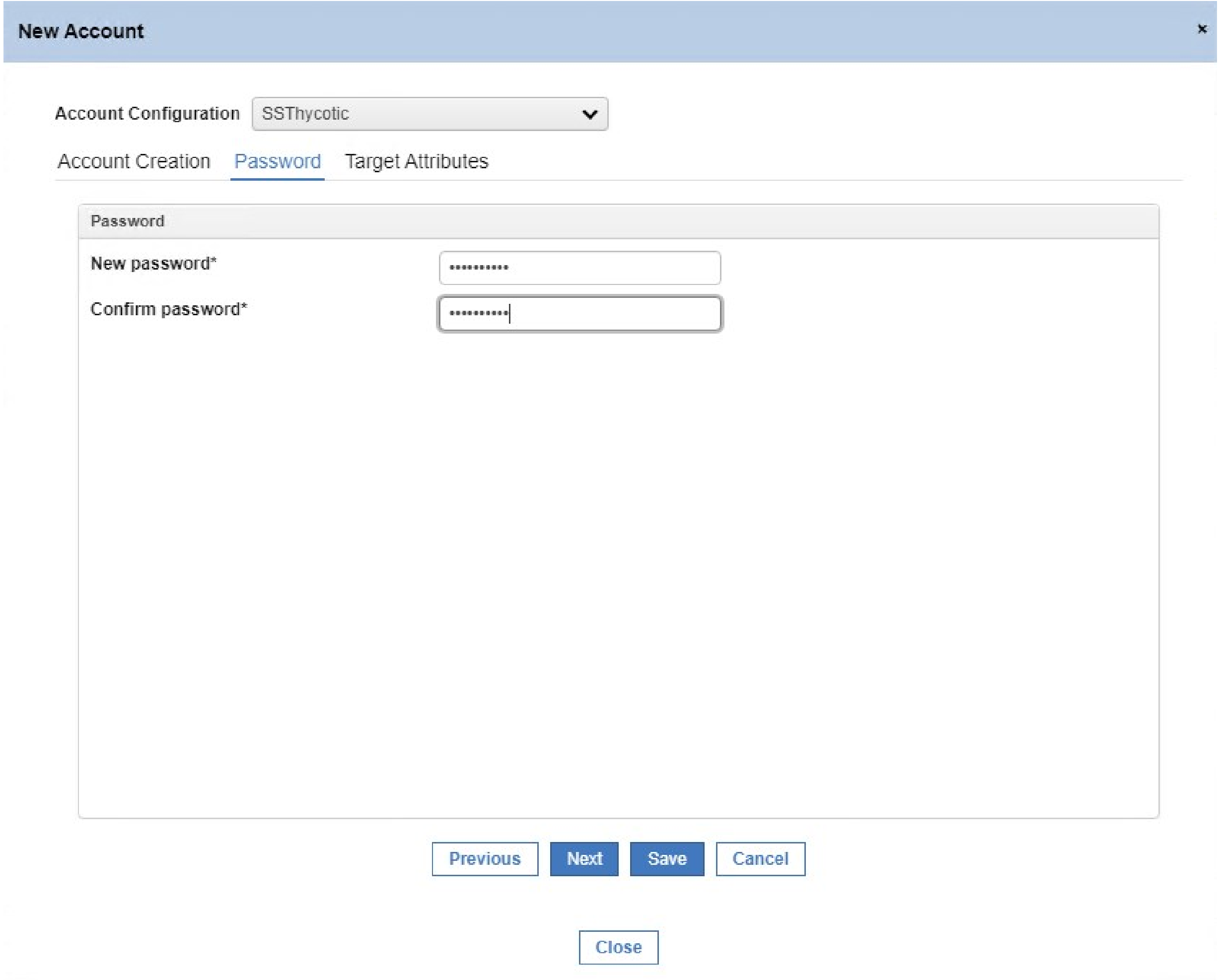
Name	Description
SSThycotic	

Default*: Yes

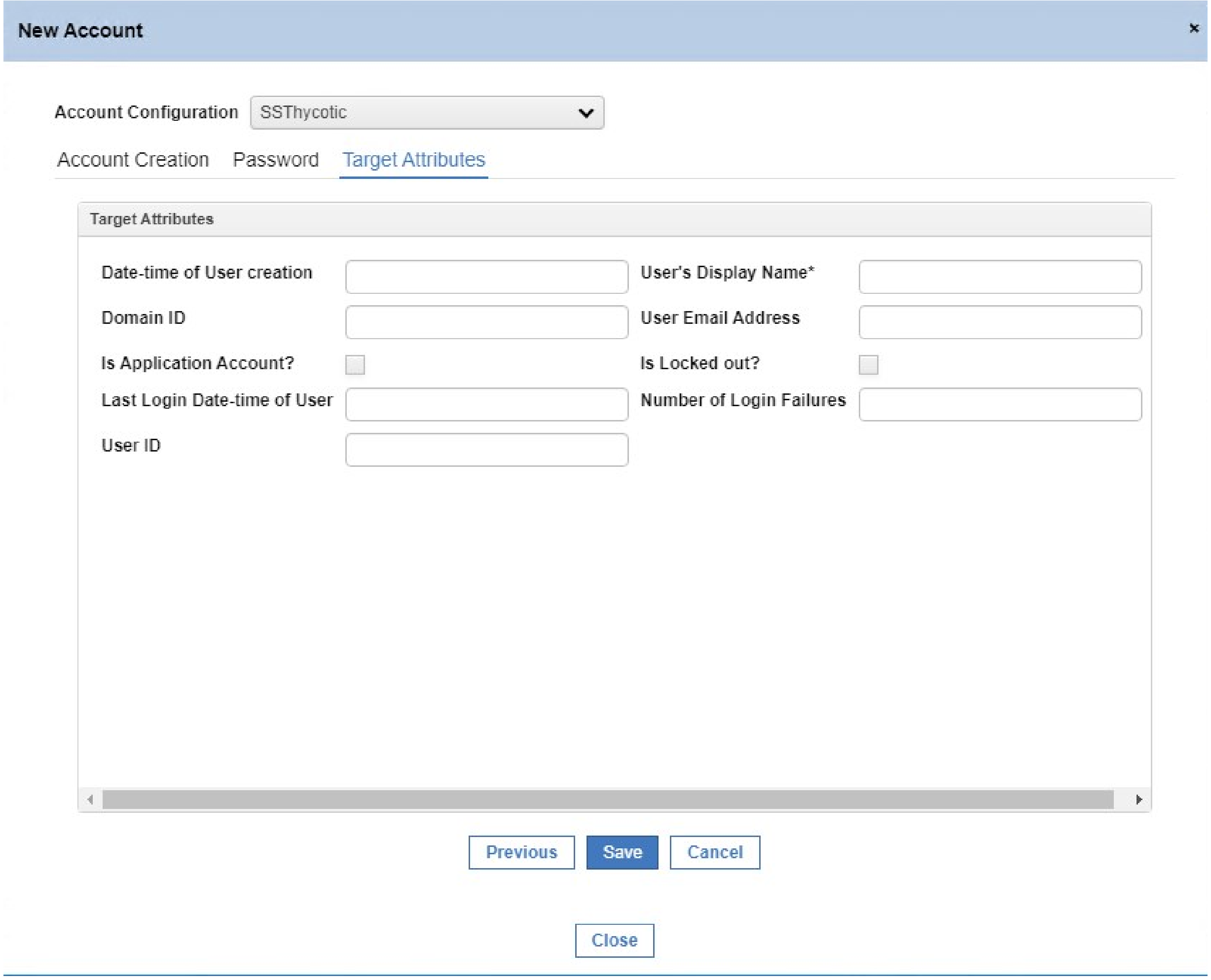
It is mandatory to have at least one default account.

19. Go to **Account Creation** tab> **Details** section > **Account ID**.

20. In the **Account ID** text box, type the account ID and click **Next**. The **Password** tab is selected.



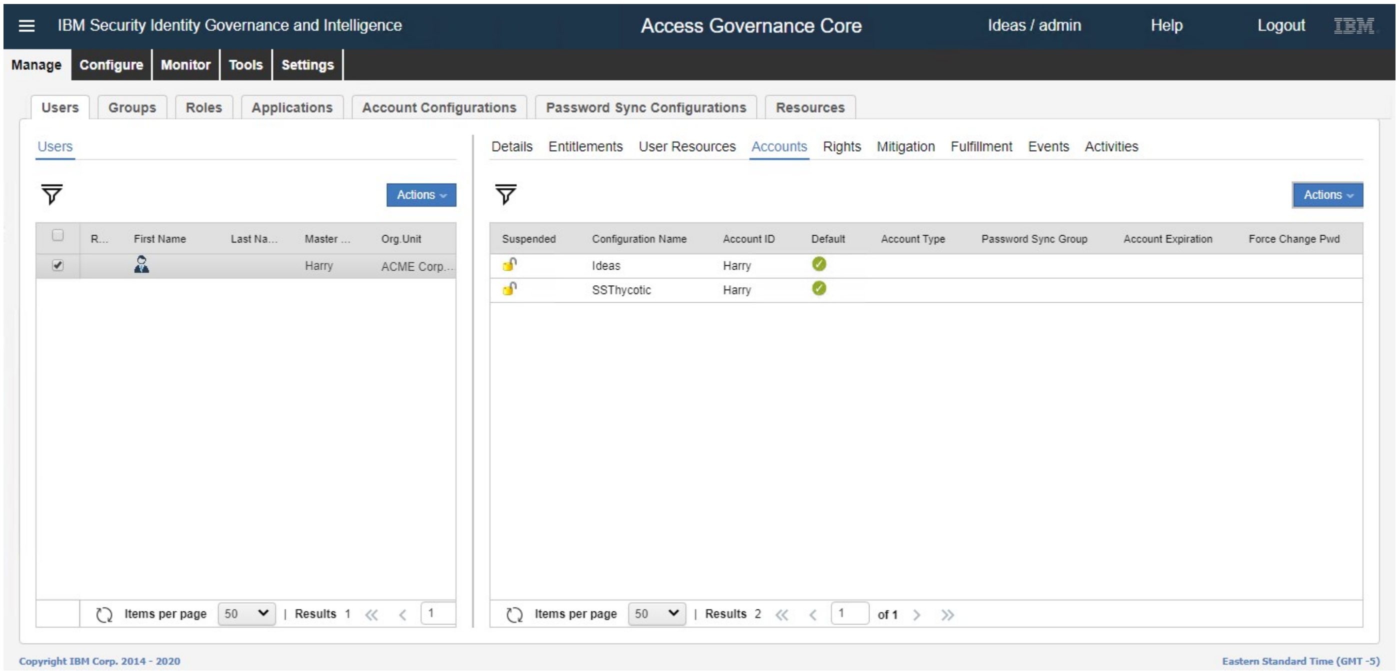
21. Fill in the required information, such as new password, confirm password, and then click **Next**. The **Target Attributes** tab is selcted.



Account Configuration: SSThycotic

22. In the **User’s Display Name** text box, type the display name for the user.

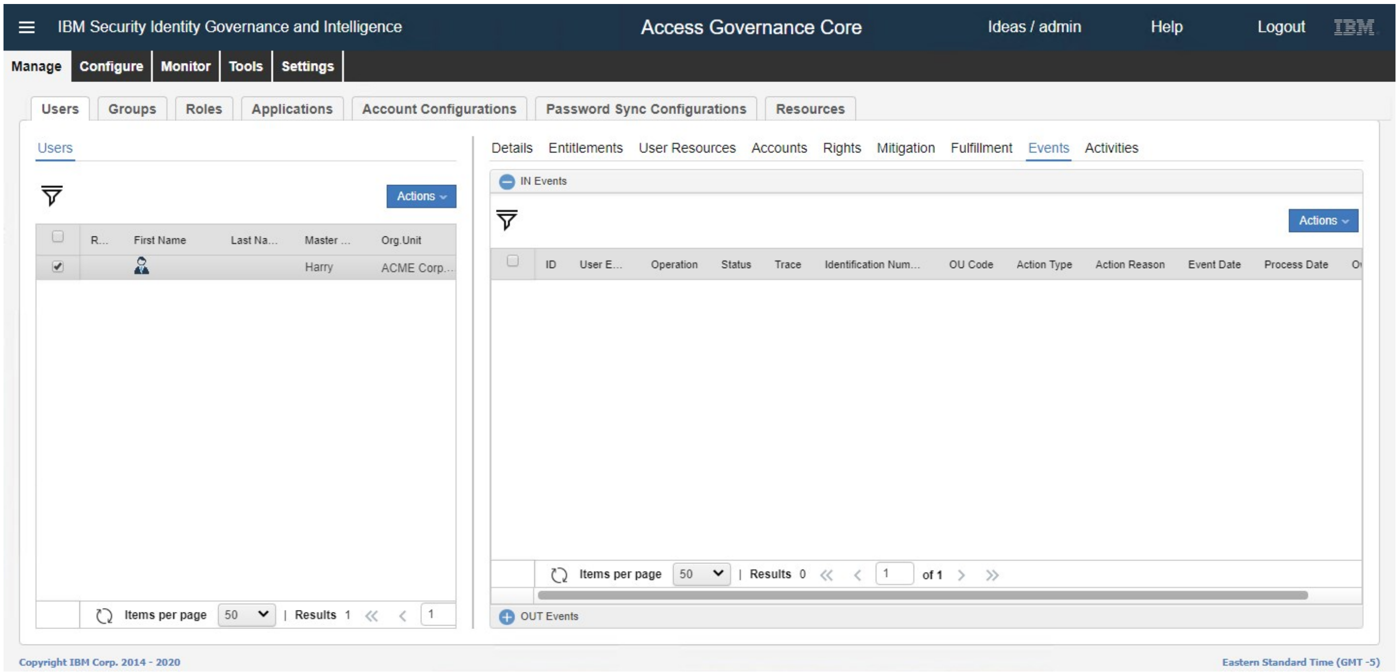
23. Click **Save**. The user is listed in the **Accounts** tab.



☐	R...	First Name	Last Na...	Master ...	Org.Unit
☑				Harry	ACME Corp...

Suspended	Configuration Name	Account ID	Default	Account Type	Password Sync Group	Account Expiration	Force Change Pwd
	Ideas	Harry	✓				
	SSThycotic	Harry	✓				

24. Click the **Events** tab.

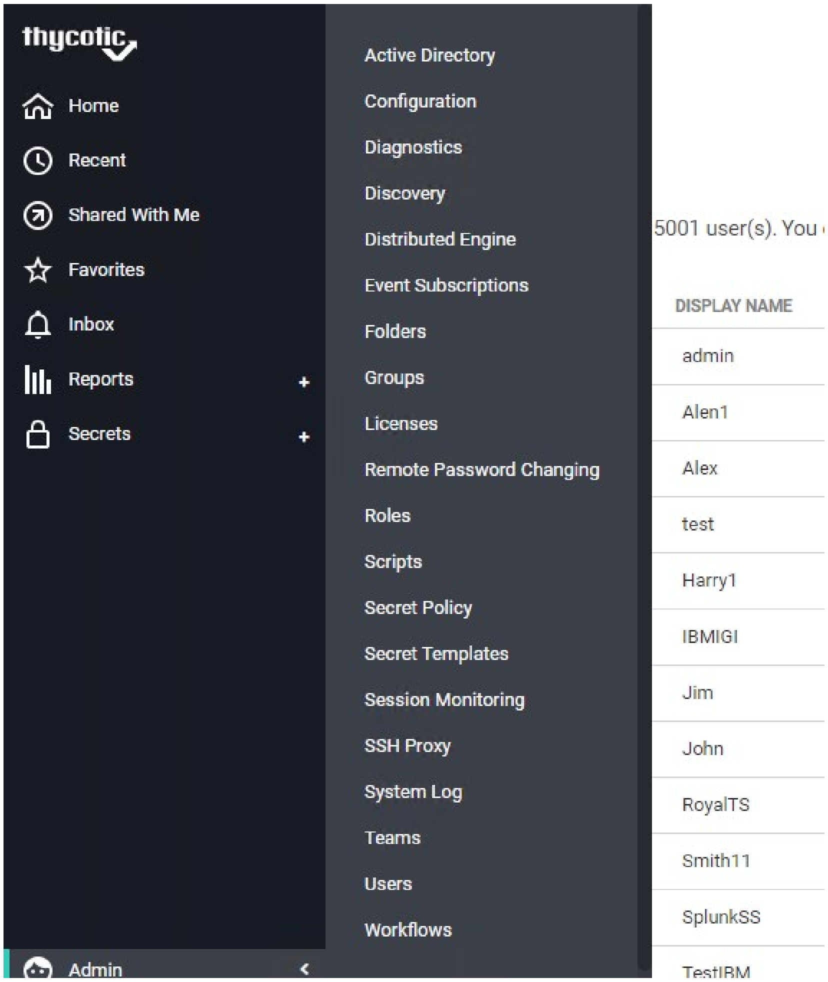


☐	R...	First Name	Last Na...	Master ...	Org.Unit
☑				Harry	ACME Corp...

