IBM Security Privileged Identity Manager
Version 2.1.0

Installation and Configuration Guide

IBM

IBM Security Privileged Identity Manager
Version 2.1.0

Installation and Configuration Guide

IBM

Contents

Figures

Tables

Chapter 1. Prerequisite software

Install and configure the prerequisite components before you install the IBM®
Security Privileged Identity Manager virtual appliance.

Installing and configuring the database server

You must install the database server first before installing the IBM Security
Privileged Identity Manager virtual appliance.

About this task

For detailed information about DB2® instance creation, go to the IBM DB2 product
documentation, and search for `Creating an instance using db2icrt`.

Procedure

1. Create the database instance.

   a. Create an operating system user. For example, `piminstu`.

      For Windows:

      > Add the operating system user `piminstu` as a member of the
      > following groups:
      > - `DB2ADMNS`
      > - `DB2USERS`
      >
      > **Tip:** For more information, see the operating system documentation
      > and search for `adding users to groups Windows`.

      For Linux:
      > Add this user to the **root** group and set the **root** group as the
      > primary group for user `piminstu`:
      > ```
      > useradd -g root piminstu
      > ```

   b. Change the password for user `piminstu`:

      Note:
      - For Windows users, this step is **not** applicable if you have set your
        password to **Never Expire** in the previous step.
      - This step is compulsory for Unix and Linux users.

      For example, on Unix and Linux:
      ```
      passwd piminstu
      ```

      For example, on Windows:
      ```
      net user piminstu *
      ```

   c. Run the following command to create a database instance:

      For Windows:
      ```
      DB2_Install_Location\bin\db2icrt -u piminstu piminstname
      ```

      For Linux:
      ```
      DB2_Install_Location/instance/db2icrt -u piminstu piminstname
      ```
      where

      DB2_Install_Location is the DB2 installation directory.

piminstu is the user.

piminstname is the instance name that you are creating. For example: `piminst`

d. Start the DB2 instance.

For Windows:

In the command line, complete the following tasks:

- Run **set DB2INSTANCE=piminst**, where `piminst` is the database instance.
- Run **db2cmd** to start the DB2 command line.
- Run **db2start**.

For Linux:

- Run **su - piminst**
- Run **db2start**.

e. Run the following commands to set up the DB2 instance:

- **db2 update dbm cfg using SVCENAME** *port_number*, where *port_number* is the port on which you want your database server to listen. For example: `50050`
- **db2set DB2COMM=tcpip**
- **db2set -all DB2COMM**
- **db2stop**
- **db2start**

2. Create the database.

IBM Security Privileged Identity Manager uses three separate databases for the three data stores: Identity, Sign-On, and Session Recording.

To create a database, take the following actions:

Important:

- For Windows, run db2cmd as the user who owns the instance. If you run db2cmd as a user who is not the instance owner, you give rights only to the current user.
- For Linux, run su - `piminstname`.

a. Start the DB2 instance.

Note: Type the following commands as the instance owner.

For Windows:

- Launch the command line as the instance owner by using the **runas** command.
- Run **set DB2INSTANCE=piminst**, where `piminst` is the database instance that you want to create.
- Run **db2cmd** to start the DB2 command line.
- Run **db2start**.

For Linux:

- Run **su - piminst**, where `piminst` is the database instance.
- Run **db2start**.

b. In the DB2 command line, type the following example commands as the instance owner.

> **Note:** If you are unable to run the commands as the instance owner, run them as a database admin user and proceed to Step 3.

> **For the Identity data stores**
>
> ```
> db2 create db idmdb using codeset utf-8 territory us pagesize
> 32 K
> ```

> **For the Single Sign-On data stores**
>
> ```
> db2 create db essodb using codeset utf-8 territory us pagesize
> 32 K
> ```

> **For the Session Recording data stores**
>
> ```
> db2 create db psrdb using codeset utf-8 territory us pagesize
> 32 K
> ```

> **Note:** Single Sign-On and Session Recording data stores with 8k or 32k page sizes are acceptable.

   c. Create a temporary table space with the following command:

```
db2 connect to psrdb
db2 create user temporary tablespace systoolstmpspace
    pagesize 32 k managed by automatic storage bufferpool ibmdefaultbp
```

> **Note:** The temporary table space page size must match the page size of the data stores in the earlier step.

3. Grant permissions.

   Note: This is only applicable if databases are created by using a database admin.

   If the databases are created by using another Administrator or SYSADMIN account (in this example db2admin is used), run the following commands to grant certain accesses to the instance owner on the data stores

   a. Grant database administration rights to all databases.

```
db2 connect to idmdb user {db2admin} using {password}
db2 GRANT DBADM, SECADM ON DATABASE TO USER piminstu
db2 disconnect current

db2 connect to psrdb user {db2admin} using {password}
db2 GRANT DBADM, SECADM ON DATABASE TO USER piminstu
db2 disconnect current

db2 connect to essodb user {db2admin} using {password}
db2 GRANT DBADM, SECADM ON DATABASE TO USER piminstu
db2 disconnect current

db2stop
db2start
```

   b. Grant archiving rights to the Privileged Session Recorder database.

```
db2 connect to psrdb user db2admin using password
db2 grant execute on module sysibmadm.utl_file to user piminstu with
grant option
db2 grant execute on module sysibmadm.utl_dir to user piminstu with
grant option
```

Installing and configuring the directory server

You must install and configure the directory server before you install the virtual appliance.

Before you begin

You must have the database server installed.

Procedure

1. For information about installing the directory server, see documentation that the directory server product provides. For example, access the documentation at http://www.ibm.com/support/knowledgecenter/SSVJJU/welcome?lang=en and search for **Installing and Configuring**.

2. Configure the directory server for IBM Security Privileged Identity Manager virtual appliance by creating and configuring the directory server instance.

   a. Create a user.

      - Windows

        In the command line, enter:

        LDAP_Install_Location\sbin\idsadduser -u ldapinst -w ldapinstpwd

        where ldapinst is the user name and also the LDAP instance name, and ldapinstpwd is the password.

      - UNIX and Linux

        In the command line, enter:

        LDAP_Install_Location/sbin/idsadduser -u ldapinst -w ldapinstpwd -g idsldap

        where ldapinst is the user name and also the LDAP instance name, ldapinstpwd is the password, and idsldap is the default LDAP group.

   b. Create a directory server instance.

      In the command line, enter:

      LDAP_Install_Location/sbin/idsicrt -I *ldapinst* -e *encryptionseed* -l *location*

      where

      ldapinst is the user name and LDAP instance name.

      encryptionseed is a random string that must be more than 12 characters. For example, mysecretsalt. See idsicrt

      location specifies the location to store the configuration files and logs of a directory server instance. For Linux, you might specify the instance home, /home/ldapinst. For Windows, use a drive letter, like C:.

      For example:

      LDAP_Install_Location/sbin/idsicrt -I *ldapinst* -e *mysecretsalt* -l */home/ldapinst*

   c. Create a database for the newly created LDAP instance.

      In the command line, enter:

      For Unix and Linux:

      LDAP_Install_Location/sbin/idscfgdb -I *ldapinst* -a *ldapinst* -w *ldapinstpwd* -t dbname -l /home/ldapinst/

      For Windows

      LDAP_Install_Location/sbin/idscfgdb -I *ldapinst* -a *ldapinst* -w *ldapinstpwd* -t dbname -l C:

      where ldapinst is the LDAP instance name and user owner, ldapinstpwd is the password for ldapinst, dbname is the new database name, and /home/ldapinst is the instance home. On Windows, the location must be a drive letter, such as C:.

d. Set the password for directory server instance Principal DN.

In the command line, enter:

LDAP_Install_Location/sbin/idsdnpw -I ldapinst -u cn=root -p password

where `ldapinst` is the LDAP instance name, `cn=root` is the Principal DN, and `password` is the Principal DN password.

e. Add the suffix (`dc=com`) in the directory server instance.

In the command line, enter:

LDAP_Install_Location/sbin/idscfgsuf -I ldapinst -s dc=com

where `ldapinst` is an LDAP instance name, and `dc=com` is the suffix.

f. Start the directory server instance.
- Windows

  Use one of the following methods:
  - Windows Services
  - Instance Administration Tool
- UNIX and Linux

  In the command line, enter:

  LDAP_Install_Location/sbin/ibmslapd -I ldapinst -n -t

  where `ldapinst` is an LDAP instance name.

g. Prepare a `ldif` file. For example, `dccom.ldif` with the following content.

```
dn:dc=com
objectclass:domain
```

Run the command:

```
LDAP_Install_Location/bin/idsldapadd -h ldap_server_host
 -p ldap_server_port -D bind_root_dn -w bind_root_password
 -f dccom.ldif
```

For example:

```
/opt/IBM/ldap/V6.4/bin/idsldapadd -h ldapserver -p 389
-D cn=root -w password
 -f <filepath to dccom.ldif>
```

Setting up the directory server for SSL connection

Set up the directory server for an SSL connection to enable secure communication between the IBM Security Privileged Identity Manager virtual appliance and the directory server.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

The GSKit command-line tool will be used to create the certificate files needed to enable SSL connection on the directory server.

Note: On 32-bit platforms use the gsk8capicmd utility, and on 64-bit platforms use the gsk8capicmd_64 utility.

Procedure

1. Create a certificate. Use the GSKit command-line tool to create a self-signed certificate and extract the certificate to make it available for secure communication.

   a. Find the GSKit on your system.
      - For Linux: Enter `gsk8capicmd` on the command line. If anything other than an error message is returned, GSKit is installed and ready to use.
      - For Windows: Open Registry Editor and look for `HKEY_LOCAL_MACHINE\ SOFTWARE\IBM\gsk8\CurrentVersion\InstallPath`. This key indicates where GSKit is installed.

   b. Prepare the location of the certificate files. For example: `/certs`

   c. Go to the designated location of certificate files and create the CMS key database.

      ```
      cd /certs
      gsk8capicmd -keydb -create -db serverkey.kdb -pw serverpwd -stash
      ```

      where, `serverkey.kdb` is the key database to be created and `serverpwd` is the password.

      For example:`C:\Program Files\IBM\gsk8\certs>"C:\Program Files\IBM\gsk8\bin\gsk8capicmd_64.exe" -keydb -create -db serverkey.kdb -pw serverpwd -stash`

   d. Create a default self-signed certificate and add it to the `serverkey.kdb` key database.

      ```
      gsk8capicmd -cert -create -db serverkey.kdb -pw serverpwd -label
      serverlabel -dn "cn=<FQDN of the LDAP Server>, DC=com" -default_cert
      yes
      ```

      For example: `C:\Program Files\IBM\gsk8\certs>"C:\Program Files\IBM\gsk8\bin\gsk8capicmd_64.exe" -cert -create -db serverkey.kdb -pw serverpwd -label ldapserver -dn "cn=ldapserver,DC=com" -default_cert yes`

   e. Copy the certs folder to `/<LDAP_Install_Location>/`. For example, `/opt/IBM/ldap/V6.3/` For more information, see:
      - Topics on securing directory communications in the *IBM Security Directory Server Administration Guide* at

        http://www.ibm.com/support/knowledgecenter/SSVJJU_6.3.1/ com.ibm.IBMDS.doc_6.3.1/welcome.htm
      - *IBM Global Security Kit GSKCapiCmd User's Guide* at

        http://www.ibm.com/support/docview.wss?uid=pub1sc22545900

2. Enable the directory server for an SSL connection. Use an LDIF file to configure SSL on the directory server and to specify a secure port.

   a. If the directory server is not running, start the server. For example, on UNIX, type this command:

      ```
      /opt/IBM/ldap/V6.4/sbin/ibmslapd -I itimldap
      ```

      Where *-I* specifies the instance.

   b. Create an LDIF file, such as `ssl.ldif`, with the following data:

      ```
      dn: cn=SSL,cn=Configuration
      changetype: modify
      replace: ibm-slapdSecurity
      ibm-slapdSecurity: ssl
      -
      replace: ibm-slapdSslKeyDatabase
      ```

```
ibm-slapdSslKeyDatabase: /certs/serverkey.kdb
-
add:ibm-slapdSslKeyDatabasePW
ibm-slapdSslKeyDatabasePW: <serverpwd>
```

Note: The empty lines that contain only the - (hyphen) character are expected for LDIF file formatting.

To change the secured port from the default port number 636, add these additional lines:

```
replace: ibm-slapdSecurePort
ibm-slapdSecurePort: 637
```

c. Run the **idsldapmodify** command, which modifies the password policy by adding the LDIF file to the process.

```
idsldapmodify -D cn=root -p <ldapport> -w <passwd> -i <filepath to ssl.ldif>
```

-D   Binds to the LDAP directory, which is `cn=root` in this example.

-p   The default LDAP port. For example, 389.

-w   Uses the *passwd* value, which is the directory server administrator password, as the password for authentication.

-i   Reads the entry modification information from an LDIF file instead of from standard input. In this example, the file is named `ssl.ldif`.

For example, `C:\Program Files\IBM\gsk8\certs>"C:\Program Files\IBM\ldap\V6.4\bin\idsldapmodify" -D cn=root -p 389 -w password -i ssl.ldif`

A successful result produces a message similar to the following one:

```
Operation 0 modifying entry cn=SSL,cn=Configuration
```

d. Test the directory server to confirm that it is listening on the default secure port 636. Follow these steps:

1) Restart the LDAP instance by using one of the following methods:
   - Windows Services
   - Instance Administration Tool

2) Determine whether the directory server is listening on port 636.

   For example, display statistics for the network interface with the directory server by typing the following command:

   For Unix and Linux

   ```
   netstat -an |grep 636.
   ```

   For Windows

   ```
   netstat -an | find "636"
   ```

   A return message that indicates the port is listening might be represented by the following example:

   ```
   tcp    0   0 9.42.62.72:636  0.0.0.0:*   LISTEN
   ```

Chapter 2. Installation

Install the IBM Security Privileged Identity Manager components that are required in your environment.

Virtual appliance installation

The IBM Security Privileged Identity Manager comes in a virtual appliance format.

The virtual appliance must be hosted on one of the supported hypervisors.

VMware support

The IBM Security Privileged Identity Manager can be installed on a VMware ESXi hypervisor.

The virtual appliance for VMware is distributed as a disk image in `.iso` format.

Setting up the virtual appliance

Create a virtual machine to host the IBM Security Privileged Identity Manager.

Procedure

1. Download the `ispim_*.iso` build.
2. Create a virtual machine on VMware ESXi.
   a. From the VMware vSphere Client, click **File** > **New** > **Virtual Machine**.
   b. In **Configuration**, select **Custom**.
   c. Provide a name for the virtual machine. The virtual machine name can contain up to 80 characters, and the name must be unique within each vCenter Server VM folder.
   d. Choose the destination storage for this virtual machine.
   e. Set virtual machine version to 8.
   f. Set the guest operating system to **Linux**. Under **Version**, select **Other 2.6.x Linux (64-bit)**.
   g. Depending on your requirements, enter the number of virtual sockets and cores per virtual sockets for the virtual machine. For example, enter the value as 2 for the following options to sum up the total number of cores to 4.
      - **Number of virtual sockets**
      - **Number of cores per virtual socket**
   h. Enter the memory size. The minimum size is 16 GB.
   i. Create three network interfaces to set up the virtual machine.
   j. Set **VMXNET 3** from a list of network adapters for better results. You can also use the **E1000** adapter to set up the virtual machine.
   k. Set the SCSI controller type to **LSI Logic Parallel**.
   l. Select the **Create a new virtual disk** option as the type of disk to use.
   m. Enter the disk size for virtual machine. The minimum size is 100 GB.
   n. Accept the default settings in the Advanced Options page.
3. Verify the settings for the virtual machine.

4. Select **Edit the virtual machine settings before completion**.
5. Click **Add** in the **Hardware** tab of the Virtual Machine Properties window.
6. Choose **CD/DVD drive**.
7. Select the type of media that you want the virtual drive to access. For example, select **Use ISO image**.
8. Browse to the data store location where you uploaded the `.iso` file.
9. Click **Finish** on the Add Hardware window.
10. Select **Connect at power on** on the Virtual Machine Properties window.
11. Click **Finish** on the Virtual Machine Properties window.

What to do next

Proceed with the IBM Security Privileged Identity Manager virtual appliance installation. See "Installing the virtual appliance on VMware."

Installing the virtual appliance on VMware
Install the IBM Security Privileged Identity Manager virtual appliance after you set up the virtual machine.

Procedure
1. When you start the virtual machine for the first time, press Enter to begin with the virtual appliance installation process.
2. Select the language that you want to use during the installation.
3. Type yes to continue.
4. When the installation process is complete, unmount the installation media.
   a. Right-click on the virtual machine and select **Edit Settings**.
   b. On the **Hardware** tab of the Virtual Machine Properties window, select **CD/DVD drive 1**.
   c. Clear these check boxes.
      - **Connected**
      - **Connect at power on**
5. Click **OK** to close the Virtual Machine Properties window.
6. Select **Yes** and click **OK** to confirm the installation media disconnection.
7. Press Enter and then press any key to continue.

What to do next

Go to "Setting up the virtual appliance" on page 12.

XenServer support
The IBM Security Privileged Identity Manager can be installed on a supported version of the Citrix XenServer hypervisor.

The virtual appliance for XenServer is distributed as a disk image in `.vhd` format.

Installing the virtual appliance on XenServer
Import the VHD image to XenServer with XenCenter to install the virtual appliance.

Before you begin

Ensure that you have the following prerequisites:
- A functional XenServer environment, which is used as the hypervisor to host the VHD image.
- A configured XenCenter installation, which is used to deploy the VHD image.

About this task

Procedure
1. On the XenCenter console, expand the XenCenter icon on the left.
2. Right-click the attached hypervisor and select **Import**.
3. In the Import Source window:
   a. Click **Browse**.
   b. Select the VHD image to be imported and click **Open**.
   c. Click **Next**.
4. In the VM Definition window:
   a. Specify the name, number of CPUs, and memory of the virtual machine.

      Note: In most scenarios, assign the virtual machine at least one processor and 2 GB of memory. These settings can be adjusted after the virtual machine starts running.
   b. Click **Next**.
5. In the Location window:
   a. Select the destination hypervisor from the drop-down list.
   b. Click **Next**.
6. In the Storage window:
   a. Select **Place imported virtual disks onto specified target SRs**.
   b. Click **Next**.
7. In the Networking window:
   a. Select the network to be used for the first management interface.
   b. Click **Next**.
8. In the OS Fixup Settings window:
   a. Select **Don't use Operating System Fixup**.
   b. Click **Next**.
9. In the Transfer VM Settings window:
   a. Specify the settings to suit your network environment.

      Note: A valid IP address, subnet, and gateway is required.
   b. Click **Next**.
10. In the Finish window, click **Finish** to start the import.

    Note: The import operation might take a considerable amount of time to complete. You can click the **Logs** tab to check the progress of the import.
11. When the import is complete, run the following commands on the XenServer console to set the image to paravirtualized mode.

```
xe vm-list (to get the uuid for the VM)
xe vm-param-set uuid=<vm uuid> HVM-boot-policy=""
xe vm-param-set uuid=<vm uuid> PV-bootloader=pygrub
xe vm-disk-list (to get the uuid for the disk - VBD entry)
xe vbd-param-set uuid=<disk uuid> bootable=true
```

For example:

```
[root@xenserver ~]# xe vm-list name-label="autodeploy"
uuid ( RO)           : 6288a6a6-8577-5444-6ed5-46d2a097be54
     name-label ( RW): autodeploy
    power-state ( RO): halted
[root@xenserver ~]# xe vm-param-set uuid=6288a6a6-8577-5444-6ed5-46d2a097be54 HVM-boot-policy=""
[root@xenserver ~]# xe vm-param-set uuid=6288a6a6-8577-5444-6ed5-46d2a097be54 PV-bootloader=pygrub
[root@xenserver ~]# xe vm-disk-list vm="autodeploy"
Disk 0 VBD:
uuid ( RO)           : b0d08251-7f08-8b4e-3913-e71052dd7b13
    vm-name-label ( RO): autodeploy
        userdevice ( RW): xvda

Disk 0 VDI:
uuid ( RO)           : 8dfa6027-1ef3-408b-a9ed-efa751d41720
        name-label ( RW): amapp-template_vdi
     sr-name-label ( RO): Local storage
      virtual-size ( RO): 107376279552

[root@xenserver ~]# xe vbd-param-set uuid=b0d08251-7f08-8b4e-3913-e71052dd7b13 bootable=true
```

12. Start the imported virtual machine.

Note: At least 3 network interfaces must be configured in order for the virtual
appliance to start. Sometimes the XenCenter must be restarted before the new
virtual appliance can be started correctly.

Setting up the virtual appliance

The appliance setup wizard runs the first time that you connect to the virtual
console of an unconfigured virtual appliance.

Before you begin

Complete the virtual appliance installation. See "Virtual appliance installation" on
page 9.

Important: During the installation, maintain the same date and time between the
system where you installed the virtual appliance and the system where you
installed the database.

About this task

Use the appliance setup wizard to manage host, port, or other configuration
details, and then apply the changes to work with the virtual appliance.

This topic also provides the instructions on how to enable Federal Information
Processing Standards (FIPS) feature on the virtual appliance.

Federal Information Processing Standards (FIPS) are guidelines that are set for
software and hardware computer security products. Products that support FIPS
standards can be set into a mode where the product uses only FIPS approved
algorithms and methods.

Security toolkits typically support both FIPS approved and non-FIPS approved functions. In FIPS mode, the product is incapable of using any non-FIPS approved methods.

Before you enable the FIPS compliance on the virtual appliance, take note of the following limitations:

- FIPS-compliant mode can be enabled only on new virtual appliance installations.
- All virtual appliances in a cluster must have the same settings. For example, if FIPS is enabled in the cluster, all members of the cluster must also have FIPS enabled.
- Virtual appliances that are operating in FIPS-compliant mode can only securely connect to FIPS-compliant systems.

Procedure

1. Provide the following user credentials when the system restarts after the IBM Security Privileged Identity Manager virtual appliance installation:
   - **Unconfigured login**: admin
   - **Password**: admin
2. On the setup wizard screen, press Enter.
3. Choose a language, then read and accept the terms.

```
Software License Agreement
Currently selected language: English
1: Select language for license display
2: Read IBM terms
3: Read non-IBM terms
4: Proceeed to acceptance

Select option: 4


By choosing 'I agree,' you agree that (1) you have had the opportunity to
review the terms of both the IBM and non-IBM licenses presented above and (2)
such terms govern this transaction. If you do not agree, choose 'I do not
agree'.
1: I agree
2: I do not agree

Select option: 1
```

4. Optional: Select option 1 to enable FIPS.

   Important: FIPS cannot be disabled once it is enabled.

```
FIP 140-2 Mode Configuration

You must enable FIPS mode in order to comply with FIPS 140-2 and NIST 800-131a.

If you select the enable FIPS mode, appliance will be rebooted immediately to
perform FIPS power-up integrity checks.
Do not choose to enable FIPS mode without reading the FIPS section in the user
guide.

If you choose to enable FIPS mode now, you cannot disable it later without
reinstalling the appliance.

FIPS 140-2 Mode is not enabled.
1: Enable FIPS 140-2 Mode
x: Exit
p: Previous screen
n: Next screen

Select option: 1




FIPS 140-2 Configuration
Enable FIPS 140-2 mode?
1: yes
2: no
Enter index: 1
You have selected to enable FIPS mode. The appliance will now reboot to perform
the FIPS integrity checks.
When appliance comes back up, you will need to login as admin useer to complete
the setup.
Enter 'YES' to confirm: YES
```

5. Reboot the system.
6. Once the system is rebooted, change the virtual appliance password and go to
   the next screen.

```
Appliance Password
Password changes are applied immediately.
Password has not been modified.
1: Change password
x: Exit
p: Previous screen
n: Next screen


Change Password
Enter old password:
Enter new password:
Confirm new password:
Password changed successfully.


Appliance Password
Password changes are applied immediately.
Password has been modified.
1: Change password
x: Exit
p: Previous screen
n: Next screen

Select option: n
```

7. Change the host name. You must use an FQDN host name.

```
Change the Host Name
Enter the new host name (FQDN): ispimva.us.example.com

Host Name Configuration
Host name: ispimva.us.example.com
1: Change the host name
x: Exit
p: Previous screen
n: Next screen

Select option: n
```

Note: The host name is identified in the SSL certificate that is issued for the
virtual appliance. In a stand-alone setup, you must use the same host name
value when you configure the target server connection for Privileged Access
Agent on client workstations, Privileged Session Gateway, and App ID Toolkit.

