Technical white paper

HP Security Manager

Troubleshooting Issues

Table of Contents

Overview 5

Log Files and Enabling Debugging 6

HP Security Manager Log Files Locations (HPSM 3.7 and later) 6

HP Security Manager Log Files Locations (before HPSM 3.7) 7

Most frequently used log files 7

Location and names of configuration files for changing the log level of the different log files 7

Changing the default log location (including logging into a mapped network drive) 9

Enabling HP Security Manager debugging (service interactions) 10

Enabling HP Security Manager debugging (Instant-On communication) 11

Enabling HP Security Manager debugging (device communication issues) 12

Enabling HP Security Manager debugging (Certificate Management) 13

Enabling HP Security Manager debugging Certificate Management: SCEP 14

Enabling HP Security Manager debugging Certificate Management: EST 15

Enabling logging for Qualys Policy Compliance 15

Enabling HPSM app/system diagnostics logging 16

Audit log files 16

Enabling FMEA (Failure Mode and Effect Analysis) logging 16

Enabling HP Print License Service debugging (HPSM 3.5 and older) 17

Required Network Ports 19

Client to Server ports 19

Server to Device ports and to hp.com (for firmware assessments) 19

Devices to Server ports 19

Server to SQL database ports 20

Server to Email ports 20

Server to Certificate Authority ports 20

Licensing ports 20

HPSM application pool to Server ports 20

Ports Diagram 21

Changing Firewall Settings and Testing Open Ports 22

Proxy for Network Service Blocking Communication 24

Installation Issues 25

Common SQL issues 25

Database Upgrade Failure 28

Using SQL script to repair/upgrade/install the database 29

Error-Maybe a DB access issue in HPSM_service.log file 31

Problems Launching Security Manager Web Interface 32

Web page not displayed while HPSM service is running and connecting to DB 32

Bindings/firewall problem 32

Browser settings causing issues 33

Web page not displayed and HPSM service is automatically stopping 34

ServerConfig could not initialized in HPSM_service.log 34

Invalid length for a Base-64 char array or string in HPSM_service.log 36

Issues when running HPSM Application Pool 37

As network service - Server Error in "/" Application, Cannot open database 37

32-Bit Applications not enabled for HPSM application pool 39

HTTP 500.19 Internal Server Error with config source reference to X-Frame-Options 40

HTTP 500.19 Internal Server Error with error code 0x800700c1 41

As a non-admin user or service account (error 503) 44

Access Denied when trying to logon to HPSM 46

Licensing Issues 47

Licensing Issues in multi-homed environment: Failed to connect to licensing server 47

Licensing does not work when HPSM's hostname is changed after installation 48

'Insufficient licenses' error after nightly maintenance task with HPSM 3.6 or newer 51

'Insufficient licenses' after upgrading to HPSM 3.10 or later 52

Flexera service Will Not Start (Flexera started and then stopped) 54

'Failed to retrieve the data' error in the HPSM dashboard and zero licenses available 55

Insufficient Licenses in HPSM dashboard and zero licenses available with description of starting order of Flexera components 56

Mixing licenses limitations 57

Other Licensing Issues before HPSM 3.7 58

Device Status Errors and Credential Failures 64

Credential Management 67

SNMP 67

Admin (EWS) Password 68
Example of Check Credentials 68
Device Communication Log Files 70
Credentials not Validated or Incorrect 71
Hanging or Slow Tasks 76
Hung Tasks vs. Slow Tasks 76
Credential Failed or Network Connection Error Impacting Performance 76
Slow device remediation, EWS Password not verified, ping and SNMP are working fine 78
Performance Impact of Instant-On Remediations 78
Slow performance and reaching max SQL connection pool with Timeouts in HPSM_service.log 80
Upgrade Issues 82
'Invalid Task: No device specified' after upgrading to HPSM 3.7 82
Web page not displayed, hangs, or Invalid Column name error after upgrading to HPSM 3.7 86
T-SQL Execution command line utility has stopped working error 88
Application Error in Event log while executing the InstallSqlScripts 90
HPSM service stops, http Error 503 in browser, and Invalid column error after upgrading 91
Task Error: Internal error in processing when re-running a task after upgrading to HPSM 3.8 and/or unable to complete a new task. 93
Task Error: After upgrading to HPSM 3.10 some tasks end up in Task Error 94
Growing Database and Nightly Maintenance failing (3.6.1 and older) 95
Growing Database and Nightly Maintenance failing (3.7 and newer) 97
Devices tab shows "Loading…" and is not showing any devices or groups after upgrade 98
After upgrading to HPSM 3.8 the Start Time of a newly created task is always showing 12:00AM 99
After upgrading to HPSM 3.10 zero devices are displayed in the UI and the event viewer shows and error with CertExpiryDate in the description and/or Certificate Expiry Date column missing 100
Certificate Installation Failures 103
Certificate installation fails on HP DesignJet Z9 103
Certificate installation issues with Microsoft CA 103
Certificate installation issues with SCEP 106
Workflow for SCEP 106
ASN1 bad tag in HPSM_service.log file using HPSM 3.7.0 or 3.7.1 and Microsoft NDES (SCEP) 107
'Bad Request to the Pki Provider' or Cannot Remediate when using dynamic passwords 108
Microsoft SCEP fails and InternalServerError in Scep.log 112
Sectigo SCEP fails when the intermediate CA certificate is in X.509 format while HPSM 3.8 and older is expecting CMS format 113
Could not retrieve Challenge password from the SCEP Server in Scep.log and questions marks in the logged RESPONSE 114

Could not retrieve Challenge password from the SCEP Server in Scep.log and questions marks in the logged RESPONSE 114
Could not retrieve Challenge password from the SCEP Server in Scep.log and when the challenge password is visible in the SCEP.log 115
Incorrect Certificate Authority Server or CA server down/unreachable 115
Incorrect Certificate Authority Name in policy 117
CA server is configured to require manual approval of the request 117
The Template Name in the policy for the certificate template is incorrect 119
Invalid ID certificate when CRL is unreachable 120
CertificateTask: Task Error (HPSM 3.8) when using RSA with SHA1 Signature 121
CertificateTask: Task Error (HPSM 3.8) when using ECDSA with Key Length P-256 122
HPSM fails to install ID certificate (Cannot Remediate) and access denied in logs, while ID certificate did get issued by CA server 124
CN value lists the IP address of the printer instead of the DNS name 126
Certificate Installation Failures with Zebra devices 127
Cannot Remediate (Required file is not found in the device) 130
Resolving Zebra device certificate issues 131
Miscellaneous 131
HPSM is recommending a firmware downgrade after a firmware assessment of the HP Color LaserJet E55040 131
Exported Reports Are Showing Garbage/Unreadable Text 133
Unable to select a date when creating a task (null visible) 133
Cannot Remediate Web Encryption or Active Ciphers (Invalid input; data value not supported) 134
HPSM always displaying Medium Risk for File Erase Mode on some legacy HP devices, such as HP LaserJet P3010 135
HPSM is unable to communicate over SNMPv3 with some legacy HP Laserjet devices 137
Missing hostname for a device even when nslookup provides a response 139
Column “Certificate Expiry Date” is missing in HPSM UI 140
HPSM_service.log file errors 140
CryptographicException error or ‘Padding is invalid and cannot be removed’ error 140
‘Unable to read table/ when table is empty. Returning empty lists’ error 141
Using Network Traces for Troubleshooting 143
Using Event Viewer for Troubleshooting 143
Appendix A Following a task in HPSM_service.log 144
Appendix B Syntax for installDBrmt.bat (HPSM 3.4 and older) 147
Appendix C Other HP Security Manager Whitepapers and Manuals 148

Overview

HP Security Manager (HPSM) is a security compliance software used to assess and remediate a fleet of devices against a desired security policy. This document provides troubleshooting techniques to use if issues arise when either installing or running HP Security Manager. As with any software, challenges can be presented by servers, operating systems, networks, devices, etc.

Security Manager relies upon Microsoft IIS and SQL Server, both of which can present challenges as well. While this document discusses known issues, new issues are always going to be encountered. Successful troubleshooting always involves removing variables to determine root cause. Internet search also an excellent troubleshooting tool as most errors are generic Microsoft errors and are likely encountered by users of other software.

Log Files and Enabling Debugging

Log files are created during installation or upgrade and when running and using HPSM. By default log level is set to "INFO" or "ERROR". Enabling debug logging is sometimes critical for finding potential issue causes such as hanging or slow tasks.

This next section will show which log locations are available. This will be followed with a section which explains how to change the log levels for the different log files.

and when to change it

HP Security Manager Log Files Locations (HPSM 3.7 and later)

By default there are three directories for a running HPSM installation with the following directories and log files:

```
C:\Program Files (x86)\HP Security Manager\log
```

EapBinding.log
EapDatPerformance.log
EapDeviceLib.log (device communication/configuration issues)
EapMpsBilling.log
EapNetworkLib.log (device communication/configuration issues)
EapResults.log
EapWppClient.log
EapWsEventing.log
Est.log (empty log, use Est.log in HP Security Manager\PkiProviders\log)
Flexera.log (licensing logging)
HPCM.log (contains only information about starting up HPCM component)
HpsmDatTransactions.log
HPSM_Service.log
HPSM_Service_FMEA.log (in beta, logs tasks only since HPSM 3.10)
HPSM_ServiceApp.log
InstantOn.log
MaintenanceTask.log
McoTranslation.log
Qualys.log
Scep.log (empty log, use Scep.log in HP Security Manager\PkiProviders\log)

```
C:\Program Files (x86)\HP Security Manager\WebApp\log
```

HPCM.log (contains only information about UI interaction with HPCM component)
HPSMWeb.log
HPSM_WebAudit.log
Scep.log (empty log, use Scep.log in HP Security Manager\PkiProviders\log)

```
C:\Program Files (x86)\HP Security Manager\PkiProviders\log
```

Est.log
HPCM.log (contains information about assess and remediation tasks for HPCM)
Scep.log

The installation or upgrade process is logged in different log files in the following temp directory:
`C:\Users\"username"\AppData\Local\Temp`[1]

MSIxxxxx.LOG (This file will begin with "MSI" and end with ".LOG" but will contain random characters in the middle as this is produced by the Microsoft Windows installer)
HPSM_Install_log.txt
HPSM_CheckIIS_log.txt (IIS configuration details)
HP_SM_Install_20230531051417.log (YearMonthDayTime)
HP_SM_UnInstall_20230531051632.log (YearMonthDayTime)

[1] When using remote access, the actual files can be in a subdirectory like Temp/1 or Temp/2.

HP Security Manager Log Files Locations (before HPSM 3.7)

Before HPSM 3.7 the word JetAdvantage was part of the installation directory, which resulted in the following directories:

```
C:\Program Files (x86)\HP JetAdvantage Security Manager\log
C:\Program Files (x86)\HP JetAdvantage Security Manager\WebApp\log
C:\Program Files (x86)\HP JetAdvantage Security
Manager\PkiProviders\log
```

HPSM 3.5 and older was using a third service: the HP Print License Service. This service was integrated into the HP Security Manager service in HPSM 3.6. A separate log file for the license server was available in the following location (only used by HPSM 3.5 and older):

```
C:\ProgramData\HP\HP Print License Service Files\HPPLS.log
```

Log file(s) created by FlexeraLicensingService (HPSM 3.5 and older)

```
C:\ProgramData\HP\HP Print License Service Files\Flexera.log
```

Most frequently used log files

For troubleshooting device specific remediation issues the EapDeviceLib.log, EapNetworkLib.log and HPSM_Service.log are needed.
For troubleshooting problems with the nightly maintenance, the MaintenanceTask.log is needed.
For troubleshooting problems with instant on, the InstantOn.log is needed.
For troubleshooting problems with tasks, the HPSM_service.log and eventually the EapDevice.lib.log and EapNetworkLib.log.
For troubleshooting assessment/remediation issues with device certificates the HPCM.logs are needed and eventually the EapDevice.lib.log and EapNetworkLib.log.
For troubleshooting assessment/remediation issues with device certificates using Scep the Scep.log and HPCM.logs are needed and eventually the EapDevice.lib.log and EapNetworkLib.log.
For troubleshooting assessment/remediation issues with device certificates using Est the Est.log and the HPCM.logs are needed and eventually the EapDevice.lib.log and EapNetworkLib.log.

Location and names of configuration files for changing the log level of the different log files

HPSM has different configuration files for changing the log level of the different log files. This section explains which config file has to be edited for the different log files. In the next section a more detailed description of the different log files will be provided.