☐	ID	User E...	Operation	Status	Trace	Identification Num...	OU Code	Action Type	Action Reason	Event Date	Process Date	O

25. At the bottom of the **Events** tab, click on **OUT Events**. The event is listed. Wait till the **Status** and the **ERC Status** is displayed as **Success**.

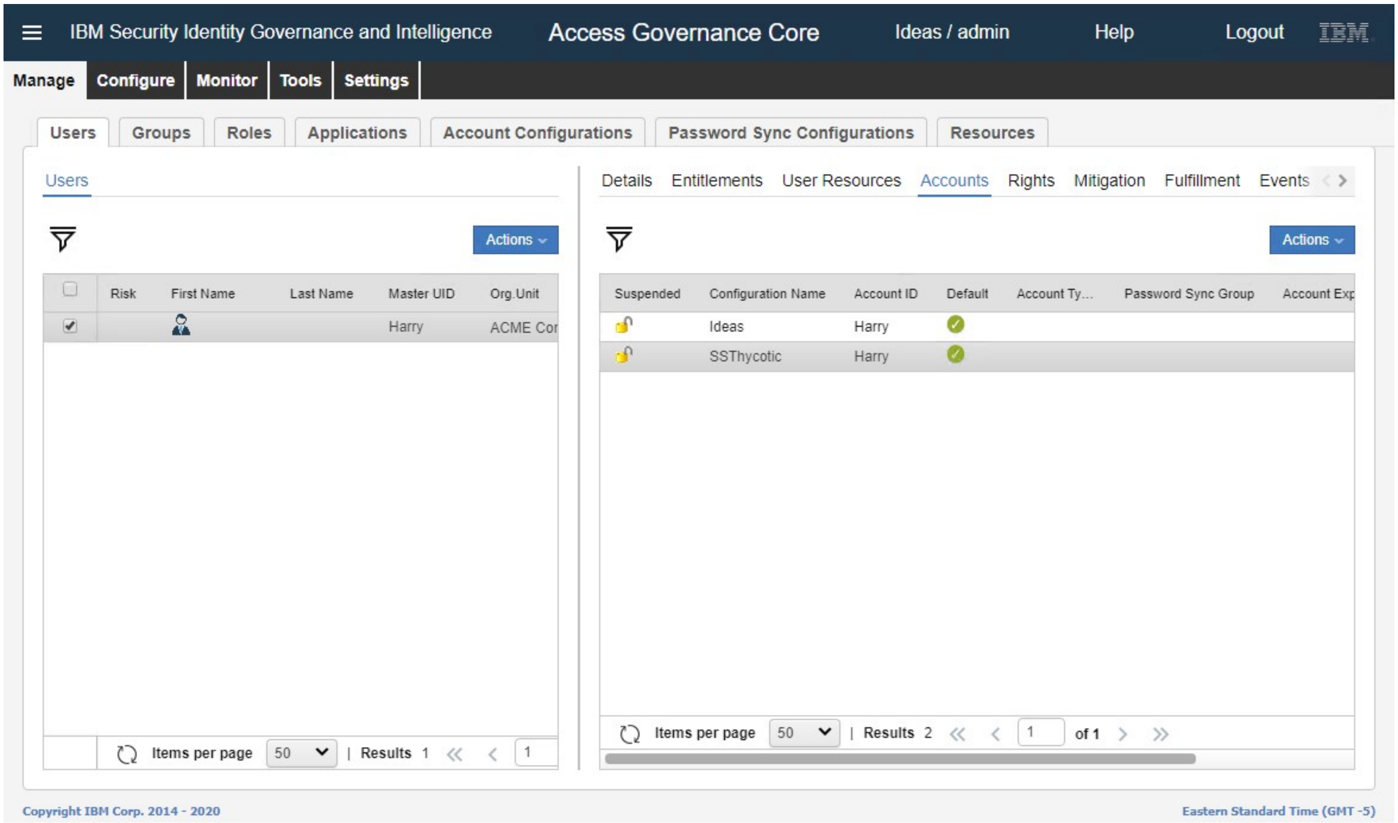
26. Go to **Secret Server | Admin | Users**.



5001 user(s). You

DISPLAY NAME
admin
Alen1
Alex
test
Harry1
IBMIGI
Jim
John
RoyalTS
Smith11
SplunkSS
TestIBM

27. The user is created in Secret Server. The user name and the display name for the user is displayed.
28. Go to **IBM IGI Administrator console** and in the menu click **Access Governance Core**.
29. Click **Manage** tab **Users I Accounts**.

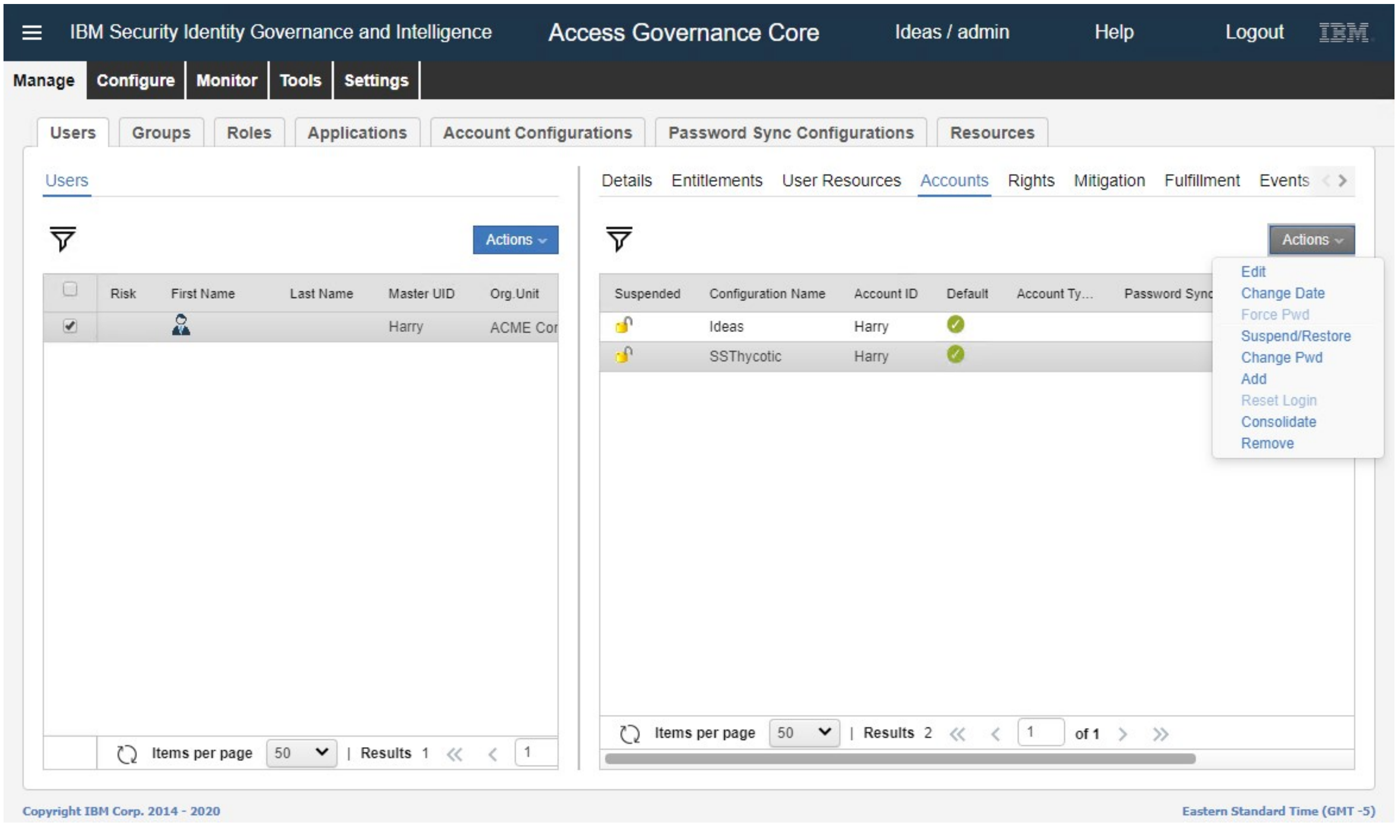


☐	Risk	First Name	Last Name	Master UID	Org.Unit
☑				Harry	ACME Cor

Suspended	Configuration Name	Account ID	Default	Account Ty...	Password Sync Group	Account Exp
	Ideas	Harry	✓			
	SSThycotic	Harry	✓			

30. Select the account.

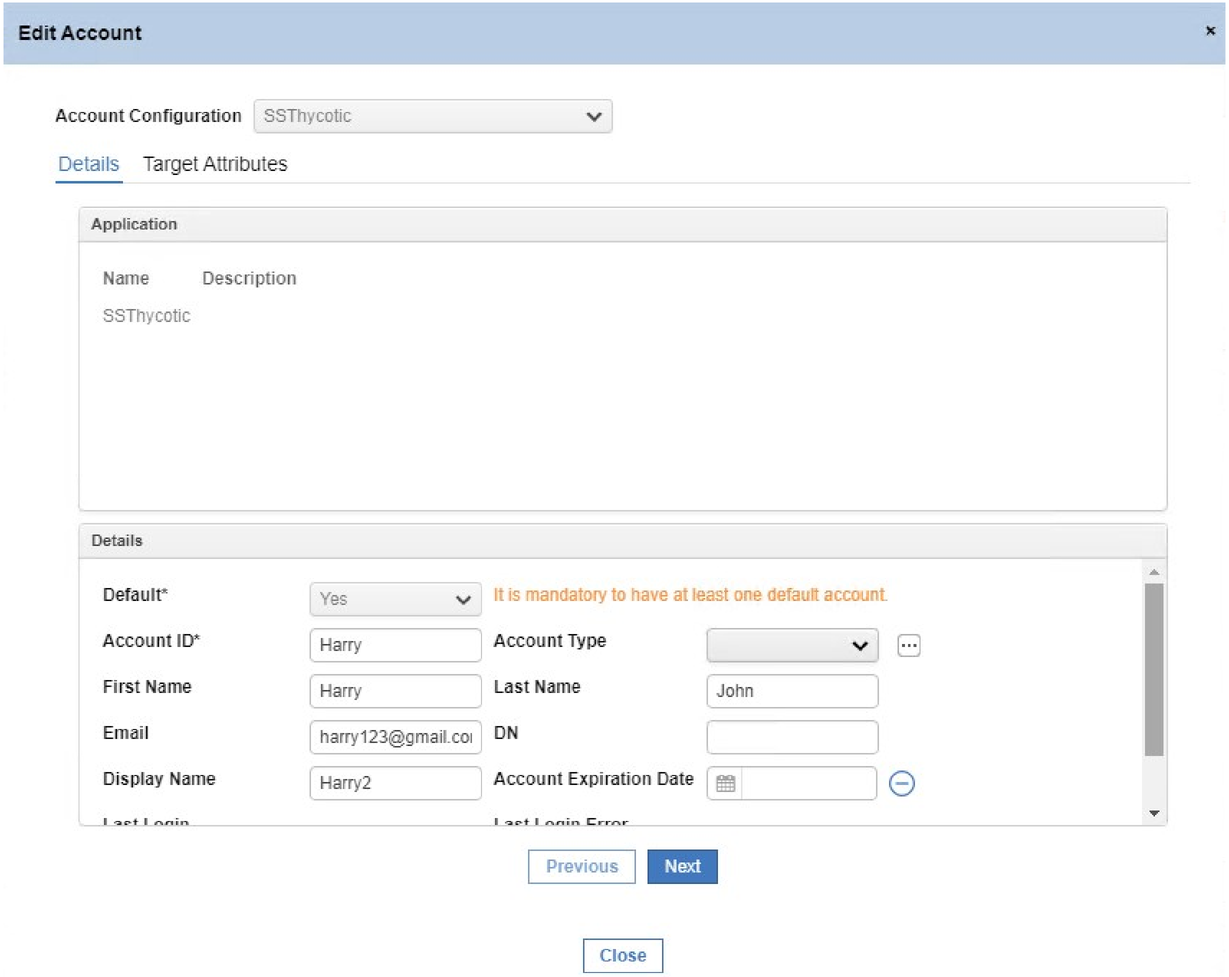
31. In the **Action** list, click **Edit**.



☐	Risk	First Name	Last Name	Master UID	Org.Unit
☑				Harry	ACME Cor

Suspended	Configuration Name	Account ID	Default	Account Ty...	Password Sync
	Ideas	Harry	✓		
	SSThycotic	Harry	✓		

32. The **Edit Account** dialog box appears.



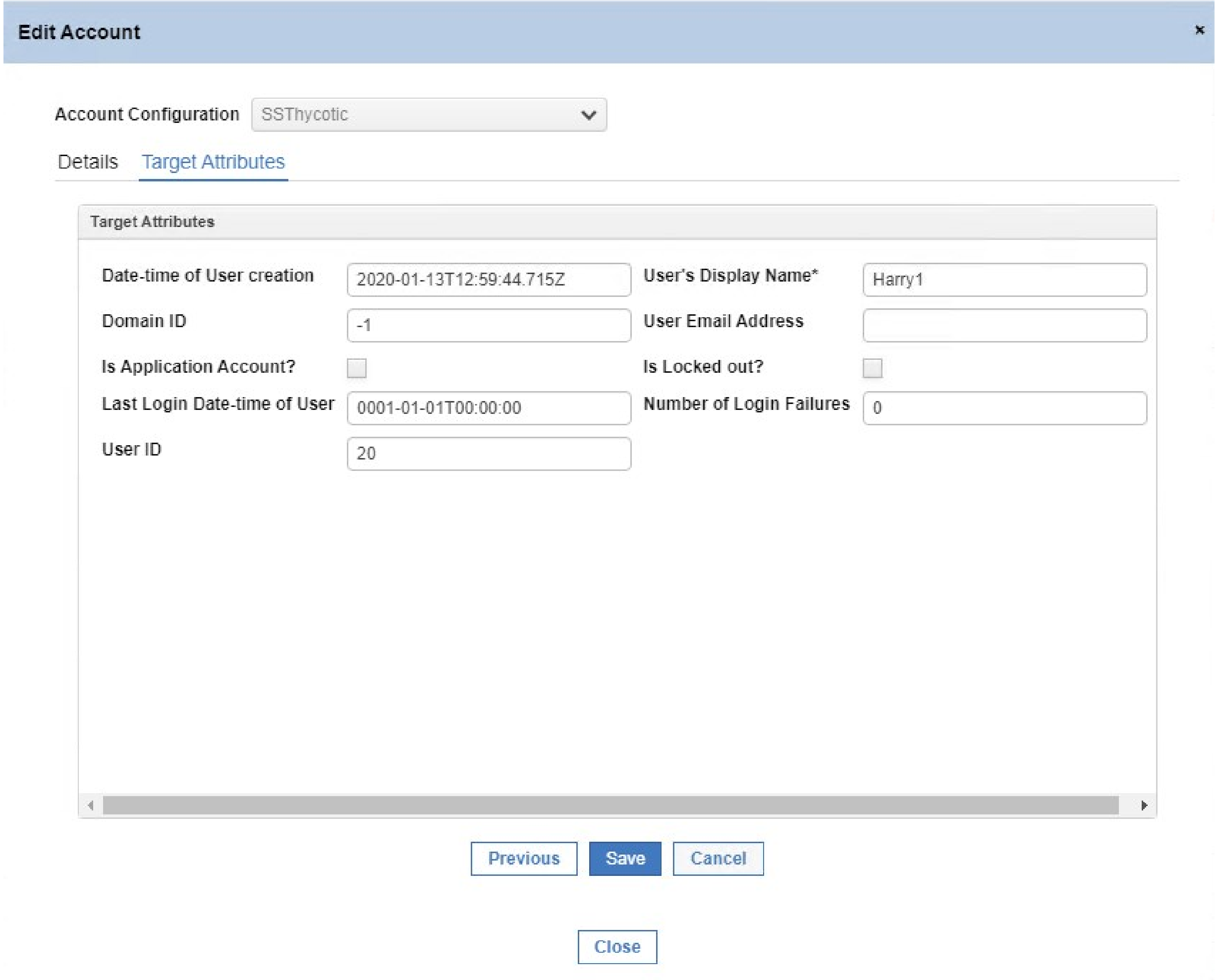
Edit Account

Account Configuration: SSThycotic

SSThycotic

Default*	Yes	It is mandatory to have at least one default account.	
Account ID*	Harry	Account Type	
First Name	Harry	Last Name	John
Email	harry123@gmail.coı	DN	
Display Name	Harry2	Account Expiration Date	
Last Login		Last Login Error	

33. Fill in the required information, such as first name, last name, email, display name, and then click **Next**. The **Target Attributes** tab appears.