8. Configure network interface M1 with the IP address, subnet mask, and default
   gateway.

   Note: If necessary, consult your network administrator to obtain the correct
   network settings for your environment.

```
Management Interface Settings
1: Display device settings
2: Display policy
3: Configure M.1
4: Configure M.2
x: Exit
p: Previous screen
n: Next screen

Select option: 3

Configure M.1
Select an IPv4 configuration mode:
1: Automatic
2: Manual
Enter index: 2
Enter the IPv4 address: 192.0.2.21
Enter the IPv4 subnet mask: 255.255.252.0
Enter the IPv4 default gateway: 192.0.2.12
Select an IPv6 configuration mode:
1: Automatic
2: Manual
Enter index: 1

Management Interface Settings
1: Display device settings
2: Display policy
3: Configure M.1
4: Configure M.2
x: Exit
p: Previous screen
n: Next screen

Select option: n
```

9. Configure the DNS for the virtual appliance.

   Note: If necessary, consult your network administrator to obtain the correct
   DNS settings for your environment.

```
DNS Configuration
No DNS servers configured.
1: Set DNS server 1
2: Set DNS server 2
3: Set DNS server 3
x: Exit
p: Previous screen
n: Next screen

Select option: 1

Set DNS Server 1
Enter the DNS Server IP address: 198.51.100.0


DNS Configuration
DNS server 1: 198.51.100.0
1: Set DNS server 1
2: Set DNS server 2
3: Set DNS server 3
x: Exit
p: Previous screen
n: Next screen

Select option: n
```

10. Configure the time settings for the virtual appliance.

```
Time Configuration
Time configuration changes are applied immediately.
Time: 08:28:58
Date: 12/09/2015
Time Zone: Asia/Kolkata
1: Change the time
2: Change the date
3: Change the time zone
x: Exit
p: Previous screen
n: Next screen

Select option: n
1: Change the time
2: Change the date
3: Change the time zone
x: Exit
p: Previous screen
n: Next screen

Select option: n
```

11. Review the summary of configuration details.

    Note: If necessary, record the details of the assigned IP address, DNS, and host name of the virtual appliance.

12. Press 1 to accept the configuration.

Results

A message indicates that the policy changes are successfully applied, and the local management interface is restarted.

What to do next

Configure the virtual appliance. See "Setting up a stand-alone or primary node for IBM Security Privileged Identity Manager" on page 17.

Selecting the virtual appliance configuration mode

In the Mode Selection page, you can set up the IBM Security Privileged Identity Manager virtual appliance as a stand-alone server or primary node, or as a member node. Select an option that is based on your deployment preference.

Before you begin

Ensure that the workstation can resolve the target host name of the virtual appliance.

About this task

IBM Security Privileged Identity Manager virtual appliance supports high availability deployment mode. A high availability deployment is a cluster of multiple servers that are active and can process requests. The virtual appliance cluster consists of one primary node, one or more member nodes, and a load balancer as a front end.

Procedure

1. On another workstation, with a web browser, type the host name of the IBM Security Privileged Identity Manager virtual appliance in the following format.

   `https://hostname:9443`

   For example: `https://pim1.jk.example.com:9443`

2. Log on to the IBM Security Privileged Identity Manager virtual appliance with the administrator credentials.

3. Select one of the mode options that are based on your requirement and click **Next**.

Setting up a stand-alone or primary node for IBM Security Privileged Identity Manager

Log on to the Initial Configuration wizard from the web user interface to complete the virtual appliance setup tasks for stand-alone or primary node for IBM Security Privileged Identity Manager.

Before you begin

- Configure the initial virtual appliance settings.
- Collect the following information:
  - Setup mode selection

    Choose from **Guided** or **Advanced** setup mode.
  - Session recording activation code
  - Application identity management activation code
  - Root CA or signer certificate configuration
  - Mail server configuration
  - Database server configuration.
  - Directory server configuration.

Procedure

1. On a client workstation with a web browser, enter the host name of the configured virtual appliance in the following format.

   `https://hostname:9443`

For example: `https://pimva1.jk.example.com:9443`

2. Log on to the IBM Security Privileged Identity Manager virtual appliance with the administrator credentials.

   Note: The default user password to log on to the virtual appliance administrator console is `admin`. If you changed the password during the virtual machine setup, use that password. If you did not change the password, use the default administrator password, which is `admin`.

   - **Configured login**: `admin`
   - **Password**: `admin`

3. Select the **Set up a stand-alone node for IBM Security Privileged Identity Manager OR Set up a Primary node for the IBM Security Privileged Identity Manager cluster** deployment mode option.

4. Choose one of the following configuration modes and click **Next page**.

Option	Actions
Guided Configuration	1. Follow the steps in the wizard. 2. Go to step 6.
Advanced Configuration	1. Use a properties response file that contains the predefined values for the configuration parameters. **Note:** The response file **must** have an extension of `.txt`, `.rsp`, `.response`, `.props`, or `.properties`. See "Sample configuration response file for the virtual appliance" in the *IBM Security Privileged Identity Manager Reference Guide*. 2. Upload the response file to the Mode Selection page. 3. Click **Next page**. 4. Go to step 11 on page 19.

5. Optional: If your deployment relies on the virtual appliance hosts file for name resolving IP addresses to host names for external resources such as the database and directory server, in navigation pane, click **Maintain Hosts File**.

   You can add the host names and IP addresses for prerequisite hosts such the database and directory server before proceeding with server configuration. `192.0.0.20 mydb.example.local`

6. On the **Session Recording Activation** and **Application Identity Management Activation** pages, take one of the following actions and click **Next page**:

   - Enter the activation code.
     – To enable the session recording feature, enter the **Session Recording Activation Code**. See "Activating the session recording feature in the virtual appliance" on page 62.
     – To enable the application identity feature, enter the **Application Identity Management Activation Code** . See "Enabling the application identity management feature in the virtual appliance" on page 63.

   Note: If you do not enter the activation codes at this stage, you can enter the activation codes after you set up the virtual appliance. These features are not enabled until you enter the activation codes.

- If you do not plan to use these features or do not have the activation codes, skip to the next page.

7. Optional: On the **Root CA Configuration** page, take one of the following actions and click **Next page**.
   - To customize the self-signed certificate, click **Update**.
   - Click **Export** if you plan to set up a cluster of virtual appliances. You must upload the exported Root CA certificate to the Load Balancer.

8. Configure the mail server and click **Next page**.

9. Configure the database settings for the following data stores and click **Next page**. For information about database settings, see Table 10 on page 45.
   - Identity
   - Single Sign-On
   - Session Recording

10. Configure the directory server and click **Next page**. For information about directory server, see Table 9 on page 43.

11. On the **Completion Setup** page, complete the following tasks that depend on the configuration mode you selected.

   Important: When the configuration process begins, do not refresh the page or close the browser session.
   - **Guided Configuration**: Review the instructions and click **Complete Setup** to complete the configuration process.
   - **Advanced Configuration**: Review the instructions and click **Start Configuration** to begin the configuration process.

   After the configuration completes, a link to restart the virtual appliance is displayed. If the mail server configuration setup is correct, an email notification is sent when the virtual appliance configuration is complete.

12. Click the restart link to restart the virtual appliance.

   Note: Check the restart status in the hypervisor console.

Related information:
Initial console setup for users

Setting up a virtual appliance cluster

To set up a virtual appliance cluster, you must have a primary node ready and running and then add member nodes to it.

Procedure

1. Set up a primary node. The primary node must be ready and running.
2. Add member nodes to the cluster.

Related information:
Initial console setup for users

Setting up a member node for the IBM Security Privileged Identity Manager

For high availability deployment mode, you can set up a member node for the IBM Security Privileged Identity Manager cluster by using the initial configuration wizard.

Before you begin

Configure the initial virtual appliance settings.

The primary and member nodes must be able to communicate with each other.

About this task

In a web browser, log on to the initial configuration wizard from the web user interface after you complete the virtual appliance logon configuration.

Use the **Set up a Member node for the IBM Security Privileged Identity Manager cluster** option to set up a member node.

Take note of the following limitations if you are enabling the FIPS compliance on the virtual appliance:
* FIPS-compliant mode can be enabled only on new virtual appliance installations.
* All virtual appliances in a cluster must have the same settings. For example, if FIPS is enabled in the cluster, all members of the cluster must also have FIPS enabled.
* Virtual appliances that are operating in FIPS-compliant mode can only securely connect to FIPS-compliant systems.

Procedure

1. In a web browser, enter the host name of the configured virtual appliance in the following format.
   ```
   https://hostname:9443
   ```

   For example: `https://pimva1.jk.example.com:9443`
2. In the **Connect to Primary** tab of the Setup Progress page, provide the details of the primary node.
   a. Type the host name in the **Primary node host name** field. For example, `pimva1.jk.example.com`.

   The `Primary node` host name must be same that was used to create the primary virtual appliance host name. That is, the value in the **Issued To** field of the primary node host name must match with the value that you entered in the **Primary node host name** field of the **Connect to Primary** tab.
   b. Type the password in the **Primary node administrator password** field. For example, `admin`.
3. Click **Test Connection** to validate the details and to verify this connection of the member node with the primary node. The system notifies that the connection to the primary node was successful.
4. Click **Next page**.

   Note: The **Next page** button is activated only when the connection to the primary node is successful.

   The **Completion** tab is displayed.
5. Click **Fetch Configuration** to obtain configuration details from the primary node. A progress bar indicates about fetching the configuration details from the primary node. The **Start Configuration** button is activated only when the **Fetch Configuration** operation is completed successfully.

6. Click **Start Configuration** to start the initial configuration for the IBM Security Privileged Identity Manager virtual appliance. The Completion page opens to indicate the data synchronization process. Do one of these actions:

- If the configuration is successful, a message indicates to restart the IBM Security Privileged Identity Manager virtual appliance. See Restarting or shutting down.

- If the configuration is not complete or not successful, a message indicates the reason. Do one of the following actions:

  - Click the **Log files** link to open the Log Retrieval and Configuration page and check for any messages and errors in the log files.

  - Click the **Click here** link to restart the configuration process in case of failures.

Synchronizing a member node with a primary node

Use the Cluster Node Configuration page to synchronize a member node with a primary node in the IBM Security Privileged Identity Manager virtual appliance.

About this task

The **Configure** > **Manage Cluster** menu is displayed only in a cluster environment and not in a stand-alone environment.

In the primary node virtual appliance console, all nodes in the cluster are displayed in the Cluster Node Configuration table.

In the member node virtual appliance console, only the current member node is displayed in the Cluster Node Configuration table.

Synchronize the following nodes in the cluster for any configuration changes that you make in the IBM Security Privileged Identity Manager virtual appliance.

Member node
> In the Cluster Node Configuration table of the Cluster Node Configuration page, select a member node for synchronization. The **Synchronize** button is not active until you select a node.
>
> Wait for the synchronization process to complete.

Primary node
> In the Cluster Node Configuration page, select one or more member nodes except the primary node for synchronization. The **Synchronize** button is not active when:
>
> - The primary node is selected.
> - The status of the selected node is displayed as Synchronizing in the **Synchronization State** column of the Cluster Node Configuration table.
>
> The primary node submits the synchronization request to each of the nodes that were selected. You can view the synchronization status in the **Synchronization State** column of the Cluster Node Configuration table.

Note: Before you do a synchronization operation, address all the notifications on the primary node.

The **Synchronization State** column displays these synchronization states:

Table 1. Synchronization state table

Status	Description	Action
Not Connected	Displays when a member node cannot connect to a primary node or when a primary node cannot connect to the member node.	Connect the member node with the primary node. For a node with the Not Connected status, click **Reconnect Node** to connect that node into the cluster. See "Reconnecting a node into the cluster" on page 66.
Not Synchronized	Displays when the member node is not synchronized with the primary node.	Synchronize the member node with the primary node. See the following procedure.
Synchronized	Displays when the member node is synchronized with the primary node.	No action is required.
Synchronizing	Displays when the member node is synchronizing with the primary node.	Wait until the synchronization is complete. Click the **Refresh** icon to get the most recent status.
Not Applicable	Displays if the cluster node is a primary node because the primary node does not require any synchronization.	No action is required.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage Cluster** > **Cluster Node Configuration**.
2. Do the following actions.
   - From the member node console, select the current member node and click **Synchronize** to synchronize it with the primary node.

     A progress bar indicates the synchronization process. It retrieves configuration information from the primary node for any configuration changes and synchronizes within the same node.
   - From the primary node console, select one or more member nodes and click **Synchronize**.

     A synchronization request is submitted to each of the node that was selected.

Results

The member node is synchronized with the primary node.

Setting up a load balancer for a virtual appliance cluster

Deploying a cluster of Privileged Identity Manager virtual appliances with a load balancer provides the required high availability for business continuity.

Before you begin

The load balancer must meet the following requirements:

- Must be a Layer-7 load balancer.

- Valid SSL certificate installed. You can install a certificate that is signed by a commercial Certificate Authority or a self-signed certificate. For a self-signed certificate, the Root CA certificate that is used to sign the load balancer certificate, must be imported into the Windows truststore to work with Privileged Access Agent.
- `underscores_in_headers` directive is enabled.
- Session affinity is enabled.

Procedure

1. Set up and configure the front-end load balancer. See "Planning for high availability" in the *IBM Security Privileged Identity Manager Planning and Deployment Guide*.
2. Package the load balancer SSL certificate with the Privileged Access Agent installation packages.
3. Configure Privileged Access Agent to use the load balancer as the IBM Security Privileged Identity Manager server.
4. Configure the load balancer settings on the virtual appliance. See "Configuring the Load Balancer settings" in the *IBM Security Privileged Identity Manager Installation and Configuration Guide*.

   ➦ developerWorks: Configuring the appliance with a load balancer

Privileged Session Gateway installation

With the Privileged Session Gateway, Privileged Users can securely access SSH-enabled resources with privileged credentials through a web browser without installing extra client software on their workstations.

You can deploy the Privileged Session Gateway in any of the following deployment configurations:
- "Single node deployment" on page 24
- "Clustered deployment" on page 24

Before you begin, choose a deployment configuration.

Table 2. Single node and clustered deployments
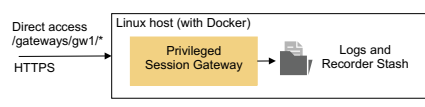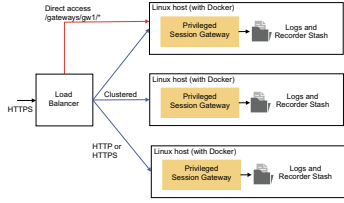
Category	Single node	Clustered
Connections	 *Figure 1. Single node deployment*	 *Figure 2. Clustered deployment*
Load balancer	None.	A Layer 7 load balancer is required with its own inbound certificate. The load balancer is configured to route traffic to each node.
Inbound certificate	The inbound certificate can be a self-signed certificate generated by the Gateway or a customer-provided certificate.	The inbound certificate can be a self-signed certificate generated by the Gateway or a customer-provided certificate.

Table 2. Single node and clustered deployments (continued)

Category	Single node	Clustered
Outbound certificate	IBM Security Privileged Identity Manager virtual appliance certificate	IBM Security Privileged Identity Manager load balancer certificate
Virtual appliance configuration	Configure the virtual appliance to point to the Privileged Session Gateway node URL. The virtual appliance must import the Privileged Session Gateway instance self-signed or CA certificate.	Configure the virtual appliance to point to the load balancer URL. The virtual appliance must import the load balancer CA certificate.

Single node deployment

Table 3. Privileged Session Gateway installation roadmap for a single node

Step	Task	Reference
1	Install the Privileged Session Gateway image.	"Installing the Privileged Session Gateway image" on page 25
2	Deploy a single node. **Important:** HTTPS setting must be enabled.	"Deploying a single node" on page 26
3	Export the Privileged Session Gateway certificate. **Note:** In a production deployment, the SSL certificate is typically replaced with the organization's own self-signed certificate or a certificate that is signed by an enterprise Certificate Authority (CA). For certificates signed by a CA, you must export the CA certificate.	"Obtaining the gateway certificate" on page 34
4	On the virtual appliance, import the Privileged Session Gateway self-signed or CA certificate.	"Adding the Privileged Session Gateway or load balancer certificate to the virtual appliance" on page 34
5	Optional: Add a hosts file entry for the Privileged Session Gateway on the virtual appliance. **Note:** Add the hosts file entry only if the DNS service that the virtual appliance looks up cannot resolve certain host names.	"Adding a hosts file entry on the gateway and virtual appliance" on page 35
6	Configure the Privileged Session Gateway URL on the virtual appliance.	"Managing the Privileged Session Gateway configuration" on page 47

Clustered deployment

Table 4. Privileged Session Gateway installation roadmap for a clustered configuration

Step	Task	Reference
1	Install the Privileged Session Gateway image.	"Installing the Privileged Session Gateway image" on page 25
2	Deploy multiple Privileged Session Gateway nodes for a clustered configuration.	"Deploying multiple nodes as a cluster" on page 32

Table 4. Privileged Session Gateway installation roadmap for a clustered configuration (continued)

Step	Task	Reference
3	Set up the load balancer for the cluster	"Setting up a load balancer for the gateway cluster" on page 32
4	Obtain the load balancer certificate.	
5	On the virtual appliance, import the load balancer self-signed or CA certificate.	"Adding the Privileged Session Gateway or load balancer certificate to the virtual appliance" on page 34
6	Optional: Add a hosts file entry for the Privileged Session Gateway on the virtual appliance. **Note:** Add the hosts file entry only if the DNS service that the virtual appliance and gateway looks up cannot resolve the host names for the virtual appliance or gateway.	"Adding a hosts file entry on the gateway and virtual appliance" on page 35
7	Configure the Privileged Session Gateway load balancer as the URL on the virtual appliance.	"Managing the Privileged Session Gateway configuration" on page 47

Installing the Privileged Session Gateway image

The Privileged Session Gateway application is distributed as a Docker image.

Before you begin

1. Install Docker on a Linux host. See https://docs.docker.com/engine/installation/.

   Note: Review the list of supported Linux distributions and follow the instructions to install the appropriate version for your environment.
   Steps for each Linux distribution vary. For example, on Red Hat Enterprise Linux, Ubuntu, and CentOS, ensure that you complete the following steps:

   - Create a Docker group.
   - Configure the docker daemon to start on boot.

2. Verify your Docker installation. Ensure that you can run the **docker run hello-world** command successfully.

About this task

The Privileged Session Gateway package consists of the following components:

ibm-session-gateway.tgz
    The Privileged Session Gateway image.

install.sh
    The installation script that installs Privileged Session Gateway. Run the script with the **--help** parameter to see the list of supported arguments.

```
./install.sh --help
Script to install or upgrade IBM Session Gateway image from file

Usage:
   ./install.sh --file <gateway image file>

Supported command-line arguments:
   --file <gateway image file>    MANDATORY: IBM Session Gateway file to be imported.
```

run.sh

The script that creates and runs a Privileged Session Gateway container.
Include the **--help** parameter to see the list of supported arguments.

```
/> ./run.sh --help
Usage:
./run.sh        [-r <responseFile>]
                [|-f|--reset]
                [|-h|--help|-?]
Supported command-line arguments:
  -r <responseFile>          MANDATORY: Response file which contains necessary configurations
  -f/--reset                 OPTIONAL: Force removal of old container, and start new container from image
  -h/--help/-?               OPTIONAL: Show help
```

ibm-session-gateway.rsp

Response file that defines an instance of the Privileged Session Gateway.

Procedure

1. On the Linux host, copy the Privileged Session Gateway package to a target location. For example: ~/session-gateway/

2. Set the executable permission for the shell scripts. From the command line, type:
   - chmod +x install.sh
   - chmod +x run.sh

3. Run the installation script install.sh.

   ./install.sh --file ibm-session-gateway.tgz

4. Verify that the image is installed.

   docker images

   Example result:

```
REPOSITORY              TAG              IMAGE ID          CREATED          SIZE
ibm-session-gateway     latest           022ef91d7b70      5 days ago       <size>
```

Deploying a single node

Deploy a single Privileged Session Gateway node for a simple deployment.

Procedure

1. Create a copy of the response file, ibm-session-gateway.rsp, and provide a new name.

   For example: gateway1.rsp

2. Obtain the Privileged Session Gateway activation key.

   Available only from 2.1.0, fix pack 3.

   a. Download the activation key package from Passport Advantage®.

   b. Extract the compressed file and open the text file.

   c. In the Privileged Session Gateway response file, enter the activation key in the **activation_key** parameter.

3. With **disable_client_authorization** set to *no*, get the Privileged Session Gateway client ID.

Available only from 2.1.0, fix pack 3.

For more information about trusted sessions, see
disable_client_authorization.

a. To obtain a Client ID, configure the Privileged Session Gateway location in the virtual appliance. See "Managing the Privileged Session Gateway configuration" in the *IBM Security Privileged Identity Manager Installation and Configuration Guide*. After the Privileged Session Gateway is configured, the Client ID is displayed in the Privileged Session Gateway configuration page.

b. In the Privileged Session Gateway response file, for the **authorized_clients** parameter, enter the client ID and the virtual appliance or load balancer URL in the required format. See Table 5 on page 28. For example:
`"123ab-123ab-1234-123AB-123AB,https://pimva.example.local"`

4. Obtain the IBM Security Privileged Identity Manager virtual appliance root certificate by selecting one of the following approaches:

To obtain the certificate by	Do
Providing the domain name of the IBM Security Privileged Identity Manager virtual appliance or load balancer.	In the response file, specify the **outbound_certificate_urls** parameter. For example: `pimva.local:443`. See Table 5 on page 28.
Exporting the certificate to a directory location.	1. Export the certificate with a `.crt` file extension in one of the following supported formats: • **X.509 Certificate (PEM)** • **Base64 Encoded X.509** **Note:** You must export the certificate with a `.crt` file extension. **Important:** In a tree representation of the certification path, the root certificate is typically represented as the first item in the certification path. For example: PIMVA. To deploy a self-signed company certificate or a CA signed certificate, export the certificate to a file in the supported format. To obtain the virtual appliance root certificate with a web browser, browse to the IBM Security Privileged Identity Manager URL: `https://<ispimva>`. See your web browser documentation on how to export the certificate for a website to a file. **Note:** In Mozilla Firefox, be sure to save the certificate with a `.crt` file extension to avoid problems. The IBM Security Privileged Identity Manager virtual appliance certificate that you obtain is an outbound certificate for the gateway. 2. Copy the exported certificate to a directory where the certificate can be retrieved. For example: `~/session-gateway/certs_out/`

5. Optional: If an enterprise CA signed certificate is required for inbound connections, complete the following steps:

a. Add the certificate to a PKCS#12 keystore. Example keystore file: `custom-root.p12`

b. Place the keystore in the Privileged Session Gateway inbound keystore directory.

For example: ~/session-gateway/certs_in/

6. In the new response file, review the required parameters.

Table 5. Configuration parameters for a single node

Parameter	Importance	Description
`gateway_id`	Required	The gateway container ID. The ID must consist only of the following characters `[a-zA-Z0-9.-]`. It is case-sensitive. For example: `gateway1` In a load balanced deployment, each gateway ID in the cluster must be unique.
`activation_key` Available only from 2.1.0, fix pack 3.	Required	The activation key for the Privileged Session Gateway. Obtain the activation key from Passport Advantage.
`outbound_certificate_urls` Available only from 2.1.0, fix pack 3.	Optional	Domain name where the outbound certificate for the virtual appliance or load balancer can be retrieved. Include the port number of the virtual appliance or load balancer that is used for listening to requests. **Note:** Alternatively, you can specify the outbound certificate with the **outbound_certificate_directory** parameter for the outbound certificates. Do not include `https://` in the value. For example: `"pimva.example.local:443"` The outbound certificates are imported later to the Gateway trust store.
`outbound_certificate_directory`	Optional	Directory where the outbound certificate for the virtual appliance or load balancer that you export can be retrieved. See step 4 on page 27. **Note:** If you are specifying outbound certificates by providing the URL for **outbound_certificate_urls**, you do not need to specify a value for **outbound_certificate_directory**. If both parameters are specified, the certificates that are found with **outbound_certificate_urls** take precedence. For example: `~/session-gateway/certs_out/` The outbound certificates are imported later by the shell script to the Gateway trust store.
`https`	Optional	The HTTP protocol to use. For a single node deployment without a load balancer, only HTTPS is supported. Set the value to `yes`. `https=yes` Default value is `no`.
`port`	Optional	The HTTP or HTTPS port number that is used for listening to requests. Default value when HTTP is enabled (**https=no**): 9080. Default value when HTTPS is enabled (**https=yes**): 9443.