To enable debugging for non-device specific issues (like problems starting a task, problems starting the service)

```
    C:\Program Files (x86)\HP Security Manager\HPSM_Service.exe.config
```

To enable debugging for issues related to device communication.

```
    C:\Program Files (x86)\HP Security Manager\EapLogConfig.xml
```

Security Manager logs events for who did what and when in two different Audit logs. Log level for this can be changed in the following file:

```
    C:\Program Files (x86)\HP Security Manager\WebApp\Web.config
```

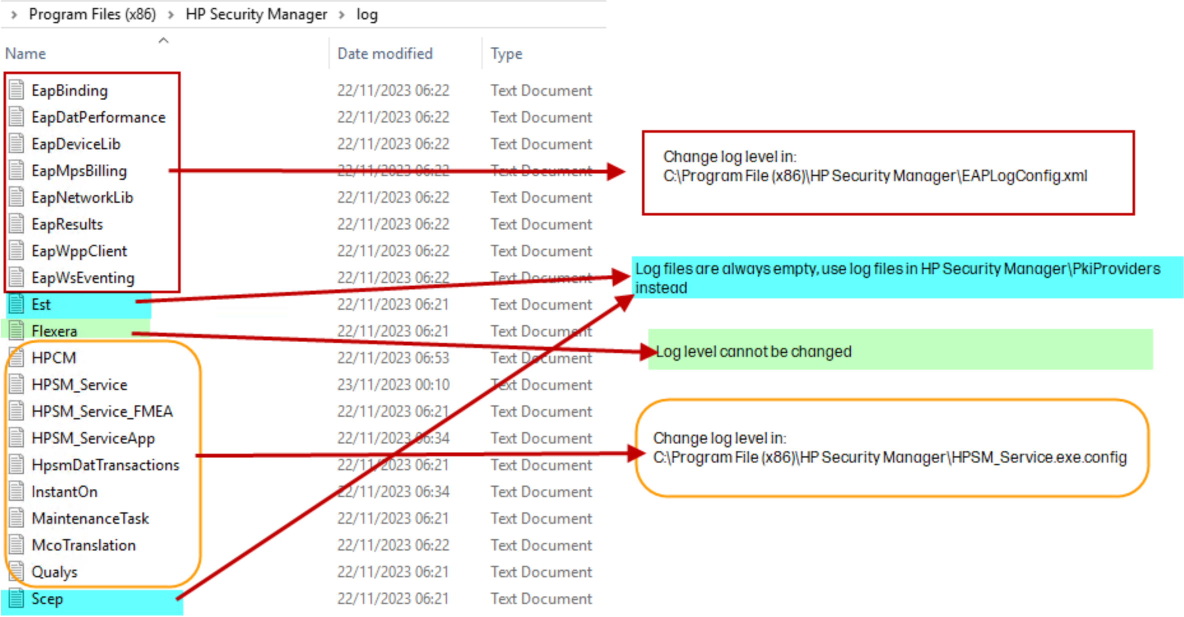
For Certificate remediation with EST, Scep the config level can be changed in the following file:

```
    C:\Program Files (x86)\HP Security Manager\HPSM_Service.exe.config
```

Warning: Making changes in the config level in the following files, will *not* have any impact on the Scep.log and EST.log file in the HP Security Manager\Webapp\log directory as those log files will *always remain empty*.

```
    C:\Program Files (x86)\HP Security Manager\
    WebApp\PkiProviders\HP.HPCM.EstClient.dll.config
    C:\Program Files (x86)\HP Security Manager\
    WebApp\PkiProviders\HP.HPCM.ScepClient.dll.config
```

In the following screenshots of the different directories, you can see in which file the log level for the different log files can be changed.



› Program Files (x86) › HP Security Manager › log

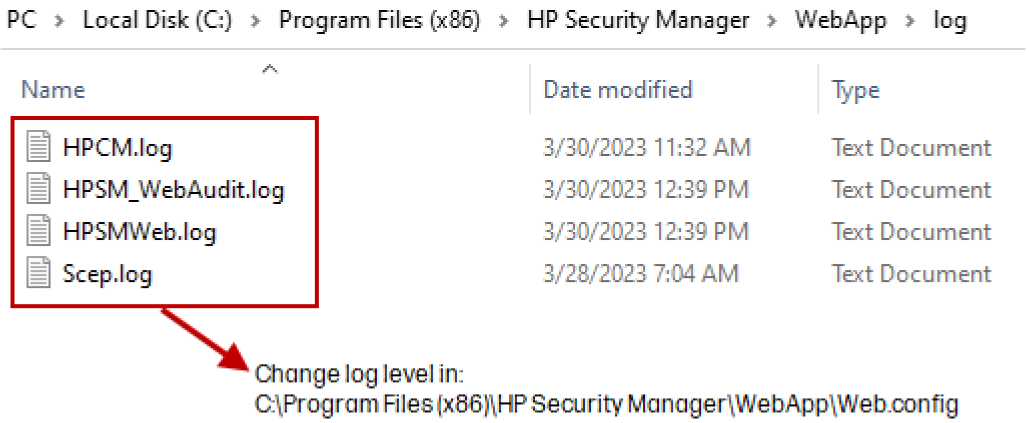
Name	Date modified	Type
EapBinding	22/11/2023 06:22	Text Document
EapDatPerformance	22/11/2023 06:22	Text Document
EapDeviceLib	22/11/2023 06:22	Text Document
EapMpsBilling	22/11/2023 06:22	Text Document
EapNetworkLib	22/11/2023 06:22	Text Document
EapResults	22/11/2023 06:22	Text Document
EapWppClient	22/11/2023 06:22	Text Document
EapWsEventing	22/11/2023 06:22	Text Document
Est	22/11/2023 06:21	Text Document
Flexera	22/11/2023 06:21	Text Document
HPCM	22/11/2023 06:53	Text Document
HPSM_Service	23/11/2023 00:10	Text Document
HPSM_Service_FMEA	22/11/2023 06:21	Text Document
HPSM_ServiceApp	22/11/2023 06:34	Text Document
HpsmDatTransactions	22/11/2023 06:21	Text Document
InstantOn	22/11/2023 06:34	Text Document
MaintenanceTask	22/11/2023 06:21	Text Document
McoTranslation	22/11/2023 06:22	Text Document
Qualys	22/11/2023 06:21	Text Document
Scep	22/11/2023 06:21	Text Document

Change log level in:
C:\Program File (x86)\HP Security Manager\EAPLogConfig.xml

Log files are always empty, use log files in HP Security Manager\PkiProviders instead

Log level cannot be changed

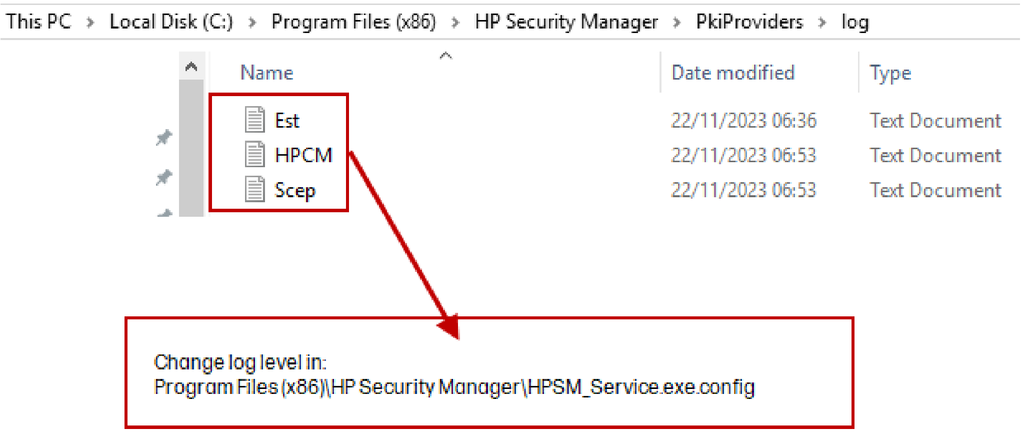
Change log level in:
C:\Program File (x86)\HP Security Manager\HPSM_Service.exe.config



PC > Local Disk (C:) > Program Files (x86) > HP Security Manager > WebApp > log

Name	Date modified	Type
HPCM.log	3/30/2023 11:32 AM	Text Document
HPSM_WebAudit.log	3/30/2023 12:39 PM	Text Document
HPSMWeb.log	3/30/2023 12:39 PM	Text Document
Scep.log	3/28/2023 7:04 AM	Text Document

Change log level in:
C:\Program Files (x86)\HP Security Manager\WebApp\Web.config



This PC > Local Disk (C:) > Program Files (x86) > HP Security Manager > PkiProviders > log

Name	Date modified	Type
Est	22/11/2023 06:36	Text Document
HPCM	22/11/2023 06:53	Text Document
Scep	22/11/2023 06:53	Text Document

Change log level in:
Program Files (x86)\HP Security Manager\HPSM_Service.exe.config

Changing the default log location (including logging into a mapped network drive)

The appender sections in the config files define the details of the log behavior (number of log file, relative , file location, max file size etc. For example for the HPSM_service.log you can find the following configuration for local logging:

```
<appender name="ServerAppender" type="Common.CustomRollingLogAppender,Common">
      <file value="log/HPSM_Service.log" />
      <appendToFile value="true" />
      <staticLogFileName value="true" />
      <immediateFlush value="true" />
      <rollingStyle value="Size" />
      <maxSizeRollBackups value="4" />
      <maximumFileSize value="50MB" />
      <layout type="log4net.Layout.PatternLayout">
           <conversionPattern value="%date %-5level %logger %identity %exception
           [%thread] - %message%newline" />
      </layout>
    </appender>
```

It’s possible to use a mapped network drive for logging, if the account running the HPSM service has full rights on the specified mapped network location. The file value will have to be changed and LockingModel type, and pseudofile with value true will have to be added to the appender configuration. See the following example:

```
<appender name="ServerAppender" type="Common.CustomRollingLogAppender,Common">
      <lockingModel type="log4net.Appender.FileAppender+MinimalLock"/>
      <file value="\\network.server.address\log\HPSM_Service.log" />
      <pseudofile value="true" />
      <staticLogFileName value="true" />
      <immediateFlush value="true" />
      <rollingStyle value="Size" />
      <maxSizeRollBackups value="4" />
      <maximumFileSize value="50MB" />
      <layout type="log4net.Layout.PatternLayout">
           <conversionPattern value="%date %-5level %logger %identity %exception
           [%thread] - %message%newline" />
     </layout>
</appender>
```

Enabling HP Security Manager debugging (service interactions)

To enable debugging for non-device specific issues (like problems starting a task, problems starting the service), edit the following lines in the **HPSM_service.exe.config** file. Make changes highlighted below in yellow and restart the **HP Security Manage**r service:

```
<logger name="NHibernate" additivity="false">
<level value="WARN" />
<appender-ref ref="ServerAppender" />
</logger>
<logger name="NHibernate.Loader.Loader">
<level value="WARN" />
<appender-ref ref="ServerAppender" />
</logger>
<logger name="Assessment">
<level value="DEBUG" />
<appender-ref ref="ServerAppender" />
</logger>
<logger name="Common">
<level value="DEBUG" />
<appender-ref ref="ServerAppender" />
</logger>
<logger name="Data">
<level value="Info" />
<appender-ref ref="ServerAppender" />
</logger>
<logger name="Task">
<level value="DEBUG" />
<appender-ref ref="ServerAppender" />
</logger>
<logger name="Service">
<level value="DEBUG" />
<appender-ref ref="ServerAppender" />
</logger>
<logger name="WCF">
<level value="INFO" />
<appender-ref ref="ServerAppender" />
```

```
</logger>
```

The Data logger (highlighted in green) refers to the interactions between the HPSM service and the SQL database. INFO level for the Data logger is fine for troubleshooting non-database related issues.

HPSM 3.4 introduced auto group policies. To see the order in which tasks are executed in the debug logs, the enableTaskSequencingLogging must be set to true.

```
<add key="enableTaskSequencingLogging" value="true" />
```

NOTE: These additional log settings will only be available if the logger value for the logger name Service is set to DEBUG.

By default, the logs will roll over when they reach 100 MB in size, and each log will only roll over one time before they will start to be deleted in each subsequent rollover. These values can also be configured in each of the configuration files mentioned previously by changing the following entries:

```
<maxSizeRollBackups value="1" />
<maximumFileSize value="100MB" />
```

Enabling HP Security Manager debugging (Instant-On communication)

From HPSM 3.6 onwards the Instant-On announcements and communication will also be logged in a separate log file. The same information will remain in the HPSM_service.log file.

To enable debugging for instant-on specific issues (like problems high instant-on load, slow Instant-On processing, devices not displaying in HPSM), edit the following lines in the **HPSM_service.exe.config** file. Make changes highlighted below in yellow and restart the **HP Security Manage**r service:

```
<logger name="Instant-On">
    <level value="DEBUG" />
    <appender-ref ref="Instant-OnAppender" />
  </logger>
```

Enabling HP Security Manager debugging (device communication issues)

To enable debugging for issues related to device communication, edit the following lines in the **EapLogConfig.xml** file. Make changes highlighted below in yellow and restart the **HP Security Manager** service.

```
<!-- **LOGGER DEFINITIONS FOLLOW**
Logging levels represented in order of increasing priority (e.g., ALL
includes everything below it, but excludes INFO):
   <level value="ALL" />
   <level value="VERBOSE"/>
   <level value="DEBUG" />
   <level value="WARN" />
   <level value="ERROR" />
   <level value="FATAL" />

To turn all logging off use:
   <level value="OFF" />  -->

   <!-- this is the primary log file for the DAT data collector -->
   <logger name="EapDeviceLibrary">
   <level value="DEBUG" />
   <appender-ref ref="EapDeviceLibAppender" />
   </logger>

   <logger name="Binding">
   <level value="INFO" />
   <appender-ref ref="EapDeviceLibAppender" />
   <appender-ref ref="EapBindingAppender" />
   </logger>

   <logger name="Pipeline">
   <level value="DEBUG" />
   <appender-ref ref="EapDeviceLibAppender" />
   </logger>

   <logger name="Results">
   <level value="DEBUG" />
   <appender-ref ref="EapResultsAppender" />
   </logger>

   <!-- ERRORs in this log file are expected, therefore it is off by
   default -->
   <logger name="EapNetworkLib">
   <level value="DEBUG" />
   <appender-ref ref="EapNetworkLibAppender" />
   </logger>

   <logger name="EapMPSBilling">
   <level value="INFO" />
   <appender-ref ref="EapMpsBillingAppender" />
   </logger>

   <logger name="EapWsEventing">
   <level value="INFO" />
```

```
<appender-ref ref="EapWsEventingAppender" />
</logger>

<logger name="McoTranslation">
<level value="ERROR" />
<appender-ref ref="McoTranslationAppender" />
</logger>
```

Brief explanation of the different log files

HPSM includes the following log file types.

- **EapDeviceLibrary -** This log shows general information like DAT version, the values returned from device, which methods will be used, etc.
- **Pipeline -** This log shows the methods (pipelines) to perform different operations. This helps to identify errors/exceptions in pipeline steps.
- **Results** - This gives the names of the config items which are processed.
- **EapNetworkLib** - This log shows the device communications. This helps to identify the retries, timeouts, etc.
- **McoTranslation** - This log file shows methods (pipelines) for custom processes.   This helps to identify errors/exceptions in custom processes. Normally not needed. Only upon request from support team.
- **Bindings** -This log shows which interface of the device has been selected. Normally not needed to enable debug mode for this, only in cases with errors like McoNotFound, McoNotSupported is listed in other log files.