Edit Account

Account Configuration: SSThycotic

Target Attributes

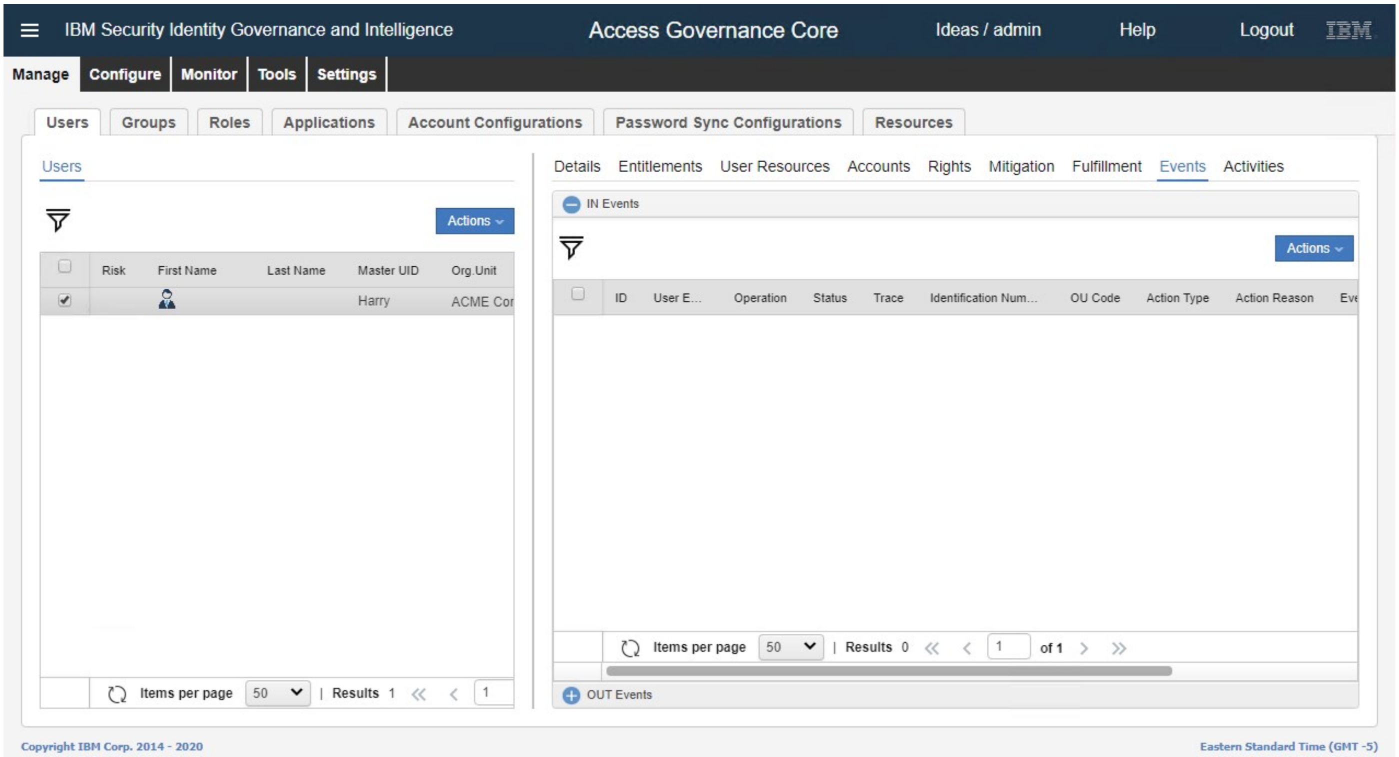
Date-time of User creation	2020-01-13T12:59:44.715Z	User's Display Name*	Harry1
Domain ID	-1	User Email Address	
Is Application Account?	□	Is Locked out?	□
Last Login Date-time of User	0001-01-01T00:00:00	Number of Login Failures	0
User ID	20		

34. In the **User's Display Name** text box, change the display name for the user.

35. Click **Save**.

36. Click the **Events** tab.

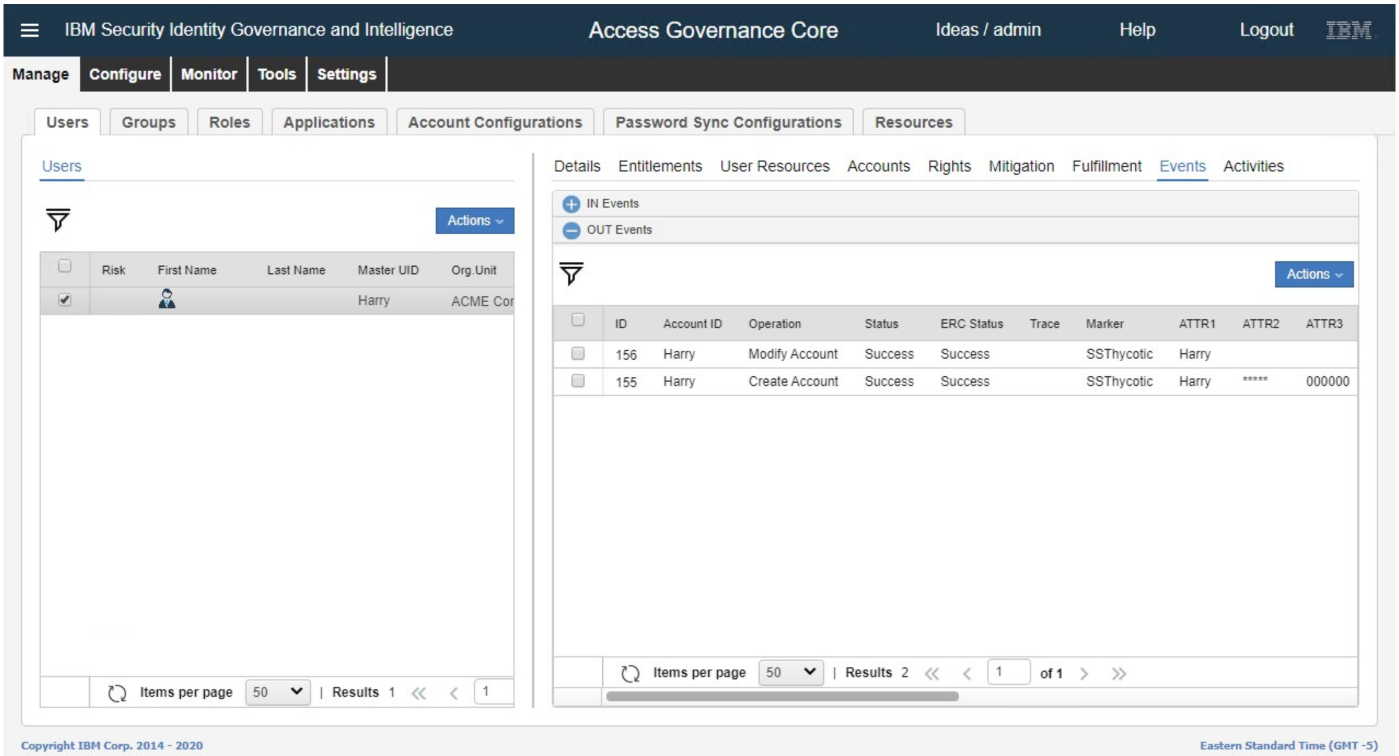
37. At the bottom of the **Events** section, click **OUT Event**.



□	Risk	First Name	Last Name	Master UID	Org.Unit
☑				Harry	ACME Cor

□	ID	User E...	Operation	Status	Trace	Identification Num...	OU Code	Action Type	Action Reason	Eve

38. The event is listed. Wait till the **Status** and the **ERC Status** is displayed as **Success**.



□	Risk	First Name	Last Name	Master UID	Org.Unit
☑				Harry	ACME Cor

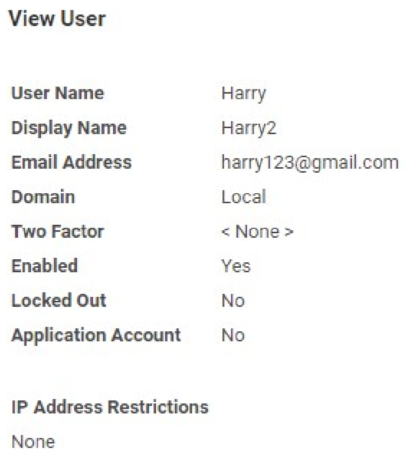
□	ID	Account ID	Operation	Status	ERC Status	Trace	Marker	ATTR1	ATTR2	ATTR3
□	156	Harry	Modify Account	Success	Success		SSThycotic	Harry		
□	155	Harry	Create Account	Success	Success		SSThycotic	Harry	*****	000000

Verifying the Integration

Check user details and change password

If you would like to verify that the integration was successful, you can test this by checking the user details and changing the password.

1. Go to the **Secret Server I Admin I Users**.
2. Click on the user that was added. The details of the user should be updated.



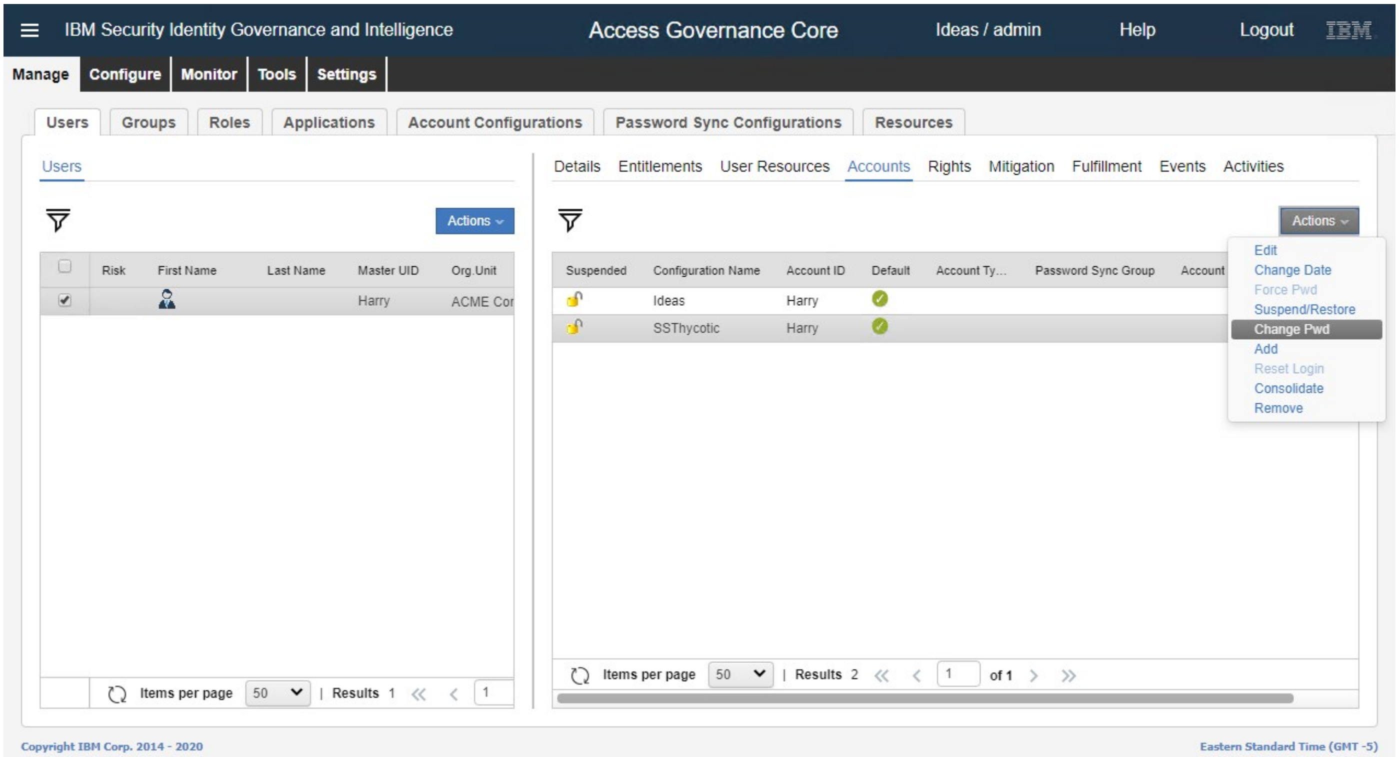
View User

User Name	Harry
Display Name	Harry2
Email Address	harry123@gmail.com
Domain	Local
Two Factor	< None >
Enabled	Yes
Locked Out	No
Application Account	No

IP Address Restrictions

None

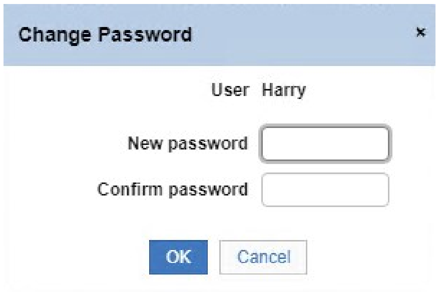
3. Go to **IBM IGI Administrator Console**.
4. In the menu, click **Access Governance Core**.
5. Click **Manage** tab I **Users I Accounts** tab.
6. Select the account.
7. In the Actions list, click **Change Pwd**.



☐	Risk	First Name	Last Name	Master UID	Org.Unit
☑				Harry	ACME Cor

Suspended	Configuration Name	Account ID	Default	Account Ty...	Password Sync Group	Account
	Ideas	Harry	✓			
	SSThycotic	Harry	✓			

8. The **Change Password** dialog box appears.



Change Password

User Harry

New password

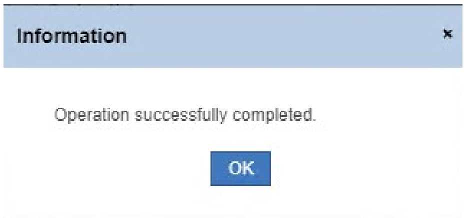
Confirm password

9. Fill in the required information, such as new password and confirm password.

10. Click **OK**.

11. A message, ‘**Operation successfully completed.**’ appears.

12. Click **Ok**.



Information

Operation successfully completed.

13. Click the **Events** tab.

14. At the bottom of the **Events** tab, click on **OUT Event**. The event is listed. Wait till the Status and the **ERC Status** is displayed as

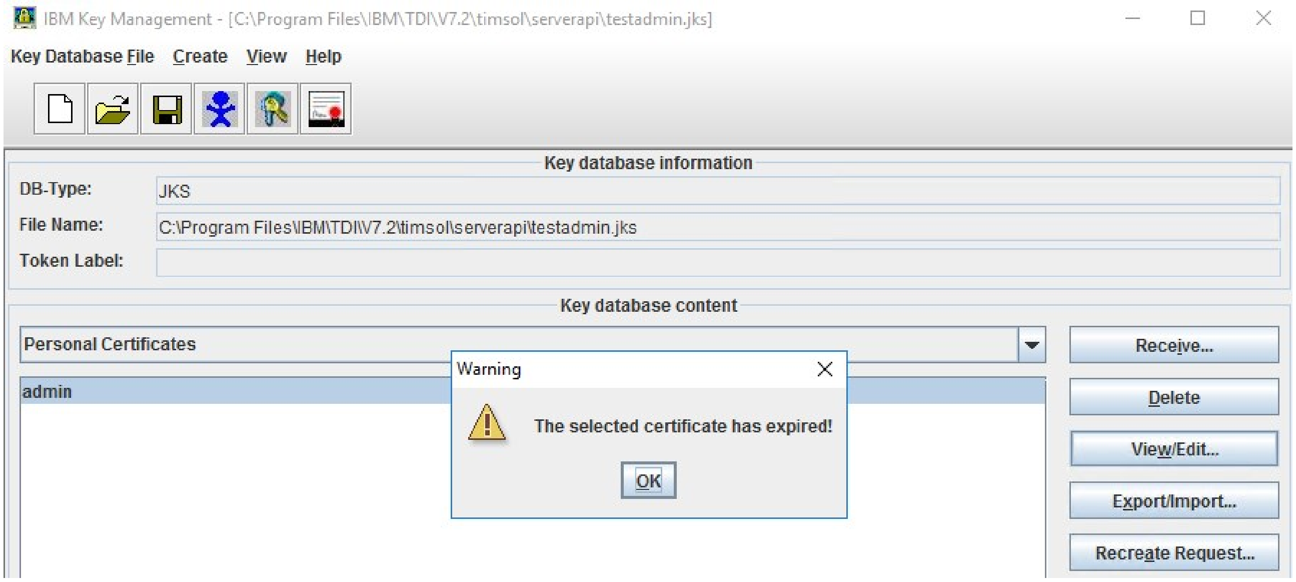
Success.

Secret Server is sucessfully integrated with IBM IGI Admin Console.