Table 5. Configuration parameters for a single node (continued)

Parameter	Importance	Description
`keystore_path`	Optional	Path to the keystore file that contains the custom inbound certificate. Production deployments typically require the use of an organization's own self-signed certificate or an enterprise signed CA certificate. To use these certificates, export and save the signed `.p12` certificate to this directory. Ensure that you specify the keystore password for the `keystore_password` parameter. For example: `~/session-gateway/certs_in/custom-root.p12`
`keystore_password`	Optional	The password for the keystore file.
`disable_client_authorization` Available only from 2.1.0, fix pack 3.	Optional	Toggles whether client authorization restriction is disabled. If set to `yes`, client authorization is disabled. Default is `no`. **Note:** If the IBM Security Privileged Identity Manager virtual appliance is version 2.1.0, and the Privileged Session Gateway is upgraded to 2.1.0 fix pack 3, disable client authorization to avoid disruptions to Privileged Session Gateway access. As soon as the IBM Security Privileged Identity Manager virtual appliance is upgraded to 2.1.0 fix pack 3, enable client authorization, and configure the `authorized_clients` parameter. **Important:** Avoid disabling client authorization. Client authorization ensures that only trusted clients such as IBM Security Privileged Identity Manager can initiate connections through the Privileged Session Gateway. See `authorized_clients`.

Table 5. Configuration parameters for a single node (continued)

Parameter	Importance	Description

`authorized_clients`
 	
Available only from 2.1.0, fix pack 3.
	Optional	The list of authorized IBM Security Privileged Identity Manager virtual appliance cluster or stand-alone instances that are allowed to connect to the Privileged Session Gateway. The list is specified as a value pair.
		
		Before you can define this parameter, you must obtain a **Client ID**. To obtain a Client ID, configure the Privileged Session Gateway location in the virtual appliance. See "Managing the Privileged Session Gateway configuration" in the *IBM Security Privileged Identity Manager Installation and Configuration Guide.*.
		
		You must enclose the assigned values for the `authorized_clients` parameter with double quotation marks (" ").
		
		Syntax:
		
		`"<client_id>,<referrer>"`
		
		`client_id`
		 The client ID that is generated when you configure the Privileged Session Gateway location in the virtual appliance dashboard. To retrieve the `client_id`, see "Managing the Privileged Session Gateway configuration" in the *IBM Security Privileged Identity Manager Installation and Configuration Guide.*.
		
		 Not case-sensitive.
		
		`referrer` The IBM Security Privileged Identity Manager virtual appliance or load balancer URL.
		
		If you are listing multiple clients, separate each value pair with a semi-colon.
		
		For example: `"123AB-123AB-1234b-123AB-123AB,https://referrer1;567a-567a-5678,https://referrer2"`
		
		Note: If this parameter is not specified and client authorization is enabled, connections are not allowed. See `disable_client_authorization`

For example:

```
# This is an example response file to start the Privileged Session Gateway container.
# Lines that begin with # or * are treated as comments.
*
* NOTE: Spaces are not allowed between parameter and attribute values.

############### MANDATORY CONFIGURATION ###################

# Identifies the gateway instance uniquely.
gateway_id=gateway1

# Activation key for the Privileged Session Gateway. Obtain the activation key from Passport Advantage.
# For example: 123AB-123AB-123AB-123AB-123AB
activation_key=

############### OPTIONAL CONFIGURATION  ###################

# It is recommended that at least outbound_certificate_directory or
# outbound_certificate_urls is specified

# Directory that contains outbound certificates which will import to Gateway Trust Store.
# The certificate file must be PEM(base64) encoded X.509 certificate file, with file extension as ".crt".
# outbound_certificate_directory=~/session-gateway/certs_out/

# List of ; delimited URLs. The Gateway parses these URL, imports the certificate and updates them.
# Do not provide https:// tag. Example URLs: "pimva.local:443"
outbound_certificate_urls="pimva.example.local:443"

# IBM Session Gateway image name. Default is 'ibm-session-gateway'.
docker_image_name=ibm-session-gateway

# IBM Session Gateway image tagname. Default is 'latest'.
docker_image_tag=latest

# Mounted directory for logs etc. Default is ~/ibm/shared/.
shared_directory=~/ibm/shared/
```

```
# If yes, use HTTPS. If no, use HTTP. Default is no.
https=yes

# HTTP or HTTPS port used to access REST APIs and GUI. If HTTP, default is 9080; if HTTPS,
# default is 9443.
port=9443

# Keystore(PKCS12 format) containing the custom inbound root cert (with private key), if not set,
the Gateway will generate
# or use a previously generated certificate.
# NOTICE: The keystore file will be copied to <shared dir>/security/custom_root.p12. If not set,
the keystore
# will be generated at <shared dir>/security/self-root.p12, and the keystore password is 'gateway'.
keystore_path=

# Password for the keystore file.
keystore_password=

# File containing outbound aliases for targets. Default is /etc/hosts.
hosts_file=/etc/hosts

# Recording segment file size (minimum is '1KB', maximum is '10MB'). Format is <integer value><unit(KB/MB)>.
 Default is '1MB'.
segment_size=1MB

# Number of uploader threads (minimum is 5, maximum is 100). Default is 5.
uploader_threads=5

# Log level for Gateway services. Valid options are: error, warning, info, debug. Default is info.
log_level=info

# If yes, there is no client restriction and the authorized_clients parameter is ignored. Default is no.
# NOT RECOMMENDED FOR USE: use this with caution because disabling client authorization can open the system
to probing attacks
disable_client_authorization=no

# Identifies the IBM Security Privileged Identity Manager  virtual appliance instance or
 load balancer (clustered deployments)
# that can connect to the Privileged Session Gateway.
# List of ";" delimited authorized client IDs and referers. The format is
 "<client id>,<referer>;<client id>,<referer>".
# If no authorized clients are listed and client authorization is not disabled, no connection order requests
 are allowed.
authorized_clients="123a-123a-1234,https://pimva.example.local"
```

7. Save the response file to a location on the computer.

    For example: `~/session-gateway/gateway1.rsp`

8. Initialize the Privileged Session Gateway image with the response file as a parameter.

    `./run.sh -f -r gateway1.rsp`

    Shared folders are created in `~/ibm/shared/<gateway_id>`

    The p12 keystore file is copied to the mounted shared folder `~/ibm/shared/<gateway_id>/security/` as `custom-root.p12`.

    If the keystore options in the response file are not specified, a self-signed certificate is automatically generated with a Common Name that is equal to the gateway ID as specified in the response file. The self-self certificate is then copied to the mounted shared folder `~/ibm/shared/<gateway id>/security/` as `self-root.p12`

9. Verify that the Privileged Session Gateway instance is started.

    `docker ps`

    Example result:

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
1052274c7aae	ibm-session-gateway:latest	"/usr/bin/supervisord"	2 hours ago	Up 2 hours	9080/tcp, 0.0.0.0:9443->9443/tcp	gateway1

    Note: Certificate and hosts file changes are only applied once after you initialize the node. To apply the changes, you must restart the node. See *Restarting a Privileged Session Gateway node* in *IBM Security Privileged Identity Manager Troubleshooting Guide*.

Deploying multiple nodes as a cluster

Deploy multiple gateway instances in a clustered configuration with a front-end load balancer for high availability.

About this task

In a clustered deployment, deploy the Privileged Session Gateway behind a load balancer. In the cluster, the load balancer routes session connection requests and traffic to the nodes.

Procedure

1. Prepare the Linux host and response file.

   See step 2 on page 26 to 7 on page 31 in "Deploying a single node" on page 26.

2. Initialize a Privileged Session Gateway node.

   ```
   ./run.sh -f -r gateway1.rsp
   ```

   where

   gateway1.rsp, might contain the following parameters:

   ```
   ...
   gateway_id=gateway1
   outbound_certificate_directory=~/session-gateway/certs_out/
   https=no
   port=9080
   activation_key=xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
   ...
   ```

   Note: To initialize more nodes on the cluster, on another prepared Linux host, run the following command to add another gateway node, gateway2, with port number 9080:

   ```
   ./run.sh -f -r gateway2.rsp
   ```

   where

   gateway2.rsp, might contain the following parameters:

   ```
   ...
   gateway_id=gateway2
   outbound_certificate_directory=~/session-gateway/certs_out/
   https=no
   port=9080
   activation_key=xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
   ...
   ```

3. Verify that the nodes are successfully initialized.

   ```
   docker ps
   ```

Setting up a load balancer for the gateway cluster

A Layer 7 load balancer is needed to route connection requests and session traffic to the Privileged Session Gateway nodes.

Before you begin

- Layer 7 load balancer is required.

  If HTTP is configured, the out-of-the-box inbound certificate does not have to be replaced.

- The load balancer must support the WebSockets protocol.

About this task

- For new connections, the load balancer routes requests to any of the active nodes. The routing strategy depends on the load balancer that you choose and configure.

- For existing connections, the load balancer routes the session traffic to the same node that accepted the initial connection request.

  Once a node accepts the connection, it returns a node-specific URL bearing the node's Gateway ID back to a user's browser. The user's browser uses this URL for subsequent exchange of session traffic with the Gateway node. As such, it is necessary to configure the load balancer with routes such that it is able to route requests that bear the node-specific URL to the correct Privileged Session Gateway node.

Procedure

1. Install and configure the front-end load balancer. See "Planning for high availability" in the *IBM Security Privileged Identity Manager Planning and Deployment Guide*.

2. If HTTPS is enabled on the Privileged Session Gateway node, obtain the Privileged Session Gateway SSL certificates and add them to the load balancer.

3. Configure the load balancer settings for Privileged Session Gateway.

   You need two types of routes:

   - Load-balanced route matching to all nodes in the cluster.

   - Static routes for each gateway node, matching /gateways/<gateway_id>, which must also have WebSockets protocol upgrade enabled

   The context root determines which URLs the load balancer routes traffic to.

   The following example is a fragment of a typical `nginx` load balancer routing configuration.

   In this cluster configuration, two Privileged Session Gateway nodes are hosted on separate Docker hosts, `gateway-node1` and `gateway-node2`. The two nodes run with the same ports, with Gateway IDs of `gateway1` and `gateway2`, respectively.

```
upstream backend  {
  server gateway-node1:9080;
  server gateway-node2:9080;
}

server{
   listen 443 ssl;

   server_name          ibm-session-gateway;
   ssl_certificate      /etc/nginx/ssl/new-cert.cert;
   ssl_certificate_key  /etc/nginx/ssl/new-cert.key;

   location / {
        proxy_pass  http://backend;
   }

   location ~* gateways/gateway1 {
        proxy_pass          http://gateway-node1:9080;
        proxy_http_version  1.1;
        proxy_set_header    Upgrade $http_upgrade;
        proxy_set_header    Connection "upgrade";
   }

   location ~* gateways/gateway2 {
        proxy_pass          http://gateway-node2:9080;
        proxy_http_version  1.1;
```

```
                    proxy_set_header    Upgrade $http_upgrade;
                    proxy_set_header    Connection "upgrade";
            }
        }
```

Post-installation tasks

Complete the Privileged Session Gateway post-installation tasks before you
configure the Privileged Session Gateway location in the virtual appliance.

Obtaining the gateway certificate

Obtain the Privileged Session Gateway certificate so that you can add the
certificate to the virtual appliance certificate store.

About this task

For certificates that are signed by a certification authority (CA), export the CA
certificate.

Procedure

1. Browse to the gateway URL `https://<session_gateway>:<port number>/v1`.

   For example: `https://ibm-session-gateway:9443/v1`.

   Note: For a clustered deployment with a load balancer, you might not need to
   specify the URL with the port number. For example: `https://ibm-session-
   gateway/v1`.

   An **Insecure notification** or similar page might be displayed for the
   unrecognized certificate.
2. Export the certificate to a file.

   See your web browser documentation on how to export the certificate for a
   web site to a file.

Adding the Privileged Session Gateway or load balancer
certificate to the virtual appliance

For a single node deployment, add the Privileged Session Gateway certificate to
the virtual appliance and the Privileged Session Gateway. For a clustered
deployment, add the Privileged Session Gateway load balancer certificate to the
virtual appliance.

About this task

In an IBM Security Privileged Identity Manager virtual appliance cluster, add the
certificate to the primary node. After you add the certificate to the primary node,
synchronize the other nodes.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Configure** >
   Manage Server Setting > **Manage Certificates**.
2. Select the `ispim` certificate store.
3. Click **Edit**.
4. Click **Upload**.
5. Click **Browse** and select the certificate that you obtained.
6. Enter a label name. For example: `ibm-session-gateway`
7. Click **Save**.

8. Restart the services for the changes to take effect.

Adding a hosts file entry on the gateway and virtual appliance

This step is optional. Add the hosts file entry only if the DNS service that the virtual appliance and gateway look up cannot resolve the virtual appliance and gateway host names.

Procedure

1. On the virtual appliance, add a hosts file entry for the gateway.

    a. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Network Settings** > **Hosts File**.

       All current host records with their IP addresses and host names are displayed.

    b. Click **New**.

    c. On the Create Host record page, specify the following information:

       Address
       Specify the IP address of the Privileged Session Gateway.

       Host Name
       Specify the host name of the Privileged Session Gateway.

    d. Click **Save**.

       Note: Hosts file entries are not synchronized to cluster members.

2. On the Privileged Session Gateway Linux host, add a hosts file entry for the virtual appliance.

    Note: You can choose to create a file that resembles a hosts file instead of modifying the system hosts file. Ensure that this file is specified in the response file.

    Add the entry to the `/etc/hosts` file on the host where the Privileged Session Gateway runs.

    Note: You may need `root` access to edit the `hosts` file.

    For example:

    ```
    192.0.0.5  pimva.example.com
    ```

    Note: If you have running Privileged Session Gateway nodes, you must restart the nodes to apply the hosts file changes. See *Restarting a Privileged Session Gateway node* in *IBM Security Privileged Identity Manager Troubleshooting Guide*.

Privileged Access Agent installation

Install the Privileged Access Agent client to provide automated shared access credential check-in and check-out for IBM Security Privileged Identity Manager.

Note: Starting from IBM Security Privileged Identity Manager, Version 2.1.0, the Privileged Access Agent client component provides automatic credential check-in and check-out. The Privileged Access Agent client component replaces the functionality of the AccessAgent client that was previously included in earlier versions with IBM Security Access Manager for Enterprise Single Sign-On. The following content might contain references to the IBM Security Access Manager for Enterprise Single Sign-On product documentation where the functions are the same.

Table 6. Equivalent AccessAgent and Privileged Access Agent references

If there are references to	Privileged Access Agent reference
AccessAgent installation paths	See "Installation paths and registry entries" on page 40.
IMS Server or IMS	IBM Security Privileged Identity Manager virtual appliance or the load balancer as the equivalent single sign-on component.
AccessAgent registry entries	See "Installation paths and registry entries" on page 40.

Note: If you have an earlier version of the AccessAgent, Version 8.2.x component installed on Windows client computers, uninstall AccessAgent first before you install the Privileged Access Agent.

Installation on a single computer (small scale)

Important: Do not use the following installation steps for a production deployment of Privileged Access Agent on a large scale for multiple computers.

Table 7. Roadmap for Privileged Access Agent installation on a single computer.

Step	Task	Reference
1	Prepare the server SSL certificates for deploying on the Privileged Access Agent computers.	"Preparing SSL certificates for Privileged Access Agent deployments" on page 38
2	Install the Privileged Access Agent silently by using the prepackaged wallet. **Note:** To enable or disable the Credential Provider, see Response file parameters (SetupHlp.ini) and search for the **EncentuateCredentialProviderEnabled** parameter.	"Installing Privileged Access Agent silently (command prompt)" on page 39
3	For deployments on Windows 10, complete the following steps. If you have enabled the Privileged Access Agent logon screen (SSO Credential Provider), disable the Windows 10 lock screen: 1. Open the Local Group Policy Editor. Click **Start** > **Run**, and enter gpedit.msc. 2. Go to **Computer Configuration** > **Administrative Templates** > **Control Panel** > **Personalization**. 3. Select the **Do not display the lock screen** policy and set it to **Enable**.	
4	If you are using Mozilla Firefox, enable single sign-on for Mozilla Firefox with the web browser extension.	Single sign-on support for Mozilla Firefox

Installation on multiple computers (large scale)

Use the following steps for a production deployment on multiple computers.

Table 8. Roadmap for Privileged Access Agent installation on multiple computers.

Step	Task	Reference
1	Prepare a prepackaged Wallet for the installer.	"Preparing a prepackaged Wallet"
2	Prepare the server SSL certificates for deploying on the Privileged Access Agent computers.	"Preparing SSL certificates for Privileged Access Agent deployments" on page 38
3	Install the Privileged Access Agent silently by using the prepackaged wallet. **Note:** To enable or disable the Credential Provider, see Response file parameters (SetupHlp.ini) and search for the **EncentuateCredentialProviderEnabled** parameter.	"Installing Privileged Access Agent silently (command prompt)" on page 39
4	For deployments on Windows 10, complete the following steps. If you have enabled the Privileged Access Agent logon screen (SSO Credential Provider), disable the Windows 10 lock screen: 1. Open the Local Group Policy Editor. Click **Start** > **Run**, and enter gpedit.msc. 2. Go to **Computer Configuration** > **Administrative Templates** > **Control Panel** > **Personalization**. 3. Select the **Do not display the lock screen** policy and set it to **Enable**.	
5	If you are using Mozilla Firefox, enable single sign-on for Mozilla Firefox with the web browser extension.	Single sign-on support for Mozilla Firefox

Preparing a prepackaged Wallet

Before you install Privileged Access Agent on multiple computers, you can prepackage a Wallet first. Prepackaging the Wallet can reduce the load on the server when new Wallets are downloaded simultaneously by clients in large-scale deployments.

Before you begin

- Prepare a client computer for installing the Privileged Access Agent. This client computer is the staging workstation.
- Ensure that the server is installed and configured.

About this task

Configuring a prepackaged Wallet is useful for large-scale deployments of Privileged Access Agent.

When Privileged Access Agent is installed on a new workstation without cached Wallets on the computer, Privileged Access Agent downloads a fresh system Wallet from the server.

By including a prepackaged Wallet, Privileged Access Agent downloads only incremental updates from the server instead of downloading a fresh system Wallet.

Important: The staging workstation host name must **not** be used on any of the actual computers that you deploy on.

Procedure

1. Prepare the prepackaged Wallets on the staging workstation.

    a. Install the Privileged Access Agent on the staging workstation. See "Installing Privileged Access Agent silently (command prompt)" on page 39

    Note: Ensure that no previous version of Privileged Access Agent is installed.

    b. Ensure that the Privileged Access Agent connects to the production server.

    The Privileged Access Agent client downloads the system data from the server. The System Wallet is created.

2. Copy the generated Wallet file to the Privileged Access Agent installer.

On the staging workstation, copy the Wallet files from:	To the Privileged Access Agent installer:

`<AccessAgent install path>\Cryptoboxes\Wallets`
 	
For example:
 	
`C:\Program Files\IBM\ISPIM\AA\Cryptoboxes\Wallets`
	`<AccessAgent installer location>\<aa version number>\<aa package guid>\Config\Cryptoboxes\Wallets`
	
	You must create the `Cryptoboxes\Wallets` folders manually.
	
	For example:
	
	For 32-bit
	`c:\<AccessAgent installer location>\aa-<version number>\{9713108D-08D5-474E-92A3-09CD7B63DB34}\Config\Cryptoboxes\Wallets`
	
	For 64-bit
	`c:\<AccessAgent installer location>\aa-<version number>_x64\{E72C4028-45BB-4EE6-8563-3066EEB39A84}\Config\Cryptoboxes\Wallets`

3. Install the new Privileged Access Agent installation program on all client computers.

    Note: If the target computer has earlier versions of Privileged Access Agent, the prepackaged Wallet is not applied. The Wallet from the earlier installation is copied to the new installation.

    Important: If you are installing a pre-packaged Wallet on a computer that was previously registered on the server, reapply the Machine Policy Template after installation. Alternatively, delete the machine entry from AccessAdmin.

Preparing SSL certificates for Privileged Access Agent deployments

You must obtain the certificates of the server or Load Balancer and include them in the Privileged Access Agent installer before you deploy the Privileged Access Agent component.

Procedure

1. Start the web browser with **Administrator** privileges and browse to the URL of the appliance or the load balancer.

   For example: `https://pim_host.example.com` or `https://loadbalancer.example.com`.

2. Export the security certificates for the server or load balancer.

   See your specific web browser documentation on how to export the certificate for a website to a file.

   For example, with Microsoft Internet Explorer, repeat the following instructions for each server:

   a. Click **File** > **Properties**.

   b. Click **Certificates**.

   c. Click the **Certification Path** tab.

   d. For each certificate with a red X in the certificate hierarchy:

      1) Select the certificate.

      2) Click **View Certificate**.

      3) Click the **Details** tab.

      4) Click **Copy to File**.

   e. Follow the instructions in the Certificate Export wizard with the following considerations:

      1) When the Export File Format page is displayed, select the **DER encoded binary x.509 (.CER)** format.

      2) Save the certificates to a location on your computer.

3. Deploy the certificates on the client computers with one of the following ways:

Do	Description

Install the certificates with the Privileged Access Agent installer	Copy the certificates to the following location in the installer:
	
	For x86 operating systems
	`aa-<version_number>\{9713108D-08D5-474E-92A3-09CD7B63DB34}\Config`
	
	For x64 operating systems
	`aa-<version_number>_x64\{E72C4028-45BB-4EE6-8563-3066EEB39A84}\Config`

Install the certificate manually	Import the certificate manually into the **Trusted Root Certification Authority** by using the **Certificates** snap-in (`certmgr.msc`). Go to the Microsoft web site and search for `deploying a certificate manually`.
Deploy certificates by using an Active Directory Group Policy	Use an Active Directory Group Policy to deploy the certificates on client computers. Go to the Microsoft web site and search for `distribute certificates by using a group policy`.

Installing Privileged Access Agent silently (command prompt)

For a silent installation, include the **silent** parameter with the **Setup.exe** command.

Procedure

1. Open the `SetupHlp.ini` response file from the `<Access Agent install package path>\<Access Agent install path>\Config` directory. For example:

   32-bit `aa-<version>\{9713108D-08D5-474E-92A3-09CD7B63DB34}\Config`

64-bit `aa-<version>_x64\{E72C4028-45BB-4EE6-8563-3066EEB39A84}\Config`

2. In the `SetupHlp.ini` response file, specify the following required parameters for a silent installation:

InstallTypeGPO
Verify that the value for the **InstallTypeGPO** parameter is 1.

ImsConfigurationPromptEnabled
Verify that the value for the **ImsConfigurationPromptEnabled** parameter is 0. The default value is 0.

Note: If the **ImsConfigurationPromptEnabled** value is set to 1, the installation is not silent. The server configuration prompt is displayed even when you include the **/silent** parameter. Parameters in the response file always take precedence over any parameters in the command prompt.

ImsServerName
Specify the virtual appliance or the Load Balancer. For example: `IMSServerName = pimva.example.com`.

3. Save the file.
4. Open the command prompt.
5. Type the following command:

32-bit `aa-<version>\`**Setup.exe /silent /language:***LCID*

64-bit `aa-<version>_x64\`**Setup.exe /silent /language:***LCID*

Where:

Setup.exe
Installs Privileged Access Agent.

/silent
Specifies a silent installation.

/language:*LCID*
Specifies the language that is displayed in Privileged Access Agent.

If the parameter is not specified, the installer uses the operating system locale to determine the language to install.

For a list of language Locale IDs (LCID), go to the Microsoft website at www.microsoft.com and search for `Locale IDs assigned by Microsoft`.

If you specify a language ID that is not supported by the installation, the parameter is ignored.

Note: The computer restarts automatically to complete the installation.

Results

You installed Privileged Access Agent silently as a background process. By default, the installation process created a log file in *%temp%*`\AAInstaller.log`.

Installation paths and registry entries

After you install the Privileged Access Agent, verify that all the program files and registry entries are successfully installed on your computer.

Privileged Access Agent program files

By default, the Privileged Access Agent program files are stored in `C:\Program Files\IBM\ISPIM\AA`.

Privileged Access Agent registry entries

Privileged Access Agent registry entries are stored in the `[HKEY_LOCAL_MACHINE\ SOFTWARE\IBM\ISPIM]` key.

Fix pack installation

Fix packs provide fixes to known problems, new functions, additional currency and application support, resiliency, and performance improvements.

Refer to the fix pack readme for more information on installing specific fix packs. See IBM Security Privileged Identity Manager Fix Packs.

Virtual appliance

The fix packs for the virtual appliance are delivered by using the following methods:
- `.fixpack`: Apply the package from the **Appliance Dashboard** and save the configuration to install the fix pack.
- `.pkg`: Apply the virtual appliance firmware update package by using a USB or the FileUpload Tool.