By default, the logs will roll over when they reach 100 MB in size, and each log will only roll over one time before they start to become deleted in each subsequent rollover. These values can also be configured in each of the configuration files mentioned previously by changing the following entries:

```
<maxSizeRollBackups value="1" />
<maximumFileSize value="100MB" />
```

In some situations (upon request from HP support), it might be required to know which information is provided by HPSM to the DAT component within HPSM. This requires changing the log level to DEBUG for the HpsmDatTransaction. Edit the following lines in the **HPSM_service.exe.config** file. Make changes highlighted below in yellow and restart the **HP Security Manage**r service:

```
<logger name="HpsmDatTransaction">
   <level value="DEBUG" />
   <appender-ref ref="HpsmDatTransactionAppender" />
</logger>
```

The corresponding log file HpsmDatTransactions.log will be updated with the internal device transaction details.

Enabling HP Security Manager debugging (Certificate Management)

When HPSM is interacting with a Microsoft (Standalone or Enterprise CA), OpenTrust CA or Symantec CA, it is using the Certificate Management log files (HPCM.log). These log files are in three locations:

```
C:\Program Files (x86)\HP Security Manager\log
C:\Program Files (x86)\HP Security Manager\PkiProviders\log
C:\Program Files (x86)\HP Security Manager\WebApp\log
```

Debug logging for ID Certificate requests can be enabled in two files:

```
C:\Program Files (x86)\HP Security Manager\HPSM_Service.exe.config
C:\Program Files (x86)\HP Security Manager\WebApp\Web.config
```

Note; when using SCEP, EST or OpenTrust separate additional log files are availabled and will have to be configured in debug mode.

Make the following changes highlighted:

```
<logger name="HPCM">
<level value="DEBUG"/>
<appender-ref ref="HPCMAppender"/>
</logger>
```

The changes in the HPSM_Service.config file require a restart of the service HP Security Manager and will enable the debug logging for the HPCM.log file in the following directories:

```
C:\Program Files (x86)\HP Security Manager\log
C:\Program Files (x86)\HP Security Manager\PkiProviders\log
```

The last file will contain information about the interaction with the CA server.
The changes in the Web.config file require a restart of IIS (or recycle the application pool HPSM) and will enable the debug logging for the HPCM.log file in the directory:

```
C:\Program Files (x86)\HP Security Manager\WebApp\log
```

Enabling HP Security Manager debugging Certificate Management: SCEP

SCEP debugging can be enabled in the **HPSM_Service.exe.config** file. Make changes highlighted below in yellow.

```
<logger name="Scep">
<level value="DEBUG" />
<appender-ref ref="ScepAppender" />
</logger>
```

The changes in the **HPSM_Service.config** file require a restart of the service HP Security Manager and will enable the debug logging for the SCEP.log file in the following directories:

```
C:\Program Files (x86)\HP Security Manager\log
C:\Program Files (x86)\HP Security Manager\PkiProviders\log
```

The last file will contain information about the interaction with the SCEP server.

Enabling HP Security Manager debugging Certificate Management: EST

EST debugging can be enabled in the **HPSM_Service.exe.config** file. Make changes highlighted below in yellow.

```
<logger name="Est">
<level value="DEBUG" />
<appender-ref ref="Appender" />
</logger>
```

The changes in the **HPSM_Service.config** file require a restart of the service HP Security Manager and will enable the debug logging for the Est.log file in the following directories:

```
C:\Program Files (x86)\HP Security Manager\log
C:\Program Files (x86)\HP Security Manager\PkiProviders\log
```

NOTE: The EST plug-in is available from HPSM 3.5 onwards.

Enabling logging for Qualys Policy Compliance

HPSM 3.5 offers service integration with Qualys. In Qualys debugging can be enabled in the HPSM_Service.exe.config file. When enabled log entries will be created when printer assessment results are sent to Qualys. Passwords are not transmitted to Qualys, only the password assessment result itself. To enable debugging for the Qualys policy integration, make changes highlighted below in yellow.

```
<logger name="Qualys">
      <level value="Debug" />
      <appender-ref ref="QualysAppender" />
    </logger>
```

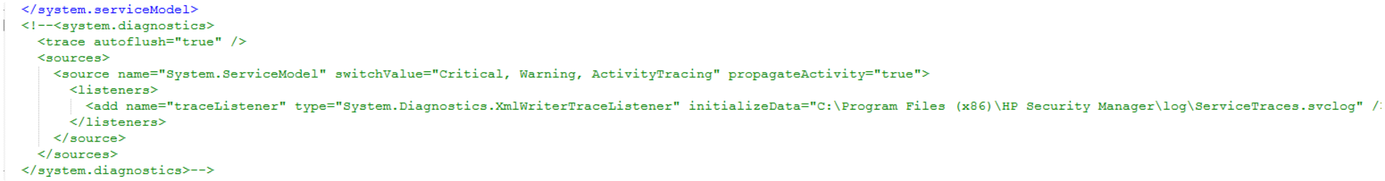
The changes in the HPSM_Service.config file require a restart of the service HP Security Manager and will enable the debug logging for the Qualys.log file in the following directories:

```
C:\Program Files (x86)\HP Security Manager\log
```

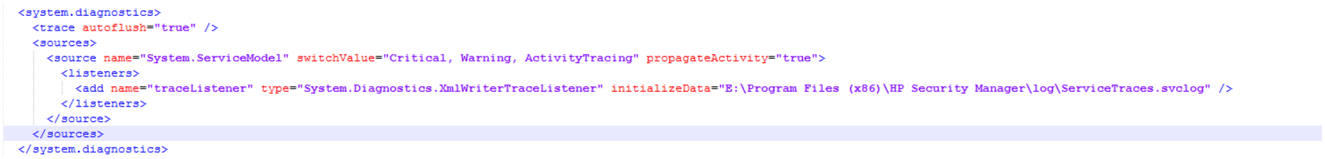
Enabling HPSM app/system diagnostics logging

It’s also possible to add logging on application level. This is normally not needed and therefore commented out by default. To enable app logging you have to make the following changes in the HPSM_service.exe.config file:

1. Add the following line under <appSettings>
   ```
   <add key="log4net.Internal.Debug" value="true"/>
   ```
2. Uncomment the system.diagnostics by removing the <!- - before <system diagnostics> and - -> after </system diagnostics>. See screenshot of this section (default value on top) and uncommented version on the bottom.



```
</system.serviceModel>
<!--<system.diagnostics>
  <trace autoflush="true" />
  <sources>
    <source name="System.ServiceModel" switchValue="Critical, Warning, ActivityTracing" propagateActivity="true">
      <listeners>
        <add name="traceListener" type="System.Diagnostics.XmlWriterTraceListener" initializeData="C:\Program Files (x86)\HP Security Manager\log\ServiceTraces.svclog" /
      </listeners>
    </source>
  </sources>
</system.diagnostics>-->
```



```
<system.diagnostics>
  <trace autoflush="true" />
  <sources>
    <source name="System.ServiceModel" switchValue="Critical, Warning, ActivityTracing" propagateActivity="true">
      <listeners>
        <add name="traceListener" type="System.Diagnostics.XmlWriterTraceListener" initializeData="E:\Program Files (x86)\HP Security Manager\log\ServiceTraces.svclog" />
      </listeners>
    </source>
  </sources>
</system.diagnostics>
```

Audit log files

Besides the debugging log files, Security Manager logs events for who did what and when in two different Audit logs:

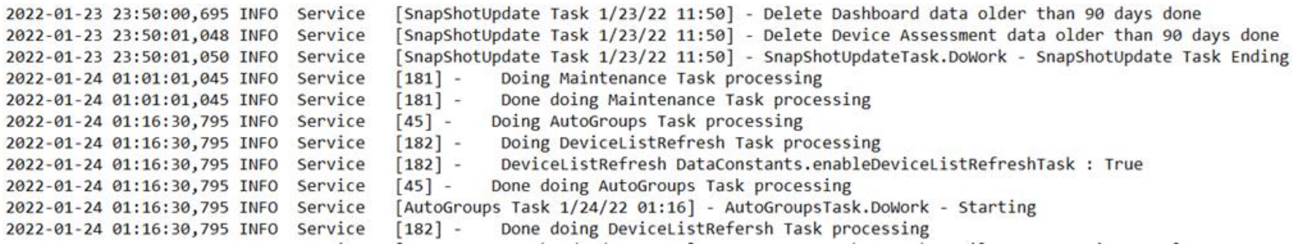
C:|Program Files (x86)|HP Security Manager|
WebApp\log\HPSM_WebAudit.log
This file will have events that are triggered from the user.

C:|Program Files (x86)|HP Security Manager|log|
HPSM_ServiceApp.log
This file contains events about stopping/starting service and license limitations.

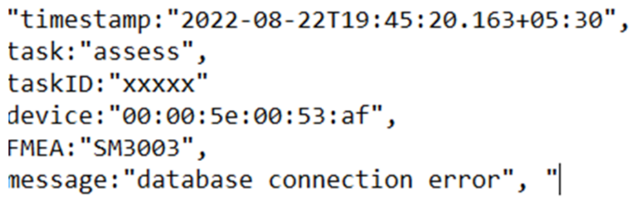
This file will have events that are triggered from HPSM service. An explanation of entries in those log files, can be found in the whitepaper Reporting, Email Alert Subscriptions & Remediation Summary, Auditing & Syslog Functionality under the section HPSM User Activity Logging (Auditing)

Enabling FMEA (Failure Mode and Effect Analysis) logging

In HPSM 3.10 a new log file was added: Fmea.log. Currently it’s in beta, disabled by default and if enabled only logging tasks. The intention of this log file is to provide structured log files. Structured logs will be in the form of key-value pair so that the logs can be easily traced via log management solutions like Splunk. This means that logs will be represented in a completely different way. Example:



```
2022-01-23 23:50:00,695 INFO  Service   [SnapShotUpdate Task 1/23/22 11:50] - Delete Dashboard data older than 90 days done
2022-01-23 23:50:01,048 INFO  Service   [SnapShotUpdate Task 1/23/22 11:50] - Delete Device Assessment data older than 90 days done
2022-01-23 23:50:01,050 INFO  Service   [SnapShotUpdate Task 1/23/22 11:50] - SnapShotUpdateTask.DoWork - SnapShotUpdate Task Ending
2022-01-24 01:01:01,045 INFO  Service   [181] -    Doing Maintenance Task processing
2022-01-24 01:01:01,045 INFO  Service   [181] -    Done doing Maintenance Task processing
2022-01-24 01:16:30,795 INFO  Service   [45] -    Doing AutoGroups Task processing
2022-01-24 01:16:30,795 INFO  Service   [182] -    Doing DeviceListRefresh Task processing
2022-01-24 01:16:30,795 INFO  Service   [182] -    DeviceListRefresh DataConstants.enableDeviceListRefreshTask : True
2022-01-24 01:16:30,795 INFO  Service   [45] -    Done doing AutoGroups Task processing
2022-01-24 01:16:30,795 INFO  Service   [AutoGroups Task 1/24/22 01:16] - AutoGroupsTask.DoWork - Starting
2022-01-24 01:16:30,795 INFO  Service   [182] -    Done doing DeviceListRefersh Task processing
```



```
"timestamp:"2022-08-22T19:45:20.163+05:30",
task:"assess",
taskID:"xxxxx"
device:"00:00:5e:00:53:af",
FMEA:"SM3003",
message:"database connection error", "
```

In order to quickly locate the errors and provide recovery mechanism its important to have FMEA matrix and appropriate error codes logged.
The different error codes will be developed overtime and provided.
In the previous example the code is SM3003, and SM3xxxx means instant-on discovery logging.

By default this logging is fully disabled. To enable it, change the value for enableStructLogs from false to true in the **HPSM_service.exe.config** file.

```
  <!--enableStructLogs: If set, additional structured and FMEA logs are
generated-->
    <add key="enableStructLogs" value="false" />
```

If you also want to have debug FMEA log entries, you have to change the FMEA appender to DEBUG in the **HPSM_service.exe.config** file.

```
    <logger name="Fmea">
      <level value="INFO" />
      <appender-ref ref="FmeaAppender" />
    </logger>
```

After making above changes, restart the HPSM service.

Enabling HP Print License Service debugging (HPSM 3.5 and older)

To enable debugging for the HP Print License Service, edit the following lines in the HP.Print.License.Host.WindowsService.exe.config file in the following directory:

```
C:\Program Files (x86)\HP JetAdvantage Security Manager\HP Print License
Service
```

Make changes highlighted below in yellow, then stop the service **HP JetAdvantage Security Manage**r and then stop the **HP Print License Service**. Restart first the **HP Print License Service** and after that restart the service **HP JetAdvantage Security Manager**.

```
<log4net>
    <appender name="FileAppender"
type="log4net.Appender.RollingFileAppender">
      <param name="File" value="C:\ProgramData\HP\HP Print License
Service\HPPLS.log" />
<param name="AppendToFile" value="true" />
<rollingStyle value="Size" />
<maxSizeRollBackups value="10" />
<maximumFileSize value="10000KB" />
<layout type="log4net.Layout.PatternLayout">
<param name="ConversionPattern" value="%d [%t] %-2p %c - %m%n"
/>
</layout>
</appender>
<root>
<!--Possible value for level 1.ALL
                           2.DEBUG
                           3.INFO
                           4.WARN
                           5.ERROR
                           6.FATAL
                           7.OFF
-->
<level value="DEBUG" />
<appender-ref ref="FileAppender" />
</root>
</log4net>
```

Required Network Ports

If a firewall is installed on the computer on which the Security Manager service runs, and the service will be accessed from the user interface on a remote computer, the firewall must be set to allow access to the service.

The older Security Manager service listens on port 8002, which must be opened in the firewall to allow remote access to the service. The new browser-based interface listens on port 7637 be default. If you do not want to allow remote access to the Security Manager web service for either version, then you can block the respective ports with a firewall.

The following tables list the ports used by HP Security Manager.

Client to Server ports

Port	Protocol	Service	Notes
7637 (version 3.0+)	TCP	HTTPS	Port set during installation to be used to secure data between client and HPSM server via browser. This port may be changed to something else by editing bindings for the HPSM web site under IIS Manager. HPSM versions 3.0 and beyond.
8002 (version 2.1.5-)	TCP	WCF-NET.TCP	WCF with message encryption - port used from a remote client interface to the Security Center service. HPSM versions 2.1.5 and prior.