Troubleshooting

How to extend the validity of the Tivoli Directory Integrator certificate

If you received a Warning '**The selected certificate has expired!**' from the Check the validity of the Tivoli Directory Integrator certificate section, you will need to extend the certificate. Please see the steps below.



DB-Type: JKS

File Name: C:\Program Files\IBM\TDI\V7.2\timsol\serverapi\testadmin.jks

Token Label:

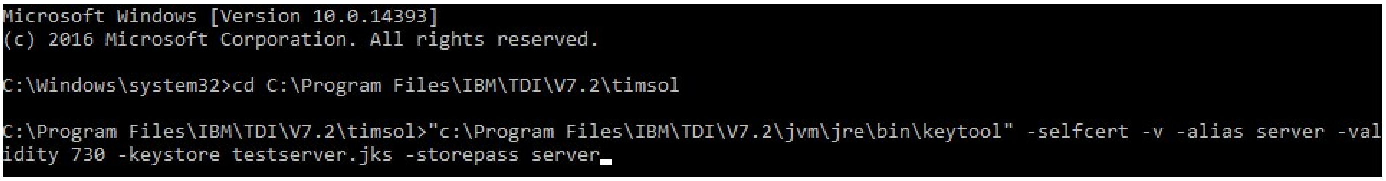
Personal Certificates

admin

The selected certificate has expired!

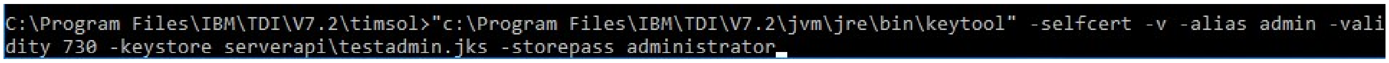
1. Click **OK**.
2. In **Windows Search**, type cmd and press **Enter**. The results are auto-populated.
3. Right-click Command Prompt and click **Run as Administrator**.
4. In the **User Account Control** dialog box, click **Yes**. The **Administrator: Command Prompt** appears.
5. To move to the timsol folder, type C:\Program Files\IBM\TDI\V7.2\timsol and press Enter.
6. Run the following eight commands:

   a. "c:\Program Files\IBM\TDI\V7.2\jvm\jre\bin\keytool" -selfcert -v -alias server -validity 730 -keystore testserver.jks -storepass server



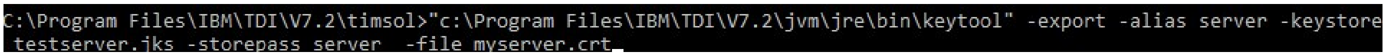
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Program Files\IBM\TDI\V7.2\timsol

C:\Program Files\IBM\TDI\V7.2\timsol>"c:\Program Files\IBM\TDI\V7.2\jvm\jre\bin\keytool" -selfcert -v -alias server -val
idity 730 -keystore testserver.jks -storepass server_
```

   b. "c:\Program Files\IBM\TDI\V7.2\jvm\jre\bin\keytool" -selfcert -v -alias admin -validity 730 -keystore serverapi\testadmin.jks -storepass administrator



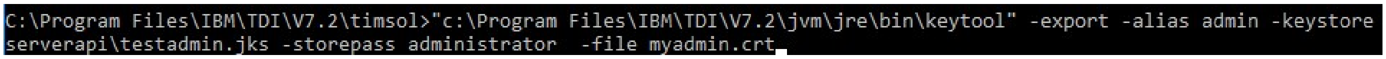
```
C:\Program Files\IBM\TDI\V7.2\timsol>"c:\Program Files\IBM\TDI\V7.2\jvm\jre\bin\keytool" -selfcert -v -alias admin -vali
dity 730 -keystore serverapi\testadmin.jks -storepass administrator_
```

   c. "c:\Program Files\IBM\TDI\V7.2\jvm\jre\bin\keytool" -export -alias server -keystore testserver.jks -storepass server -file myserver.crt



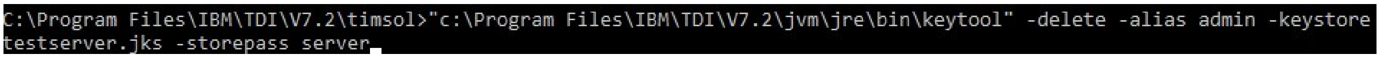
```
C:\Program Files\IBM\TDI\V7.2\timsol>"c:\Program Files\IBM\TDI\V7.2\jvm\jre\bin\keytool" -export -alias server -keystore
 testserver.jks -storepass server  -file myserver.crt_
```

   d. "c:\Program Files\IBM\TDI\V7.2\jvm\jre\bin\keytool" -export -alias admin -keystore serverapi\testadmin.jks -storepass administrator -file myadmin.crt



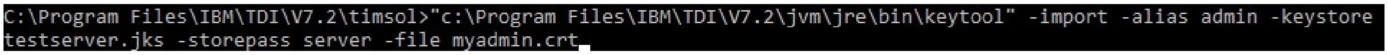
```
C:\Program Files\IBM\TDI\V7.2\timsol>"c:\Program Files\IBM\TDI\V7.2\jvm\jre\bin\keytool" -export -alias admin -keystore
serverapi\testadmin.jks -storepass administrator  -file myadmin.crt
```

e. "c:\Program Files\IBM\TDI\V7.2\jvm\jre\bin\keytool" -delete -alias admin -keystore testserver.jks -storepass server



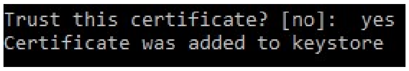
```
C:\Program Files\IBM\TDI\V7.2\timsol>"c:\Program Files\IBM\TDI\V7.2\jvm\jre\bin\keytool" -delete -alias admin -keystore
testserver.jks -storepass server
```

f. "c:\Program Files\IBM\TDI\V7.2\jvm\jre\bin\keytool" -import -alias admin -keystore testserver.jks -storepass server -file myadmin.crt



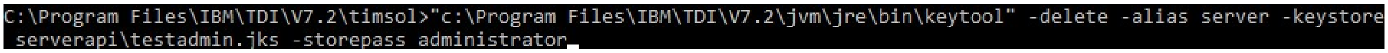
```
C:\Program Files\IBM\TDI\V7.2\timsol>"c:\Program Files\IBM\TDI\V7.2\jvm\jre\bin\keytool" -import -alias admin -keystore
testserver.jks -storepass server -file myadmin.crt
```

Note: To trust this certificate, type yes.



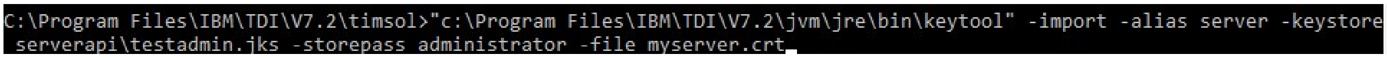
```
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

g. "c:\Program Files\IBM\TDI\V7.2\jvm\jre\bin\keytool" -delete -alias server -keystore serverapi\testadmin.jks -storepass administrator



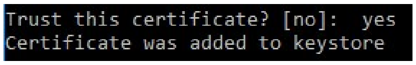
```
C:\Program Files\IBM\TDI\V7.2\timsol>"c:\Program Files\IBM\TDI\V7.2\jvm\jre\bin\keytool" -delete -alias server -keystore
 serverapi\testadmin.jks -storepass administrator
```

h. "c:\Program Files\IBM\TDI\V7.2\jvm\jre\bin\keytool" -import -alias server -keystore serverapi\testadmin.jks -storepass administrator -file myserver.crt



```
C:\Program Files\IBM\TDI\V7.2\timsol>"c:\Program Files\IBM\TDI\V7.2\jvm\jre\bin\keytool" -import -alias server -keystore
 serverapi\testadmin.jks -storepass administrator -file myserver.crt
```