Privileged Session Gateway

The fix pack for the Privileged Session Gateway is delivered as a compressed file, `.zip`.

Privileged Access Agent

The fix pack for the Privileged Access Agent is typically delivered in the form of Windows installer patch files, `.msp`.

Chapter 3. Configuration

With the Appliance Dashboard, you can manage the virtual appliance configuration for data store, directory server, and mail server. You can also customize the server properties, manage logs, Active Directory and certificates.

To manage the configured virtual appliance, log on to the **Appliance Dashboard** at `https://hostname:9443`. For example: `https://pimva1.jk.example.com:9443`.

Managing the directory server configuration

Use the Directory Server Configuration page to configure the directory server in the IBM Security Privileged Identity Manager virtual appliance.

Before you begin

Install and configure the directory server.

About this task

Configure or reconfigure the directory server options. See Table 9.

Table 9. Directory server configuration details

Field name	Description and examples
Configure	**Host name** The name of the computer that hosts the directory server. The host name must be specified in FQDN, IPv4, or IPv6. Example: `pimldap.example.com` **Port** The directory service port. Example: 389 If you opted for secure communication, use 636. **Principal DN** The principal distinguished name. Example: `cn=root` **Password** The password for the Principal DN. **Organization name** The name of the enterprise or the organization. Example: `JK Enterprises` **Default organization short name** The abbreviation or short form of the organization name. Example: `jke` **IBM Security Privileged Identity Manager DN Location** The directory server DN location. Example: `dc=com`

Table 9. Directory server configuration details (continued)

Field name	Description and examples
Reconfigure	**Host name** The name of the computer that hosts the directory server. The host name must be specified in FQDN, IPv4, or IPv6. Example: `pimldap.example.com` **Port** The directory service port. Example: 389 If you opted for secure communication, use 636. **Principal DN** The principal distinguished name. Example: `cn=root` **Password** The password for the Principal DN.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage External Entities** > **Directory Server Configuration**.
2. Click **Configure**.
3. In the Directory Server configuration details pane, specify the expected variables.
4. Click **Save Configuration** to complete this task.

   Note: The directory server configuration takes some time. Do not refresh or close the page. Wait for the configuration process to complete.
5. Optional: To reconfigure an existing directory server configuration, do these steps:
   a. From the Directory Server configuration table, select a record.
   b. Click **Reconfigure**.
   c. In the Edit directory server configuration details window, edit the configuration variables. See Table 9 on page 43.
   d. Click **Save Configuration**.
   e. Click **Yes** to confirm.

   Note: The directory server reconfiguration takes some time. Do not refresh or close the page. Wait for the reconfiguration process to complete.
6. Optional: To unconfigure an existing directory server configuration, do these steps:
   a. From the Directory Server configuration table, select a record.
   b. Click **Unconfigure**.
   c. Click **Yes** to confirm.

Managing the database server configuration

Use the Database Server Configuration page to configure the database server for the IBM Security Privileged Identity Manager virtual appliance.

About this task

Configure or reconfigure the data store options for the database server. See Table 10.

Table 10. Data stores configuration options

Data store	Description
`Identity data store`	**Host name** The name of the computer that hosts the data store. Example: `pimidstore.example.com`. **Port** The data store service port. Example: `50000`. **Database Name** The name of the IBM Security Privileged Identity Manager database. Example: `idmdb`. **Database Administrator ID** The user with database administrator privileges. Example: `piminst`. **Note:** During the database configuration for a virtual appliance, the user must be the database owner. For example, `piminst`. This database owner must be the same user who created the database. **Database Administrator Password** The password for the user with database administrator privileges.
`Single Sign-On data store`	**Host name** The name of the computer that hosts the data store. Example: `pimidstore.example.com`. **Port** The data store service port. Example: `50000`. **Database Name** The name of the IBM Security Access Manager for Enterprise Single Sign-On database. Example: `essodb` **Database Administrator ID** The user with database administrator privileges. Example: `piminst`. **Note:** During the database configuration for a virtual appliance, the user must be the database owner. For example, `piminst`. This database owner must be the same user who created the database. **Database Administrator Password** The password for the user with database administrator privileges.

Table 10. Data stores configuration options (continued)

Data store	Description

Session Recording data store	**Host name**
	   The name of the computer that hosts the data store. Example: `pimidstore.example.com`.
	
	Port The data store service port. Example: `50000`.
	
	Database Name
	   The name of the IBM Security Privileged Identity Manager database. Example: `psrdb`.
	
	Database Administrator ID
	   The user with database administrator privileges. Example: `piminst`.
	   Note: During the database configuration for a virtual appliance, the user must be the database owner. For example, `piminst`. This database owner must be the same user who created the database.
	
	Database Administrator Password
	   The password for the user with database administrator privileges.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage External Entities** > **Database Server Configuration**.

2. Click the **Configure**.

   Note: The next data store in the **Configure** menu, Single Sign-On data store, is only activated after you configure the Identity data store. Likewise, the Session Recording data store is activated in the **Configure** menu after you configure the Single Sign-On data store.

3. Specify the data store configuration details. See Table 10 on page 45.

4. Click **Save Configuration** to complete this task.

5. Click **OK**.

   Note: The database server configuration takes some time. Do not refresh or close the page. Wait for the configuration process to complete.

6. Optional: To reconfigure an existing database server configuration, do these steps:

   a. From the Database Server Configuration table, select a record.

   b. Click **Reconfgure**.

   c. In the Edit Identity data store details window, edit the details. For more information, see Table 10 on page 45.

      Note: The **Database Name** and **Database Administrator ID** fields are not editable during reconfiguration.

   d. Click **Save Configuration**.

   e. Click **Yes** to confirm.

      Note: The database server reconfiguration takes some time. Do not refresh or close the page. Wait for the reconfiguration process to complete.

7. Optional: To unconfigure an existing identity store, do these steps:

a. From the Database Server Configuration table, select a record.
b. Click **Unconfigure**.
c. Click **Yes** to confirm the deletion.

Configuring the Load Balancer settings

Use the Load Balancer Configuration page to configure the Load Balancer with the IBM Security Privileged Identity Manager virtual appliance.

Before you begin

You must work from the `Primary node` to configure or reconfigure the Load Balancer.

About this task

Configure the Load Balancer to support the working of your cluster or to distribute the workload across a cluster.

The Load Balancer Configuration page contains these columns:

Load Balancer DNS
> Displays the host name of the Load Balancer.

Last modified on
> Displays the date and time when the current Load Balancer DNS was last modified.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage External Entities** > **Load Balancer Configuration** to open the Load Balancer Configuration page.
2. Click **Configure** to open the Load Balancer details pane.
3. Provide the value in the **Load Balancer DNS** field. For example, enter the value as `pimva1.jk.example.com`.

   Note: The specified host name must be a valid and a fully qualified domain name that can be resolved by the DNS server.
4. Click **Save Configuration** to complete the configuration.
5. Optional: To reconfigure the Load Balancer, do the following steps.
   a. Select the **Load Balancer DNS** record from the Load Balancer Configuration page.
   b. Click **Reconfigure**.
   c. Follow steps 3 and 4.

      The IBM Security Privileged Identity Manager virtual appliance is reconfigured with the new load balancer information.

Managing the Privileged Session Gateway configuration

Specify the location of the Privileged Session Gateway so that Privileged Users can connect to managed resources through the Self-service console.

Before you begin

- Install the Privileged Session Gateway. See "Privileged Session Gateway installation" on page 23.
- Ensure that a two-way communication link is successful between the Privileged Session Gateway and the virtual appliance. From both the virtual appliance and Privileged Session Gateway, you can use the command line interface tools, `nslookup` and `ping`.

  Tip: Check the firewall configuration of the Linux host for the Privileged Session Gateway to ensure that the necessary ports are open.

About this task

Table 11. Privileged Session Gateway configuration details

Button	Description and examples
Configure	**Privileged Session Gateway URL** The fully qualified URL of the Privileged Session Gateway. For example: `https://ibm-session-gateway:9443`
Reconfigure	**Privileged Session Gateway URL** The fully qualified URL of the Privileged Session Gateway. For example: `https://ibm-session-gateway:9443`
Unconfigure	Remove the existing Privileged Session Gateway configuration.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Configure** > **Manage External Entities** > **Privileged Session Gateway Configuration**.
2. Click **Configure**.
3. In the Reconfigure Privileged Session Gateway window, specify the target location for the Privileged Session Gateway

   Note: Select the check box to regenerate the client ID.
4. Click **Save Configuration**.
5. Restart the **Identity** service from the **Server Control** widget. See "Viewing and using server controls" in the *IBM Security Privileged Identity Manager Administrator Guide*.

Managing the external user registry configuration

Use the External User Registry Configuration page to configure an external Active Directory user registry in the IBM Security Privileged Identity Manager virtual appliance. All user authentication is delegated to the configured user registry.

Before you begin

Complete the following tasks:
- Install and configure the directory server.
- Create the directory server DN location.
- Add the following required users to Active Directory:
  - `pim manager`

- isimsystem or equivalent IBM Security Privileged Identity Manager system user name
- Bind user

For isimsystem or equivalent IBM Security Privileged Identity Manager system user, the following conditions apply:
- Do **not** use space characters
- The Display Name must be the same as the login ID
- The user can be defined anywhere in the base DN
- The default name can be changed

For the bind user, the following conditions apply:
- Do **not** use space characters
- The Display Name must be the same as the login ID
- The user can be defined anywhere in the base DN

For the default pim manager user, the following conditions apply:
- The default pim manager name cannot be changed.
- The user can be defined anywhere in the base DN

For example, if the base DN that you are providing for the external registry configuration is cn=users,dc=example,dc=com, then the bind user, pim manager, and the IBM Security Privileged Identity Manager system user must be defined in this base DN.

About this task

Active Directory users do not automatically get IBM Security Privileged Identity Manager accounts. Users can be on-boarded with one of the following ways:
- Manually, where the user name is set to the Active Directory user name.
- Automatically, where users are reconciled by using the AD OrganizationalPerson identity feed in the administrative console.

After the external user registry is configured, existing IBM Security Privileged Identity Manager users will not be able to log in.

Note: The IBM Security Privileged Identity Manager user password management options and features must be disabled when the IBM Security Privileged Identity Manager virtual appliance is configured to authenticate users against an external user registry.

Important: After the external user registry is configured, you must customize or disable the default New Account Template before rolling out to new users. IBM Security Privileged Identity Manager password information that show in the default New Account Template are not applicable when an external user registry is configured.

You cannot unconfigure the external user registry or change it to use a different Active Directory domain.

Table 12. External Active Directory configuration details

Button	Description and examples
Configure	**Directory server host name (FQDN)** The fully qualified domain name of the computer that hosts the directory server. Example: `pimldap.example.com` **Domain DNS name** The full DNS name of the domain. For example: `example.com` **Domain NetBIOS name** The name that will be used by earlier versions of Windows to identify the domain. For example: `EXAMPLE` **Port** The directory service port. Default: 389 If you choose secure communication, the default value is automatically set to 636. **Bind user DN** The full distinguished name (DN) of an Active Directory user account that has privileges to search for users. Example: `CN=pimbind,CN=Users,DC=example,DC=com` **Note:** The user account does not need to have domain admin privileges. **Bind user password** The Active Directory password for the bind user. **Base DN of users** The distinguished name (DN) of the starting point for directory server searches. Example: `CN=Users,DC=example,DC=com` **Privileged Identity Manager system user name** The name of the Privileged Identity Manager system user name. Default: `isimsystem` **Privileged Identity Manager system user password** The password for the Privileged Identity Manager system user.

Table 12. External Active Directory configuration details (continued)

Button	Description and examples
Reconfigure	**Directory server host name (FQDN)** The fully qualified domain name of the computer that hosts the directory server. Example: `pimldap.example.com` **Port** The directory service port. Default: 389 If you choose secure communication, the default value is automatically set to 636. **Bind user DN** The full distinguished name (DN) of an Active Directory user account that has privileges to search for users. Example: `CN=pimbind,CN=Users,DC=example,DC=com` **Note:** The user account does not need to have domain admin privileges. **Bind user password** The Active Directory password for the bind user. **Base DN of users** The distinguished name (DN) of the starting point for directory server searches. Example: `CN=Users,DC=example,DC=com` **Privileged Identity Manager system user name** The name of the Privileged Identity Manager system user name. Default: `isimsystem` **Privileged Identity Manager system user password** The password for the Privileged Identity Manager system user.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage External Entities** > **External User Registry Configuration**.

2. Click **Configure**.

3. In the External User Registry configuration details pane, specify the expected variables. For more information, see Table 12 on page 50.

4. Click **Save Configuration** to complete this task.

   Note: The directory server configuration takes some time. Do not refresh or close the page. Wait for the configuration process to complete.
   After the Active Directory is successfully configured, the new entry is displayed on the External User Registry Configuration page.

5. For a clustered deployment, synchronize member nodes of the cluster with the primary node.

6. Restart the IBM Security Privileged Identity Manager again on the primary node.

7. Optional: To reconfigure an existing external user registry, do these steps:

   a. From the External User Registry Configuration table, select the user registry.

   b. Click **Reconfigure**.

   c. In the Edit External User Registry Configuration Details window, edit the configuration variables. See Table 12 on page 50

d. Click **Save Configuration** to complete this task.

Configuring IBM Security Access Manager Reverse Proxy (WebSEAL) to front the virtual appliance

Enable WebSEAL on the IBM Security Privileged Identity Manager virtual appliance as a front proxy so users can put 2-factor, or strong authentication mechanisms into web consoles.

Before you begin

You must know the WebSEAL login ID that you created.

WebSEAL use the login ID to authenticate by using HTTP Basic Authentication. See Basic Authentication Header.

You must ensure that the WebSEAL login ID is provisioned as a user in the IBM Security Privileged Identity Manager user registry. See Creating user profiles.

Procedure

1. In the Virtual appliance dashboard, click **Configure** > **Manage External Entities** > **WebSEAL Configuration**.
2. In WebSEAL Configuration, select the WebSEAL configuration.
3. Click **Reconfigure**.
4. In Reconfigure WebSEAL, do the following tasks:
   - Select **Enabled**.
   - Specify the WebSEAL login ID that you created.
5. Click **Save Configuration**.

Managing mail configuration

Use the Mail Server Configuration page to configure the email notifications for the IBM Security Privileged Identity Manager virtual appliance.

About this task

Table 13 on page 53 provides the mail server options that you can configure or reconfigure.

Table 13. Mail Server Configuration

Button	Mail Server options
Configure	**Mail server** Specify the name of the computer that hosts the mail server. For example, `localhost`. The acceptable formats for the mail server are FQDN, IPv4, and IPv6. **Port** Specify the service port of the mail server. For example: 25. **Mail from** Specify the email address from which the email is sent. For example, `admin@sgp.ibm.com`.
Reconfigure	**Mail server** Specify the name of the computer that hosts the mail server. For example, `localhost1`. The acceptable formats for the mail server are FQDN, IPv4, and IPv6. **Mail from** Specify the address from which the email is sent. For example, `admin1@sgp.ibm.com`.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Configure** > **Manage Server Setting** > **Mail Server Configuration**. The Mail Server Configuration page displays the Mail Server Configuration table.
2. Click **Configure**.
3. In the Mail Server Configuration Details window, specify the expected variable values. For information, see Table 13.
4. Click **Save Configuration** to complete this task.
5. Optional: To reconfigure an existing mail server configuration, do these steps:
   a. From the Mail Server Configuration table, select a record. For example, `Mail Configuration`.
   b. Click **Reconfigure**.
   c. In the Edit Mail Configuration Details window, edit the details. For more information, see Table 13.
   d. Click **Save Configuration**.
6. Optional: To unconfigure an existing mail server configuration, do these steps:
   a. From the Mail Server Configuration table, select a record.
   b. Click **Unconfigure**.
   c. Click **Yes** to confirm the deletion.

Managing the server properties

You can update the property values in the IBM Security Privileged Identity Manager virtual appliance to customize the IBM Security Privileged Identity Manager Server.

Before you begin

You must be familiar with the property keys and values of the IBM Security Privileged Identity Manager supplemental property files before you do this task. See the *Supplemental property files* section of the IBM Security Identity Manager documentation for details: http://www.ibm.com/support/knowledgecenter/SSRMWJ_6.0.0.2/com.ibm.isim.doc_6.0.0.2/reference/ref/ref_ic_props_supp.htm.

Procedure

1. From the menu, select **Configure** > **Advanced Configuration** > **Update Property**.
2. Select the property to update from the list, and click **Edit**.
3. Edit its property value and click **Save Configuration**.

   You can customize following IBM Security Privileged Identity Manager properties:

Table 14. Available IBM Security Privileged Identity Manager properties in the IBM Security Privileged Identity Manager virtual appliance

Supplemental property files	Properties and values
`adhocreporting.properties`	**applyACIAtRuntime = false** **availableForNonAdministrators = true**
`ReportDataSynchronization.properties`	**accountSynchronizationStrategy = old** **accountSynchronizationStrategy = old** **authorizationOwnerSynchronizationStrategy = old** **groupSynchronizationStrategy = old** **organizationalContainerSynchronizationStrategy = old** **personSynchronizationStrategy = old** **roleSynchronizationStrategy = old** **serviceSynchronizationStrategy = old**
`SelfServiceUI.properties`	**enrole.ui.pageSize = 10** **enrole.ui.pageLinkMax = 100** **enrole.ui.maxSearchResults = 1000** **enrole.ui.maxSearchResults.users = 100**

Table 14. Available IBM Security Privileged Identity Manager properties in the IBM Security Privileged Identity Manager virtual appliance (continued)

Supplemental property files	Properties and values
enRole.properties	enrole.connectionpool.incrementcount = 3
	enrole.connectionpool.initialpoolsize = 50
	enrole.connectionpool.maxpoolsize = 100
	enrole.connectionpool.protocol = plain ssl
	enrole.workflow.notifyoption = 1
	enrole.workflow.notifypassword = true
	enrole.workflow.notifyaccountsonwarning = false
	enrole.workflow.maxretry = 2
	enrole.workflow.retrydelay = 60000
	enrole.workflow.skipapprovalforrequester = false
	enrole.workflow.disablerequesteeapproval = false
	enrole.workflow.disablerequesterapproval = false
	enrole.workflow.skipfornoncomplianctaccount = true
	enrole.reconciliation.accountcachesize = 2000
	enrole.reconciliation.threadcount = 8
	remoteservices.remotepending.restart.retry = 1440
	remoteservices.remote.pending.testing.max.duration = 1200
	enrole.CreatePassword = true
	enrole.accesscontrollist.refreshInterval = 10
	enrole.recyclebin.enable = false
	enrole.lifecyclerule.partition.size = 100
	com.ibm.ispim.passwordRotation.maxCredsRotatePerCycle = 200
ui.properties	enrole.ui.customerLogo.image = ibm_banner.gif
	enrole.ui.customerLogo.url = www.ibm.com
	enrole.ui.pageSize = 50
	enrole.ui.pageLinkMax = 10
	enrole.ui.maxSearchResults = 1000
	enrole.ui.report.maxRecordsInReport = 5000
	ui.challengeResponse.showAnswers = true
	ui.userManagement.includeAccounts = true
	ui.challengeResponse.bypassChallengeResponse = true
	ui.passwordManagement.generatePassword = true

Managing feed files

You can upload feed files and use them in the IBM Security Privileged Identity Manager virtual appliance.

Procedure

1. From the menu, select **Configure** > **Manage Server Setting** > **Upload Feed File**.
2. Click **New**.
3. Click **Browse** to search for the feed file to upload. The feed files are in `/userdata/identity/feeds`.

   The `/userdata/identity/feeds` location is required while creating feeds in Administrative console.

Managing certificates

Administrators can view and manage the list of certificates that the virtual appliance uses to securely connect with different endpoints.

About this task

Certificates are typically issued to a particular computer or service. The certificate stores are typically managed by virtual appliance administrators. Virtual appliance administrators can manage the trust store of the virtual appliance, and its SSL certificate store.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Configure** > **Manage Server Setting** > **Certificates**. The Certificate Stores page displays these certificate keystores.
   - `ispim` The trust store for the virtual appliance
   - `https` The SSL certificate store.

   The Certificate Stores table displays these columns.

   Name The display name that is associated with the keystore.

   Type The type that is associated with the keystore.
2. Select a keystore that you want to manage.

   Note: If you are adding an entry for the Privileged Session Gateway, add the entry to the `ispim` trust store.
3. Click **Edit**. When you select a particular keystore to edit, the navigation path is displayed on the Certificates page. The navigation path identifies the keystore that you are currently editing. For example, if you select `https`, the path is **Certificate Stores** > **https**.

   On the Certificates page, the certificates are specified under these tabs.
   - **Personal Certificates** (only available for https keystore)
   - **Signer Certificates**

   These tabs display the following certificate columns.

   Label The display name that is associated with the certificate.

   Subject
   The name of the workstation, device, or certificate authority to whom the certificate is supplied.

   Issuer Information about the certificate authority that supplied the certificate.

   Not Valid Before
   The date and time from which the certificate is valid.

Not Valid After

> The date and time after which the certificate is no longer valid.

Key Size

> The key length that is associated with the certificate.

Version

> The X.509 version number.

Remarks

> Additional information about the certificate. The field is either `DEFAULT` or empty. If the remark shows `DEFAULT`, it is the default certificate in the certificate store.

4. On the Certificates page, do one of the following actions from the toolbar:

Option	Description
Upload	1. For the signer certificate, click the **Signer** tab.
	Import the following types of certificates:
	• DER-encoded form certificates.
	• PEM (Privacy-enhanced Electronic Mail) Base64 encoded DER certificate.
	The certificate file must have a `.pem` or `.der` extension.
	You must give the certificate a unique label name.
	You must restart the server after importing a certificate.
	Do these steps:
	a. Click **Upload** to display the Upload Certificate window.
	b. Click **Browse** to search and select the file that you want to import.
	The certificate information is displayed in the Files to upload table.
	c. In **Label**, specify an ID for the certificate.
	d. For a personal certificate, in **Password**, specify a password.
	e. Click **Save**.
	f. For a signer certificate, restart the server after you import a certificate.
	2. For personal certificates, click the **Personal** tab.
	Import the certificate, which is stored inside the PKCS12 certificate store types.
	The certificate store must have a `.p12` extension.
	Do these steps:
	a. Click **Upload** to display the Upload Certificate window.
	b. Click **Browse** to search and select the file that you want to import.
	The certificate store information is displayed in the Files to upload table.
	c. In **Label**, specify the label of the certificate you want to upload. The label must match the label of the certificate inside the `.p12` certificate store file.
	d. For a personal certificate, in **Password**, specify a password.
	e. Click **Save**.

Option	Description
Export	1. Select a certificate record. 2. Click **Export** to back up the certificate. 3. Specify a location where you want to back up the exported certificate.
Refresh	Update the list of displayed certificates.
Delete	Delete the selected certificate from the certificate store. Only certificates that are uploaded previously by the virtual appliance administrator can be deleted.
Set default This control is only available for personal certificates	Specify one of the certificates as the default certificate in the certificate store. If a personal certificate is set as a default of the https keystore, the certificate will be used as the SSL certificate for SSL connections. **Note:** If a personal certificate is used as a SSL certificate, the certificate common name (CN) **must** match the virtual appliance host name. Otherwise, SSL connections will fail when performing some of the operations.

Configuring cipher suites

Administrators can restrict the number of allowed cipher suites that are used for HTTPS and SSH sessions when you connect to the virtual appliance.

About this task

A cipher suite is a combination of algorithms that can be used for authentication, data encryption, key exchange, and message authentication for a secure network connection.

The following cipher suites for Application HTTPS are allowed:
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA

The App ID client and Privileged Access Agent communicate with the server over HTTPS. The cipher suites used by the App ID client and Privileged Access Agent are provided by the Java™ Runtime Environment and Windows. Ensure that the cipher suite configuration of the Java Runtime Environment or Windows match the cipher suites that are configured on the server. A successful HTTPS connection can only occur when both client and server share at least one matching cipher suite.

The following cipher suites for Management HTTPS are allowed:
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

The following cipher suites for SSH are allowed:
- aes128-ctr

- aes192-ctr
- aes256-ctr
- arcfour256
- arcfour128
- arcfour

If there are multiple cipher suites enabled, the cipher suite that is selected is dependent on the web browser and server negotiation. The order of the cipher suites are not important.

Procedure

1. From the menu of the **Appliance Dashboard**, click **Configure** > **Manage Server Setting** > **Cipher Suites Configuration**.
2. Select one of the following configurations:
   - **Cipher Suites Configuration for Application HTTPS**
   - **Cipher Suites Configuration for Management HTTPS**
   - **Cipher Suites Configuration for SSH**
3. Click **Reconfigure**.
4. In the resulting dialog box that displays, select the cipher suites that you want to enable or disable.