Server to Device ports and to hp.com (for firmware assessments)

Port	Protocol	Service	Notes
80 and 8080	TCP	HTTP	Port used for HTTP communication to devices only when SSL is not supported on the device. Also used to gather the latest firmware versions from the web if firmware assessments are enabled and configured to dynamically retrieve from web.
443	TCP	HTTPS	Port used for secure HTTP communication to devices, HTTP Web over SSL.
N/A	ICMP	PING	Internet Control Message Protocol - port used to check if node is active.
161	UDP	SNMP	Simple Network Management Protocol - port used for many configuration items on devices as well as discovery of devices.
7627	TCP	SOAP-HTTP	Web service port used to manage communications on HP FutureSmart devices.

Devices to Server ports

Port	Protocol	Service	Notes
3329	TCP	HP Instant-On Security	Secure port (uses SSL) used from the device to the Security Manager service for Instant-On discovered devices.

Server to SQL database ports

Port	Protocol	Service	Notes
1433	TCP	MS SQL	Standard DB Connection - port used from the Security Manager service to a remote SQL database with a default instance. Can be customized in a configuration file.
1434	UDP	MS SQL Browser service	Standard connection to SQL browser service to retrieve the TCP port for the named SQL instance
dynamic	TCP	MS SQL	Standard DB connection to a named SQL instance using dynamic ports

Server to Email ports

Port	Protocol	Service	Notes
25	SMTP	Simple Mail Transfer Protocol	Typical port used for communication to mail server if Automated Output feature is enabled. Port can be customized under File, Settings, Automated Output.

Server to Certificate Authority ports

Port	Protocol	Service	Notes
135	TCP	DCOM/RPC	Certificate management - port used between Security Manager service and CA server.
Random allocated high TCP ports above 1024	TCP	DCOM/RPC	Certificate management - port used between Security Manager service and CA server.

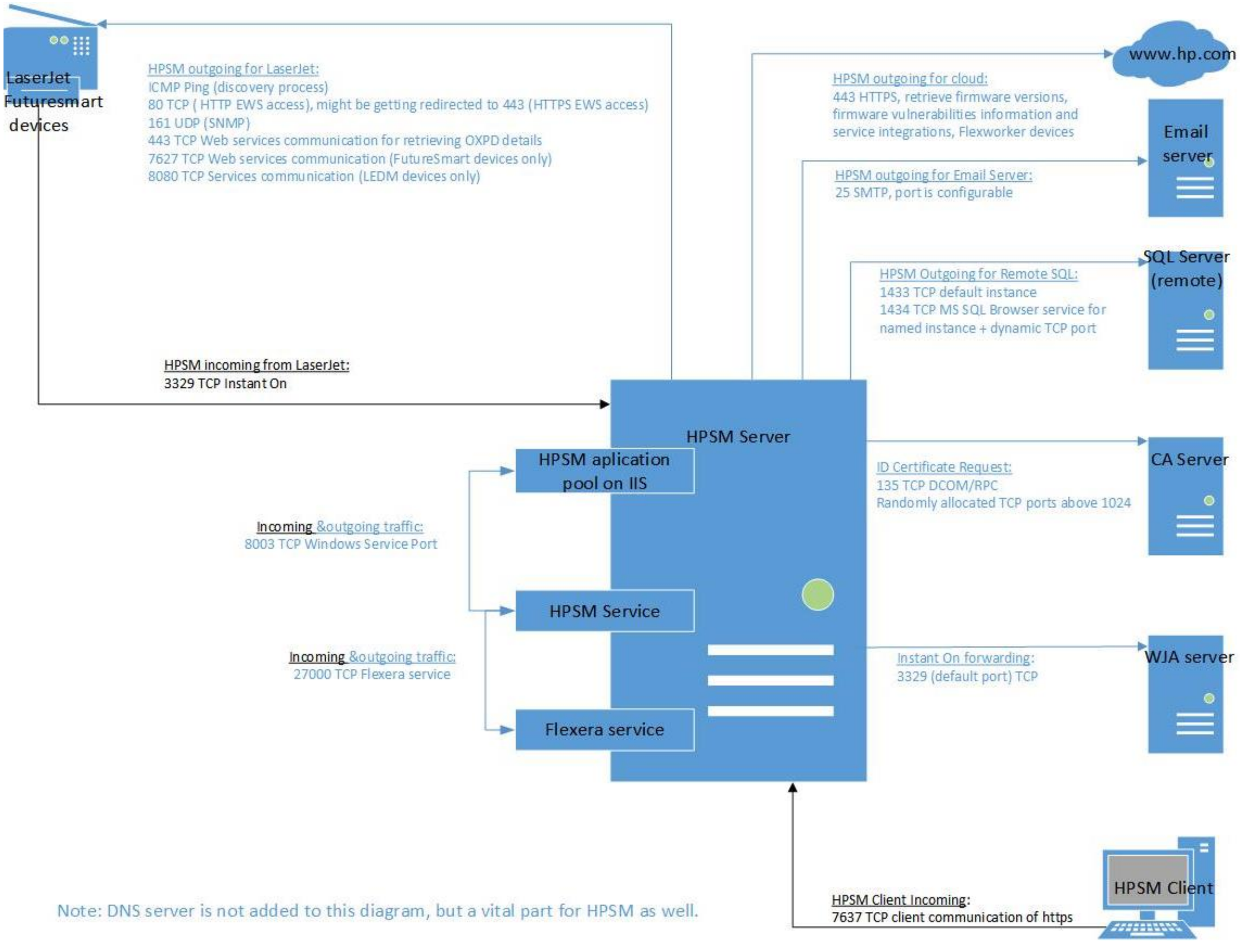
Licensing ports

Port	Protocol	Service	Notes
7000	TCP	HP Print License Service	Licensing heartbeat – Heartbeat port used between the Security Manager service and the HP Print License service. This is the communication between two services on the same machine and needs to be open on the incoming and outgoing port (HPSM 3.5 and older)
8888	TCP	HP Print License Service	Licensing - port used between the Security Manager service and the HP Print License service. This is the communication between two services on the same machine and needs to be open on the incoming and outgoing port (HPSM 3.5 and older)
27000	TCP	Flexera service	Licensing - port used by the Flexera service (lmgrd.exe). This port is used to communicate between the FlexeraLicensingService and the HP Print License Service. These two services reside on the same machine and therefore this port needs to be open for incoming and outgoing communication.

HPSM application pool to Server ports

Port	Protocol	Service	Notes
8003	TCP	HPSM Windows Service Port	Communication between HPSM application pool and HPSM service.

Ports Diagram


LaserJet Futuresmart devices
HPSM outgoing for LaserJet:
ICMP Ping (discovery process)
80 TCP (HTTP EWS access), might be getting redirected to 443 (HTTPS EWS access)
161 UDP (SNMP)
443 TCP Web services communication for retrieving OXPD details
7627 TCP Web services communication (FutureSmart devices only)
8080 TCP Services communication (LEDM devices only)
HPSM incoming from LaserJet:
3329 TCP Instant On
www.hp.com
HPSM outgoing for cloud:
443 HTTPS, retrieve firmware versions, firmware vulnerabilities information and service integrations, Flexworker devices
Email server
HPSM outgoing for Email Server:
25 SMTP, port is configurable
SQL Server (remote)
HPSM Outgoing for Remote SQL:
1433 TCP default instance
1434 TCP MS SQL Browser service for named instance + dynamic TCP port
HPSM Server
HPSM aplication pool on IIS
Incoming &outgoing traffic:
8003 TCP Windows Service Port
HPSM Service
Incoming &outgoing traffic:
27000 TCP Flexera service
Flexera service
CA Server
ID Certificate Request:
135 TCP DCOM/RPC
Randomly allocated TCP ports above 1024
WJA server
Instant On forwarding:
3329 (default port) TCP
HPSM Client
HPSM Client Incoming:
7637 TCP client communication of https

Note: DNS server is not added to this diagram, but a vital part for HPSM as well.

Changing Firewall Settings and Testing Open Ports

When configuring firewalls, an administrator can either open ports used by the application (see the tables in *Required Network Ports*) or allow certain program executables access through the firewall. For the latter, Security Manager includes two separate services represented by three executables:

C:|Program Files (x86)|HP Security Manager|HPSM_Service.exe
C:|Program Files (x86)|HP Security Manager|HPQ.exe
C:|Program Files (x86)|HP Security Manager|Imgrd.exe

Security Manager primarily uses the following ports to communicate to devices:

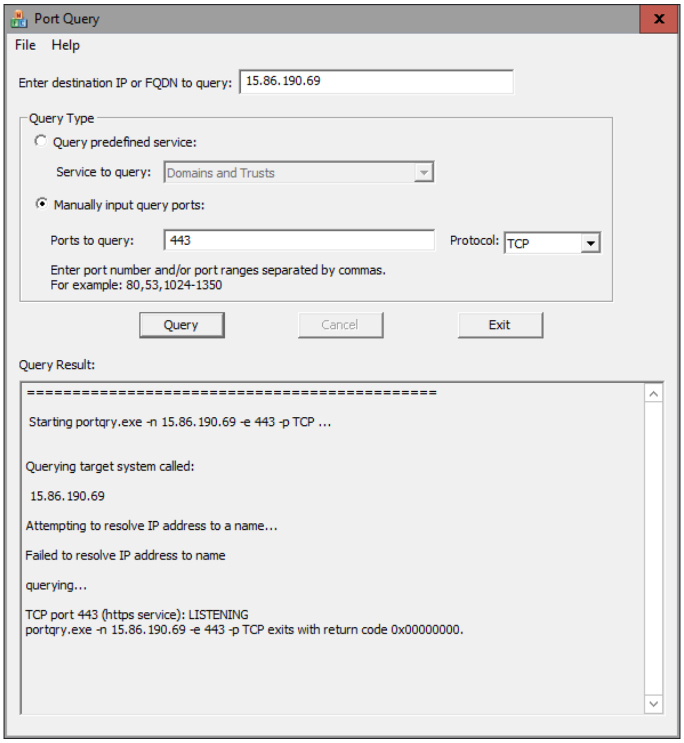
- 80 – used for non-encrypted HTTP traffic to device
- 161 – SNMP traffic to device
- 443 – encrypted traffic to device
- 7627 – web services traffic to device

HPSM 3.5 and older also uses the following executable:
C:|Program Files (x86)|HP JetAdvantage Security Manager|HP Print
License Service\HP.Print.License.Host.WindowsService.exe

Therefore, these ports need to be open for Security Manager to effectively manage devices. Security Manager and Web Jetadmin are very similar in how they communicate to devices. If Web Jetadmin is managing devices fine without credential failures and you are certain Security Manager has matching credentials in its Credential Store, as a test you might install Security Manager on the same machine as Web Jetadmin to determine if port issues exist on the Security Manager server.

PortQry, a free Microsoft utility, can also be used to determine if ports are open between the Security Manager server and the device. The Port Query user interface tool makes it easy to quickly enter an IP Address for a printer and the port to be queried.

Results will be displayed whether the port is Listening or Not Listening.



Enter destination IP or FQDN to query: 15.86.190.69

Query Type

○ Query predefined service:

Service to query: Domains and Trusts

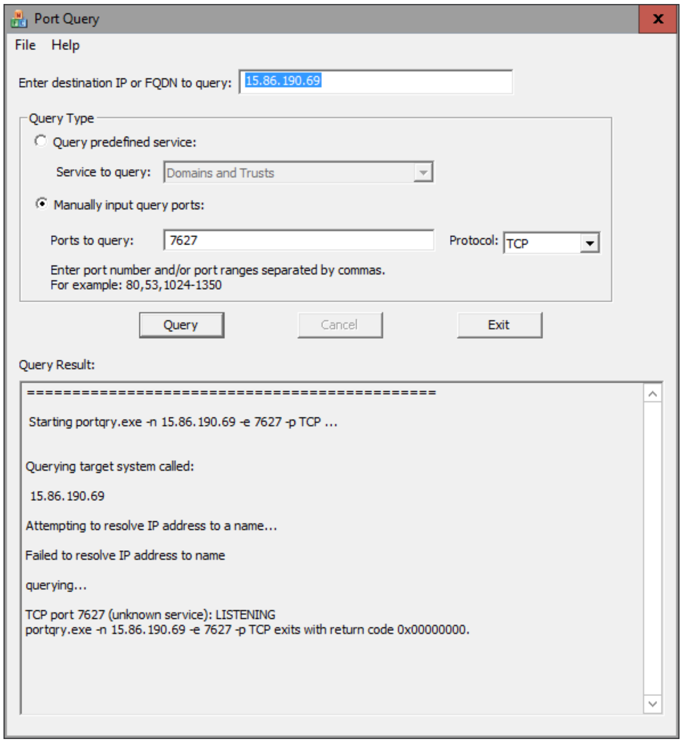
● Manually input query ports:

Ports to query: 443 Protocol: TCP

Enter port number and/or port ranges separated by commas.
For example: 80,53,1024-1350

Query Result:

```
=============================================

 Starting portqry.exe -n 15.86.190.69 -e 443 -p TCP ...


Querying target system called:

 15.86.190.69

Attempting to resolve IP address to a name...

Failed to resolve IP address to name

querying...

TCP port 443 (https service): LISTENING
portqry.exe -n 15.86.190.69 -e 443 -p TCP exits with return code 0x00000000.
```



Enter destination IP or FQDN to query: 15.86.190.69

Query Type

○ Query predefined service:

Service to query: Domains and Trusts

● Manually input query ports:

Ports to query: 7627 Protocol: TCP

Enter port number and/or port ranges separated by commas.
For example: 80,53,1024-1350

Query Result:

```
=============================================

 Starting portqry.exe -n 15.86.190.69 -e 7627 -p TCP ...


Querying target system called:

 15.86.190.69

Attempting to resolve IP address to a name...

Failed to resolve IP address to name

querying...

TCP port 7627 (unknown service): LISTENING
portqry.exe -n 15.86.190.69 -e 7627 -p TCP exits with return code 0x00000000.
```

Proxy for Network Service Blocking Communication

Security Manager runs under the Network Service account be default. It is possible that Network Service has been configured to use a proxy. If Security Manager reports credential failures on the fleet when no passwords are present on the fleet, it is possible a proxy is blocking the ability for Security Manager to query the pages it requires from the device to determine if an Admin Password is set for the Embedded Web Server (EWS).