Note__: To trust this certificate, type yes.



```
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

Note: Go to C:\Program Files\IBM\TDI\V7.2\timsol and verify that certificates myadmin and myserver are added to the timsol folder.

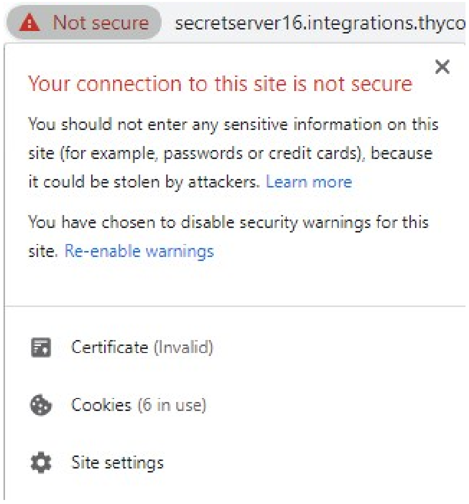
7. Go to C:\Program Files\IBM\TDI\V7.2\timsol and copy the testserver.jks file.
8. Go to C:\Program Files\IBM\TDI\V7.2 and paste the testserver.jks file.
9. Go to C:\Program Files\IBM\TDI\V7.2\timsol\serverapi and copy testadmin.jks file.
10. Go to C:\Program Files\IBM\TDI\V7.2\serverapi and paste testadmin.jks file.

How to Import the Thycotic Certificate

For secure connection between Thycotic Secret Server and IBM IGI, you will need to import Thycotic certificate.

To import Thycotic certificate:

1. Click **Not secure** part of the Thycotic Server URL . **Your connection to this site is not secure** dialog box appears.



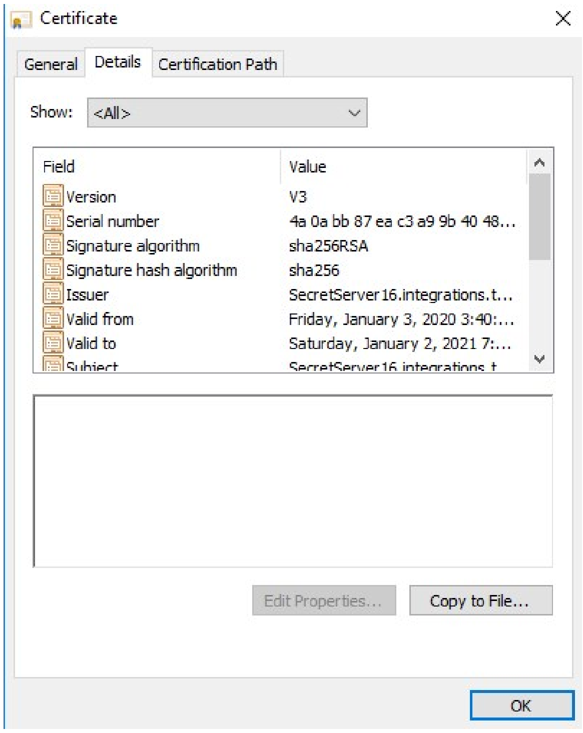
Not secure secretserver16.integrations.thyco

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

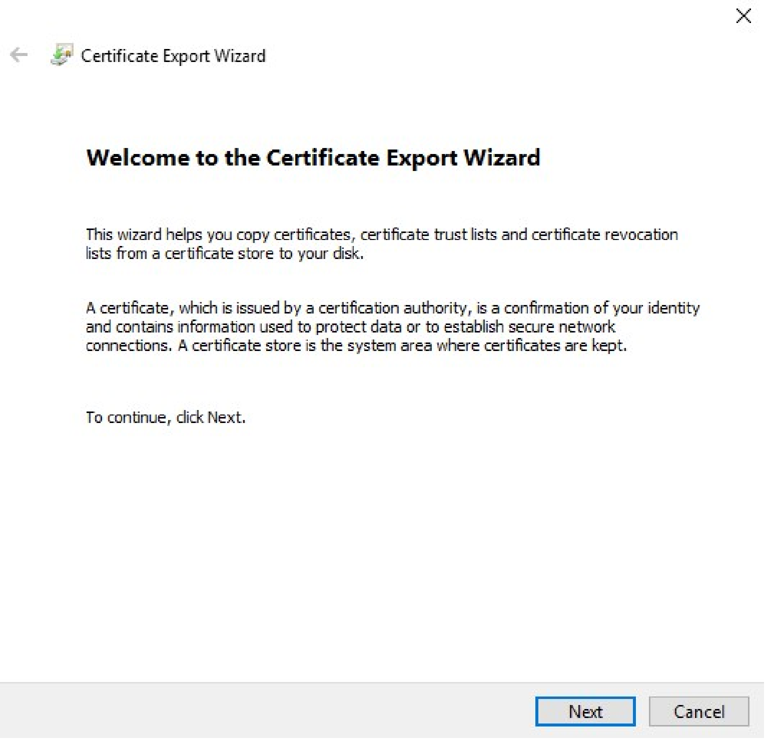
You have chosen to disable security warnings for this site. Re-enable warnings

2. Click **Certificate (Invalid)**. The **Certificate** dialog box appears.



Field	Value
Version	V3
Serial number	4a 0a bb 87 ea c3 a9 9b 40 48...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	SecretServer16.integrations.t...
Valid from	Friday, January 3, 2020 3:40:...
Valid to	Saturday, January 2, 2021 7:...
Subject	SecretServer16.integrations.t

3. Click **Details I Copy to File**. The **Welcome to the Certificate Export Wizard** appears.



Certificate Export Wizard

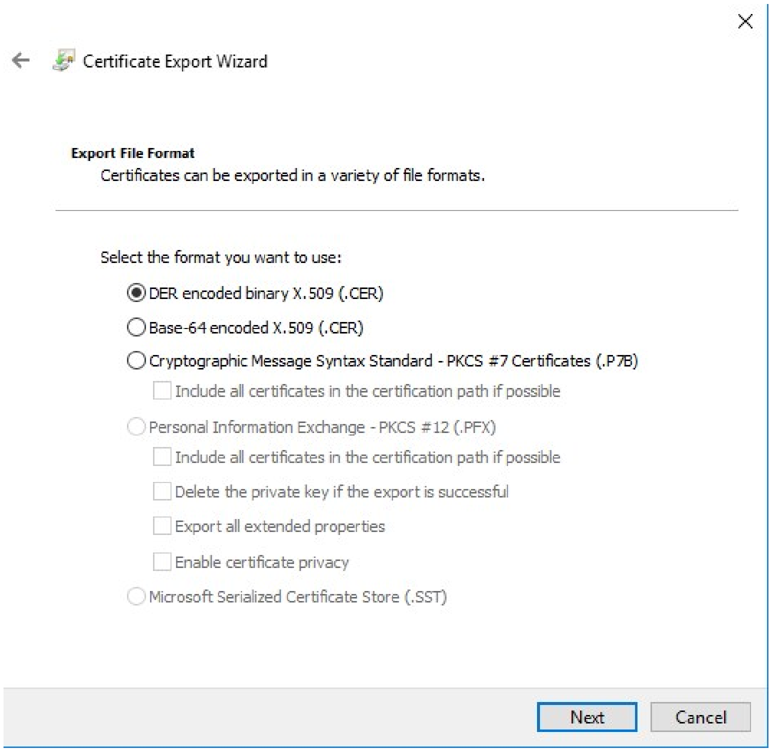
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

4. Click **Next**. The **Export File Format** panel appears.



Certificate Export Wizard

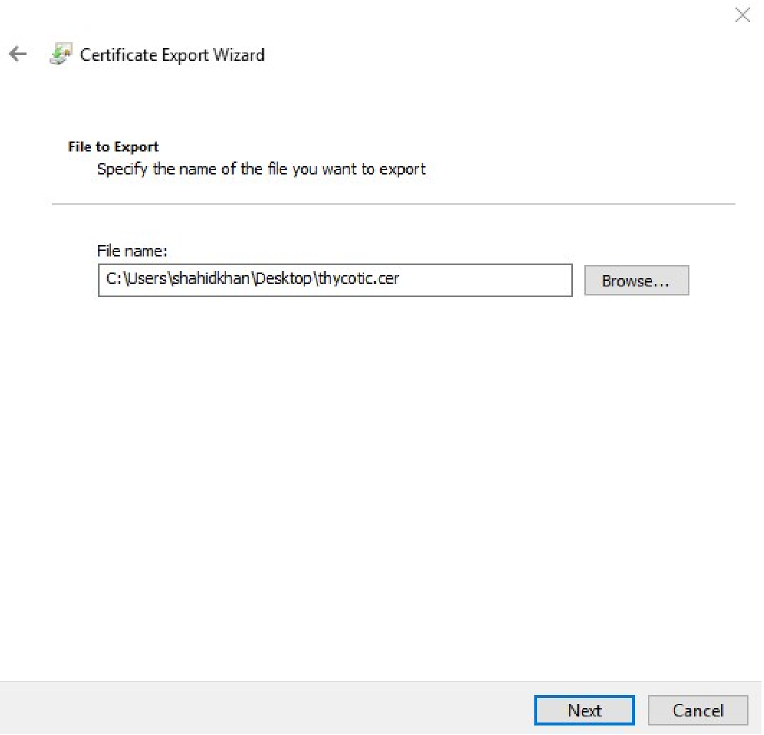
Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ● DER encoded binary X.509 (.CER)
- ○ Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ○ Personal Information Exchange - PKCS #12 (.PFX)
  - □ Include all certificates in the certification path if possible
  - □ Delete the private key if the export is successful
  - □ Export all extended properties
  - □ Enable certificate privacy
- ○ Microsoft Serialized Certificate Store (.SST)

5. Click **Next**. The **File to Export** panel appears.


Certificate Export Wizard

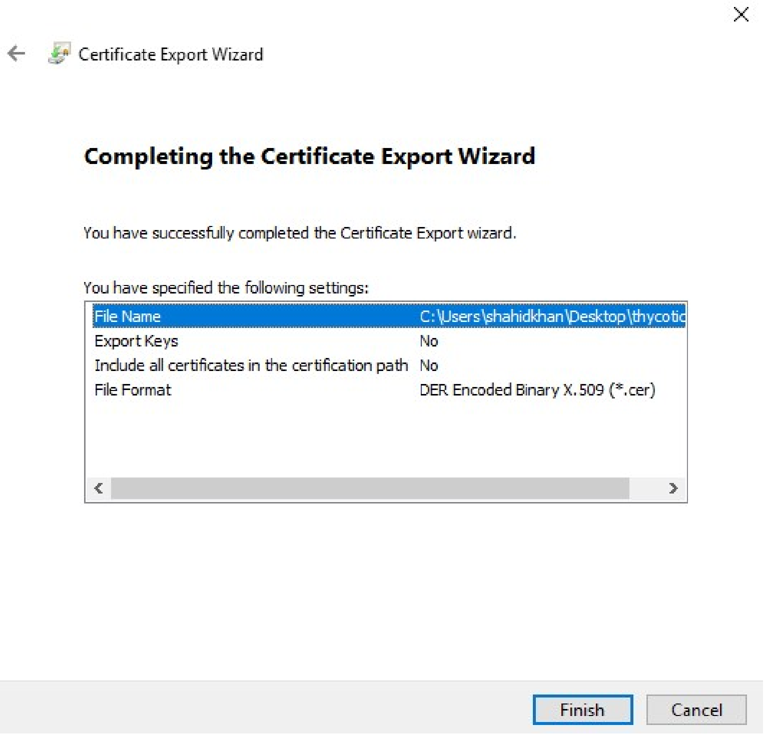
File to Export

Specify the name of the file you want to export

File name:

C:\Users\shahidkhan\Desktop\thycotic.cer

6. In the **File name** text box, type the name for the certificate to be exported.
7. Click **Browse** and select the location where you want to export the certificate.
8. Click **Next**. The **Completing the Certificate Export Wizard** appears.


Certificate Export Wizard

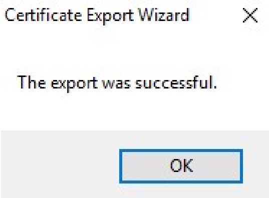
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\shahidkhan\Desktop\thycotic
Export Keys	No
Include all certificates in the certification path	No
File Format	DER Encoded Binary X.509 (*.cer)

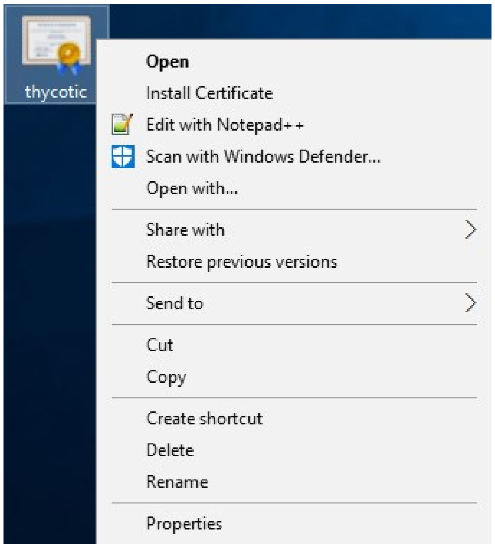
9. Click **Finish**. The message, '**The export was successful.**' appears. The certificate is exported to the location selected.



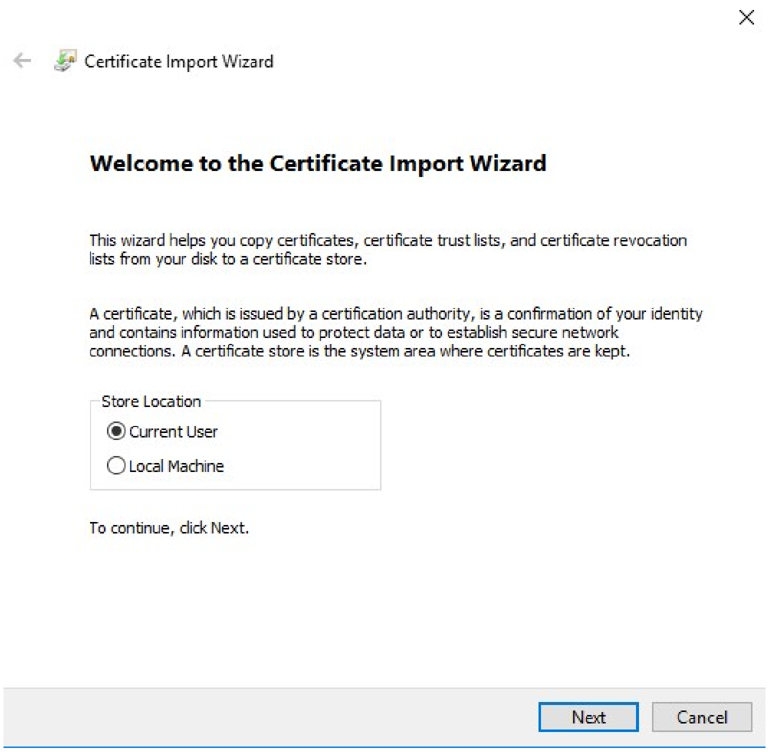
Certificate Export Wizard

The export was successful.

10. Right-click the certificate where you have exported and click **Install Certificate**.



11. The **Welcome to the Certificate Import Wizard** appears.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

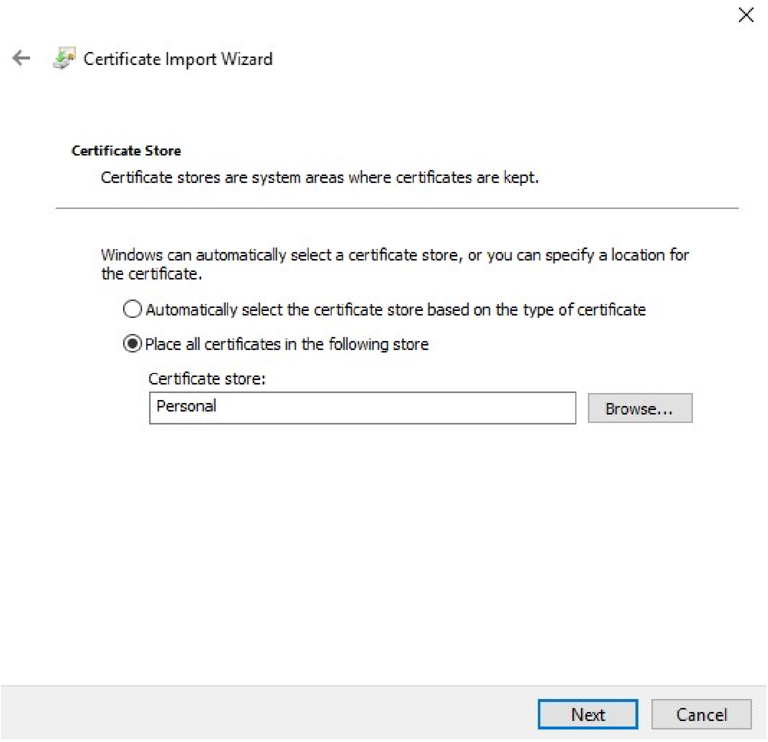
Store Location

● Current User

○ Local Machine

To continue, click Next.

12. In the **Store Location** area, select **Current User** and then click **Next**. The **Certificate Store** panel appears.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

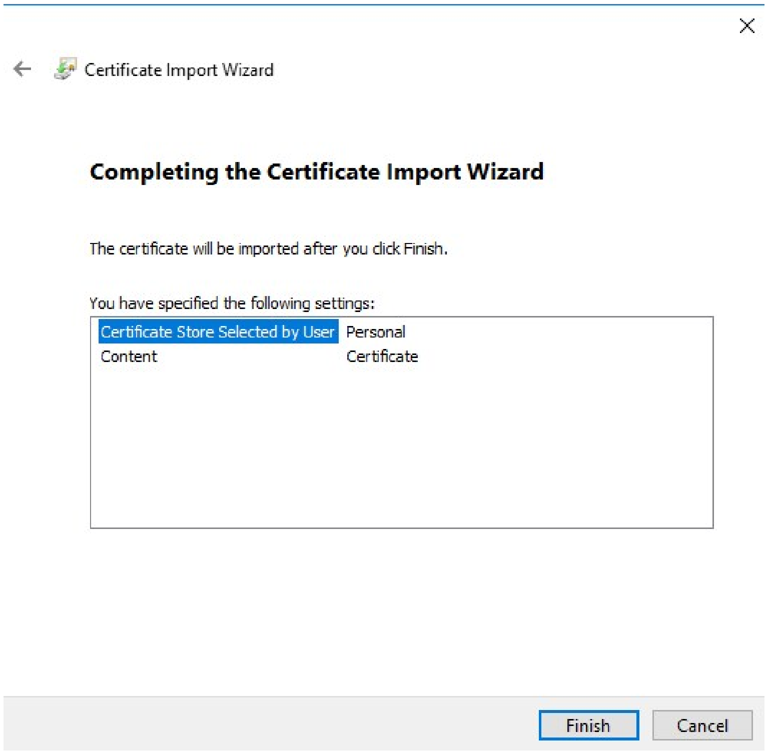
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Personal

13. Select **Place all certificates in the following store** and then click **Browse**.

14. Select **Personal** folder and then click **Next**. The **Completing the Certificate Import Wizard** panel appears.



Certificate Import Wizard

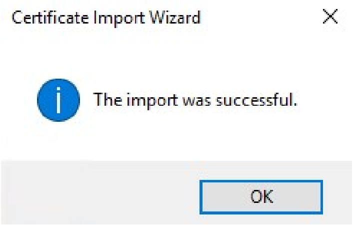
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Personal
Content	Certificate

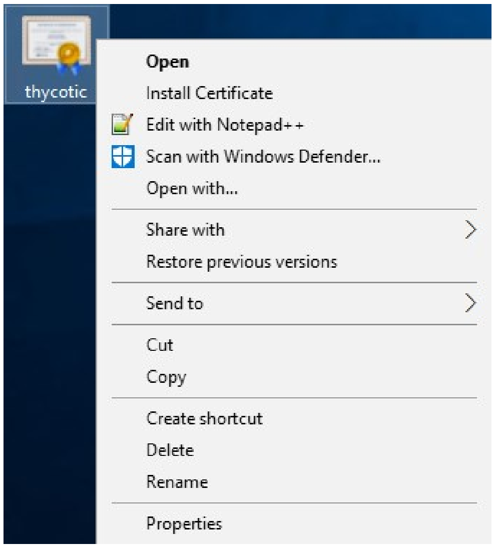
15. Click **Finish**. The message '**The import was successful.**' appears.



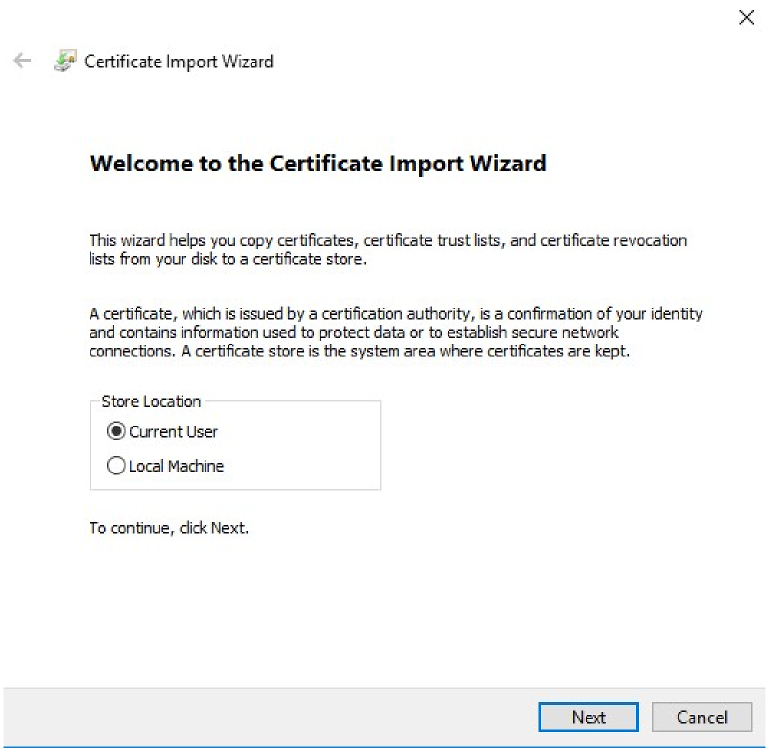
Certificate Import Wizard

The import was successful.

16. Right-click the certificate where you have exported and click **Install Certificate**.



17. The **Welcome to the Certificate Import Wizard** appears.



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

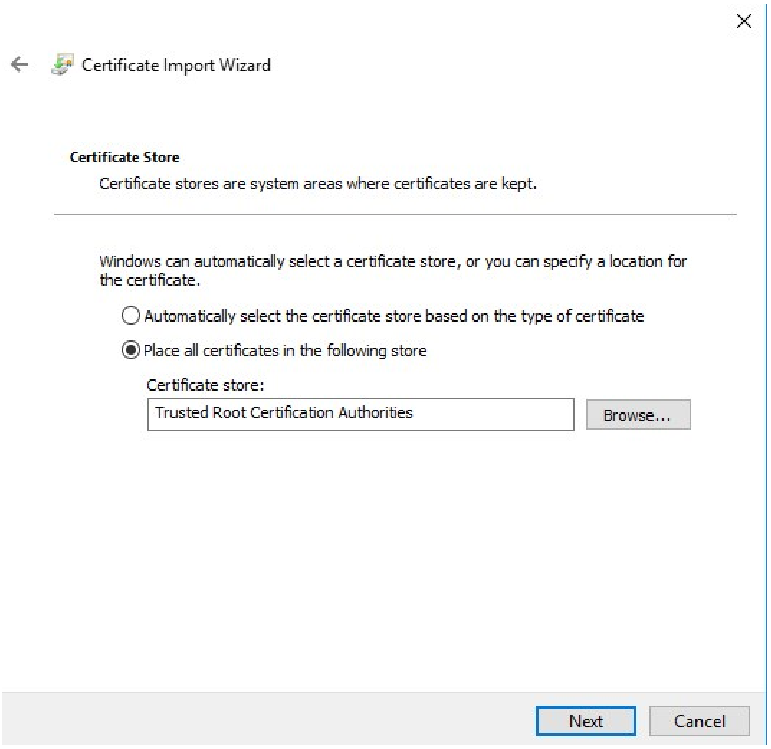