   Note: You cannot disable all the ciphers.
5. Click **Save Configuration** to complete this task. In a clustered deployment, the primary node is restarted automatically.
6. For clustered deployments, for each member node, restart the local management interface. Complete the following tasks:
   a. In the local management interface, type **lmi**.
   b. Type **restart**.

Configuring RFID authentication

You can use RFID cards as a second factor for user authentication with Privileged Access Agent on personal workstations.

Before you begin
- For middleware, check the hardware and software requirements for supported middleware and card readers.
- For card readers, check with your vendor for devices that are compatible with the middleware.

About this task

RFID authentication support requires RFID card middleware, an RFID card, and an RFID card reader.

You can also use the **Setup Assistant** in AccessAdmin for a guided configuration process.

Procedure

1. Log on to AccessAdmin.
2. Set the policies for RFID authentication.

a. Under **Machine Policy Templates**, select a new template, or an existing template, then click **Authentication Policies**.

b. In **Authentication second factors supported**, type `RFID`.

3. Apply the machine policy template to workstations.

a. Under **Machines**, click **Search**.

b. Click the computer name link.

c. Under **Machine policy template assignment**, select a template from the list.

d. Click **Assign**.

Managing log configuration

You can view component-specific and appliance log files to troubleshoot any appliance-related issues. You can also configure the file size and settings of the log files in the Log Configuration page.

About this task

Note: To configure and manage log files for the Privileged Session Gateway, see *Log files for the Privileged Session Gateway* in *IBM Security Privileged Identity Manager Troubleshooting Guide*.

Procedure

1. From the top-level menu in the **Appliance Dashboard**, select **Manage** > **Maintenace** > **Log Retrieval and Configuration**.

2. Select the appropriate tab for each category of logs.

3. Select **Configure** to set the file size and roll over settings for all logs.

Retrieving logs

Use the Log Retrieval and Configuration page to view the log files. You can also use the page to configure the server log settings for the IBM Security Privileged Identity Manager virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Manage** > **Maintenance** > **Log Retrieval and Configuration**.

2. Take any of the following actions:

   - To display a log file, click **View**.
   - To save a log file, click **Download**.
   - To remove a log file, click **Clear**.
   - To display all the log files again, click **Refresh**.

Table 15. Available logs to help you diagnose or troubleshoot

Tab	Log Files	File Name
Appliance These files help you to debug any configuration failures that occur in the virtual appliance.	Identity data store configuration	dbConfig.stdout
	Single Sign-On data store configuration	essoDbConfig.log
	Session Recording data store configuration	sessrecConfig.log
	Directory server configuration	ldapConfig.stdout
	Server system out	ispim_appliance_system.log
	Server Message	messages.log
Identity Helps you identify issues in the identity application.	Server System Out	SystemOut.log
	Server System Error	SystemErr.log
	Application Message	msg.log
	Application Trace	trace.log
	Identity Access Log	access.log
Single Sign-On Helps you identify issues in the single sign-on application.	Server System Out	SystemOut.log
	Server System Error	SystemErr.log
Session Recording Helps you identify issues in the session recording application.	Server System Out	SystemOut.log
	Server System Error	SystemErr.log

Configuring logs

You can configure different options to manage the quantity and size of the log files.

Procedure

1. From the top-level menu of the **Appliance Dashboard,** select **Manage** > **Maintenance** > **Log Retrieval and Configuration**.
2. To set the log settings, click **Configure**.
3. Provide the following details:

   Maximum size for log file rotation
   > The size of the log file that you want to keep.

   Maximum number of historical log files
   > The maximum number of historical log files that you want to keep.
4. Click **Save Configuration**.

Managing the core dump files

Use the Core Dumps page to delete or download core dump files in the IBM Security Privileged Identity Manager virtual appliance.

About this task

A core dump file can be generated in the virtual appliance for many reasons. A core dump file stores a large amount of raw data for further examination. Use the core dump files to diagnose or debug errors in the virtual appliance.

Note: To configure and manage core dump file collection for the Privileged Session Gateway nodes, see *Core dump files* in *IBM Security Privileged Identity Manager Troubleshooting Guide*.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Manage** > **Maintenance** > **Core Dumps**. The Core Dumps page displays a table with a list of core dump files.
2. On the Core Dumps page, do one of the following actions.

Table 16. Core dump file management actions

Action	Description
Refresh	Click **Refresh** to display the most recent version of the data.
Delete	1. From the **File name** column, select a core dump file. **Note:** To delete multiple core dump files, select more files. To select all the core dump files, select the check box next to **File name**. 2. Click **Delete**. 3. Click **Yes** to confirm.
Download	1. From the **File name** column, select a core dump file. **Note:** You can select only 1 core dump file at a time for download. A message is displayed if you select multiple core dump files. 2. Click **Download**. **Note:** The core dump file is downloaded in an archived format such as `.zip`. **Note:** To view the contents of a core dump file, open the downloaded file.

Activating the session recording feature in the virtual appliance

You can activate the session recording feature in the IBM Security Privileged Identity Manager virtual appliance to record privileged identity sessions for auditing, security forensics, and compliance.

Before you begin

By default, session recording is not activated in the IBM Security Privileged Identity Manager virtual appliance. If you purchased the IBM Privileged Session Recorder feature and want to enable it, you must have the activation code to complete this task.

About this task

This task covers only how to activate the feature in the virtual appliance.

To enable or disable session recording for automatic logon sessions that initiated with the Privileged Access Agent, you can modify the `pid_recorder_enabled` policy in AccessAdmin.

To enable or disable session recording for sessions that are initiated by using the Privileged Session Gateway, you can modify the session recording policy in the administrative console.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Maintenance** > **Session Recording Activation**. The Session Recording page is displayed.
2. In **Session Recording Activation Code**, enter your activation code.
3. Click **Activate** to enable session recording.
4. For clustered deployments, synchronize the member nodes.
5. Restart the server.

Enabling the application identity management feature in the virtual appliance

You can activate the application identity management feature in the IBM Security Privileged Identity Manager virtual appliance to manage, automate, and track the application credentials.

Before you begin

By default, application identity management is not activated in the IBM Security Privileged Identity Manager virtual appliance. If you purchased the IBM Security Privileged Identity Manager for Applications feature and want to enable it, you must have the activation code to complete this task.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Maintenance** > **Application Identity Activation**. The Application Identity Management page is displayed.
2. In **Application Identity Management Activation Code**, enter your activation code.
3. Click **Activate**.
4. For clustered deployments, synchronize the member nodes.
5. Restart the server.

Configuring multiple Active Directory nodes for failover

Use failover domain controllers to configure high availability for the external user registry.

Procedure

1. Log in to the IBM Security Privileged Identity Manager Virtual Appliance dashboard.

2. Click **Configure** > **Manage External Entities** > **External User Registry Configuration**.

3. Select the directory server and click **Reconfigure**.

4. In the **Failover controllers** tab, click **New** to add a host name for the Active Directory failover server.

5. Click **Save Configuration**.

   Note: The primary and failover domain controllers must use the same connection transport security. If SSL is enabled on the primary controller, it must also be enabled on all failover controllers.

Configuring DB2 for automatic client reroute (ACR)

Configure the DB2 in ACR mode to automatically reroute to a secondary database server.

Procedure

1. Log in to the IBM Security Privileged Identity Manager Virtual Appliance dashboard.

2. Click **Configure** > **Manage External Entities** > **Database Server Configuration**.

3. Select a database server and click **Reconfigure**.

4. In the **DB2 ACR** tab, fill in the following details:

   Retry interval for client reroute
   > Specifies the amount of time, in seconds, between retries for automatic client reroute.

   Maximum retries for client reroute
   > Specifies the maximum number of connection retries that are attempted by the automatic client reroute function if the primary connection to the server fails. The property is only used when Retry interval for client reroute is set.

   Alternate server names
   > Specifies the list of alternate server name or names for the DB2 server. If more than one alternate server name is specified, the names must be separated by commas. For example, host1, host2.

   Alternate port numbers
   > Specifies the list of alternate server port or ports for the DB2 server. If more than one alternate server port is specified, the ports must be separated by commas. For example, 5000, 50001.

5. Click **Save Configuration**.

   Note:
   - All database servers must use the same transport security. If SSL is enabled on the primary database server, it must also be enabled on all alternate servers.
   - When SSL is enabled, all database servers should use SSL certificates issued by the same Certification Authority. If self-signed certificates are used, the SSL certificates for the alternate servers need to be manually added to the **ispim** trust store before database configuration.

Chapter 4. Maintenance

See this section for information about the IBM Security Privileged Identity Manager maintenance.

Changing a member node to a primary node

Use the Cluster Node Configuration page to change a member node to primary node in the IBM Security Privileged Identity Manager virtual appliance.

Before you begin

No active `Primary` node must exist in this cluster.

About this task

You might want to change a member node to a primary node in the cluster for maintenance and other tasks.

The **Configure** > **Manage Cluster** menu is displayed only in a cluster environment and not in a stand-alone environment.

Procedure

1. On a member node, from the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage Cluster** > **Cluster Node Configuration**.
2. Select the member node that you want to make as a primary node from the list of available nodes.
3. Click **Make Primary**.
4. Click **Yes** to confirm the changes.

Changing a primary node to a member node

Use the Cluster Node Configuration page to change a primary node to member node in the IBM Security Privileged Identity Manager virtual appliance.

Before you begin

You must work from a primary node to change it to a member node.

About this task

You might want to change a primary node to a member node due to the following reasons:

- Change the node in the cluster for maintenance and other tasks. To promote some other member node to primary node, you must first change the current primary node to member node.
- Remove a damaged or affected primary node from the cluster configuration. You must first remove such affected node from the Load Balancer configuration.

The **Configure** > **Manage Cluster** menu is displayed only in a cluster environment and not in a stand-alone environment.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage Cluster** > **Cluster Node Configuration**.
2. Select the primary node that you want to make as a member node from the list of available nodes.
3. Click **Make Member**.
4. Click **Yes** to confirm the changes.

Removing a node from the cluster

Use the Cluster Node Configuration page to remove a node from the cluster.

Before you begin

Remove the node from the Load Balancer configuration so that no user requests are routed to this node.

About this task

You can remove a member node only from a primary node, but you cannot remove the primary node itself.

You might want to remove a damaged or affected member node from the cluster configuration. You must first remove such affected node from the Load Balancer configuration. After the node is removed, it no longer functions as part of the cluster unless you add it back to the cluster.

The **Configure** > **Manage Cluster** menu is displayed only in a cluster environment and not in a stand-alone environment.

Procedure

1. From the **Appliance Dashboard** top-level menu, click **Configure** > **Manage Cluster** > **Cluster Node Configuration**.
2. Select a member node that you want to remove from the list of available nodes.
3. Click **Remove Node**.
4. Click **Yes** to confirm.

Results

The selected node is removed from the cluster.

Reconnecting a node into the cluster

Use the Cluster Node Configuration page to reconnect a node into the cluster of the IBM Security Privileged Identity Manager virtual appliance.

About this task

Depending on your requirement, you can reconnect a node into the cluster due to the following reasons:

- Adding a previously configured node to a cluster to increase scalability.
- A node that was shut off for maintenance is revived and must be introduced back in the cluster.

- If you see a reconnect notification on the **Appliance Dashboard** of a member node.

You can reconnect only a member node back to the cluster from the **Appliance Dashboard** of a member node. You must provide the primary node details to reconnect a node into the cluster.

The **Configure** > **Manage Cluster** menu is displayed only in a cluster environment and not in a stand-alone environment.

Procedure

1. From the **Appliance Dashboard** top-level menu, click **Configure** > **Manage Cluster** > **Cluster Node Configuration**.
2. Select the member node.
3. Click **Reconnect Node**. The Reconnect Node pane is displayed.
4. In the Reconnect Node pane, provide the details for the node that you want to reconnect into the cluster.

   Primary node host name
   > The host name of the primary node. For example, `pimva1.jk.example.com`.

   Primary node administrator
   > The user ID of the primary node administrator. For example, `admin`.

   Primary node administrator password
   > The administrator password of the primary node. For example, `admin`.
5. Click **Yes** to confirm.

Results

The member node is reconnected into the cluster.

Reconfiguring the data store connection

You can reconfigure the data store if the data store configuration changes. For example, if the data store is moved to a different server host.

Procedure

1. Make a backup of the database. On the database server that runs for DB2, complete the following steps:
   a. Log on as the instance owner. For example: `db2admin`.
   b. Close all connections to the IBM Security Privileged Identity Manager database. If necessary, run the following command to force all connections to close:

      `db2 force application all`
   c. Back up the data store database:

      `db2 backup database IDM_DB to OLD_DB2_BACKUP_DIR`

      where

      - `IDM_DB` is the name of the IBM Security Privileged Identity Manager data store database. For example: `idmdb`
      - `OLD_DB2_BACKUP_DIR` is a directory path to store the backup. For example:

         Linux or UNIX systems
         > `/tmp/db2`

> **Windows systems**
>
> ```
> c:\temp\db2
> ```

2. Restore the backup of the database.

   Install the new version of DB2. For this reconfiguration, ensure that you create the database instance and database with the same name. Users must have the same rights and privileges as those setup on the previous system.

   - To create a new database instance and a database, see "Installing and configuring the database server" on page 1.
   - Copy the contents of the IBM Security Privileged Identity Manager data store backup directory to the target server. For example: tmp/db2.
   - Ensure that the database instance owner you create has permission to read the target directory and files within.

   To restore the DB2 data on the target database server, complete the following steps:

   a. Launch DB2 command line as the instance owner.

      Windows

      1) Launch the Windows command line.
      2) Run the following command:

         ```
         set DB2INSTANCE=piminst
         ```

         where `piminst` is the database instance.

      3) Run **db2cmd** to launch the DB2 command line.

      Linux

      Run the following command:

      ```
      su - piminst
      ```

      where `piminst` is the database instance.

   b. In the DB2 command line, enter the following commands to restore the database by using the migrated DB2 data:

      ```
      restore db idmdb from OLD_DB2_TEMP_DATA
      ```

      where

      - `idmdb` is the IBM Security Privileged Identity Manager data store database name.
      - `OLD_DB2_TEMP_DATA` is the location of the migrated DB2 data that you copied over from the previous version. For example: `c:\temp\db2`

   c. Stop and start the DB2 server to reset the configuration.

      After you create the IBM Security Privileged Identity Manager data store database, stop, and start the DB2 server to allow the changes to take effect.

      Enter the following commands:

      ```
      db2stop
      db2start
      ```

      Note: If the `db2stop` fails and the database remains active, enter the following commands to deactivate the database:

      ```
      db2 force application all
      db2stop
      ```

3. Reconfigure the data store.

   a. From the IBM Security Privileged Identity Manager administrative console, click **Menu** > **Database Configuration**.

   b. Select the existing data store that you want to set up and click **Reconfigure**. Provide the details and click **Save Configuration**.

c. Restart the server for the corresponding data store to complete the process.

4. For clustered deployments, complete the following steps:

   a. Synchronize the member nodes.

   b. Restart the server.

Reconfiguring the directory server connection

You can reconfigure the directory server if the directory server configuration changes.

Procedure

1. Make a backup of the directory server.

   On the server running IBM Security Directory Server for IBM Security Privileged Identity Manager, complete the following steps:

   a. Log on as an Administrator with root privileges.

   b. Open a command window.

   c. Go to the `TDS_HOME`/sbin directory and type the following command:

   `db2ldif -s ldap_suffix -o ldap_output_file -I ldap_instance_name`

   where:

   `ldap_suffix` is the name of the suffix. For example: `dc=com`.

   `ldap_output_file` is the name of the `ldif` output file. For example: `old_ldif_data.ldif`.

   `ldap_instance_name` is the name of the LDAP server instance, which can be obtained through the IBM Security Directory Server Instance Administration tool.

   d. Use the backup of the schema file `V3.modifiedschema` from the `OLD_ITDS_INSTANCE_HOME\etc` directory of the IBM Security Directory Server instance home directory.

2. Restore the backup of the database.

   Install a version of IBM Security Directory Server that IBM Security Privileged Identity Manager supports. For this reconfiguration, ensure that you take the following actions:

   - Create and use the same root suffix.

   - Use the same encryption seed value as the old Directory Server instance. If not, you must export the data from the old Directory Server instance to use the seed and salt keys from the new instance.

   Copy the contents of the IBM Security Privileged Identity Manager directory server backup `ldif` file and schema file to the target server.

   To restore the directory server data on the target directory server, complete the following steps:

   a. Log on as an Administrator with root privileges.

   b. Stop the LDAP server.

   c. Copy the schema file `V3.modifiedschema` that you copied over from the previous server to the `NEW_ITDS_INSTANCE_HOME\etc` directory of the IBM Security Directory Server instance.

   Note: If you customized or modified the schema files, manually merge the changes into the new schema files.

   d. From `TDS_HOME/sbin`, run the command:

   `bulkload -i OLD_ITDS_TEMP_DATA\ldif_output_file -I ldap_instance_name`

where:

`OLD_ITDS_TEMP_DATA` is the temporary directory location of the IBM Security Directory Server data you copied over from the previous server. For example, `C:\temp\51data\ids\`.

`ldif_output_file` is the name of the file that you exported in a previous task. For example, `old_ldif_data.ldif`

`ldap_instance_name` is the name of the LDAP server instance. For example, `itimldap`. You can obtain use the IBM Security Directory Server Instance Administration tool to obtain the instance name.

For more information, see Bulkload command errors.

   e. Stop and start the IBM Security Directory Server to activate the changes.

3. Reconfigure the IBM Security Directory Server.

   a. From the IBM Security Privileged Identity Manager administrative console, go to **Menu** > **Directory Server Configuration**.

   b. Select the directory server and click **Reconfigure**. Provide the details and click **Save Configuration**.

   c. Restart the Identity server to complete the process.

4. For clustered deployments, complete the following steps:

   a. Synchronize the member nodes.

   b. Restart the server.

Setting up the disaster recovery environment

Learn how to set up an IBM Security Privileged Identity Manager disaster recovery environment.

About this task

Before you set up the disaster recovery environment, take note of the following assumptions:

- The IBM Security Privileged Identity Manager disaster recovery setup is only a temporary measure in case of emergencies. It operates at a lower capacity as compared to the Production site. In case of a cluster setup, only the primary node of IBM Security Privileged Identity Manager is replicated to the disaster recovery site.

- The hostname of the disaster recovery load balancer remains the same as the one in Production, only the load balancer's virtual IP is updated on the disaster recovery DNS entry. You do not need to reconfigure Privileged Access Agent to reflect a new IMS Server URL.

- The managed privileged resources or target endpoints (for example, Linux hosts) are situated in a different network zone from both the IBM Security Privileged Identity Manager production and disaster recovery network. This assumes that at any one time, both the Production site and the disaster recovery site are able to reach the privileged resources network, and therefore the network connectivity to those resources is not be impacted by IBM Security Privileged Identity Manager disaster recovery failover.

- The Privileged Session Gateway is situated in a different network zone from both the IBM Security Privileged Identity Manager production and DR network. In a DR failover scenario, the DR PIM points to the same instance of Privileged Session Gateway as configured in production, and is assumed to have network connectivity to it. In this case, the disaster recovery load balancer's CA certificate must be imported into Privileged Session Gateway as a trusted certificate.

If the virtual appliance is on a cluster setup, take note of the following items:

- Ensure that the certificates used on the disaster recovery load balancer has the same common name/cn attribute as the Production load balancer. This is to ensure that the Privileged Access Agent workstations remain unaffected by the swinging from Production to disaster recovery.
- Ensure that the signer CA that issued the certificate for the disaster recovery load balancer is trusted on the workstations that has Privileged Access Agent deployed on it.

Note: The following steps are required only if you are setting up the disaster recovery environment for the first time or have made any configuration changes with the Production VA's Local Management Interface (LMI) or Command Line Interface (CLI).

Procedure

1. On the primary node virtual appliance, perform a virtual machine image backup and restore it in the disaster recovery environment.

   Important: Ensure that the following components have a disaster recovery equivalent and that the necessary data replication is setup properly between the Production and disaster recovery environment.
   - Database Server
   - Directory Server
   - Mail Server
   - Load Balancer (Only if the virtual appliance is on cluster setup)
   - Windows AD Secondary domain controller (Only if the virtual appliance is on external user registry setup)

2. Start the replicated virtual appliance in the disaster recovery environment.

3. Once the virtual appliance is completely start up, perform a network reconfiguration with the CLI.

   a. If the VA is given a different hostname on the DR site, update the hostname on the VA. The host name configuration can be accessed from **VA CLI** > **Management** > **Hostname**.

   b. Update the DNS server configuration on the VA to point to the DNS server that is on the DR network zone. The DNS configuration can be accessed from **VA CLI** > **Management** > **DNS**.

   c. If the VA was configured with static IP address before the backup, update the network interface configuration on the VA with the new network details. The Network interface configuration can be accessed from **VA CLI** > **Management** > **Interfaces**.

   d. Reboot the virtual appliance.

4. Once the virtual appliance is rebooted, perform the following reconfiguration:

   a. Login to the virtual appliance local management interface (LMI).

   b. Update the hostname of the directory server to the hostname of the disaster recovery directory server instance. Click **Configure** > **Manage Middleware** > **Directory Server Configuration** > **Reconfigure**.

   c. Update the hostname of the database server to the disaster recovery database server instance. Click **Configure** > **Manage Middleware** > **Database Server Configuration** > **Reconfigure**.

   Note: Ensure that you update for each existing configured data store.

d. Restart the Identity, Single Sign-on and Session Recording (if configured) services. At the LMI home page, click **Server Control** > **Restart** > **Reason for restart** > **Others** to perform a full restart.

   e. Update the hostname of the mail server to the DR mail server instance. Click **Configure** > **Manage Middleware** > **Mail Server Configuration** > **Reconfigure**

   f. Restart the Identity service. At the LMI home page, click **Server Control** > **Restart** > **Reason for restart** > **Identity data store configuration**.

   g. Optional: If you have an external user registry configured, update the hostname of the external user registry to the disaster recovery external user registry. Click **Configure** > **Manage Middleware** > **External User Registry Configuration** > **Reconfigure**.

   h. Reboot the virtual appliance.

Backing up the IBM Security Privileged Identity Manager deployment

You must back up both the virtual appliance and the components in the data tier.

Virtual appliance backup

Depending on which hypervisor (VMware ESXi or Citrix XenServer) you are deploying IBM Security Privileged Identity Manager on, use the Snapshot Management Tool in the respective hypervisors to back up the deployment.

To back up the IBM Security Privileged Identity Manager virtual appliance, take a hypervisor snapshot of the virtual appliance.

For stand-alone setup:
* Take a hypervisor snapshot of the stand-alone virtual appliance.

For clustered setup:
* Take hypervisor snapshots of the Primary node, and **all** member nodes of the cluster.

Data tier backup

Ensure that the following components of the data tier are included as part of the backup.
1. Database Server
   * Identity data store
   * Single Sign-On data store
   * Session Recording data store (only if the Session Recording feature is activated)
2. Directory Server

To back up the data tier, use the available backup tools that are provided by the respective products, for example IBM DB2 or IBM Security Directory Server.

Installing a fix pack

Install a fix pack on the IBM Security Privileged Identity Manager virtual appliance to address software maintenance updates for reliability and performance enhancements.

Before you begin

Restriction: You cannot uninstall a fix pack by using the local management interface. You must use the command-line interface to uninstall a fix pack.

Important: For stand-alone or primary node installations of IBM Security Privileged Identity Manager, ensure that the initial configuration is completed before a fix pack installation is performed. See "Setting up a stand-alone or primary node" in the *IBM Tivoli® Security Role Management Assistant Installation and Configuration Guide*.

Fix packs are applied to your active partition. You can manually create a backup of your active partition before you apply a fix pack so that you can roll back your changes.

About this task

If a fix pack is installed on your IBM Security Privileged Identity Manager virtual appliance, you can view information about who installed the fix pack, comments, patch size, and the installation date.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Updates and Licensing** > **Fix Packs**. The Fix Packs page is displayed.
2. On the Fix Packs page, click **New**.
3. In the Add Fix Pack window, click **Browse for fix pack** to locate the fix pack file.
4. Select the fix pack file, and click **Open**. The Browse for fix pack table displays the fix pack details.
5. Click **Save Configuration** to install the fix pack.

Upgrade the virtual appliance

Use the following tasks to upgrade the virtual appliance.

Important:

- For stand-alone or primary node installations of IBM Security Privileged Identity Manager, ensure that the initial configuration is completed before you upgrade the virtual appliance. See "Setting up a stand-alone or primary node" in the *IBM Tivoli Security Role Management Assistant Installation and Configuration Guide*.
- For IBM Security Privileged Identity Manager versions prior to version 2.0.2, you must create at least three network interfaces before you upgrade the virtual machine.