A utility named bitsadmin can be used to determine if a proxy is present on local service accounts and can clear these settings. Try the following command to determine if network Service is using a proxy:

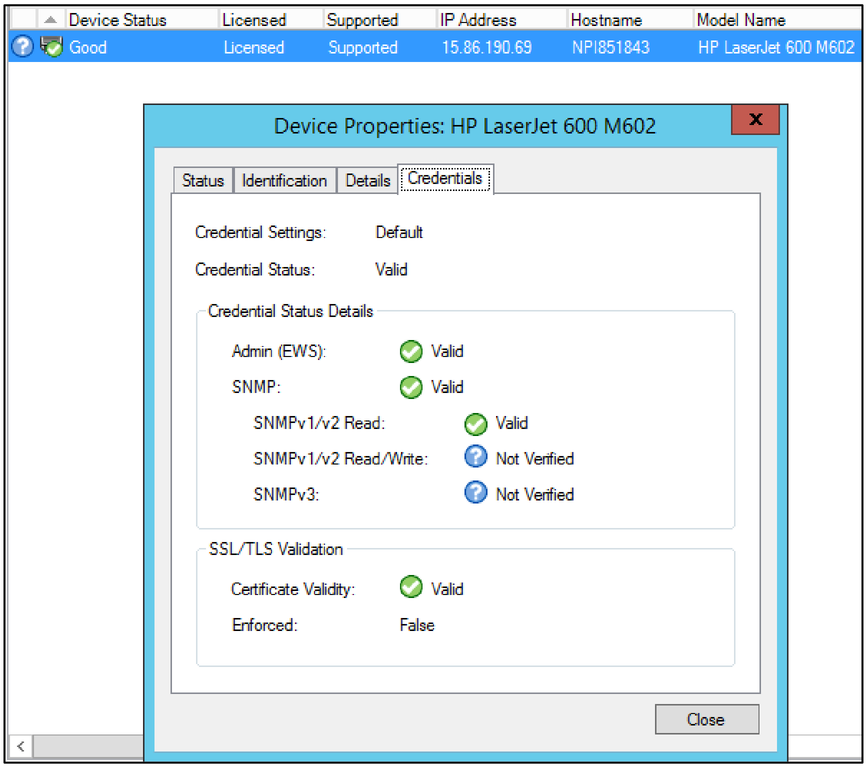
```
Bitsadmin /util /getieproxy networkservice
```

Possible values include:

- NO_PROXY—Do not use a proxy server.
- AUTODETECT—Automatically detect the proxy settings.
- MANUAL_PROXY—Use an explicit proxy list and bypass list. Specify the proxy list and bypass list immediately following the usage tag. For example, MANUAL_PROXY proxy1,proxy2 NULL.

If the command returns MANUAL_PROXY or AUTODETECT, try setting Network Service to run without a proxy by typing the following command:

```
Bitsadmin /util /setieproxy networkservice NO_PROXY
```



Device Status	Licensed	Supported	IP Address	Hostname	Model Name
Good	Licensed	Supported	15.86.190.69	NPI851843	HP LaserJet 600 M602

Device Properties: HP LaserJet 600 M602

Credential Settings: Default

Credential Status: Valid

Credential Status Details

Admin (EWS): ✓ Valid

SNMP: ✓ Valid

SNMPv1/v2 Read: ✓ Valid

SNMPv1/v2 Read/Write: ? Not Verified

SNMPv3: ? Not Verified

SSL/TLS Validation

Certificate Validity: ✓ Valid

Enforced: False

Installation Issues

Security Manager uses the Microsoft installer for installing and upgrading the software. If anything goes wrong during installation, the logs file for the installation attempt may provide some clues.

For proper Security Manager installation and operation, specific Microsoft software must be present. The requirements are listed in the install and setup guide.

If these are not present on the system, the installation process installs some of the required software. The installer checks for the presence of IIS and attempts to enable it and necessary configuration elements if not present. The installer also provides an option to install SQL Express if desired or to use an existing SQL server location. It launches a series of SQL scripts to ensure the database is at the current schema version to match the software version. Proper permissions need to be present for the user running the upgrade on the SQL database for the installer to upgrade the database.

Common SQL issues

By far the most common reason an installation goes awry is related to SQL issues. Whether using local or remote SQL Server, Express or Full, the rules are essentially the same. In every case, Security Manager needs access to a SQL server instance. It can either create a new database, upgrade an existing database, or attach to an existing database, depending upon the situation and the user rights. If Security Manager is instructed to install SQL Express on the local machine, a SQL instance and database for Security Manager will be created by the Security Manager installer. If Security Manager is pointed to an existing local or remote SQL server and instance during installation, proper rights must be present for the user running the installation to be able to create or update a SQL database wherever SQL server may reside. Proper rights must also exist on the database itself for the user which the Security Manager service runs under to be able to read from and write to the database.

TIP: When installing and upgrading Security Manager, by default the user permissions of the user who is logged into the machine and running the installer executable will be used and must have proper rights on the SQL server to either create a database or update an existing database. All the installer does is run SQL scripts to create or alter a database, and naturally any user running those commands needs to have proper SQL rights. In this case it is the Windows user who is running the installer. During the installation it is possible to select a different windows user for installing/upgrading the database.

Creating a database requires Create database rights on the SQL instance. Upgrading an existing database requires DBO rights on the database. For normal operation of Security Manager after installation, the user running the Security Manager service (default as Network Service) needs to have permissions to at least read and write to the database, DBO rights preferred.

Each Security Manager installation must point to its own unique database, multiple installations cannot share a database. The instance can be named or default, and the instance can have as many databases as possible including a Web Jetadmin database. Several techniques are available to allow Security Manager to install/use a SQL database in any location.

There are three scenarios where Security Manager will interact with Microsoft SQL:

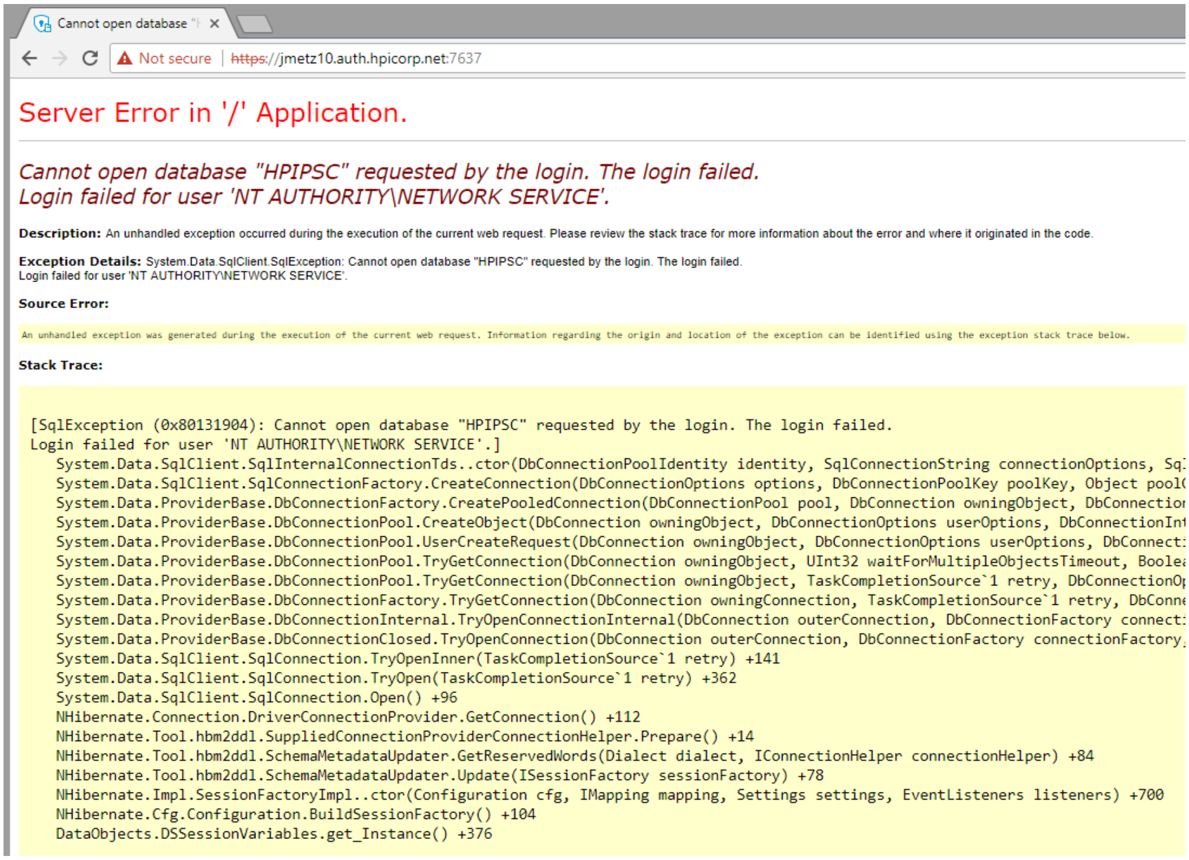
- Creating a database during installation of Security Manager
- Upgrading a database during upgrading of Security Manager from one version to another
- Running Security Manager to manage security features on a fleet of devices

Each scenario requires a different set of SQL rights for potentially different users.

- **Create Database** – Windows user running the installer executable needs at minimum Create Database rights on the SQL instance. SA rights would certainly work.
- **Upgrade Database** – Windows user running the installer executable to upgrade versions needs DBO rights on the database to perform potential commands on the database such as insert, update, alter, create table.
- **Run Security Manager** – the Windows account that runs the Security Manager service (default of Network Service) needs DBO rights on the database to perform operations such as reading and writing.
  NOTE: The "HP Security - Using SQL Server" whitepaper explains how to run with less rights or a different account if desired.

The first sign of trouble if something goes wrong might be an error when launching Security Manager that indicates the SQL database cannot be opened.

In the following error, the message indicates that Windows Authentication is attempting to login the user the Security Manager runs under (Network Service in this case) into the correct remote server\instance name but is being rejected.



Server Error in '/' Application.

Cannot open database "HPIPSC" requested by the login. The login failed.
Login failed for user 'NT AUTHORITY\NETWORK SERVICE'.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Cannot open database "HPIPSC" requested by the login. The login failed.
Login failed for user 'NT AUTHORITY\NETWORK SERVICE'.

Source Error:

```
An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.
```

Stack Trace:

```
[SqlException (0x80131904): Cannot open database "HPIPSC" requested by the login. The login failed.
Login failed for user 'NT AUTHORITY\NETWORK SERVICE'.]
   System.Data.SqlClient.SqlInternalConnectionTds..ctor(DbConnectionPoolIdentity identity, SqlConnectionString connectionOptions, Sq
   System.Data.SqlClient.SqlConnectionFactory.CreateConnection(DbConnectionOptions options, DbConnectionPoolKey poolKey, Object pool
   System.Data.ProviderBase.DbConnectionFactory.CreatePooledConnection(DbConnectionPool pool, DbConnection owningObject, DbConnectio
   System.Data.ProviderBase.DbConnectionPool.CreateObject(DbConnection owningObject, DbConnectionOptions userOptions, DbConnectionIn
   System.Data.ProviderBase.DbConnectionPool.UserCreateRequest(DbConnection owningObject, DbConnectionOptions userOptions, DbConnect
   System.Data.ProviderBase.DbConnectionPool.TryGetConnection(DbConnection owningObject, UInt32 waitForMultipleObjectsTimeout, Boole
   System.Data.ProviderBase.DbConnectionPool.TryGetConnection(DbConnection owningObject, TaskCompletionSource`1 retry, DbConnectionO
   System.Data.ProviderBase.DbConnectionFactory.TryGetConnection(DbConnection owningConnection, TaskCompletionSource`1 retry, DbConne
   System.Data.ProviderBase.DbConnectionInternal.TryOpenConnectionInternal(DbConnection outerConnection, DbConnectionFactory connect
   System.Data.ProviderBase.DbConnectionClosed.TryOpenConnection(DbConnection outerConnection, DbConnectionFactory connectionFactory
   System.Data.SqlClient.SqlConnection.TryOpenInner(TaskCompletionSource`1 retry) +141
   System.Data.SqlClient.SqlConnection.TryOpen(TaskCompletionSource`1 retry) +362
   System.Data.SqlClient.SqlConnection.Open() +96
   NHibernate.Connection.DriverConnectionProvider.GetConnection() +112
   NHibernate.Tool.hbm2ddl.SuppliedConnectionProviderConnectionHelper.Prepare() +14
   NHibernate.Tool.hbm2ddl.SchemaMetadataUpdater.GetReservedWords(Dialect dialect, IConnectionHelper connectionHelper) +84
   NHibernate.Tool.hbm2ddl.SchemaMetadataUpdater.Update(ISessionFactory sessionFactory) +78
   NHibernate.Impl.SessionFactoryImpl..ctor(Configuration cfg, IMapping mapping, Settings settings, EventListeners listeners) +700
   NHibernate.Cfg.Configuration.BuildSessionFactory() +104
   DataObjects.DSSessionVariables.get_Instance() +376
```

Use the following log file to find potential causes:

C:|Program Files (x86)|HP Security Manager|log|HPSM_Service.log

A successful login attempt will display the server\instance, database name, database version and Security manager version:

```
2018-01-11 11:31:29,338 INFO  Service   [4] - TaskSupervisor.Init - HPSM Starting

2018-01-11 11:31:41,427 INFO  Service   [4] - Successfully started DSSessionVariables() -
hibernate  session

2018-01-11 11:31:41,430 INFO  Service   [4] - ScheduleTaskManager.RetryDBConnection Testing
DB   connection to: Server=(local)\EXP2014;initial catalog=HPIPSC;Integrated Security=SSPI;

2018-01-11 11:31:41,437 INFO  Service   [4] -  - Done TestDBConnection

2018-01-11 11:31:41,437 INFO  Service   [4] - ScheduleTaskManager.RetryDBConnection Testing
DB   connection successfull to: Server=(local)\EXP2014;initial catalog=HPIPSC;Integrated
Security=SSPI;

2018-01-11 11:31:41,593 INFO  Service   [4] - Service Starting up - Init()

2018-01-11 11:31:42,571 INFO  Service   [4] - Service Version:

3.1.0.65238

2018-01-11 11:31:42,594 INFO  Service   [4] - Shrinking the DB log file
```

This would happen if Network Service did not have DBO rights to use the database. Use SQL Management Studio to confirm the user running the Security Manager service has DBO rights.