Store Location

● Current User

○ Local Machine

To continue, click Next.

18. In the **Store Location** area, select **Current User** and then click **Next**. The **Certificate Store** panel appears.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

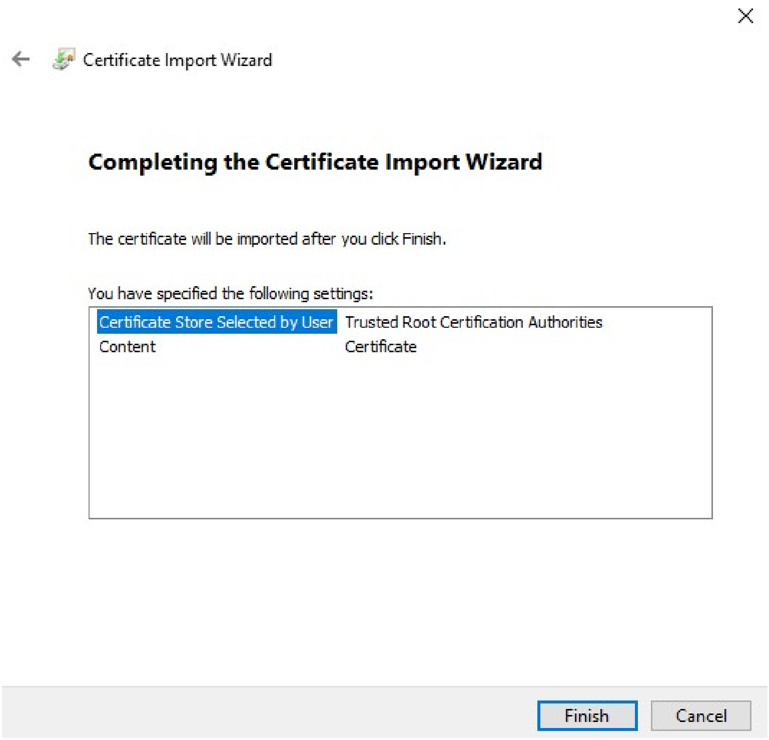
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

19. Select **Place all certificates in the following store** and then click **Browse**.

20. Select **Trusted Root Certification Authorities** folder and then click **Next**. The **Completing the Certificate Import Wizard** panel appears.



Certificate Import Wizard

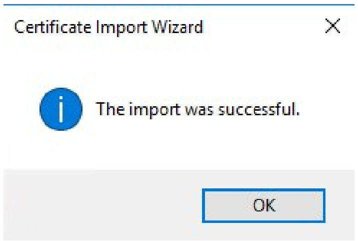
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

21. Click **Finish**. The message '**The import was successful.**' appears.

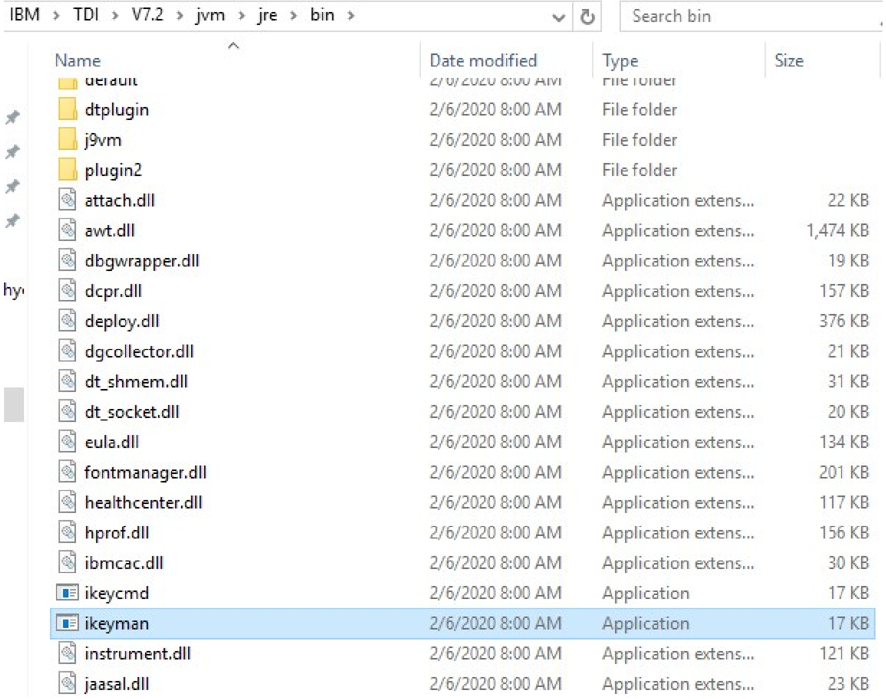


Certificate Import Wizard

The import was successful.

How to Add the Thycotic certificate

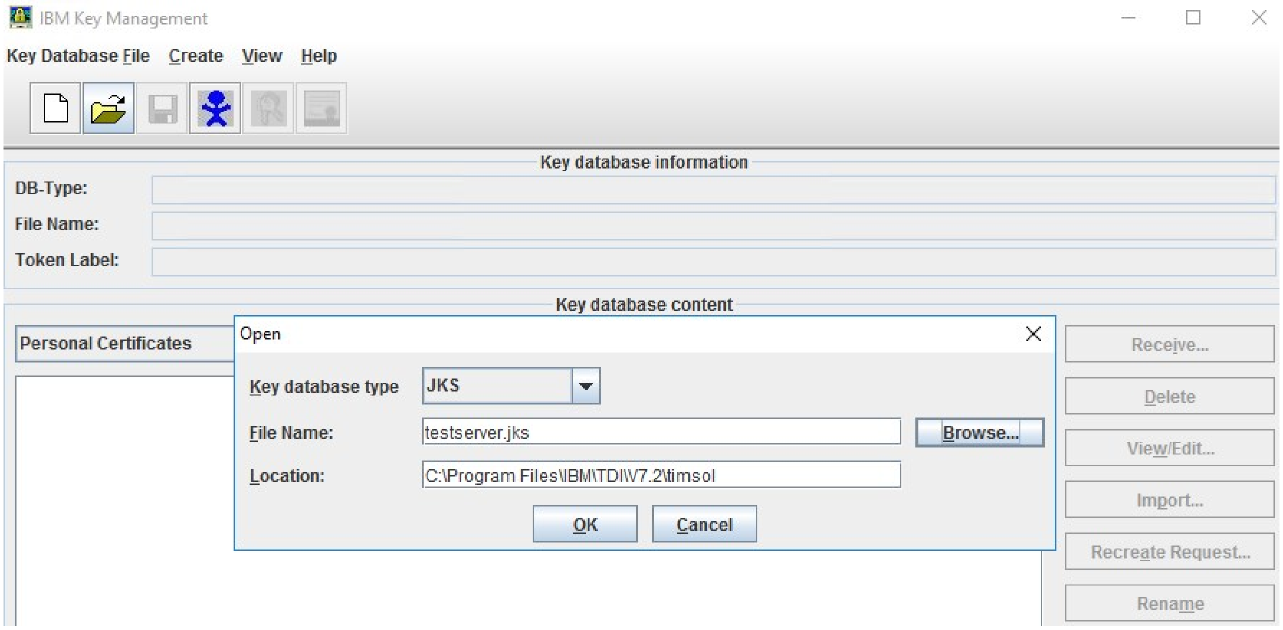
1. Go to C:\Program Files\IBM\TDI\V7.2\jvm\jre\bin.



Name	Date modified	Type	Size
default	2/6/2020 8:00 AM	File folder	
dtplugin	2/6/2020 8:00 AM	File folder	
j9vm	2/6/2020 8:00 AM	File folder	
plugin2	2/6/2020 8:00 AM	File folder	
attach.dll	2/6/2020 8:00 AM	Application extens...	22 KB
awt.dll	2/6/2020 8:00 AM	Application extens...	1,474 KB
dbgwrapper.dll	2/6/2020 8:00 AM	Application extens...	19 KB
dcpr.dll	2/6/2020 8:00 AM	Application extens...	157 KB
deploy.dll	2/6/2020 8:00 AM	Application extens...	376 KB
dgcollector.dll	2/6/2020 8:00 AM	Application extens...	21 KB
dt_shmem.dll	2/6/2020 8:00 AM	Application extens...	31 KB
dt_socket.dll	2/6/2020 8:00 AM	Application extens...	20 KB
eula.dll	2/6/2020 8:00 AM	Application extens...	134 KB
fontmanager.dll	2/6/2020 8:00 AM	Application extens...	201 KB
healthcenter.dll	2/6/2020 8:00 AM	Application extens...	117 KB
hprof.dll	2/6/2020 8:00 AM	Application extens...	156 KB
ibmcac.dll	2/6/2020 8:00 AM	Application extens...	30 KB
ikeycmd	2/6/2020 8:00 AM	Application	17 KB
ikeyman	2/6/2020 8:00 AM	Application	17 KB
instrument.dll	2/6/2020 8:00 AM	Application extens...	121 KB
jaasal.dll	2/6/2020 8:00 AM	Application extens...	23 KB

2. Right-click ikeyman file and select **Run as administrator**.

3. In the **User Account Control** dialog box, click **Yes**. The **IBM Key Management** dialog box appears.



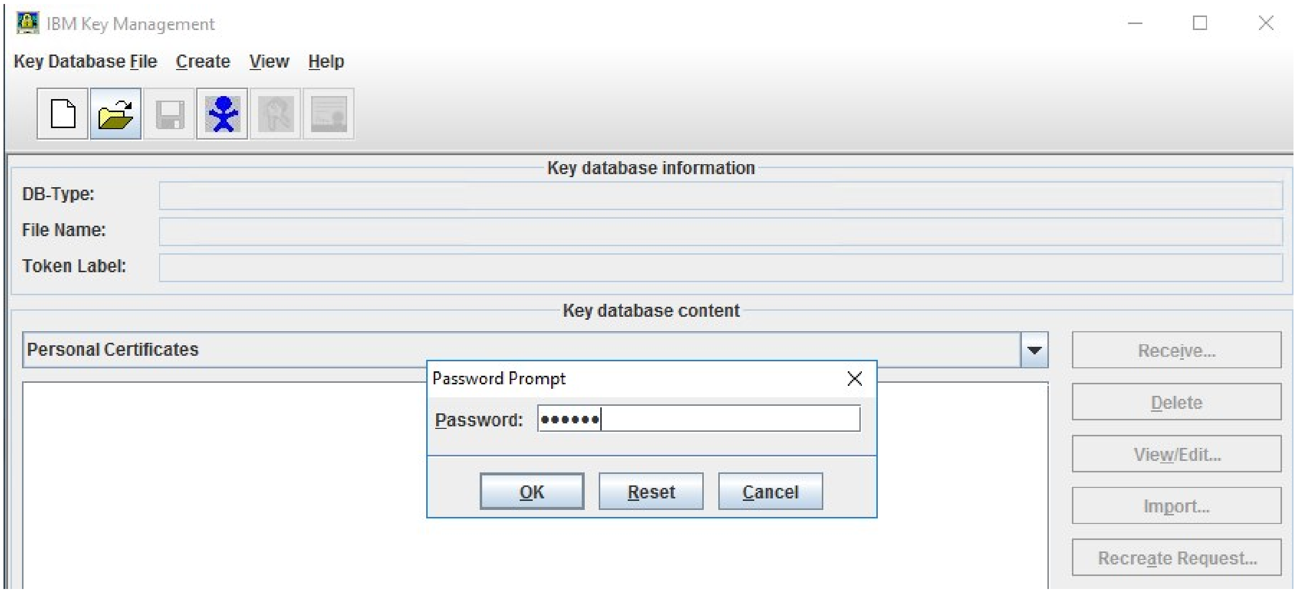
Open

Key database type: JKS

File Name: testserver.jks

Location: C:\Program Files\IBM\TDI\V7.2\timsol

4. Click open 📂 icon. The **Open** dialog box appears.
5. Click **Browse** and navigate to C:\Program Files\IBM\TDI\V7.2\timsol and double-click the timsol folder.
6. Select testserver.jks and click **Open**. The **Open** dialog box appears.
7. Click **OK**. The **Password Prompt** dialog box appears.



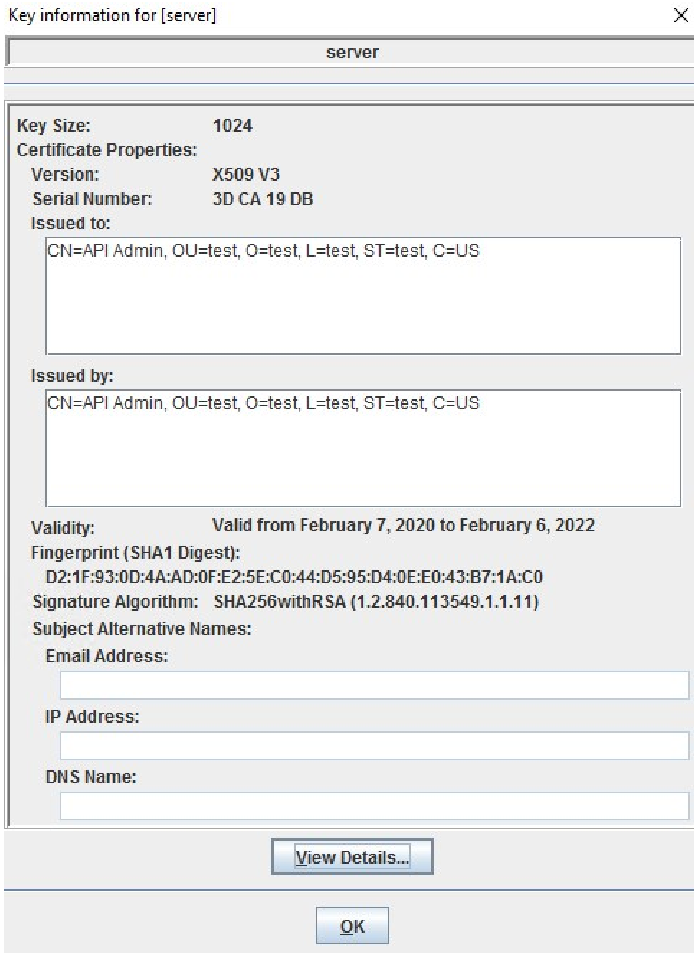
Password Prompt

Password: ••••••

8. In the **Password** text box, type the password and click **OK**.

   Note: The default password for testserver.jks is server.

9. In the **IBM Key Management** dialog box, click **View/Edit**. The certificate details appear.



Key information for [server]

server

Key Size: 1024

Certificate Properties:

Version: X509 V3

Serial Number: 3D CA 19 DB

Issued to:

CN=API Admin, OU=test, O=test, L=test, ST=test, C=US

Issued by:

CN=API Admin, OU=test, O=test, L=test, ST=test, C=US

Validity: Valid from February 7, 2020 to February 6, 2022

Fingerprint (SHA1 Digest):

D2:1F:93:0D:4A:AD:0F:E2:5E:C0:44:D5:95:D4:0E:E0:43:B7:1A:C0

Signature Algorithm: SHA256withRSA (1.2.840.113549.1.1.11)

Subject Alternative Names:

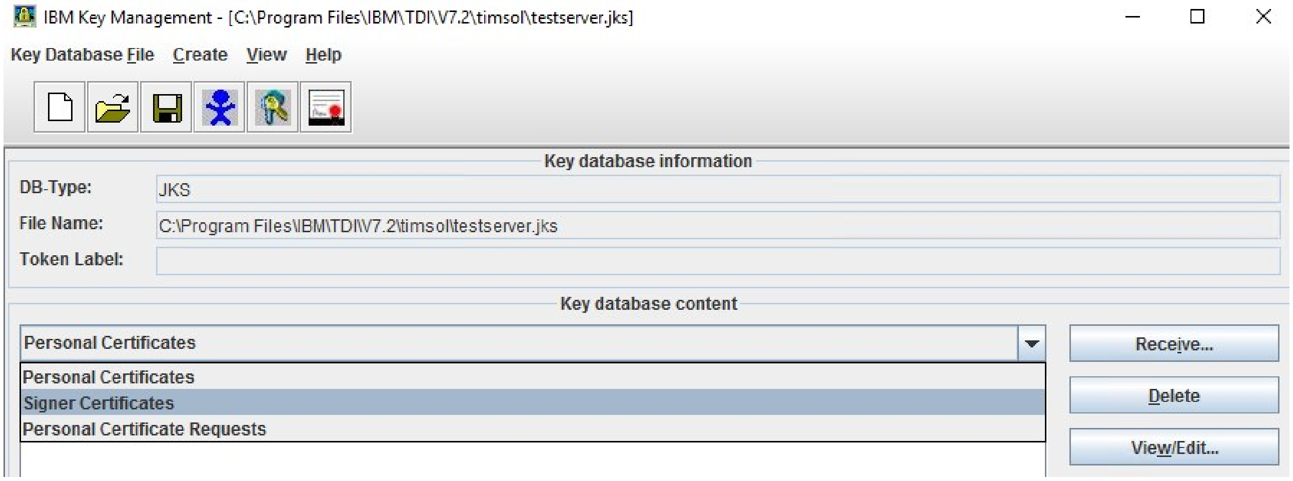
Email Address:

IP Address:

DNS Name:

10. Verify the validity of the certfificate and close the dialog box.

11. From the type of certificate list, select **Signer Certificates**.



IBM Key Management - [C:\Program Files\IBM\TDI\V7.2\timsol\testserver.jks]

Key database information

DB-Type: JKS

File Name: C:\Program Files\IBM\TDI\V7.2\timsol\testserver.jks

Token Label:

Key database content

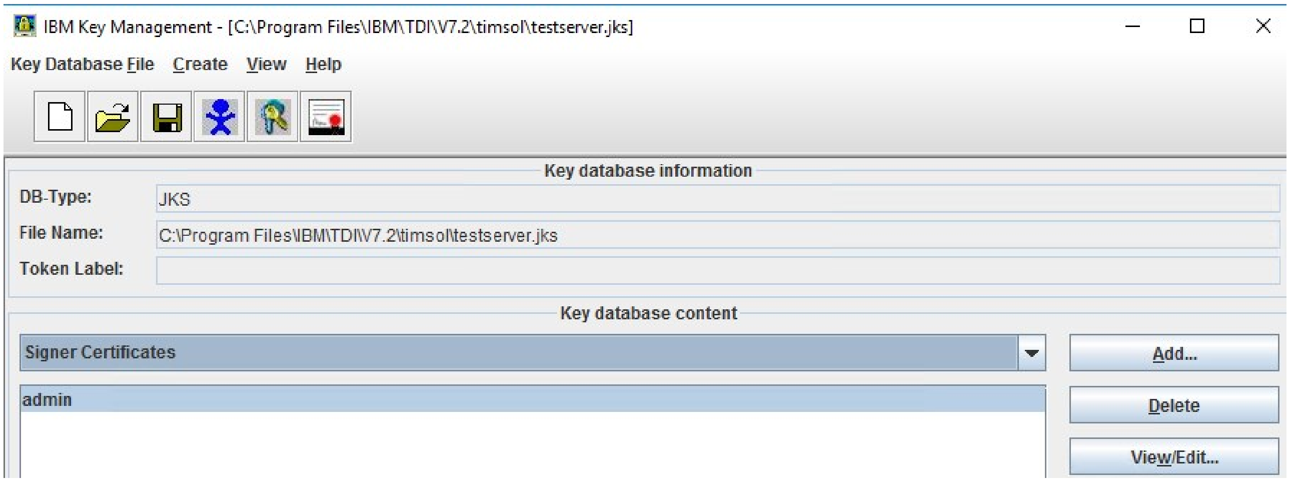
Personal Certificates

Personal Certificates

Signer Certificates

Personal Certificate Requests

12. The type of **Signer Certificate** as **admin** is listed. Click **Add**. The **Open** dialog box appears.



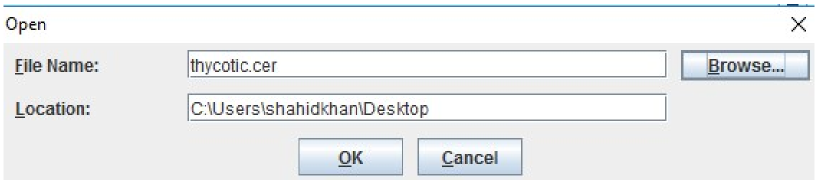
DB-Type: JKS
File Name: C:\Program Files\IBM\TDI\V7.2\timsol\testserver.jks
Token Label:

Signer Certificates

admin

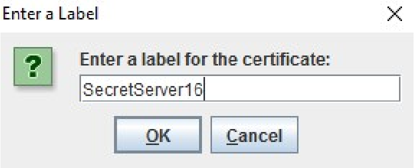
13. Click **Browse** and navigate to the location of thycotic.cer.

14. Select thycotic.cer and click **Open**. The **Open** dialog box appears.



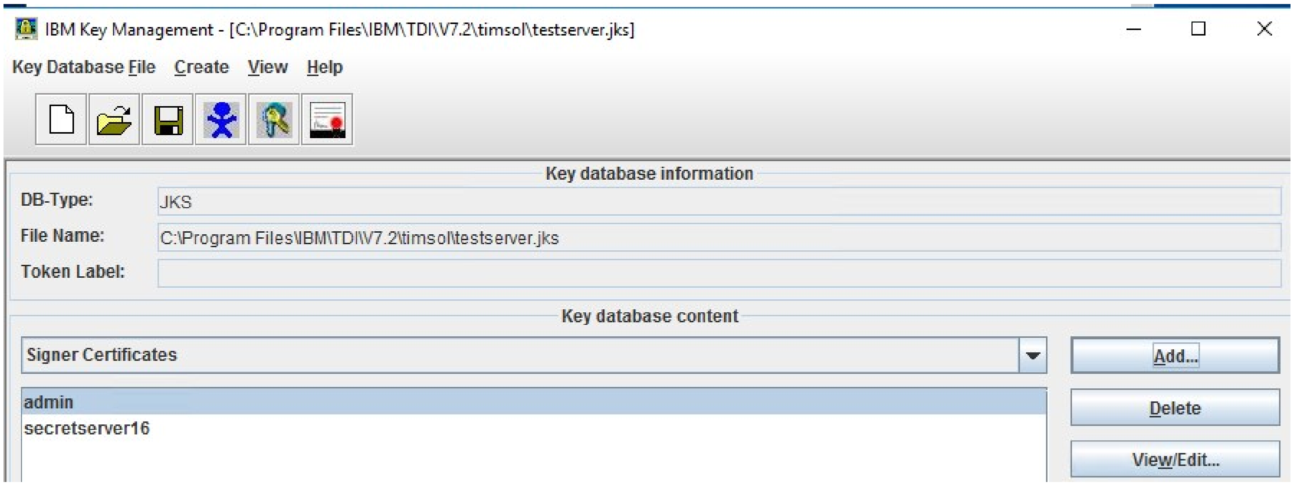
File Name: thycotic.cer
Location: C:\Users\shahidkhan\Desktop

15. Click **OK**. The **Enter a Label** dialog box appears.