Upgrading the IBM Security Privileged Identity Manager virtual appliance from a USB device

Install the firmware update to upgrade the IBM Security Privileged Identity Manager virtual appliance.

Before you begin

Before you apply the firmware update to upgrade the IBM Security Privileged Identity Manager virtual appliance, back up your data tier, which is all the databases and the directory server.

Important:
- When you upgrade the virtual appliance, all existing snapshots are deleted.
- The upgraded virtual appliance cannot use snapshots that are created for older versions of the virtual appliance.

About this task

The virtual appliance has two partitions with separate firmware on each partition. The partitions are swapped during the firmware updates to roll back the firmware updates when required. Either partition can be active on the virtual appliance.

In the factory-installed state, Partition 1 is active and contains the firmware version of the currently released product. When you apply a firmware update, the update is installed on Partition 2, and your policies and settings are copied from Partition 1 to Partition 2.

The IBM Security Privileged Identity Manager virtual appliance restarts the system by using Partition 2, which is now the active partition.

You must use the command-line interface (CLI) to install the upgrade.

You can only upgrade the primary node in a clustered deployment. Member nodes have to be reinstalled and joined to the primary node. See "Upgrading the cluster" on page 77.

Procedure

1. Download the `ispim_*.pkg` build.
2. Access the command-line interface (CLI) of the virtual appliance by using either an `ssh` session or the console.
3. Copy the `ispim_*.pkg` to a USB device.
4. Attach the USB device to your virtual system.
5. In the virtual appliance CLI, run the **ispim** command to display the `ispim` prompt.
6. At the `ispim` prompt, complete the following steps.
   a. Run the **firmware_update** command.
   b. Run the **list_firmware** command to list the firmware updates from the USB device.
   c. Run the **transfer_firmware** command to transfer the firmware updates from the USB device to the virtual system.
   d. Run the **install_firmware** command.
   e. Select the index of the firmware update that you want to install to the virtual system and press Enter.

      The results are as follows.
      - The upgrade process formats Partition 2 and installs the new firmware.
      - When you apply the firmware update, your policies and settings are copied from Partition 1 to Partition 2.

- On completion, the process indicates you must restart the virtual system.

f. Type the **reboot** command and press **Enter** to restart the virtual system by using Partition 2. Partition 2 is now the active partition.

The results are as follows.

- After the virtual appliance restarts from the Partition 2, all Partition 1 configuration information is applied to the Partition 2.
- After the configuration is applied to the virtual appliance, the process indicates you to restart the virtual appliance.

g. Restart the virtual appliance to complete the upgrade process.

h. Optional: Back up Partition 2 in to Partition 1 after the successful completion of the firmware upgrade. The backup process overwrites the information that is in Partition 1.

Do the following actions:

1) Check and fix any errors if the upgrade process failed.
2) Use Partition 1 to set it as the active partition and restart it.

   Partition 1 now becomes the active partition.

Upgrading the IBM Security Privileged Identity Manager virtual appliance with firmware update transfer utility

The IBM Security Privileged Identity Manager virtual appliance allows only firmware updates by USB device. Starting at firmware release 2.0.1 (2.0.1-ISS-PIM-FP0002), firmware (`.pkg`) files can be transferred with the attached Java utility. A USB device is no longer required to update the virtual appliance.

Before you begin

You must install the firmware release 2.0.1 (2.0.1-ISS-PIM-FP0002) or later before you can install the firmware release 2.0.2 with this utility.

About this task

This utility performs the same function as the command-line interface (CLI) command of the virtual appliance, which is as follows:

`ispim > upgrade > install`

Procedure

1. Download the `ispim_*.zip` package from the IBM Fix Pack Central.
2. Extract the `ispim_*.pkg` build to a location of your choice.
3. Copy the utility to a system where Java, Version 1.7 is installed.
4. Copy these files to the file system.
   - The `.pkg` firmware update file.
   - The keystore (`jks`) file.
5. Run the following Java command to upload the `.pkg` file.

   Usage:

   ```
   java -jar FileUpload.jar Hostname AdminId AdminPassword Truststore Filepath Truststore
        Password Absolute path to pkg file
   ```

   Example:

   ```
   java -jar FileUpload.jar pimva.ibm.com:9443 admin admin /work/temptrust.jks WebAS
        /Downloads/pimva_2.0.2.pkg
   ```

6. Use the supplied `temptrust.jks` file if you did not update the default certificates.

   If you previously updated the default certificate on the virtual appliance, `temptrust.jks` does not work. Use an updated `jks` file that is based on your updated certificate.

7. Access the command-line interface (CLI) of the virtual appliance to install the firmware with the following command.

   Note: Run this command after you transfer the `.pkg` file.

   `ispim > firmware_update > install_firmware`

Upgrading the Privileged Session Gateway

During an upgrade, old and new instances of the Privileged Session Gateway can co-exist side by side.

Running sessions on existing nodes do not have to be interrupted during an upgrade.

Table 17. Privileged Session Gateway upgrade process

Step	Process	Reference
1	Get the new versions of the Privileged Session Gateway files. For example: • Privileged Session Gateway image • `install.sh` • `run.sh`	
2	Install the new Privileged Session Gateway image. Run `install.sh` providing the new Privileged Session Gateway image as an argument.	Installing the Privileged Session Gateway
3	Start new Privileged Session Gateway nodes. Run `run.sh` with the appropriate response file.	"Deploying a single node" on page 26 "Deploying multiple nodes as a cluster" on page 32
4	For clustered deployments, configure new nodes in the load balancer.	"Setting up a load balancer for the gateway cluster" on page 32
5	Remove older versions of the Privileged Session Gateway nodes from the load-balanced route and reload the load balancer configuration. **Important:** Do not restart the load balancer.	"Enhance availability by using monitoring URLs" on page 77

Table 17. Privileged Session Gateway upgrade process (continued)

Step	Process	Reference

6	Remove the older versions, only when the sessions that are running within the node stop.
	
	1. Monitor the sessions that are running on the instance by using the Privileged Session Gateway status REST API.
	`https://<hostname>:<port>/v1/gateways/<gateway_id>/status`
	
	2. If live sessions no longer exist, remove the older instances.
	  a. Stop and remove a node.
	    `docker stop <gateway_id> && docker rm <gateway_id>`
	  b. Verify that the node is removed.
	    `docker ps -a`
	
	Note: Repeat this step until the older instances are removed.	

Upgrading the cluster

You can only upgrade the primary node in a clustered deployment. Reinstall member nodes and join them to the primary node.

Procedure

1. Stop the member nodes.
2. Remove member nodes from the cluster.
   a. In the primary node, from the Appliance Dashboard, click **Configure** > **Manage Cluster**.
   b. Select the nodes and remove them.
3. Upgrade the primary node. See "Upgrading the IBM Security Privileged Identity Manager virtual appliance from a USB device" on page 73.
4. Verify that the node was successfully upgraded.
5. Create new member virtual appliances, with the same version of the upgraded primary node.
6. Join the nodes to the upgraded primary node.
7. Modify the load balancer configuration with the changes, if required.

Enhance availability by using monitoring URLs

Monitoring URLs let system administrators write scripts to monitor the uptime and the responsiveness of both the IBM Security Privileged Identity Manager virtual appliance and the Privileged Session Gateway.

You do not have to authenticate to access Monitoring URI. These URIs can be used by any third-party tool to obtain data about responsiveness.

Privileged Session Gateway

You can retrieve status about the general Privileged Session Gateway service or for individual Privileged Session Gateway instances.

Response format

- For overall Privileged Session Gateway service:

  `status: status code`
- For individual Privileged Session Gateway instances

  `status: status code, connections: number`

Where:

`status code` can be `OK`, `DEGRADED`, or `SEVERE`.

`connections` is the number of active connections for the container.

The response code is 200 if the service is running successfully, and 500 if the service is not.

Response 200 (application/json):

`Response: {"status": "OK"}`

Response 500 (application/json)

`Response: {"status": "DEGRADED"}`

For Privileged Session Gateway service -

URI: `https://gateway_hostname:`*`port`*`/v1/status`

`Response: {"status": "OK"}`

For specific Privileged Session Gateway instance -

URI: `https://`*`gateway_hostname:port`*`/v1/gateways/`*`container_id`*`/status`

`Response: {"status":"OK", "connections": "3"}`

Virtual appliance

Response format

`Service name: response code, Time taken in milliseconds:ms`

Response code is 0 if services are unavailable and 200 if the service is running.

`Example: "Identity":"0", "Time taken in milliseconds":401`

For Identity service -

URI:`https://`*`hostname`*`:9443/monitor/response?Service=Identity`

`Response: {"Identity":"0", "Time taken in milliseconds":401}`

For SingleSignOn service -

URI:`https://`*`hostname`*`:9443/monitor/response?Service=SingleSignOn`

`Response: {"SingleSignOn":"0","Time taken in milliseconds":8}`

For SessionRecorder service -

URI:`https://`*`hostname`*`:9443/monitor/response?Service=SessionRecorder`

`Response: {"SessionRecorder":"0","Time taken in milliseconds":2}`

For All in a single request -

URI:`https://`*`hostname`*`:9443/monitor/response`

```
Response:
{"Identity":"200","SessionRecorder":"200","SingleSignOn":"200",
"Identity Time taken in milliseconds":529,"SessionRecorder Time
taken in milliseconds":400,"SingleSignOn Time taken in
milliseconds":361}
```

Chapter 5. Reports

The IBM Security Privileged Identity Manager solution supports the IBM Cognos®
reporting framework for report generation.

IBM Cognos reporting framework

Use the IBM Cognos reporting framework to create and analyze Privileged Identity
Manager reports. With this framework, you can modify the schema and generate
reports in different formats.

The IBM Cognos reporting framework includes the following item:

Static reports
Ready-to-use reports that are bundled with the IBM Security Privileged
Identity Manager reporting package.

IBM Cognos Analytics reporting components

This topic describes the IBM Cognos reporting components that you might use
while you work with the Privileged Identity Manager Cognos-based report models.

Query Studio
Query Studio is the reporting tool for creating simple queries and reports
in IBM Cognos Analytics. To use Query Studio effectively, you must be
familiar with your organization's business and its data. You might also
want to be familiar with other components of IBM Cognos Analytics.

Report Studio
Report Studio is a Web-based report authoring tool that professional report
authors and developers use to build sophisticated, multiple-page,
multiple-query reports against multiple databases. With Report Studio, you
can create any reports that your organization requires, such as invoices,
statements, and weekly sales and inventory reports.

Your reports can contain any number of report objects, such as charts,
crosstabs, lists, and also non-BI components such as images, logos, and live
embedded applications that you can link to other information.

IBM Cognos Analytics Connection
IBM Cognos Analytics Connection is the portal to IBM Cognos Analytics
software. IBM Cognos Analytics Connection provides a single access point
to all corporate data available in IBM Cognos Analytics software.

You can use IBM Cognos Analytics Connection to create and run reports
and cubes and distribute reports. You can also use it to create and run
agents and schedule entries.

Prerequisites for IBM Cognos report server

To work with the Privileged Identity Manager Cognos-based reports, set up the
IBM Cognos report server.

You must install the software in the following table.

Table 18. Software requirements for IBM Cognos report server

Software	For more information, see
IBM Cognos Business Intelligence Server	1. Access the IBM Cognos Analytics documentation at https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. Search for **Installation and Configuration Guide**. 3. Search for the installation information and follow the procedure.
Web server	1. Access the IBM Cognos Analytics documentation at https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. In the right pane of the home page, under **Supported hardware and software** section, click **IBM Cognos Business Intelligence software environments**. 3. Click the product version tab. For example, **10.2.1** 4. Click **Software** in the **Requirements by type** column under the section **IBM Cognos Business Intelligence**. 5. Search for **Web Servers** section.
Data sources	1. Access the IBM Cognos Analytics documentation at https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. In the right pane of the home page, under **Release Notes** section, click **IBM Cognos Analytics software environments**. 3. Click the product version tab. For example, **11.0** 4. Click **Software** in the **Requirements by type** column under the section**IBM Cognos Analytics**. 5. Search for **Data Sources** section.

Installation of IBM Cognos reporting components

Installation of IBM Cognos reporting components is optional. You need these components only if you use the Privileged Identity Manager Cognos-based reports.

You must complete the installation and data synchronization process before you can access and work with Privileged Identity Manager Cognos-based reports.

The following table describes the installation and synchronization process.

Table 19. Installation and data synchronization process

Task	For more information
Install IBM Cognos Analytics.	1. Access https://www.ibm.com/support/ knowledgecenter/SSEP7J_11.0.0/ com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. Search for **Install Cognos BI on one computer**.
Complete the data synchronization.	1. Access the IBM Security Privileged Identity Manager product documentation. 2. Search for **Data Synchronization**. **Note:** Run the data synchronization before you generate the reports to obtain the latest report data.

Cognos reporting

The Privileged Identity Manager Cognos-based reports are available at IBM Passport Advantage:

- `ISPIMReportingPackage_2.1.0.zip`

Note:

- To install previous versions, refer to the specific version of IBM Cognos Analytics product documentation.
- If you are upgrading from older versions of IBM Cognos Analytics, see Upgrade IBM Cognos Analytics.
- You must set the locale to English or to any supported language before you run any of the reports. See "Setting language preferences" on page 92. Otherwise, you might encounter a "Language not supported" issue.

Configuration of IBM Cognos reporting components

After you install the prerequisites for the IBM Cognos Analytics server, configure the Framework Manager, and create a content store database. Then, configure the web gateway and web server.

During the database configuration process, ensure that you complete the points in the following note.

Note:

- IBM Cognos reporting does not support Microsoft SQL Server database as a content store. Use DB2 database instead.
- Set the `JAVA_HOME` environment variable to point to the JVM used by the application server.
- You must use the enterprise database as IBM Cognos content store.
- Delete the existing data source and create a new data source to enable an option of generating DDL during creation of the content store database. For information about data source creation, see "Creating a data source" on page 84.

The following table describes the configuration process.

Table 20. Configure IBM Cognos reporting components

Task	For more information
Create a content store in the database.	1. Access the IBM Cognos Analytics documentation at https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. Search for **Start IBM Cognos Configuration** and complete the steps as per your operating system. 3. Search for **Create a content store database**.
Configure the web gateway.	1. Access the IBM Cognos Analytics documentation at https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. Search for **Configure the gateway**.
Configure your web server.	1. Access the IBM Cognos Analytics documentation at https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. Search for **Configure your web server**.

Setting report server execution mode

You must have a report server execution mode that is set to 32-bit mode for the report packages that do not use dynamic query mode.

Procedure

1. Start IBM Cognos Analytics Configuration.
2. In the **Explorer** panel, click **Environment**.
3. Click the **Value** box for **Report server execution mode**.
4. Select **32-bit**.
5. From the **File** menu, click **Save**.

What to do next

Restart the IBM Cognos Analytics service. Complete the following steps:

1. Access the IBM Cognos Analytics documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp.
2. Search for **Restarting the IBM Cognos Analytics service to apply configuration settings**.

Setting environment variables

You must set the database environment variables for a user before you start the IBM Cognos processes.

Procedure

1. Access the IBM Cognos Analytics documentation at http://pic.dhe.ibm.com/ infocenter/cbi/v10r2m1/https://www.ibm.com/support/knowledgecenter/ SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html.
2. Search for **Database environment variables**.

What to do next

Start the Cognos service from IBM Cognos Configuration to host the IBM Cognos portal. Complete the following steps:

1. Access the IBM Cognos Analytics documentation at https://www.ibm.com/ support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/ welcome.html.
2. Search for **Starting or stopping the Cognos service**.

Importing the report package

Import the report package to work with the static reports.

Before you begin

- Copy the reporting package files to the directory where your deployment archives are saved. The default location is `c10_location/deployment`. For more information about the reporting packages, see "Installation of IBM Cognos reporting components" on page 80.
- To access the **Content Administration** area in IBM Cognos Administration, you must have the required permissions for the administration tasks secured feature.

Procedure

1. Access the IBM Cognos Gateway URI. For example, `https://hostname:port/ ibmcognos/cgi-bin/cognos.cgi`. The *localhost* is the IP address or network host name where IBM Cognos gateway is configured. The *portnumber* is the port on which the IBM Cognos gateway is configured.
2. Go to **Launch**.
3. In the IBM Cognos Administration window, click the **Configuration** tab.
4. Click **Content Administration**.
5. Clear the history.
6. On the toolbar, click `New Import` icon. The New Import wizard opens.
7. In the **Deployment Archive** box, select the reporting package **ISPIMReportingPackage_2.1.0**.
8. Click **Next**.
9. In the **Specify a name and description** window, you can add the description and screen tip.
10. Click **Next**.
11. In the **Select the public folders and directory content** window, select the model that is displayed.
12. In the **Specify the general options** page, select whether to include access permissions and references to external namespaces, and an owner for the entries after they are imported.
13. Click **Next**. The summary information opens.
14. Review the summary information. Click **Next**.
15. In the **Select an action** page, click **Save and run once**.

16. Click **Finish**.
17. Specify the time and date for the run.
18. Click **Run**.
19. Review the run time. Click **OK**.
20. When the import file operation is submitted, click **Finish**.

Results

You can now use the report package to create reports and to run the sample reports. The sample reports are available in the reporting model on the **Public Folders** tab in the IBM Cognos portal.

Creating a data source

To work with the Privileged Identity Manager Cognos-based reports, you must create a data source.

Before you begin

- If you are working with DB2 database client, copy the file db2cli.dll from the DB2 client installation directory to the *<IBM Cognos installation directory>*/bin folder.
- Catalog the database if the data source is remote. Use the following commands:
  - db2 catalog tcpip node <alias-name> remote <remote-DB-server> server <port-no>
  - db2 catalog database <remote-dbe> as <alias-name> at node <alias-name>

About this task

You must use the following data source names:

- ISPIM - This data source name is used to establish connection to the IBM Security Privileged Identity Manager database.
- ISAMESSO - This data source name is used to establish connection to the IBM Security Access Manager for Enterprise Single Sign-On database.
- PSR - This data source name is used to establish connection to the Privileged Session Recording database.

Procedure

1. Access the IBM Cognos Business Intelligence product documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp.
2. Search for **Creating a data source** and complete the steps.

What to do next

Note: Corrupted attribute names are displayed in the reports for Arabic, Chinese, Hebrew, Japanese, Korean, and Russian languages. Double-byte character set (DBCS) characters appear to be corrupted in the reports. Edit the data source so that the data flow is in Unicode format. Complete the following steps:

1. On the Work with Reports page, click **Launch** > **IBM Cognos Administration**.
2. Click **Configuration** to open the data source connection.
3. Click *<data_source>*. For example: ISPIM.
4. Under the **Actions** column, click **Set properties-*<data_source>***.

5. On the **Set properties-<*data_source*>** window, click **Connection**.

6. In the **Connection String** field, click the pencil symbol to edit the connection string.

7. In the **Collation Sequence** field, type @UNICODE.

8. Click **OK**.

9. Run the report to verify that the text is no longer corrupted.

Enabling the drill-through for PDF format

You must enable the drill-through functionality to run the drill-through reports in the PDF format.

Before you begin

Disable any pop-up blocking software in the browser.

Procedure

1. Open IBM Cognos Configuration.

2. Specify the fully qualified domain name for all the URIs that are defined.

3. Save the configuration.

4. Restart the IBM Cognos service. Complete the following steps:

   a. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp.

   b. Search for **Restarting the IBM Cognos service to apply configuration settings**.

5. In the **Explorer** window, click **Environment**.

6. In the **Group Properties** window, copy the value in the **Gateway URI** box.

7. Paste the copied **Gateway URI** value in the supported browser.

8. Run the report that you want.

Results

The drill-through report is run successfully in the PDF format.

Security layer configuration around the reports

An access to the reports can be restricted to a set of authorization roles. The users can create the authorization roles and associate them with the reporting entities. Only entitled users can access the data model or reports.

Authentication and authorization for IBM Cognos reports

IBM Cognos Business Intelligence administrators can set up the folders that store the reports. They can then secure those folders so that only authorized users can view, change, or perform other tasks by using the reports in the folder. To set up access control on the reports, administrators can set up the user authentication and define the access control for the set of users.

User authentication setup by using LDAP

You can configure IBM Cognos 10.2.1 Fix Pack 1 components to use an LDAP namespace for authentication when the users are in an LDAP user directory.

Configuring an LDAP Namespace for IBM Directory Server

If you configure a new LDAP namespace for use with the IBM Directory Server, you must modify the necessary settings and change the values for all properties of the IBM Directory objects.

Procedure

1. Open IBM Cognos Configuration.
2. In the Explorer window, under **Security**, right-click **Authentication**.
3. Click **New resource** > **Namespace**.
4. In the **Name** box, type a name for your authentication namespace.
5. In the **Type** list, click **LDAP-General default values**.
6. Click **OK**. The new authentication namespace resource appears in the Explorer window, under the **Authentication** component.
7. In the Properties window, for the **Namespace ID** property, specify a unique identifier for the namespace.

   Tip: Do not use colons (:) in the Namespace ID property.
   For **Host and Port**, specify `<Hostname>:<port>`. For example, `localhost:389`.
8. Specify the values for all other properties to ensure that IBM Cognos 10.2.1 Fix Pack 1 can locate and use your existing authentication namespace.
   - For **Base Distinguished Name**, specify the entry for a user search.
   - For **User lookup**, specify `(uid=${userID})`.
   - For **Bind user DN and password**, specify `cn=root`. For example, `cn=root` as a user name and `secret` as a password.

     Note: Specify the values if you want an LDAP authentication provider to bind to the directory server by using a specific bind user DN and password. If no values are specified, an LDAP authentication namespace binds as anonymous.
9. If you do not use external identity mapping, use bind credentials to search an LDAP directory server. Complete the following items.
   - Set **Use external identity** to **False**.
   - Set **Use bind credentials for search** to **True**.
   - Specify the user ID and password for **Bind user DN and password**.
10. To configure an LDAP advanced mapping properties, see the values that are specified in the following table.

Table 21. LDAP advanced mapping values

Mappings	LDAP property	LDAP value
Folder	Object class	`organizationalunit, organization, and container`
	Description	`description`
	Name	`ou, o, and cn`
Group	Object class	`groupofnames`
	Description	`description`
	Member	`member`
	Name	`cn`
Account	Object class	`inetorgperson`

Table 21. LDAP advanced mapping values (continued)

Mappings	LDAP property	LDAP value
	Business phone	`telephonenumber`
	Content locale	`(leave blank)`
	Description	`description`
	Email	`mail`
	Fax/Phone	`facsimiletelephonenumber`
	Given name	`givenname`
	Home phone	`homephone`
	Mobile phone	`mobile`
	Name	`cn`
	Pager phone	`pager`
	Password	`userPassword`
	Postal address	`postaladdress`
	Product locale	`(leave blank)`
	Surname	`sn`
	Username	`uid`

If the schema is modified, you must make extra mapping changes.

11. To prevent the anonymous access, complete the following steps:

    a. Go to **Security** > **Authentication** > **Cognos**.

    b. Set **Allow anonymous access?** to **False**.

12. From the **File** menu, click **Save**.

Results

A new LDAP namespace is configured with the appropriate values.

What to do next

Create the users in an LDAP. See "Creating users in an LDAP."

Creating users in an LDAP

See the example in this procedure that uses an LDAP utility to create users in LDAP.

Procedure

1. Open an LDAP utility. For example, if you are using the IBM Directory Server, the LDAP utility is `idsldapadd`.

2. Import the sample file `LdapEntries.ldif` that lists all the users who are authorized to access the reports. See the following example.

Results

After the successful import operation, you can see the users that are created in `ou=users,ou=SWG`.

Example

A sample file: `LdapEntries.ldif`

In this example, dc=com is the root entry. Specify the entry according to the schema that you use.

```
dn: ou=SWG, dc=com
ou: SWG
objectClass: top
objectClass: organizationalUnit

dn: ou=users,ou=SWG, dc=com
ou: users
objectClass: top
objectClass: organizationalUnit

dn: uid=steves,ou=users,ou=SWG, dc=com
uid: steves
userPassword:: hello123
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Wiley
cn: Steves

dn: uid=PortalAdmin,ou=users,ou=SWG, dc=com
userPassword:: hello123
uid: PortalAdmin
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Poon
cn: Chuck

dn: uid=william,ou=users,ou=SWG, dc=com
userPassword:: hello123
uid: william
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Hanes
cn: William

dn: uid=lucy,ou=users,ou=SWG, dc=com
userPassword:: hello123
uid: lucy
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Haye
cn: Lucy
```

What to do next

Authenticate IBM Cognos Analytics by using an LDAP user. Complete these steps:

1. Access the IBM Cognos Analytics Gateway URI. For example,
   http://*localhost:portnumber*/ibmcognos/cgi-bin/cognos.cgi. The *localhost* is
   the IP address or network host name where IBM Cognos Analytics gateway is
   configured. The *portnumber* is the port on which the IBM Cognos Analytics
   gateway is configured.
2. Select the configured **Namespace**, and click **OK**.
3. Enter your LDAP user ID and password.
4. Click **OK**.