Also, make sure the Security Manager service was restarted after making the changes to the database rights.

Ensure the **HPSM_Service.exe.config** file contains the correct entries:

- The server or instance name is not correct. Double-check the spelling of each.
- It is possible network related issues are preventing the connection to the remote instance. Common troubleshooting steps include:
- Fully qualify the remote SQL server name in the configuration file if name resolution issues are present or use the IP address instead of the hostname.
- TCP/IP must be enabled on the remote SQL server instance. Use SQL Server Configuration Manager to confirm.
- Check firewall settings to ensure the port that is used for the remote connection is open. The default port is 1433.
- SQL Server may default to using a dynamic port. Either configure to use a fixed port or start the SQL Browser service to allow for remote connections.
- Use SQL Management Studio and/or Windows ODBC to connect to the remote SQL server/instance from the same machine as Security Manager to at least prove a Windows user account can access the server/instance from the Security Manager machine.
- If the HPSM_Service.log indicates table columns are missing, the database may not have been upgraded due to insufficient rights by the user running the upgrade. This scenario is described previously in this document with steps on how to uninstall/reinstall to rectify.
- The database tables should always begin with DBO as the schema i.e., DBO.DeviceTable.

If some of the tables begin with a Windows username as the schema, it is very likely that the user who upgraded or created the database was a member of a Windows group when assigned SQL rights.

The default schema for a user can be defined by using the DEFAULT_SCHEMA option of CREATE USER or ALTER USER. If no default schema is defined for a user account, SQL Server will assume DBO is the default schema.

IMPORTANT: If the user is authenticated by SQL Server as a member of a group in the Windows operating system, no default schema will be associated with the user. If the user creates an object, a new schema will be created and named the same as the user, and the object will be associated with that user schema. The fix to this scenario is to either rename the schema in the affected tables to indicate DBO, or better yet, assign a default schema of DBO to the Windows group to which the user belongs.

Database Upgrade Failure

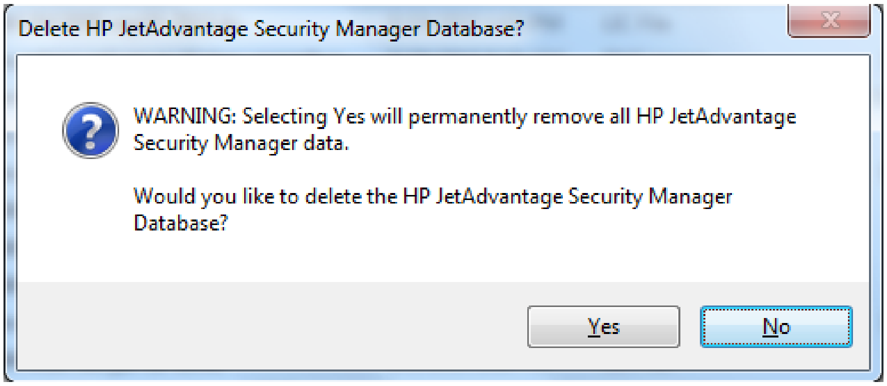
A very common scenario involves the installer completing the installation, but improper rights were present on the account running the installer to upgrade the SQL database tables. When this happens, you have a new Security Manager version trying to use older SQL tables. The log files are filled with statements indication tables and/or columns are missing the database.

Two options exist in the case:

- Roll back to the previous version
- Attempt to repair the database to match the Security manager version

To roll back to the previous version, follow these steps:

1. Under Programs and Features, uninstall Security Manager and when asked if you would like to delete the database, select **No**.



Delete HP JetAdvantage Security Manager Database?

WARNING: Selecting Yes will permanently remove all HP JetAdvantage Security Manager data.

Would you like to delete the HP JetAdvantage Security Manager Database?

2. Finish the uninstall and when prompted, keep the license files intact.
3. Install the previous version, pointing to the remote server\instance where the database still resides.
   NOTE: Since the database was never upgraded when Security Manager was upgraded earlier, it should still match the previous Security manager version and work fine with it.
4. Make sure the proper rights/permissions are in place before attempting the upgrade again.

Using SQL script to repair/upgrade/install the database

SQL scripts are also available that can repair the database and upgrade it to match the Security manager version to update the database. This is certainly a much faster resolution to the problem. The scripts are installed with HPSM (InstallSqlScripts.zip in the following directory:

C:|Program Files (x86)|HP Security Manager)

The scripts can be run by someone such as the DBA who has proper rights to upgrade the database.

The SQL scripts are run manually from a command prompt. They essentially mimic the SQL files the installer runs when "install a new or update an existing database" is selected.

The script is launched by executing a batch file named InstallOrUPgradeRemoteDb.bat. The zip file contains a Readme called **Readme_InstallSQLscripts.txt** with explanation and syntax of the SQL scripts.

NOTE: Before HPSM 3.5 the script was called InstallDBrmt.bat and did not have an option to specify the databasename. The syntax for the installDBrmt.bat script is explained in Appendix B.

When you run the SQL scripts from a command line, you must use the proper syntax It will not tell you if your syntax is bad, but the log files that are created in the folder where you ran the scripts will be full of errors if the syntax is bad.

If you use bad syntaxes, the command line will display as if it is creating tables. It is not. Log files are created in the same folder containing the scripts. The logs will be filled with errors if permissions are not correct or improper syntax was used.

The script first looks to see if the database is present. If not present, the script will create the database if the user running the script has Create Database rights on the SQL instance. If an existing database is present, the script walks through a routine to see what schema is present and updates to the latest schema, if the user running the scripts has DBO rights on the database.

After the script completes, restart the HP Security Manager service. All should be well as the software and database now match schema versions. See the whitepaper *HP Security Manager – Using Microsoft SQL Server* for more information on running the SQL scripts.

If Security Manager still generates errors while attempting to launch or hangs indefinitely, the database is probably still not upgraded. If you have a new Security Manager trying to use an old database, statements display over and over in the service log indicating required tables are not present:

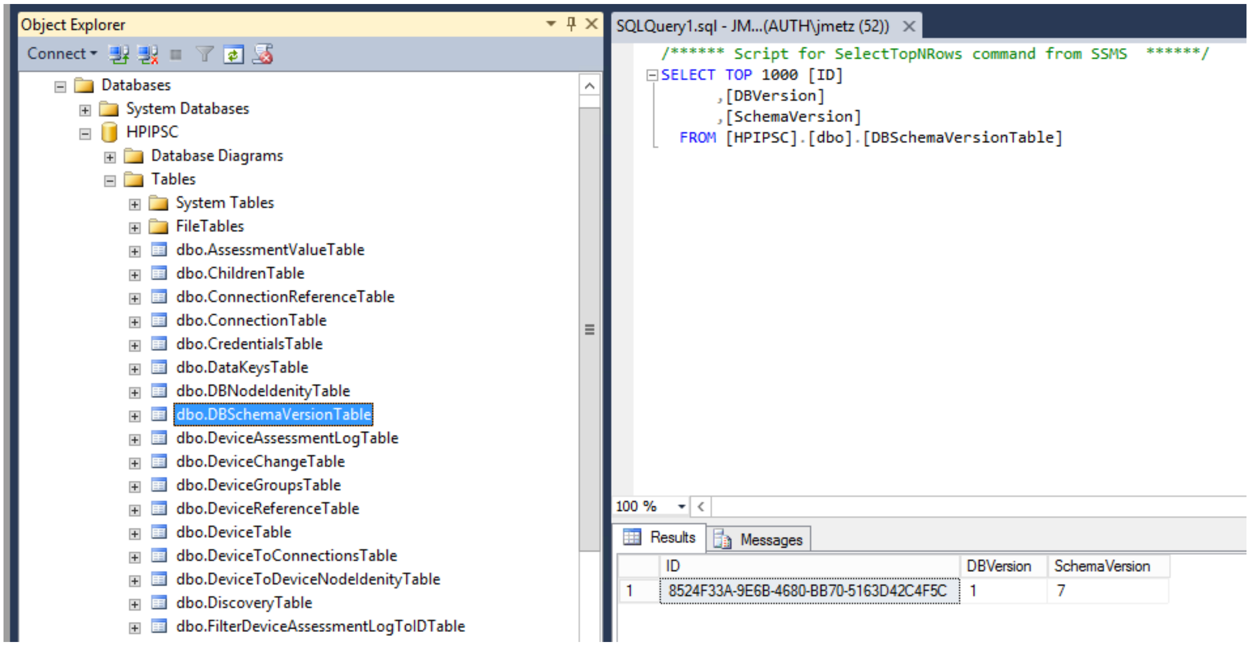
```
2018-01-04 14:33:53,731 ERROR
NHibernate.Util.ADOExceptionReporter [4] - Invalid object name 'ScheduledReportsTable'.
```

In this example, ScheduledReportsTable is a new table only available in the 3.1 version of Security Manager, and it is complaining it cannot find the table. That is very typical of new version using an old database.

Here is a screen shot generated by viewing the database using SQL Management Server showing the table that provides the database schema version. It should be version 7 for Security Manager 3.1.

The HPSM_Service.log file also indicates the schema version. Notice too how there is a **DBO.ScheduledReportsTable**. That is another quick method to see if the database is upgraded or not.

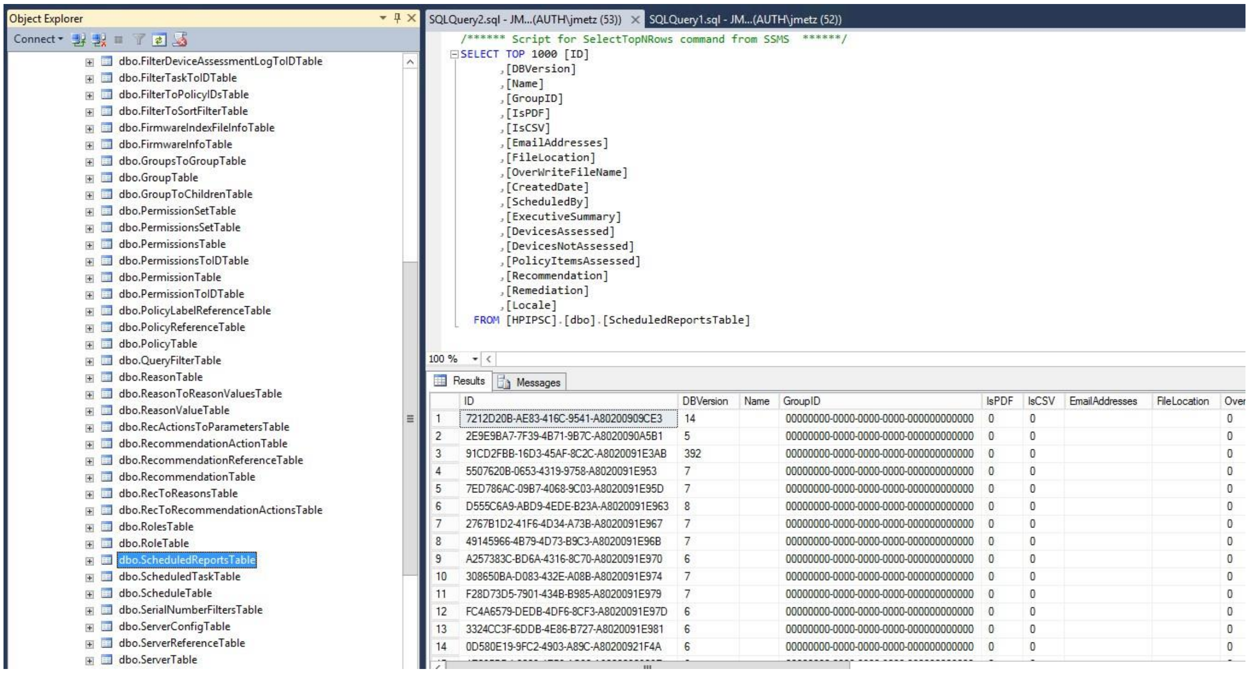
Figure: Schema version indicated



```sql
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP 1000 [ID]
      ,[DBVersion]
      ,[SchemaVersion]
  FROM [HPIPSC].[dbo].[DBSchemaVersionTable]
```

	ID	DBVersion	SchemaVersion
1	8524F33A-9E6B-4680-BB70-5163D42C4F5C	1	7

Figure: Scheduled Reports Table listed



```sql
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP 1000 [ID]
      ,[DBVersion]
      ,[Name]
      ,[GroupID]
      ,[IsPDF]
      ,[IsCSV]
      ,[EmailAddresses]
      ,[FileLocation]
      ,[OverWriteFileName]
      ,[CreatedDate]
      ,[ScheduledBy]
      ,[ExecutiveSummary]
      ,[DevicesAssessed]
      ,[DevicesNotAssessed]
      ,[PolicyItemsAssessed]
      ,[Recommendation]
      ,[Remediation]
      ,[Locale]
  FROM [HPIPSC].[dbo].[ScheduledReportsTable]
```

	ID	DBVersion	Name	GroupID	IsPDF	IsCSV	EmailAddresses	FileLocation	Over
1	7212D20B-AE83-416C-9541-A80200909CE3	14		00000000-0000-0000-0000-000000000000	0	0			0
2	2E9E9BA7-7F39-4B71-9B7C-A8020090A5B1	5		00000000-0000-0000-0000-000000000000	0	0			0
3	91CD2FBB-16D3-45AF-8C2C-A8020091E3AB	392		00000000-0000-0000-0000-000000000000	0	0			0
4	5507620B-0653-4319-9758-A8020091E953	7		00000000-0000-0000-0000-000000000000	0	0			0
5	7ED786AC-09B7-4068-9C03-A8020091E95D	7		00000000-0000-0000-0000-000000000000	0	0			0
6	D555C6A9-ABD9-4EDE-B23A-A8020091E963	8		00000000-0000-0000-0000-000000000000	0	0			0
7	2767B1D2-41F6-4D34-A73B-A8020091E967	7		00000000-0000-0000-0000-000000000000	0	0			0
8	49145966-4B79-4D73-B9C3-A8020091E96B	7		00000000-0000-0000-0000-000000000000	0	0			0
9	A257383C-BD6A-4316-8C70-A8020091E970	6		00000000-0000-0000-0000-000000000000	0	0			0
10	308650BA-D083-432E-A08B-A8020091E974	7		00000000-0000-0000-0000-000000000000	0	0			0
11	F28D73D5-7901-434B-B985-A8020091E979	7		00000000-0000-0000-0000-000000000000	0	0			0
12	FC4A6579-DEDB-4DF6-8CF3-A8020091E97D	6		00000000-0000-0000-0000-000000000000	0	0			0
13	3324CC3F-6DDB-4E86-B727-A8020091E981	6		00000000-0000-0000-0000-000000000000	0	0			0
14	0D580E19-9FC2-4903-A89C-A80200921F4A	6		00000000-0000-0000-0000-000000000000	0	0			0

This can happen due to the following reasons:

- The account running the Security Manager installer does not have DBO rights on the database
- during an upgrade.
- The user chooses “connect to and existing database” instead of “install or upgrade an existing database” during an upgrade attempt but the database was never upgraded manually using the SQL scripts.
- The SQL scripts are run to manually upgrade the database but the account running the scripts does not have DBO permissions on the database to upgrade it.
- The SQL scripts may be the broken ones included in the Security Manager folder of version 3.1.
- The SQL scripts are run using the wrong syntax on the command line.