Enter a label for the certificate: SecretServer16

16. In the **Enter a Label for the certificate** text box, type the label and then click **OK**. The certificate is listed in the **Key database content** section.

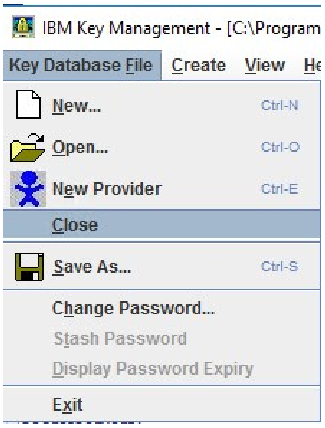


DB-Type: JKS
File Name: C:\Program Files\IBM\TDI\V7.2\timsol\testserver.jks
Token Label:

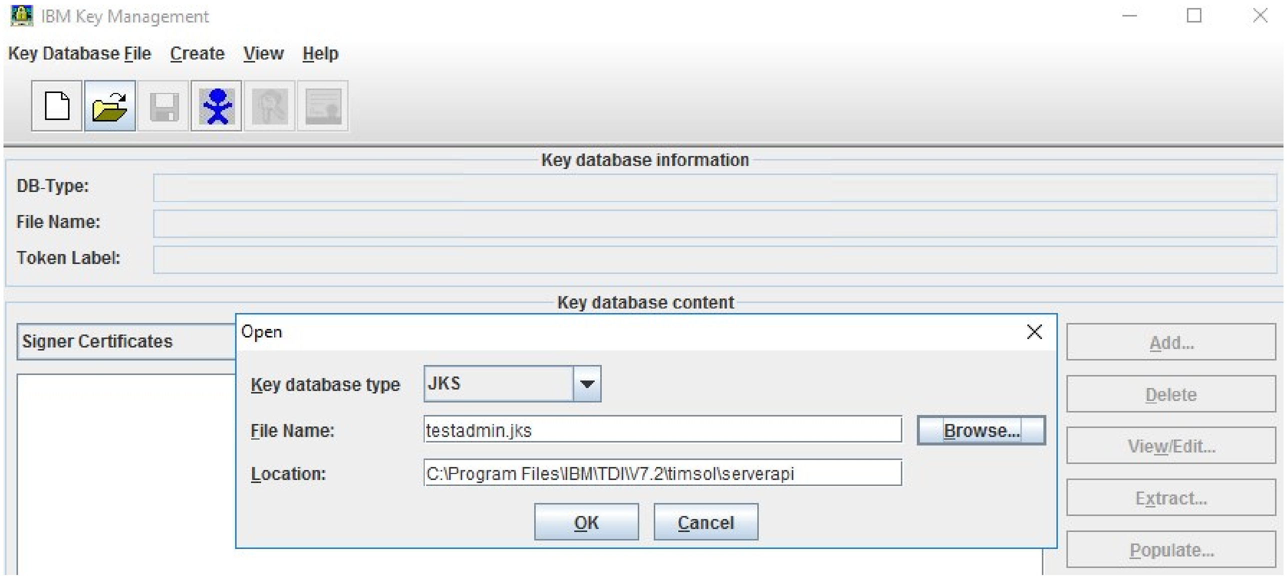
Signer Certificates

admin
secretserver16

17. Click Key **Key Database File** tab | **Close**. The certificate is saved.



18. Click open icon. The **Open** dialog box appears.



Key database type: JKS

File Name: testadmin.jks

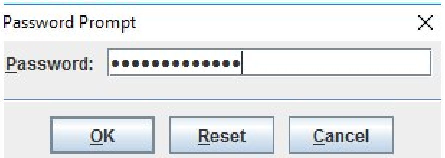
Location: C:\Program Files\IBM\TDI\V7.2\timsol\serverapi

19. Click **Browse** and navigate to C:\Program Files\IBM\TDI\V7.2\timsol.

20. Double-click timsol folder and then double-click serverapi folder.

21. Click testadmin.jks and click **Open**.

22. Click **OK**. The **Password Prompt** dialog box appears.

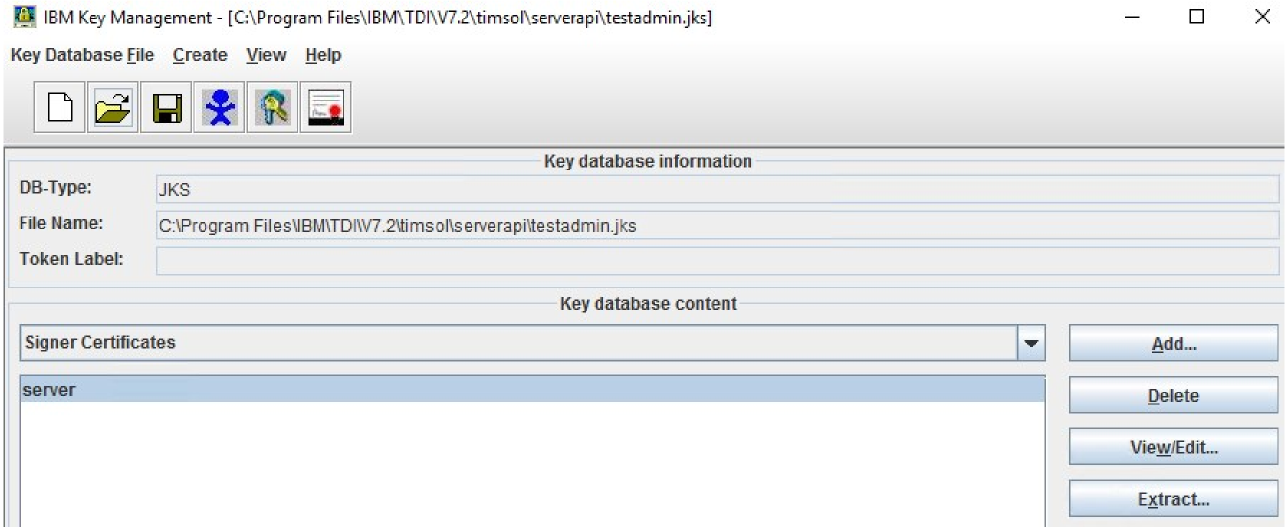


Password: •••••••••••••

23. In the **Password** text box, type the password and click **OK**.

Note: The default password for testadmin.jk is administrator.

24. Click **OK**. The certificate is listed in the **Key database content** section.


IBM Key Management - [C:\Program Files\IBM\TDI\V7.2\timsol\serverapi\testadmin.jks]

Key database information

DB-Type: JKS

File Name: C:\Program Files\IBM\TDI\V7.2\timsol\serverapi\testadmin.jks

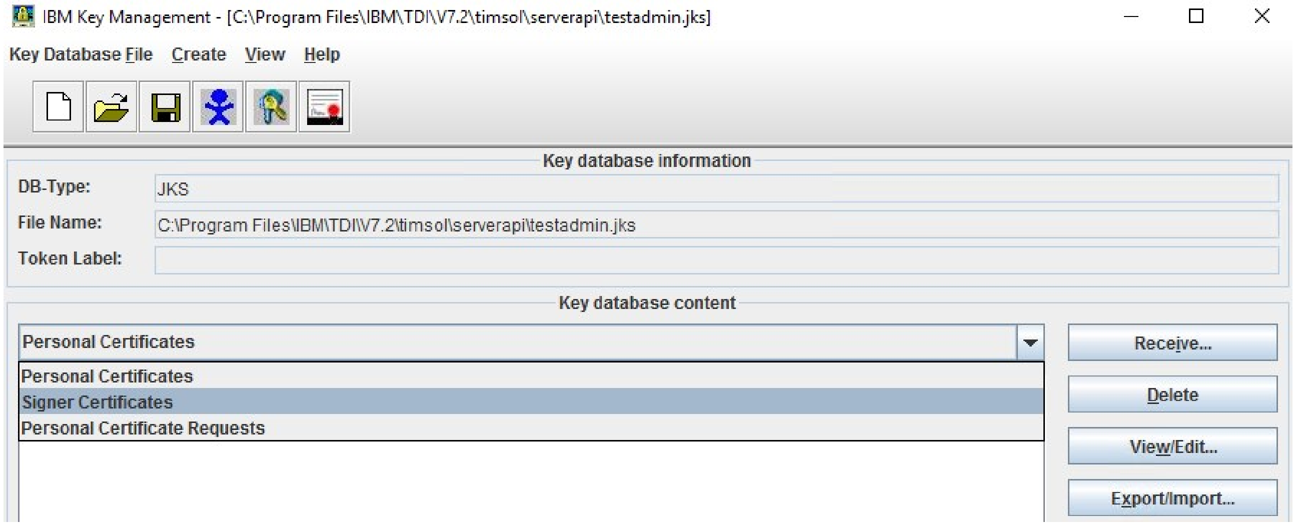
Token Label:

Key database content

Signer Certificates

server

25. From the type of certificate list, select **Singer Certificates**.


IBM Key Management - [C:\Program Files\IBM\TDI\V7.2\timsol\serverapi\testadmin.jks]

Key database information

DB-Type: JKS

File Name: C:\Program Files\IBM\TDI\V7.2\timsol\serverapi\testadmin.jks

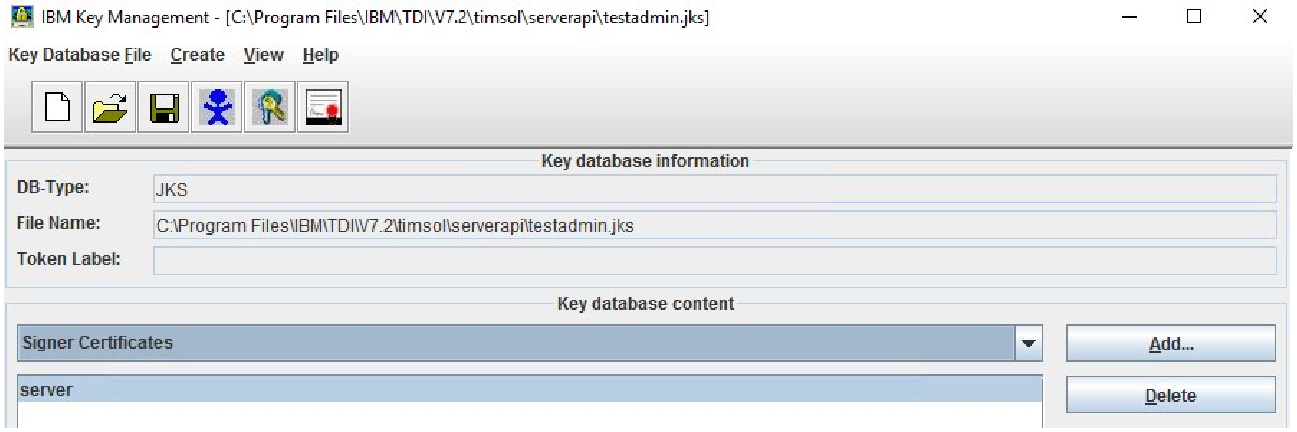
Token Label:

Key database content

Personal Certificates

Personal Certificates
Signer Certificates
Personal Certificate Requests

26. Click the certificate name **server** and click **Add**.


IBM Key Management - [C:\Program Files\IBM\TDI\V7.2\timsol\serverapi\testadmin.jks]

Key database information

DB-Type: JKS

File Name: C:\Program Files\IBM\TDI\V7.2\timsol\serverapi\testadmin.jks

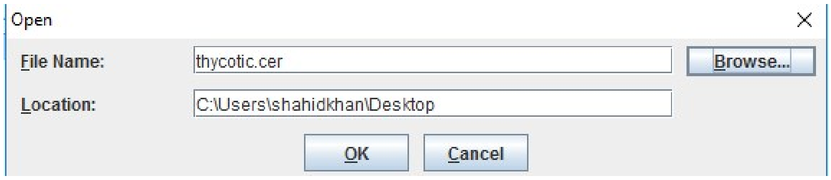
Token Label:

Key database content

Signer Certificates

server

27. The **Open** dialog box appears.

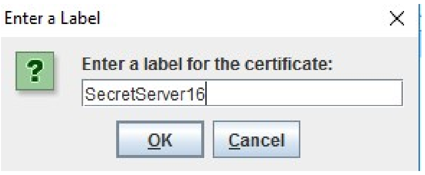


File Name: thycotic.cer

Location: C:\Users\shahidkhan\Desktop

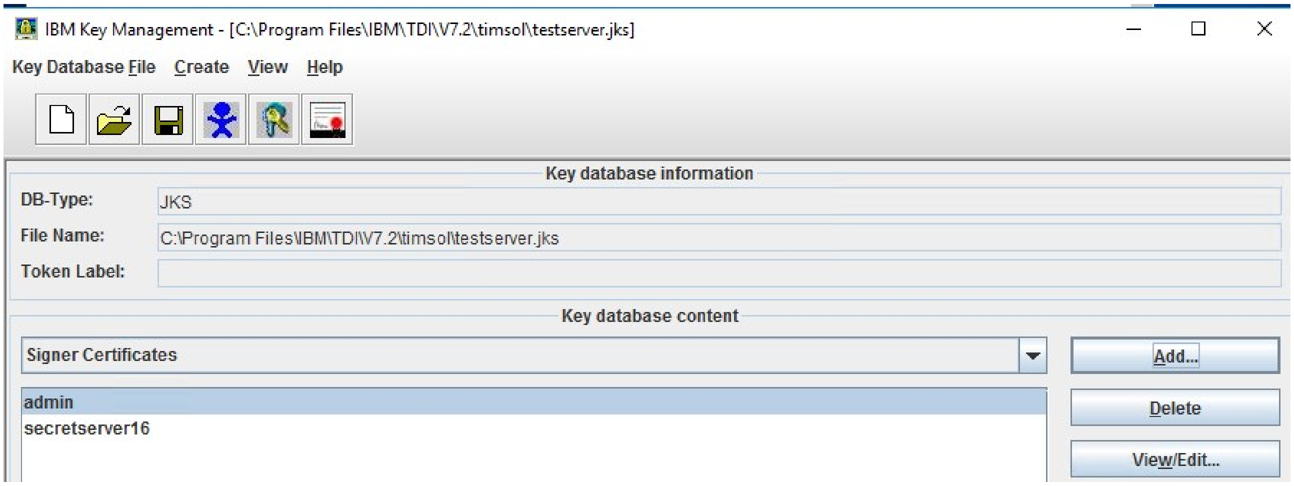
28. Click **Browse** and navigate to the location of thycotic.cer.

29. Click **Open** and then in the **Open** dialog box click **OK**. The **Enter a label** dialog box appears.



Enter a label for the certificate: SecretServer16

30. In the **Enter a label for the certificate** text box, type the label and then click **OK**. The certificate is listed in the **Key database content** area.



DB-Type: JKS

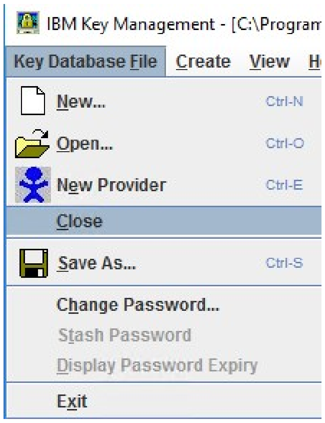
File Name: C:\Program Files\IBM\TDI\V7.2\timsol\testserver.jks

Token Label:

Signer Certificates

admin
secretserver16

31. Click **Key Database File** tab | **Close**. The certificate is saved.



QRadar

Below are the following integrations that are available with IBM:

- Secret Server Dashboard Extension
- QRadar DSM

Introduction

Meeting Information Security Compliance Mandates: Secret Server and QRadar Security Intelligence Platform Integration and Configuration

Leveraging Secret Server event data with IBM's QRadar Security Intelligence Platform can give organizations deep insight into the use of privileged accounts (such as Windows local administrator, service or application accounts, UNIX root accounts, Cisco enable passwords and more). Used together, these tools provide secure access to privileged accounts and provide greater visibility to meet compliance mandates and detect internal network threats.

THE SECRET SERVER APPROACH TO PRIVILEGED ACCOUNT MANAGEMENT

Many environments that have strict Information Security policies also require methods to control and monitor access to privileged accounts. Enterprises often apply security policies such as physical access restrictions to hardware, network firewalls, appropriate-use guidelines, and user account restrictions. In the case of privileged accounts, access is more difficult to track and verify. Implementing privileged account management software such as Secret Server enables organizations to strictly control and track access.