Access control definition for the reports and reporting packages

You can define the access control for the LDAP users who are the members of a role that is defined in the IBM Cognos Analytics namespace. Access can be granted to those users who are the members of a defined role.

A user who has the system administrator privileges can grant the access.

Initially, all users are the members of the system administrator. Therefore, you can log in with your LDAP user authentication in IBM Cognos Analytics and access the administration section before you restrict the administration access.

Restricting administration access and adding an LDAP user to system administrator role

You can restrict the IBM Cognos Analytics administration access by using the system administrators role in IBM Cognos Analytics namespace. You can also add an LDAP user to the system administrator role for IBM Cognos Analytics report administration.

Procedure

1. Log in to IBM Cognos Analytics with an LDAP user whom you want to assign the system administrator role.
2. Go to **Launch**, and click **IBM Cognos Analytics Administration**.
3. Click the **Security** tab.
4. In the **Users, Groups, and Roles** section, click **Cognos**.
5. Navigate to **System Administrator** role.
6. Click the **More** link.
7. Under **Available actions**, click **Set properties**.
8. Click the **Members** tab.
9. Click the **Add** link.
10. Under **Available entries** section, click an LDAP namespace.
11. Select the **Show users in the list** check box.
12. Select the user whom you want to assign the system administrator role and make it into selected entries list.
13. Click **OK**.
14. Select **Everyone** from the members entry.
15. Click the **Remove** link to ensure that only the added users can have the system administration access.
16. Click **OK**.
17. Click the **Permissions** tab.
18. Verify that the system administrators are listed and they are provided all the permissions.

    If no permissions are provided, then select the system administrators and grant all the permissions. Select the **Override the access permissions acquired from the parent entry** check box to grant the permissions.
19. Click **OK**.

Results

An LDAP user is added with the system administrator role.

What to do next

Create a role and add LDAP users as the members to that role. See "Creating a role and adding LDAP users as members."

Creating a role and adding LDAP users as members

The topic describes the procedure to create a role in IBM Cognos and add the members from an LDAP namespace to it.

Procedure

1. Log in to IBM Cognos with an LDAP user who has the system administrator privileges. For example, `PortalAdmin`.
2. Go to **Launch**, and click **IBM Cognos Administration**.
3. Click the **Security** tab.
4. In the **Users, Groups, and Roles** section, click **Cognos**.
5. Click the **New Role** icon from the palette.
6. Specify the name for a role. For example, `ISPIMAuditor`.
7. Add the description and the screen tip.
8. Click **Next**.
9. Under **Select the members**, click **Add**.
10. Under **Available Entries Directory**, click an LDAP namespace.
11. Select the **Show users in the list** check box.
12. Select the users whom you want to add as the members to the role and make it into selected entries list.
13. Click **OK**.
14. Click **Finish**.

Results

A new role is created and LDAP users are added as the members to the new role.

Defining an access to the report by using a role

You can define an access to the report by using a role. All the members of a role can access the report or reports.

Procedure

1. Log in to IBM Cognos with an LDAP user who has the system administrator privileges. For example, `PortalAdmin`.
2. Under **Public Folders**, click the reporting package **ISPIMReportingPackage_2.1.0**.
3. Click the **More** link on the **Actions** toolbar that is associated with the report for which you want to provide the access.
4. Under **Available actions**, click **Set properties**.
5. Click the **Permissions** tab.
6. Select the **Override the access permissions acquired from the parent entry** check box.
7. Click **Add** link at the bottom of the list of entries.
8. Click **Cognos**.
9. Select the role that you want to add and make it to the selected entries.
10. Click **OK**.

11. Select the role and grant the permissions.

12. Optional: Remove other roles for which you do not want to provide the access.

13. Click **OK**.

Results

An access is defined to the report by using a role and all the members of a role can access the reports.

Defining an access to the reporting package by using a role

You can define an access to the report package by using a role. All the members of a role can access the report package.

Procedure

1. Log in to IBM Cognos with an LDAP user who has the system administrator privileges. For example, `PortalAdmin`.

2. Under **Public Folders**, click the **More** link on the **Actions** toolbar that is associated with the report package **ISPIMReportingPackage_2.1.0**.

3. Under **Available actions**, click **Set properties**.

4. Click the **Permissions** tab.

5. Select the **Override the access permissions acquired from the parent entry** check box.

6. Click the **Add** link at the bottom of the list of entries.

7. Click **Cognos**.

8. Select the role that you want to add and make it to the selected entries.

9. Click **OK**.

10. Select the role and grant the permissions.

11. Optional: Remove other roles for which you do not want to provide the access.

12. Click **OK**.

Results

An access is defined for the reporting package by using a role and the members of a role can access the reporting package.

References for IBM Cognos report security configuration

Use the following references that provide information about the topics that are related to the security configuration for the IBM Cognos reports.

Access the IBM Cognos Analytics documentation at https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html and search for the following terms.

- **Security model**.
- **Authentication providers**.
- **Add or remove members of a cognos group or role**.
- **Create a cognos group or role**.
- **Authorization**.
- **Access permissions and credentials**.

Globalization overview

You can use the globalization features of IBM Security Privileged Identity Manager Cognos report models to produce the reports in your own language.

Language support overview

IBM Security Privileged Identity Manager Cognos reports support the following languages.

- de=German
- en=English
- es=Spanish
- fr=French
- it=Italian
- ja=Japanese
- ko=Korean
- pt_BR=Brazilian Portuguese
- ru=Russian
- zh_CN=Simplified Chinese
- zh_TW=Traditional Chinese

Messages or terms related to the globalization

In the reports, some of the column values might display the term `Language not supported`

> When you select the language that is not supported by the reporting model, the value in the column is displayed as `Language not supported`.

Setting language preferences

You can personalize the way data appears in IBM Cognos workspace by changing your preferences. You can set the product language or content language to get the preferred output format of the reports.

Before you begin

Install and configure the IBM Cognos Analytics.

Procedure

1. In the IBM Cognos Analytics window, click **My Area Options** menu button.
2. Click **My Preferences**.
3. In the Set Preferences window, under the **Regional options** section, select **Product language**. Product language specifies the language that the IBM Cognos user interface uses.
4. In the Set Preferences window, under the **Regional options** section, select **Content language**. Content language specifies the language that is used to view and produce content in IBM Cognos such as data in the reports.
5. Click **OK**.

Results

You can view the reports or user interface in the language that you specified.

Enabling session recording replay from the report

To watch the recording of the user session on the managed resource, enable the option to replay session recording from the User Activity Audit Report. Configure the **PrivilegedIDAuditQuery** data items.

Before you begin

The Privileged Session Recording feature must be activated.

About this task

When you specify the values for the data item expressions, ensure that you put the values in single quotes.

Procedure

1. Open IBM Cognos Analytics.
2. In **Team content**, open the Single Sign-On Privileged ID Audit Report. The report opens in edit mode.
3. Click the **More** button ⋮ next to the **Single Sign-On Privileged ID Audit Report** and click **Edit report**.
4. Click the **Queries** button on the left panel.
5. Double-click **PrivilegedIDAuditQuery**. The list of its corresponding data items are displayed.
6. Double-click the **Privileged Session Recording Machine** data item. The Data Item Expression window is displayed with the Single Sign-On Privileged ID Audit Report in edit mode.
7. In **Expression Definition**, add the host name or the IP address of the IBM Security Privileged Identity Manager virtual appliance. For example: `pimva.example.com`.
8. Double-click the **Privileged Session Recording Server Port** data item. The Data Item Expression window is displayed with the Single Sign-On Privileged ID Audit Report in edit mode.
9. In **Expression Definition**, add the port number 443.
10. Save the changes to the Single Sign-On Privileged ID Audit Report.

Enabling the Privileged Session Gateway replay from the report

Enable the Privileged Session Gateway replay from the report to view the recordings from the Privileged Session Recorder console.

Procedure

1. Open IBM Cognos Analytics.
2. In **Team content**, click **ISPIMReportingModel_2.1** > **Session Gateway Acess History Report**.
3. Click the **More** button ⋮ next to the **Session Gateway Acess History Report** and click **Edit report**. The IBM Cognos Report Studio is displayed in a new window with the **Session Gateway Acess History Report** in edit mode.
4. Click the **Queries** button on the left panel.
5. In the **Session Gateway Access History** query, select **PSR Server**.

6. In the Data item expression- PSR Server window, edit the **Expression** to your Privileged Session Recording server hostname or IP address.
7. Save the changes to the **Session Gateway Acess History Report**.

Chapter 6. AccessProfiles

An AccessProfile contains instructions on handling automation for an application. It enables session recording support to your client application logon workflows and enables single sign-on automation to privileged identity management workflows.

To modify the bundled AccessProfiles, you must install AccessStudio on an administrative computer to develop custom AccessProfiles. See Installing the AccessStudio.

Creating your own privileged identity management AccessProfiles

Use the IBM Security Privileged Identity Manager AccessProfile to develop or enhance your own privileged identity management scenarios.

Before you begin

- Install AccessStudio.
- Ensure that you have the Privileged Identity Management AccessProfiles. The virtual appliance includes a collection of bundled AccessProfiles. For additional AccessProfiles, go to the AccessProfile Library.

Procedure

1. In AccessStudio, open the sample AccessProfile.
2. Build or enhance the Privileged Identity Management AccessProfiles. For more information, see "Modifying AccessProfiles" on page 108.
3. Debug and start your AccessProfile.
4. Upload your AccessProfile to the IBM Security Privileged Identity Manager server.

Privileged Session Recorder widgets

Use the Privileged Session Recorder widgets in the bundled AccessProfiles to add session recording support to your client application logon workflows.

Do not modify the widgets.
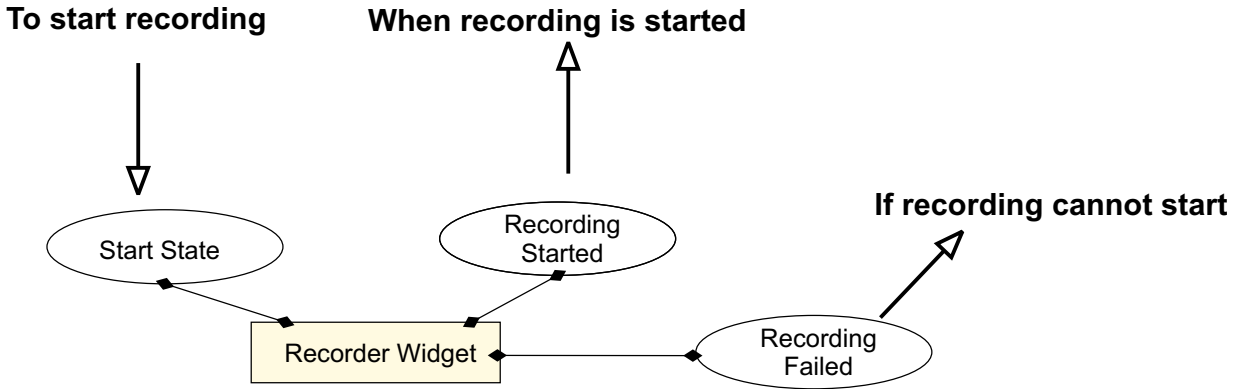
Figure 3. How the Privileged Session Recorder widgets work

Each recorder widget has an entry state, a success exit state, and a failed exit state. Some of the recorder widgets might have more than two pinnable states. For more information about pinnable states and widgets, see the *IBM Security Access Manager for Enterprise Single Sign-On AccessProfile Widgets Guide*.

IBM Security Privileged Identity Manager bundled AccessProfiles are integrated with the session recording widgets. The widgets start session recording when shared access identities are checked out.

Session recording stops when the target application is closed.

When you develop or customize an AccessProfile, add the appropriate recorder widget to the state.
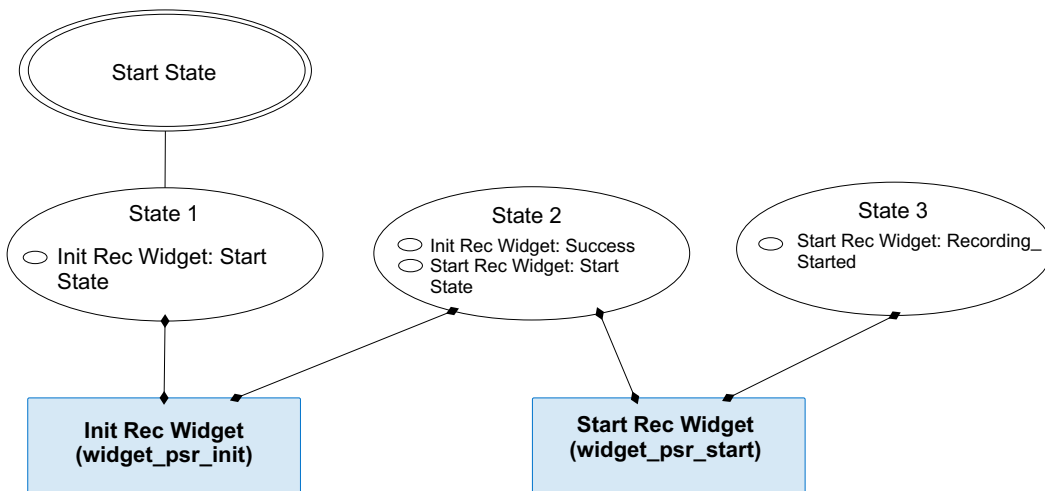
Figure 4. Example of a basic recording AccessProfile (check out and check in is omitted)

The following Privileged Session Recorder widgets are included:

Widget_PSR_Init
Generates the recording ID which will be used when the recording starts. Displays the message of consent dialog box.

Widget_PSR_Start
Starts a session recording. For example:

- Starts recording when a privileged identity is checked out.
- Starts recording when a secured application is started.

Note: Use the **Widget_PSR_Start** widget after the **profile_checkout_widget** widget. If you use the **Widget_PSR_Start** without a preceding check out widget, the recording interface will not have the shared credentials that it requires. The AccessProfile might not work as expected.

Widget_PSR_Pause
Pauses a session recording. For example, you can pause recording when confidential information from a personal application is being displayed in the application. Pausing a recording avoids including the confidential details in the session recording.

Widget_PSR_Resume
Resumes a session recording that is paused. For example, you can resume recording after the confidential information is no longer shown.

Widget_PSR_Stop
Stops a session recording. For example, you can stop recording when a privileged identity is checked in.

Privileged Session Recorder with the bundled AccessProfiles work in the following ways:

- Recording starts when the shared access user ID is checked out, and the user agrees to give consent for recording.

  If the IBM Privileged Session Recorder Server connection is interrupted or the Privileged Session Recorder service is stopped on the client workstation, any mouse or key input for the client application might be blocked depending on the policies you configure in AccessAdmin.

  For more information, see Policies for Privileged Access Agent.

- Recording automatically stops when the application is closed. For PuTTY, the bundled AccessProfile is designed to stop the recording when the session is inactive.

Initializing a session recording

Initialize a session recording with the **Widget_PSR_Init** widget. The widget generates a Recording ID for the recording.

Procedure

1. Add the **Widget_PSR_Init** to the AccessProfile.
2. Pin the **Init_Recording** state from the **Widget_PSR_Init** widget.
3. Specify the necessary parameters to pass to the widget.

   Recorded Application Window's XPath
   Specifies the window signature.

   User Consent Dialog Message
   Specifies the user consent dialog box message.

Recorder Bag (Type: Account Data Bag)
> Specifies the account data bag for internal use by the recording widgets.

Recording ID [Type: Property Store Item]
> The ID to be associated with the recording.

Starting a session recording

Start an initialized session recording with the `Widget_PSR_Start` widget.

About this task

When a recording is started on the client workstation, a recorder tray notification is displayed in the Windows notification area.

Note: Use the `Widget_PSR_Start` widget after the `profile_checkout_widget` widget. If you use the `Widget_PSR_Start` without a preceding check out widget, the recording interface will not have the shared credentials that it requires. The AccessProfile might not work as expected.

Table 22. Different application types use different parameter values for successful recordings with the `Widget_PSR_Start` widget. .

Parameters	VMware vSphere	Microsoft Remote Desktop Services	PuTTY (Terminal)	IBM Personal Communications (Terminal)
Listen to child process?	1	0	0	0
Terminal Window Signature	Not applicable.	Not applicable.	Passed by reference.	Passed by reference.
Recording Mode	1	1	0	0

Parameters that are used by other bundled AccessProfiles might be different.

Procedure

1. Add the `Widget_PSR_Start` to the AccessProfile.
2. Pin the `Start_Recording` state from the `Widget_PSR_Start`.
3. Specify the necessary parameters to pass to the widget.

   PIM Bag (Type: Account Data Bag)
   > Specifies the temporary data holder or cache that stores user credentials that must be checked in or checked out after Privileged Access Agent captures credentials from the application.

   Application Name (Type: Account Data Bag)
   > Specifies the application name that is recorded.

   Recorder Bag (Type: Account Data Bag)
   > Specifies the account data bag for internal use by the recording widgets.

   ISIM Authentication Service (Type: Account Data Bag)
   > Specifies the configured IBM Security Identity Manager authentication service ID as an account data bag.

   Custom Metadata Name (Type: Property Store Item)
   > Specifies a custom metadata attribute as a property store item.

   Custom Metadata Value (Type: Property Store Item)
   > Specifies a custom metadata value as a property store item.

Recording ID [Type: Property Store Item]
The ID to be associated with the recording.

Listen to events from child process?
Set to **1** to include child processes in the parent process session recording for certain screen-based recordings. For example, the **Listen to events from child process?** parameter is enabled in the VMware vSphere bundled AccessProfile to address the scenario in which a virtual machine is opened in a separate window. The parameter is set to **0** in the bundled AccessProfile for terminal applications.

Terminal Window Signature [Type: Property Store Item]
Specifies the unique identifier of the terminal application window element. For example, for PuTTY, the terminal window signature is `/child::wnd[@title~"".*- PuTTY"" and @class_name=""PuTTY""]`. The property name is `Parent_Wnd_Signature`.

Recording Mode [Type: Property Store Item]
Set to **1** to start screen capture based recordings for Windows-based applications such as Microsoft Remote Desktop and VMware vSphere. Set **Recording Mode** to **0** to enable text-based recording for terminal applications such as PuTTY or IBM Personal Communications.

4. In the next state, pin the **Recording_Started** state from the **Widget_PSR_Start**.

Stopping a session recording

A recording stops when the monitored client application is closed. You can also stop a session recording with the **Widget_PSR_Stop** widget.

Procedure

1. Add the **Widget_PSR_Stop** to the AccessProfile.
2. Pin the **Stop_Recording** state from the **Widget_PSR_Stop** widget.
3. Specify the necessary parameters to pass to the widget.

PIM Bag (Type: Account Data Bag)
Specifies the temporary data holder or cache that stores user credentials that must be checked in or checked out after Privileged Access Agent captures credentials from the application.

Capture Mode (Type: Account Data Bag)
Specifies whether screen capture already started for the account data bag.

Recorder Bag (Type: Account Data Bag)
Specifies the account data bag for internal use by the recording widgets.

Recording Mode [Type: Property Store Item]
Pass the same value as in **Widget_PSR_Start**.

Pausing a session recording

You can pause a recording that is in progress by adding an instance of the **Widget_PSR_Pause** widget to your AccessProfile. For example, you can pause recording when confidential information is being displayed in an application. Pausing avoids including the confidential information in the session recording.

Procedure

1. In AccessStudio, open your AccessProfile.
2. Add an instance of the **Widget_PSR_Pause** widget to the AccessProfile.

3. With a state in the AccessProfile selected, pin the `Pause_Recording` pinnable state.
4. With the pinned state selected, specify the necessary account data bag parameters in the **Form Editor**.

   An *account data bag* is a temporary data holder or cache that stores user credentials.

   PIM Bag (Type: Account Data Bag)
   Specifies the temporary data holder or cache that stores user credentials that must be checked in or checked out after Privileged Access Agent captures credentials from the application.

   Capture Mode (Type: Account Data Bag)
   Specifies whether screen capture already started for the account data bag.

   Recorder Bag (Type: Account Data Bag)
   Specifies the account data bag for internal use by the recording widgets.

   Recording Mode [Type: Property Store Item]
   Pass the same value as in **Widget_PSR_Start**.

5. In the next AccessProfile state, pin the `Recording_Paused` pinnable state.

Resuming a recording session

You can resume a recording session in an AccessProfile with the bundled **Widget_PSR_Resume** widget.

Procedure

1. In AccessStudio, open your AccessProfile.
2. Add an instance of the **Widget_PSR_Resume** widget to the AccessProfile.
3. With a state in the AccessProfile selected, pin the `Resume_Recording` pinnable state from the widget.
4. Specify the necessary parameters to pass to the widget.

   Recording Mode [Type: Property Store Item]
   Pass the same value as in **Widget_PSR_Start**.

5. Add another state.
6. Pin the `Recording_Resumed` state to the new state you added.

Shared access widgets

Use the bundled shared access widgets to add single sign-on automation to privileged identity management workflows.

Each shared access widget has an entry state, a success exit state, and sometimes, an alternate exit state.
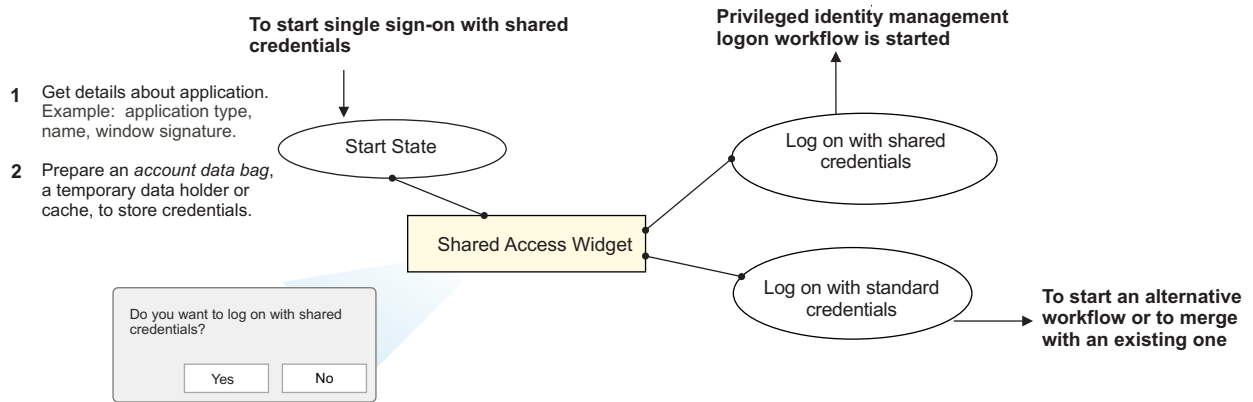
Figure 5. How a shared access widget is used in an AccessProfile

When you develop or customize an AccessProfile, pin the appropriate shared access widget to the state.

The bundled AccessProfiles for RDP, PuTTY, IBM Personal Communications, and VMware vSphere for IBM Security Privileged Identity Manager demonstrate how you can use the widgets to log on with shared credentials. The AccessProfiles are labeled in the following way profile_*appname*_main.