Error-Maybe a DB access issue in HPSM_service.log file

A “Maybe a DB access issue” error is listed in the HPSM_service.log file:

```
Error,3/28/2021 4:31:41 AM,HP JetAdvantage Security Manager,0,None,"Error - Maybe a DB access issue
- calling SetRecoveryMode() System.Data.SqlClient.SqlException (0x80131904): This server is part of
Recovery Model exception list, Database Recovery Model should be in FULL for this server. If need any
clarification, Please reach out SQL Operation team Supervisor(s)
```

HPSM re-indexes during the nightly maintenance and changes the DB Recovery mode to SIMPLE before indexing and then restores the previous setting after the re-indexing operation has been completed. If the HPSM service does not have the rights to change the recovery model, then the error will display.

This re-indexing can be disabled by setting the **IndexPerformanceTuning** to **true** in the HPSM_service.exe.config file, followed by a restart of the HPSM service.

Problems Launching Security Manager Web Interface

First, check if the HPSM service is still running. When the HPSM service is running in debug mode you can also check the HPSM_service.log file if the HPSM service can connect correctly to the database. If the HPSM service is running and can connect to the database, then you need to check the HPSM application pool.

Is the application pool still running after some time, or is it automatically getting stopped?
If it is getting stopped, check the HPSMWeb.log and event viewer for more information.

Web page not displayed while HPSM service is running and connecting to DB

The following two subsections (bindings/firewall problem and browser setting causing issues) describes issues when HPSM service can connect to the database.

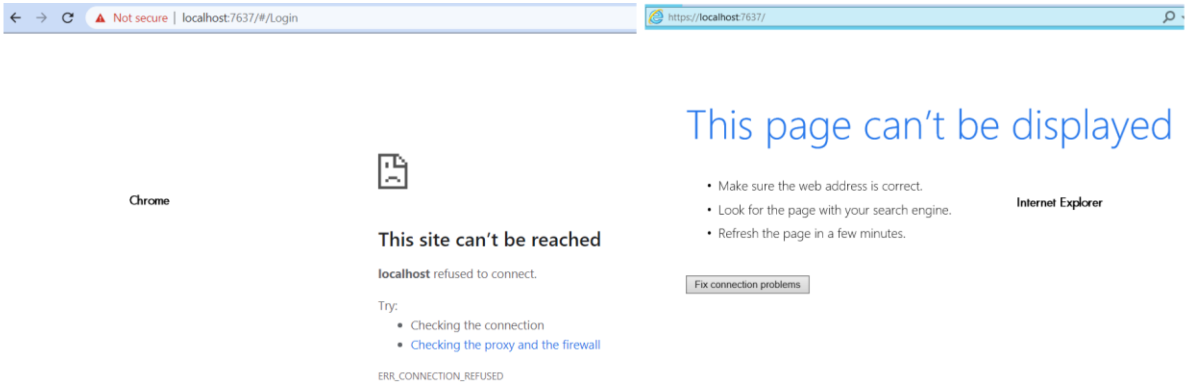
Bindings/firewall problem

The Security Manager browser-based interface requires Internet Information Services (IIS) to operate. The installer will verify that IIS is enabled with the proper settings enabled and will offer to enable the proper settings if desired. The Installation Guide specifies the proper IIS setting to be enabled to perform the configuration manually if preferred.

If the installer fails to set some of the IIS settings, it may be necessary to configure them manually. Since the installer is attempting to enable IIS, it may prompt for a machine restart. You can use IIS Manager under Administrative Tools to determine if the HPSM application pool and HPSM web site are present and configured properly.

An easy test to determine if IIS is functioning properly is to see if you can browse to the default IIS web page: http://localhost:80. If you can't browse to the default page, it is likely you will not be able to browse to the Security Manager page either.

When you still cannot access the web page, you might receive the following error message in your browser when Security Manager is launched in a browser:



This site can't be reached

localhost refused to connect.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED

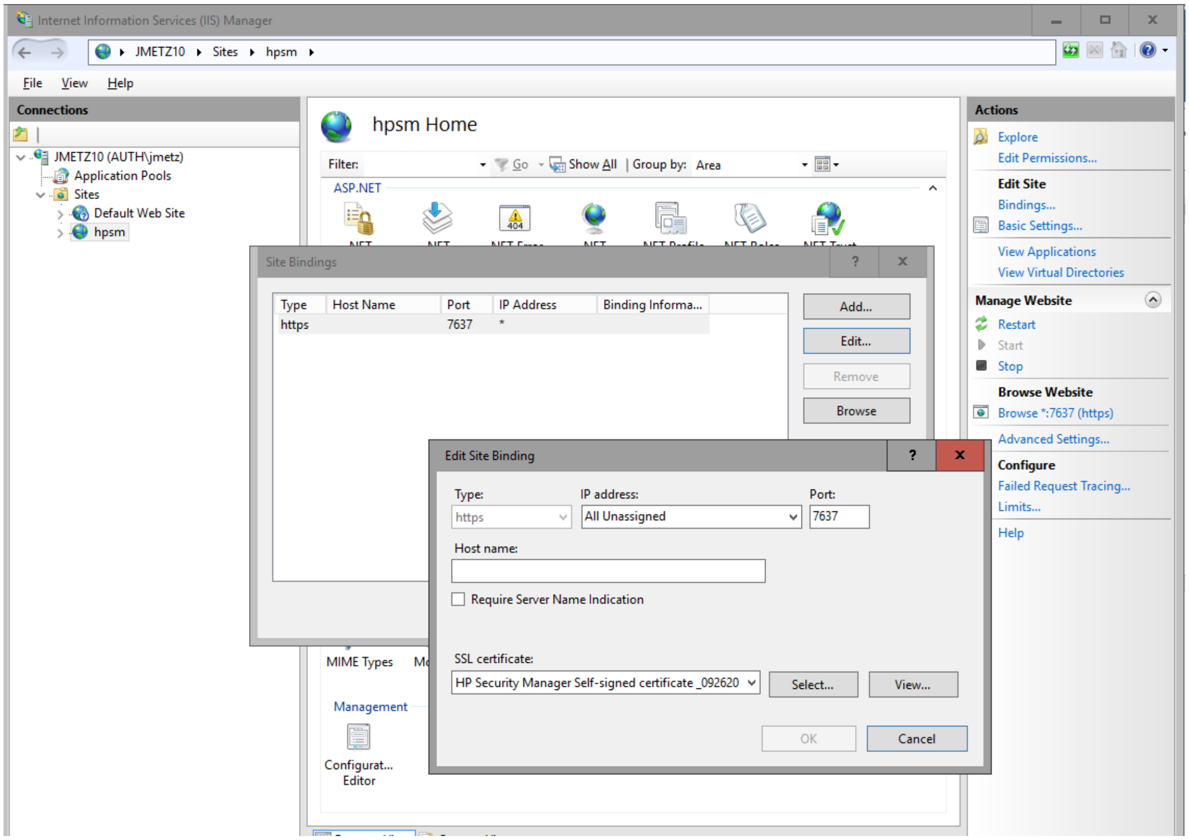
This page can't be displayed

- Make sure the web address is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

If the application pool is still running after attempting to reach the page, then there is a binding problem of firewall.

To change this port, or if the port is being blocked, it can be changed by configuring the bindings for the HPSM web site under IIS Manager. Expand **Sites** in the left pane, select **HPSM**, and then select **Bindings**.

Figure: HPSM Binding settings



Site Bindings

Type	Host Name	Port	IP Address	Binding Informa...
https		7637	*	

Edit Site Binding

Type: https

IP address: All Unassigned

Port: 7637

Host name:

□ Require Server Name Indication

SSL certificate: HP Security Manager Self-signed certificate _092620

Make sure that the **Type** is set to https, **Port** to 7637 and that as an **SSL certificate** the HP Security Manager Self signed self-certificate or a server certificate is selected. Change it to a different port if it is blocked by the firewall or open the port in the firewall.

The self-signed certificate allows the data to be encrypted between client and server, while an existing server certificate not only encrypts data but also provides trust that the server is who it says it is. IIS will always search and bind for the server certificate in the personal store of computer account. An identity certificate needs to be of the type "Server Authentication" to provide trust.

Issues have been seen in cases where there are multiple certificates to choose from with the same name during installation, and if an improper certificate is chosen, the bindings will not be created for the web site. Security Manager will not launch, and the HPSM web site will also contain a couple of icons instead of the 20 or so it should contain. The easy fix to this problem is to select the correct port for the bindings (7637). The icons will display, and Security Manager will run properly.

Browser settings causing issues

The new browser-based interface supports either Microsoft Internet Explorer (IE) or Google Chrome. The following settings may need to be configured on certain machines or operating systems if Security Manager is having difficulty loading and the application pool is running correctly.

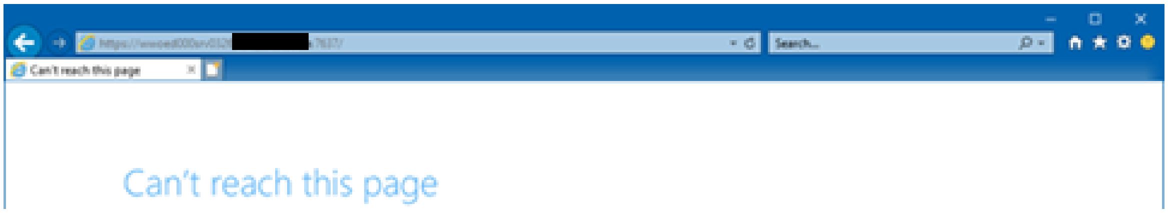
If the login screen for Security Manager is not displaying, remove the **Display intranet sites in Compatibility View** setting. To do this, click the ALT key to open the options in IE. Under **Tools**, select **Compatibility View**, and then clear the **Display intranet sites in Compatibility View** option.

Internet Explorer may require the “Bypass proxy server for local addresses” box to be checked under Internet Options, Connections, LAN Settings if the login screen for Security Manager is not displaying.

Windows 10 may require HTTP2 to be disabled in the browser if Security Manager continually logs out the user.

Web page not displayed and HPSM service is automatically stopping

In some situations, you might see that the HPSM service is stopping quickly after starting the service. When trying to browse to the application you will see errors like **Can’t reach this page**.



Can’t reach this page

This can have multiple reasons and the HPSM.service.log will have to be used to find out why this happened.