Enterprises that implement Secret Server gain the ability to grant or deny granular access to critical systems. When access is granted, use of that access is tracked based on a wide range of events. While alerting is core functionality within Secret Server, managing real-time events on the aggregate can be cumbersome. Leveraging QRadar to manage these real-time events allows users to build customized risk analysis into their privileged account management policies. Mitigating internal privilege account threats helps organizations meet compliance requirements like Sarbanes-Oxley Act (SOX), Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and the Federal Information Security Management Act (FISMA).

RISKS AND BENEFITS

Unmanaged privileged accounts often enjoy unchecked access across a wide array of systems, networks, and databases. Unmitigated top-level access, in the wrong hands, can be devastating to an organization. The potential for liability is not limited to internal data and productivity loss, but can include criminal and civil penalties for unauthorized disclosure of private or regulated information. Implementing an enterprise-level privileged account management system (Secret Server) with a realtime event managementsystem (QRadar Security Intelligence Platform) allows organizations to mitigate risk. Critical systems can only be accessed by pre-defined users. IT Security Auditors are able to track access based on the needs of the enterprise.

Getting Started with QRadar

Before configuring QRadar to integrate with Secret Server you will need to make sure you have met all of the system requirements.

Prerequisites

System Requirements

Product		Details
QRadar		
	Version	v7.3.0 or later
	Hardware	For further information about system requirements for QRadar please visit: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/c_siem_deploy_ov.htmll
Secret Server		
	Version	Thycotic Secret Server version 8.9 or later.
	Hardware	For further information about system requirements for Secret Server please visit: https://docs.thycotic.com/ss/10.8.0/secret-server-setup/system-requirements/index.md.l

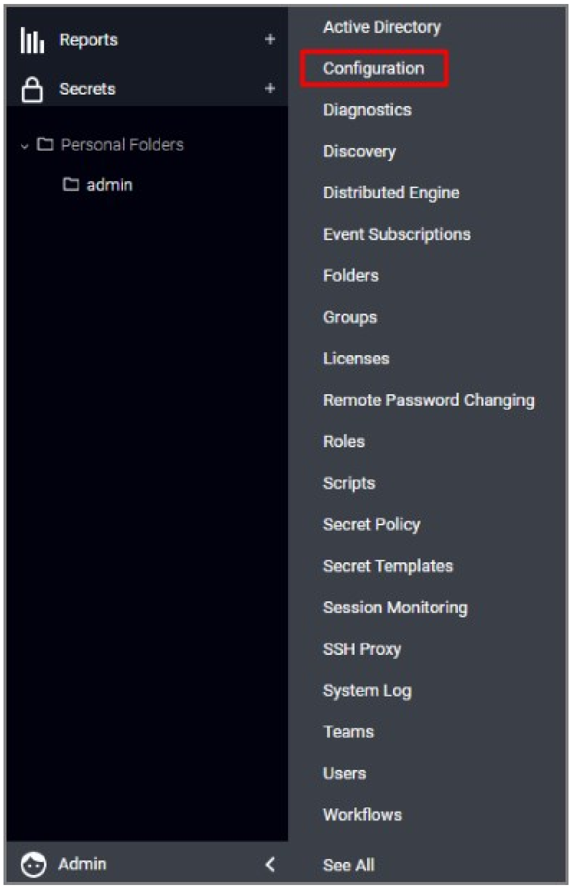
Configuration

- Exporting Logs from Secret Server
- Upload a Custom Parser
- QID Mappings
- How to export the event mappings along with the Custom DSM

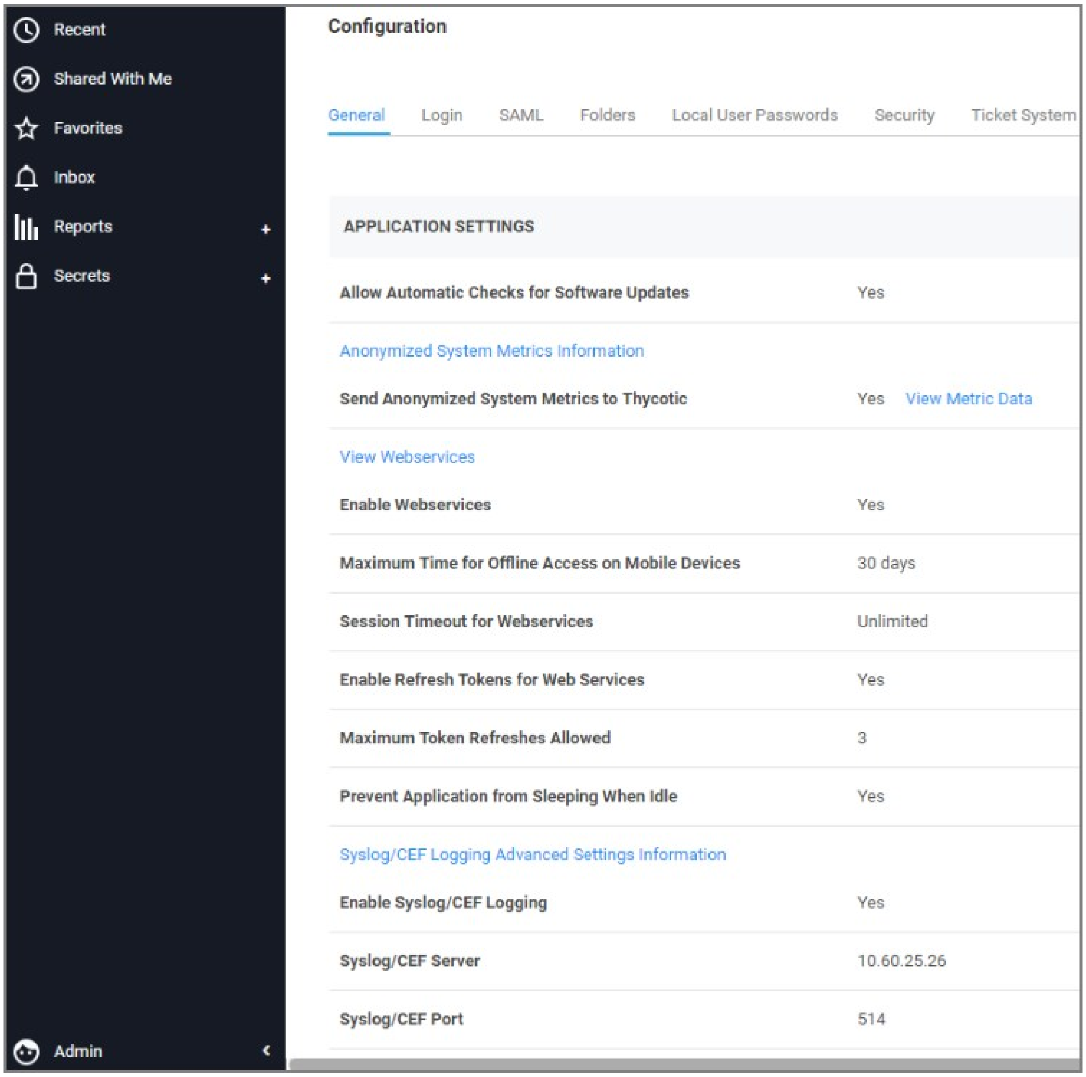
Exporting Logs from Secret Server

To export event logs from Secret Server to QRadar, begin by logging in to Secret Server as an Administrator.

1. From the **ADMIN** menu, select **Configuration**.



2. Scroll to the bottom of the page and click **Edit**.
3. Select the **Enable Syslog/CEF Logging** check box and fill in the QRadar Server IP, Port, Protocol (“TCP” for this example) before clicking Save.
4. Data will immediately begin flowing to your QRadar instance. See the figure below from the Secret Server **Configuration** menu:


Recent
Shared With Me
Favorites
Inbox
Reports +
Secrets +
Admin ‹

Configuration

General | Login | SAML | Folders | Local User Passwords | Security | Ticket System

APPLICATION SETTINGS

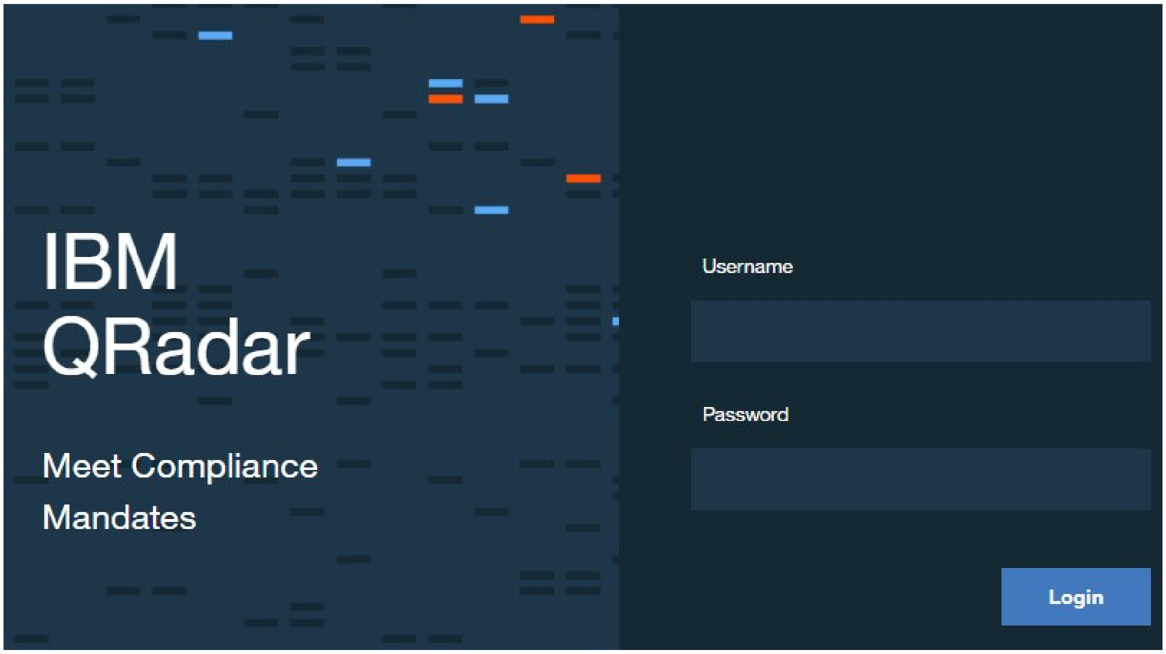
Allow Automatic Checks for Software Updates	Yes
Anonymized System Metrics Information	
Send Anonymized System Metrics to Thycotic	Yes View Metric Data
View Webservices	
Enable Webservices	Yes
Maximum Time for Offline Access on Mobile Devices	30 days
Session Timeout for Webservices	Unlimited
Enable Refresh Tokens for Web Services	Yes
Maximum Token Refreshes Allowed	3
Prevent Application from Sleeping When Idle	Yes
Syslog/CEF Logging Advanced Settings Information	
Enable Syslog/CEF Logging	Yes
Syslog/CEF Server	10.60.25.26
Syslog/CEF Port	514

Upload a Custom Parser

1. Save the following as an xml file. This is an example of a Custom Parser that you will need to upload in step 8.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
 <ns2:device-extension xmlns:ns2="event_parsing/device_extension">

   <pattern id="EventCategory-Pattern-1" type="JavaPattern" use-default-pattern="false">\|\d+\|(.*)\|\d\|msg</pattern>

   <pattern id="EventName-Pattern-1" type="CefKey">$id$</pattern>

   <pattern id="SourceIp-Pattern-1" type="CefKey">src</pattern>

   <pattern id="UserName-Pattern-1" type="CefKey">suser</pattern>

   <pattern id="AllEvents" type="JavaPattern">(.*?)</pattern>
      <match-group order="1" device-type-id-override="4001">

      <matcher order="1" field="EventCategory" pattern-id="EventCategory-Pattern-1" capture-group="\1" enable-substitutions="true"/>

      <cef-matcher order="1" field="EventName" pattern-id="EventName-Pattern-1" enable-substitutions="true"/>

      <cef-matcher order="1" field="SourceIp" pattern-id="SourceIp-Pattern-1" enable-substitutions="true"/>

      <cef-matcher order="1" field="UserName" pattern-id="UserName-Pattern-1" enable-substitutions="true"/>

      <event-match-multiple pattern-id="AllEvents" send-identity="UseDSMResults" force-qidmap-lookup-on-fixup="true"/>
   </match-group>
</ns2:device-extension>
```

2. Log into **QRadar** on your web browser.



3. Click the **Admin** tab.