The widgets trigger the privileged identity management credential check-out workflows automatically when a supported application is detected.
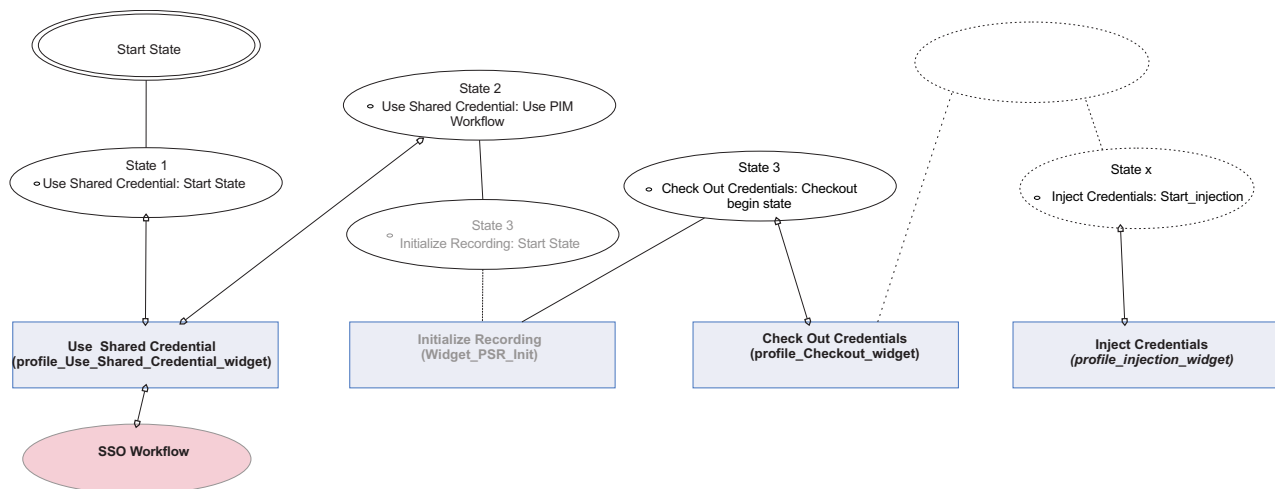
Figure 6. Example of a basic privileged identity AccessProfile that logs on with shared credentials. The check-in widget is not shown.

The following shared access widgets are included:

profile_use_shared_credential_widget
Specifies the type of credential logon workflow. Prompts the user to choose whether to log on with managed privileged credentials or not.

Table 23. Types of credential logon workflows.

Log on with a shared credential	Action
Yes	The widget triggers the privileged identity management logon work flow with a shared credential
No	The process exits, or triggers a standard single sign-on credential workflow, if one is available.

You can use the single sign-on pinnable state to merge existing AccessProfiles that you might have for the same application. By merging AccessProfiles, an application can support both alternate and privileged identity management workflows.

profile_checkout_widget
Checks out a shared credential. This widget triggers the following actions:
* Prompts the user for IBM Security Privileged Identity Manager credentials. This process checks if the user has adequate privileges to check out credentials from a role.
* Prompts the user for the credential role to check out.

profile_<*app*>_injection_widgets
Injects shared access credentials into the user name and password fields for application logon. The bundled AccessProfiles use separate injection widgets for screen-based applications and terminal or mainframe applications.
* `profile_RDP_and_vSphere_injection_widget`: Used by RDP and VMware vSphere Client.
* `profile_term_mf_injection_widget`: Used by IBM Personal Communications and PuTTY.

profile_<*app*>_chkin_widget
Checks in the credential. There are separate check-in widgets for screen-based applications and terminal or mainframe applications.
* The check-in widget is not required in the following scenarios:
  – The application is closed by the user
  – The application closes unexpectedly due to a system issue.

  The credential is still checked in automatically by the Privileged Access Agent client.
* The check-in widget is required in some terminal scenarios. For example, in a PuTTY session with a checked out credential, you type `exit` and the session becomes inactive. The widget is required to check in the credential.

The bundled AccessProfiles work in the following ways:
* The shared credential is checked out when the user agrees to use a shared credential from a selected role.

  The user is authenticated against the configured shared access authentication service. An authentication service for IBM Security Privileged Identity Manager is in the user wallet. A credential from the role is retrieved from the credential vault. The credential is added to the user wallet. The credential is then injected into the user name and password fields for the configured application.

  Note: To hide the shared credential message of consent prompt for non-privileged identity users, you can create a user policy template for

privileged users. See the IBM Security Privileged Identity Manager AccessAdmin policy configuration page for IBM Security Privileged Identity Manager.

- Shared credential is checked in when the application is closed.

  If the IBM Security Privileged Identity Manager Server is not available, `bgmonitor` tries again until a threshold is reached. The threshold is configurable in the AccessAdmin policy configuration page for IBM Security Privileged Identity Manager.

The `bgmonitor` component is a service that ensures credentials are always checked-in on the client when an application closes unexpectedly or the system fails. The `bgmonitor` service provides the following features:

- Monitors for lease expiry of credentials.
- Starts when credential checkout is started by the AccessProfile.
- Only one instance of this process runs at a time.

A corresponding **bgmonitor** AccessProfile exists on the server. The **bgmonitor** AccessProfile triggers the `bgmonitor` process on the client when an application fails to check in any credentials.

Choosing a shared credentials logon workflow

Use a shared access credential logon workflow to prompt users for the logon workflow. Use a shared credentials logon workflow for privileged identity management. Use the alternate single sign-on workflow to merge with other existing workflows or to trigger alternative actions.

Procedure

1. Add the **profile_use_shared_credential_widget** to the AccessProfile.
2. Pin the **Start state** from the **profile_use_shared_credential_widget** widget.
3. Specify the parameters to pass to the widget.

   Parent_Wnd_Signature [Property Store Item]
   Specifies the unique identifier of the application window element. For example, for PuTTY, the window signature is `/child::wnd[@title~"".*-PuTTY"" and @class_name=""PuTTY""]`. The property name is `Parent_Wnd_Signature`.

   CICO_injection_bag [Type: Account Data Bag]
   Specifies the temporary data holder or cache that stores credentials that must be checked in or checked out after Privileged Access Agent captures credentials from the application.

Checking out credentials

Check out shared credentials from a repository and store the credentials in an account data bag.

Procedure

1. Add the **profile_checkout_widget** widget to the AccessProfile.
2. Pin the **Check out begin state** from the **profile_checkout_widget** widget.
3. Specify the parameters to pass to the widget.

   CICO_injection_bag [Type: Account Data Bag]
   Specifies the temporary data holder or cache that stores credentials that must be checked in or checked out after Privileged Access Agent captures credentials from the application.

ItimSvcURL [Type: Property Store Item]
URL of the IBM Security Privileged Identity Manager check-in and check-out service. For example: `https://pimhost:9081/WAR_CICO/services/CICOManager`

Username window [Type: Property Store Item]
Windows signature for username window. Optional.

Password window [Type: Property Store Item]
Window signature for a password window. Optional.

ISIM Authentication Service (Type: Account Data Bag)
Specifies the configured IBM Security Identity Manager authentication service ID as an account data bag.

Check out done boolean [Type: Property Store Item]
Specify whether check-out operation is successful. 1 for a successful check-out.

RoleSelectionDlgParentHwndSignature [Type:Property Store Item]
Signature of the role selection dialog box parent window. If the parameter is an empty string, the role selection dialog box parent window is NULL.

Application Name (Type: Account Data Bag)
Specifies the application name that is recorded.

Recording ID [Type: Property Store Item]
The ID to be associated with the recording.

Injecting credentials

Inject the credentials that you checked out from the credential vault into a logon dialog prompt or username or password field with the widgets. There are different injection widgets for terminal applications and screen-based applications.

Before you begin

If necessary, check out credentials from the credential vault.

About this task

The bundled injection widgets are dependent on the type of application.

To get started with advanced profiling requirements for custom applications, start with the following injection widgets as an example.

1. Identify the type of application workflow that you want to develop.

   For example, for a screen-based application, use the Remote Desktop Connection and vSphere Client examples. For a text-based or terminal application, use the PuTTY and IBM Personal Communications.

2. Open the injection widgets and the main application AccessProfile in AccessStudio.

3. Trace and observe the logon workflows that lead to a successful state in the main AccessProfiles. For example: `profile_RDP_main`, `profile_putty_main`

4. Copy the types of states, actions, scripts, and triggers that you can use.

5. Copy and modify the example VBScript actions that are used to pass parameters to each action.

6. Retrace the workflows that lead to alternate or failed exit states.

Procedure

1. Add the **profile_<appname>_inject_widget**widget to the AccessProfile.
2. Pin the **Injection begin state** from the **profile_<appname>_inject_widget** widget.
3. Specify the parameters to pass to the widget.

Table 24. Injection widget parameters for different application types.

Application	Parameters
Screen-based application **profile_RDP_and_vSphere_injection_widget**	
• VMware vSphere Client • Microsoft Remote Desktop Connection	**CICO_injection_bag [Type: Account Data Bag]** Specifies the temporary data holder or cache that stores credentials that must be checked in or checked out after Privileged Access Agent captures credentials from the application. **Username window [Type: Property Store Item]** Windows signature for username window. Optional. **Password window [Type: Property Store Item]** Window signature for a password window. Optional.
Terminal or mainframe application **profile_term_mf_injection_widget**	
IBM Personal Communications	**CICO_injection_bag [Type: Account Data Bag]** Specifies the temporary data holder or cache that stores credentials that must be checked in or checked out after Privileged Access Agent captures credentials from the application. **Username window [Type: Property Store Item]** Windows signature for username window. Optional. **Password window [Type: Property Store Item]** Window signature for a password window. Optional. **wnd_for_text_identication_on_mainframe_screen [Type: Property Store Item]** Window for identifying text on the mainframe screen. **Text is found for injecting username [Type: Property Store Item]** Text that is identified as a field to trigger for injecting username. **Text is found for injecting password [Type: Property Store Item]** Text that is identified as a field to trigger for injecting the password. **Text is first displayed for access denied or failure [Type: Property Store Item]** Text that is first displayed when access is denied or access has failed. **Text is found for successful logon [Type: Property Store Item]** Text that is first displayed when logon is successful. **Text is found for not injecting password [Type: Property Store Item]** Text that is displayed if the password is not injected successfully.

Table 24. Injection widget parameters for different application types. (continued)

Application	Parameters
PuTTY	**CICO_injection_bag [Type: Account Data Bag]** Specifies the temporary data holder or cache that stores credentials that must be checked in or checked out after Privileged Access Agent captures credentials from the application. **Username window [Type: Property Store Item]** Windows signature for username window. Optional. **Password window [Type: Property Store Item]** Window signature for a password window. Optional. **Text is first displayed for access denied or failure [Type: Property Store Item]** Text that is first displayed when access is denied or access has failed. **Text is found for successful logon [Type: Property Store Item]** Text that is first displayed when logon is successful. **Text is found for not injecting password [Type: Property Store Item]** Text that is displayed if the password is not injected successfully.

Checking in credentials

Use the check-in widget to check in shared credentials.

Procedure

1. Add the **profile_<appname>_chkin_widget** widget to the AccessProfile.
2. Pin the **Check in begin state** for one of the following check-in widgets.
   - **profile_RDP_and_vSphere_chkin_widget**
   - **profile_term_mf_chkin_widget**
3. Specify the parameters to pass to the widget.

Table 25. Check-in widget parameters for different application types.

Application	Parameters
Screen-based application **profile_RDP_and_vSphere_injection_widget**	
• VMware vSphere Client • Microsoft Remote Desktop Connection	**CICO_injection_bag [Type: Account Data Bag]** Specifies the temporary data holder or cache that stores credentials that must be checked in or checked out after Privileged Access Agent captures credentials from the application. **Username window [Type: Property Store Item]** Windows signature for username window. Optional. **Password window [Type: Property Store Item]** Window signature for a password window. Optional.
Terminal or mainframe application **profile_term_mf_injection_widget**	

Table 25. Check-in widget parameters for different application types. (continued)

Application	Parameters
IBM Personal Communications	**CICO_injection_bag [Type: Account Data Bag]** Specifies the temporary data holder or cache that stores credentials that must be checked in or checked out after Privileged Access Agent captures credentials from the application. **Username window [Type: Property Store Item]** Windows signature for username window. Optional. **Password window [Type: Property Store Item]** Window signature for a password window. Optional. **wnd_for_text_identication_on_mainframe_screen [Type: Property Store Item]** Window for identifying text on the mainframe screen. **Text is found for injecting username [Type: Property Store Item]** Text that is identified as a field to trigger for injecting user name. **Text is found for injecting password [Type: Property Store Item]** Text that is identified as a field to trigger for injecting the password. **Text is first displayed for access denied or failure [Type: Property Store Item]** Text that is first displayed when access is denied or access has failed. **Text is found for successful logon [Type: Property Store Item]** Text that is first displayed when logon is successful. **Text is found for not injecting password [Type: Property Store Item]** Text that is displayed if the password is not injected successfully.

Table 25. Check-in widget parameters for different application types. (continued)

Application	Parameters
PuTTY	**CICO_injection_bag [Type: Account Data Bag]** Specifies the temporary data holder or cache that stores credentials that must be checked in or checked out after Privileged Access Agent captures credentials from the application. **Username window [Type: Property Store Item]** Windows signature for username window. Optional. **Password window [Type: Property Store Item]** Window signature for a password window. Optional. **Text is first displayed for access denied or failure [Type: Property Store Item]** Text that is first displayed when access is denied or access has failed. **Text is found for successful logon [Type: Property Store Item]** Text that is first displayed when logon is successful. **Text is found for not injecting password [Type: Property Store Item]** Text that is displayed if the password is not injected successfully.

Modifying AccessProfiles

Modify the bundled AccessProfiles, learn how to use the widgets, or create your own AccessProfiles, to adapt to changes in applications and endpoint logon requirements.

To use session recording for customized AccessProfiles, see the bundled privileged identity management AccessProfiles that use the Recorder widgets.

To customize advanced AccessProfiles that are not covered, see the *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide*. Alternatively, search the IBM website for "Advanced AccessProfile Redbooks®" for guidance.

Custom mainframe applications

Some custom mainframe applications have more logon requirements.

For example:
* Specifying more logon credential fields for credential injection.
* Simulating different keyboard keys to shift the terminal entry focus.

Use the privileged identity management AccessProfiles for IBM Personal Communications as a template.

Modifying the bundled AccessProfile for the IBM Personal Communications application

Modify the bundled IBM Personal Communications AccessProfile to customize its behavior.

Before you begin

- Install AccessStudio.
- Install the IBM Personal Communications client.
- Open the Personal Communications application.
- Upload the AccessProfiles to the server. See "Uploading AccessProfiles to the virtual appliance" on page 112.

Tip: Before you apply any modifications, you can take a local backup of the AccessProfile. To back up the AccessProfile to file, you can save the AccessProfile to a location on your computer.

Procedure

1. Start AccessStudio.
2. Import the Privileged Identity Management AccessProfile package into the AccessStudio workspace by clicking **File** > **Import data from IMS**.
3. In the **AccessProfile** pane, open `profile_PCOMM_main`.
4. Select the **States** tab.
5. In the **AccessProfile** state diagram canvas, select the **Run a VBScript or JScript** action under the second state.
6. In the **Properties** pane, select the **Form Editor** tab.
7. Click **Open Script Editor**.
8. Edit the script.
   a. Select a unique text from the mainframe application screen.
   b. Remove the variable portion of the text.
   c. Retain the non-variable portion of the text in the form of a regular expression. For example:
      - **Unique text:** `WELCOME UserA`
      - **Variable:** `UserA`
      - **Non-variable:** `WELCOME`
      - **Regular expression of the non-variable text:** `WELCOME.*`

        This regular expression matches any instances of text that might be displayed as:
        ```
          WELCOME
        -WELCOME-
        EXAMPLE APPLICATION WELCOME
        ```
        This regular expression does not match the following instances:
        ```
        welcome
        Welcome
        Example Welcome
        W.E.L.C.O.M.E
        ```
   d. Modify the second argument for each `pc.SetPropValue` entry. You can add the regular expression or replace the existing regular expression.
      ```
      pc.SetPropValue "text_to_identify_the_welcome_screen",
         "^.*WELCOME.*$|.*User\sID\s:.*"

      pc.SetPropValue "text_to_identify_and_initiate_PIM_workflow",
         ".*WELCOME\sTO\sCICS.*|.*User\sID\s:.*"

      pc.SetPropValue "text_is_found_for_injecting_username",
         ".*[Ll]ogin.*:.*|.*LOGIN.*:.*|.*WELCOME\sTO\sCICS.*|.*Userid.*|
         .*User\sID.*"

      pc.SetpropValue "text_is_found_for_injecting_password",
         ".*(?i)(please type your password|missing password).*"
      ```

```
                    pc.SetpropValue "text_is_found_for_not_injecting_password",
                       ".*(?i)(your userid is invalid).*"

                    pc.SetPropValue "text_is_first_displayed_for_access_denied_or_failure",
                       ".*[Dd]enied.*|.*DENIED.*|.*[Ii]nvalid.*|.*not\sdefined\.*"

                    pc.SetPropValue "text_is_found_for_successful_logon",
                       ".*[Ll]ast login.*:.*|.*LAST LOGIN.*:.*|.*Microsoft\sWindows.*|
                       .*Sign-on\sis\scomplete.*|.*Enterprise\sSummary.*"

                    pc.SetPropValue "Wnd_sig_Username",
                       "/child::wnd[@class_name=""PCSWS:Main:00400000""]"

                    pc.SetPropValue "wnd_for_text_identication_on_mainframe_screen",
                       "/child::wnd[@class_name=""PCSWS:Main:00400000""]/
                       child::wnd[@class_name=""PCSWS:Pres:00400000"" and @ctrl_id=2]"

                    pc.SetPropValue "Parent_Wnd_Signature",
                       "/child::wnd[@class_name=""PCSWS:Main:00400000""]/
                       child::wnd[@class_name=""PCSWS:Pres:00400000"" and @ctrl_id=2]"

                    'Displays a consent dialog box with a custom message before starting
                     session recording.
                    pc.SetPropValue "recording_consent_dialog_custom_message", ""


                    'Specifies the parent window signature for the consent dialog message
                    pc.SetPropValue "recording_consent_dialog_parent_xpath",
                       "/child::wnd[@class_name=""PCSWS:Main:00400000""]/
                        child::wnd[@class_name=""PCSWS:Pres:00400000"" and @ctrl_id=2]"

                    'Specifies the additional custom metadata that will be passed to the
                        Privileged Session Recorder Server during session recording
                    'For example, pc.SetPropValue "param_custom_metadata", "Department_Name"
                    pc.SetPropValue "param_custom_metadata", ""

                    'Specifies the value for the above specified
                     custom metadata that will be passed to the Privileged Session Recorder
                     Server during session recording
                    'For example, pc.SetPropValue "param_value", "IT"
                    pc.SetPropValue "param_value", ""

                    'Specifies whether to enable either text based or screen based recordings
                        for terminal or Windows applications respectively
                    'For example, for Terminal applications such as PuTTY and PCOMM, to have
                       text based capture, set the value to 0. For screen based capture with
                     Windows based applications such as RDP and vSphere set the value to 1.
                    pc.SetPropValue "RecordingMode", "0"


                    'Specifies the algorithm to be used for command recognition
                     in text-based recordings. This value is ignored in screen-based recordings.
                    'Set this value to 1 for text recording of UNIX sessions. Otherwise, set it
                     to 0.
                    pc.SetPropValue "psr_command_recognition_algo", "1"
```

9. Test the AccessProfile.
   a. Start **Test Mode**.
   b. Start IBM Personal Communications.
10. After the test is completed, save the AccessProfile. The AccessProfile on the server is updated.

   Note: If you are working from a local copy of the AccessProfile, remember to publish the completed AccessProfile to the server.

Modifying the bundled AccessProfile for the PuTTY application

You can modify the bundled PuTTY application AccessProfile to customize its behavior.

Before you begin

- Install AccessStudio.
- Install the PuTTY client.
- Open the PuTTY application.
- Upload the AccessProfiles to the server. See "Uploading AccessProfiles to the virtual appliance" on page 112.

Tip: Before you apply any modifications, you can take a local backup of the AccessProfile. To back up the AccessProfile to file, you can save the AccessProfile to a location on your computer.

Procedure

1. Start AccessStudio.
2. Import the Privileged Identity Management AccessProfile package into the AccessStudio workspace by clicking **File** > **Import data from IMS**.
3. In the **AccessProfile** pane, open profile_putty_main.
4. Select the **States** tab.
5. In the **AccessProfile** state diagram canvas, select the **Run a VBScript or JScript** action under the second state.
6. In the **Properties** pane, select the **Form Editor** tab.
7. Click **Open Script Editor**.
8. Edit the script.
   a. Select a unique text from the mainframe application screen.
   b. Remove the variable portion of the text.
   c. Retain the non-variable portion of the text in the form of a regular expression. For example:
      - **Unique text:** WELCOME UserA
      - **Variable:** UserA
      - **Non-variable:** WELCOME
      - **Regular expression of the non-variable text:** WELCOME.*

        This regular expression matches any instances of text that might be displayed as:

        ```
          WELCOME
        -WELCOME-
        EXAMPLE APPLICATION WELCOME
        ```

        This regular expression does not match the following instances:

        ```
        welcome
        Welcome
        Example Welcome
        W.E.L.C.O.M.E
        ```
   d. Modify the second argument for each pc.SetPropValue entry. You can add the regular expression or replace the existing regular expression.

      ```
      pc.SetpropValue "text_is_found_for_injecting_password",
        ".*[Pp]assword.*|.*PASSWORD.*"

      pc.SetpropValue "text_is_found_for_not_injecting_password",
        ".*[Dd]enied.*|.*DENIED.*"

      pc.SetPropValue "text_is_first_displayed_for_access_denied_or_failure",
        ".*[Dd]enied.*|.*DENIED.*|.*[Ii]nvalid.*|.*not\sdefined\.*"

      pc.SetPropValue "text_is_found_for_successful_logon",
        ".*[Ll]ast login.*:.*|.*LAST LOGIN.*:.*|.*$.*|.*>.*|.*#.*|
        .*Microsoft\sWindows.*|.*Sign-on\sis\scomplete.*|
      ```

```
                   .*Enterprise\sSummary.*"

pc.SetPropValue "Parent_Wnd_Signature",
   "/child::wnd[@title~""".*- PuTTY""" and @class_name=""""PuTTY""""]"

pc.SetPropValue "wnd_for_text_identication_on_mainframe_screen",
   "/child::wnd[@title~""".*- PuTTY""" and @class_name=""""PuTTY""""]"

'Displays a consent dialog box with a custom message before starting
   session recording.

'Specifies the text that would appear on the consent
 message (custom consent message) for session recording
pc.SetPropValue "recording_consent_dialog_custom_message", ""

'Specifies the parent window signature for the consent dialog message
pc.SetPropValue "recording_consent_dialog_parent_xpath",
    "/child::wnd[@title~""".*- PuTTY""" and @class_name=""""PuTTY""""]"

'Specifies the additional custom metadata that will be passed to the
    Privileged Session Recorder Server during session recording
'For example, pc.SetPropValue "param_custom_metadata", "Department_Name"
pc.SetPropValue "param_custom_metadata", ""

'Specifies the value for the above specified custom metadata
  that will be passed to the Privileged Session Recorder Server during
  session recording
'For example, pc.SetPropValue "param_value", "IT"
pc.SetPropValue "param_value", ""

'Specifies whether to enable either text based recordings for terminals
 or screen based recordings for Windows based applications.
'For example, for Terminal applications such as PuTTY and PCOMM, to enable
 text-based recordings, set the value to 0.  For Windows based applications
 such as RDP and vSphere, to have screen based capture, set the value to 1.
pc.SetPropValue "RecordingMode", "0"


'Specifies the algorithm to be used for command recognition
 in text-based recordings. This value is ignored in screen-based recordings.
'Set this value to 1 for text recording of UNIX sessions. Otherwise, set it
 to 0.
pc.SetPropValue "psr_command_recognition_algo", "1"
```

9. Test the AccessProfile.

   a. Start **Test Mode**.

   b. Start PuTTY.

10. After the test is completed, save the AccessProfile. The AccessProfile on the server is updated.

   Note: If you are working from a local copy of the AccessProfile, remember to publish the completed AccessProfile to the server.

Uploading AccessProfiles to the virtual appliance

To activate and use an AccessProfile, upload the AccessProfile to the IBM Security Privileged Identity Manager virtual appliance.

Before you begin

- If you have multiple AccessProfiles, see Multiple AccessProfiles for the same client application for a better understanding before you upload AccessProfiles to the IBM Security Privileged Identity Manager virtual appliance.
- You must be logged on to Privileged Access Agent as an administrator.

Procedure

1. Open AccessStudio.
2. Select the AccessProfile or associated information from the Data type pane.

3. Click **Upload selected data to IMS** from the toolbar.

Related information:

    AccessProfile Library

    AccessStudio product documentation

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web

sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not

been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability
These terms and conditions are in addition to any terms of use for the IBM website.

Personal use
You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use
You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at http://www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings

can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering uses other technologies that collect each user's user name, password or other personally identifiable information for purposes of session management, authentication, single sign-on configuration, usage tracking, or functional purposes. These technologies can be disabled, but disabling them will also eliminate the functionality they enable.

This Software Offering does not use cookies to collect personally identifiable information. The only information that is transmitted between the server and the browser through a cookie is the session ID, which has a limited lifetime. A session ID associates the session request with information stored on the server.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details/us/en sections entitled "Cookies, Web Beacons and Other Technologies" and "Software Products and Software-as-a Service".

IBM ®

Printed in USA