ServerConfig could not initialized in HPSM_service.log

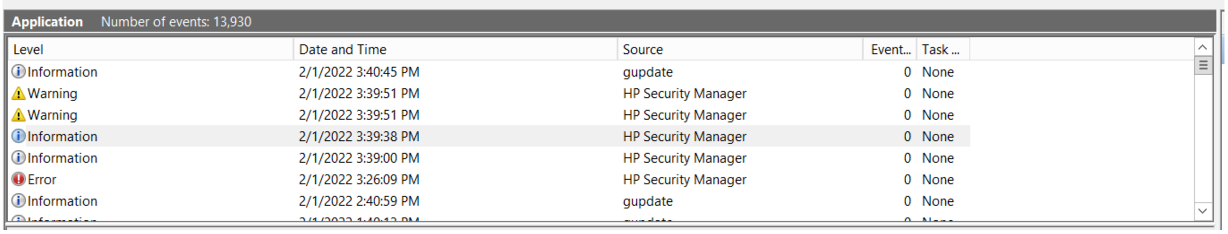
Entries like the following might be listed in the HPSM.service.log file:

```
022-01-27 02:01:40,807 INFO  Service   [4] - TaskSupervisor.Init - HPSM Starting
2022-01-27 02:01:52,229 INFO  Service   [4] - Successfully started DSSessionVariables() - hibernate
session
2022-01-27 02:01:52,244 INFO  Service   [4] - ScheduleTaskManager.RetryDBConnection Testing DB
connection to: Server=WWOED000SRV0327;initial catalog=HPSECMGR;Integrated Security=SSPI
2022-01-27 02:01:52,244 INFO  Service   [4] -  - Done TestDBConnection
2022-01-27 02:01:52,244 INFO  Service   [4] - ScheduleTaskManager.RetryDBConnection Testing DB
connection successful to: Server=WWOED000SRV0327;initial catalog=HPSECMGR;Integrated
Security=SSPI
2022-01-27 02:01:52,244 INFO  Service   [4] - Service Starting up - Init
2022-01-27 02:01:52,369 INFO  Service   [4] - BizLogicMgr.IsValidProductDB - productId 6F1BC5E1-A0C9-
4CEF-B065-BBF5F487F289 metaData.ID6F1BC5E1-A0C9-4CEF-B065-BBF5F487F289
2022-01-27 02:01:52,526 ERROR Service   [4] - BizLogicMgr.ValidateServerCertificate Certificate error:
{0}RemoteCertificateChainErrors
2022-01-27 02:01:52,526 ERROR Service   [4] - BizLogicMgr.Init - Error ServerConfig not initialized -
Unknown error: System.Security.SecurityException: The source was not found, but some or all event
logs could not be searched.  To create the source, you need permission to read all event logs to make
sure that the new source name is unique.  Inaccessible logs: Security, State.__   at
System.Diagnostics.EventLog.FindSourceRegistration(String source, String machineName, Boolean
readOnly, Boolean wantToCreate)__   at System.Diagnostics.EventLog.SourceExists(String source,
String machineName, Boolean wantToCreate)__   at
System.Diagnostics.EventLogInternal.VerifyAndCreateSource(String sourceName, String
currentMachineName)__   at System.Diagnostics.EventLogInternal.WriteEntry(String message,
EventLogEntryType type, Int32 eventID, Int16 category, Byte[] rawData)__   at
```

```
System.Diagnostics.EventLog.WriteEntry(String source, String message, EventLogEntryType type, Int32
eventID, Int16 category, Byte[] rawData)__   at Common.DataConstants.SetURLSetting(String
settingName, String defaultValue, String& memberSetting)__   at
Common.DataConstants.InitializeFromAppConfig()__   at
LocksmithBusinessLogic.BizLogicMgr.Init(Boolean& startSSLListner)__The Zone of the assembly that
failed was:__MyComputer
2022-01-27 02:01:52,526 ERROR Service   [4] - HP Security Manager: Unexpected Error Initializing -
Shuting down:  System.Security.SecurityException: The source was not found, but some or all event logs
could not be searched.  To create the source, you need permission to read all event logs to make sure
that the new source name is unique.  Inaccessible logs: Security, State.__   at
System.Diagnostics.EventLog.FindSourceRegistration(String source, String machineName, Boolean
readOnly, Boolean wantToCreate)__   at System.Diagnostics.EventLog.SourceExists(String source,
String machineName, Boolean wantToCreate)__   at
System.Diagnostics.EventLogInternal.VerifyAndCreateSource(String sourceName, String
currentMachineName)__   at System.Diagnostics.EventLogInternal.WriteEntry(String message,
EventLogEntryType type, Int32 eventID, Int16 category, Byte[] rawData)__   at
System.Diagnostics.EventLog.WriteEntry(String source, String message, EventLogEntryType type, Int32
eventID, Int16 category, Byte[] rawData)__   at Common.DataConstants.SetURLSetting(String
settingName, String defaultValue, String& memberSetting)__   at
Common.DataConstants.InitializeFromAppConfig()__   at
LocksmithBusinessLogic.BizLogicMgr.Init(Boolean& startSSLListner)__The Zone of the assembly that
failed was:__MyComputer
```

In this case the event source “HP Security Manager” which should become visible in the event viewer for HPSM related events can not be created/read.

Example of HPSM event message in the event viewer:



Application Number of events: 13,930

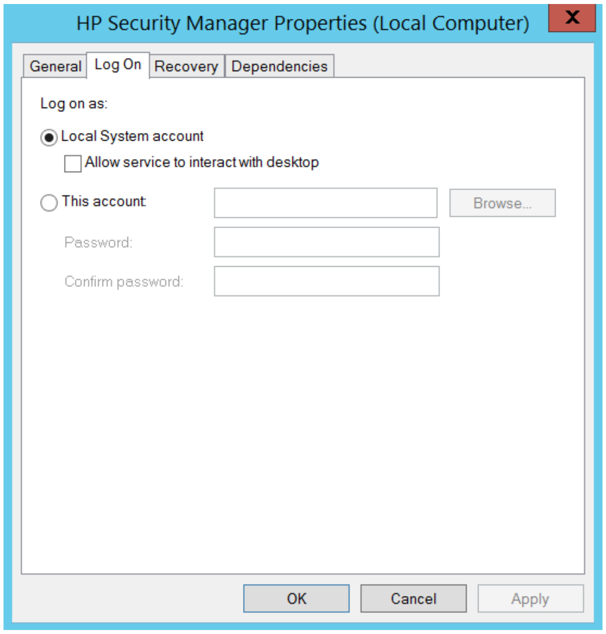
Level	Date and Time	Source	Event...	Task ...
Information	2/1/2022 3:40:45 PM	gupdate	0	None
Warning	2/1/2022 3:39:51 PM	HP Security Manager	0	None
Warning	2/1/2022 3:39:51 PM	HP Security Manager	0	None
Information	2/1/2022 3:39:38 PM	HP Security Manager	0	None
Information	2/1/2022 3:39:00 PM	HP Security Manager	0	None
Error	2/1/2022 3:26:09 PM	HP Security Manager	0	None
Information	2/1/2022 2:40:59 PM	gupdate	0	None

First, check if the account (by default Network service) running the HPSM service as at least read permissions to the corresponding registry key.

1. Open the Registry Editor:
2. Select **Start** then **Run**
3. Enter **regedt32** or **regedit**
4. Navigate/expand to the following key:
5. **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security**
6. Right-click the entry and select **Permissions**
7. Add the **Network Service** user (or the account running the HPSM service)
8. Give it **Read** permission
9. Restart HPSM service.

If the correct permissions were already available or if the issue was not resolved, try to run HPSM temporarily as Local System.

1. Go to services
2. Right-click the HP Security Manager service and select **Properties**
3. Click on the **Log On** tab and select the radio button **Local System Account**



HP Security Manager Properties (Local Computer)

Log on as:

● Local System account

□ Allow service to interact with desktop

○ This account:

Password:

Confirm password:

4. Restart HPSM service.

The event source HP Security Manager is created with the Local System Account.

After HPSM has been running for a few minutes, verify in the HPSM_service.log file that the error “Server config could not be initialized” is no longer occurring. Change HPSM service back to the desired account.

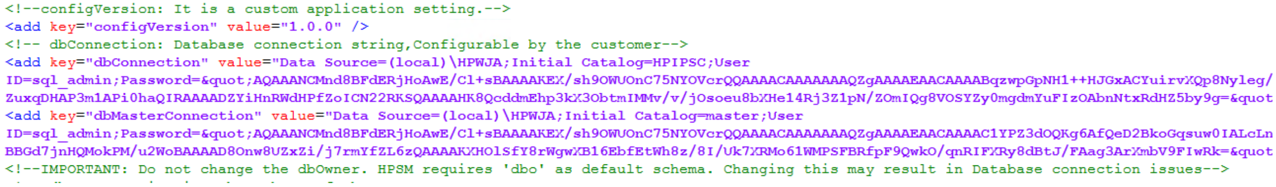
Invalid length for a Base-64 char array or string in HPSM_service.log

When the HPSM service is stopping automatically after trying to connect to the DB, you might see the following in the HPSM_service.log:

```
2023-12-14 12:23:47,771 DEBUG Service   [4] - ScheduleTaskManager.DispatchEvents Initializing
2023-12-14 12:23:47,771 INFO  Service   [4] - Service Starting up - Init
2023-12-14 12:23:47,771 DEBUG Service   [4] - BizLogicMgr - GetMetaData
2023-12-14 12:23:47,966 INFO  Service   [4] - BizLogicMgr.IsValidProductDB - productId 11870252-D338-4BCD-9EBD-8A77C043D65D metaData.ID11870252-D338-4BCD-9EBD-8A77C043D65D
2023-12-14 12:23:48,193 DEBUG Service   [4] - DecryptUsingDPAPI method called.
2023-12-14 12:23:48,193 DEBUG Service   [4] - Error - DecryptUsingDPAPI: Invalid length for a Base-64 char array or string.
```

This happens when the hpsm_service.exe.config has been configured with an sql user account to access the database and the sql password has been encrypted by HPSM during the first successful start of the hpsm service.

Example of encrypted sql user password in hpsm_service.exe.config file:



```
    <!--configVersion: It is a custom application setting.-->
    <add key="configVersion" value="1.0.0" />
    <!-- dbConnection: Database connection string,Configurable by the customer-->
    <add key="dbConnection" value="Data Source=(local)\HPWJA;Initial Catalog=HPIPSC;User
    ID=sql_admin;Password=&quot;AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAKEX/sh9OWUOnC75NYOVcrQQAAAACAAAAAAAQZgAAAAEAACAAAABqzwpGpNH1++HJGxACYuirvXQp8Nyleg/
    ZuxqDHAP3m1APi0haQIRAAAADZYiHnRWdHPfZoICN22RKSQAAAAHK8QcddmEhp3kX3ObtmIMMv/v/jOsoeu8bXHe14Rj3Z1pN/ZOmIQg8VOSYZy0mgdmYuFIzOAbnNtxRdHZ5by9g=&quot
    <add key="dbMasterConnection" value="Data Source=(local)\HPWJA;Initial Catalog=master;User
    ID=sql_admin;Password=&quot;AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAKEX/sh9OWUOnC75NYOVcrQQAAAACAAAAAAAQZgAAAAEAACAAAAC1YPZ3dOQKg6AfQeD2BkoGqsuw0IALcLn
    BBGd7jnHQMokPM/u2WoBAAAAD8Onw8UZxZi/j7rmYfZL6zQAAAAKXHOlSfY8rWgwXB16EbfEtWh8z/8I/Uk7XRMo61WMPSFBRfpF9QwkO/qnRIFXRy8dBtJ/FAag3ArXmbV9FIwRk=&quot
    <!--IMPORTANT: Do not change the dbOwner. HPSM requires 'dbo' as default schema. Changing this may result in Database connection issues-->
```

The web.config file also needs to be configured to use the SQL user account to connect to the DB and the password should have been encrypted by HPSM in the web.config file after the password has been encrypted in the hpsm_service.exe.config file.

If the sql password is not encrypted in the hpsm_service.exe.config and web.config on all locations where the database connection is specified, then you'll run in the invalid length error.

Solution: stop hpsm service and hpsm application pool. Re-edit the hpsm_service.exe.config and web.config file and make sure that the unencrypted sql password is specified.
Now start hpsm application pool
Finally start hpsm security manager service

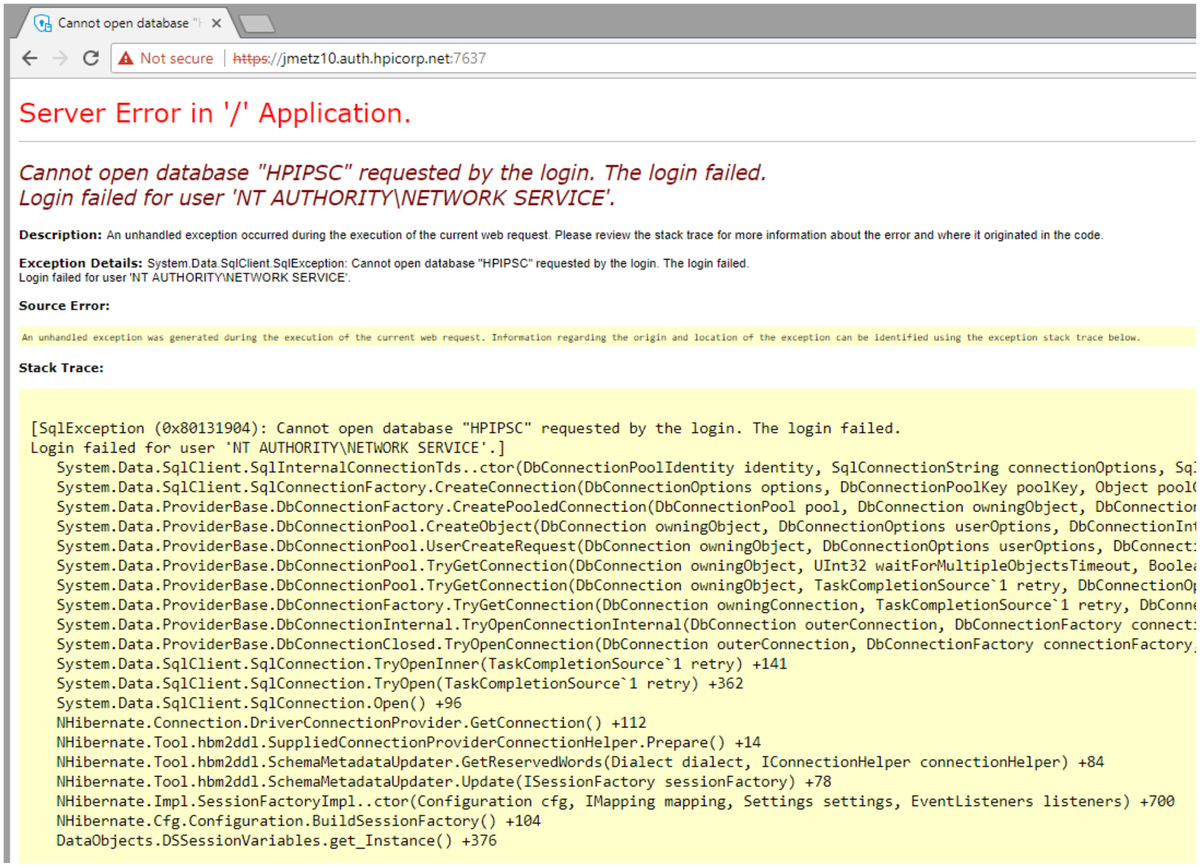
Issues when running HPSM Application Pool

As network service - Server Error in "/" Application, Cannot open database

The Security Manager service and the HPSM application pool must have the proper permissions to access the Security Manager service database.

If the service and database are installed on the same computer, the installation process manages the assignment of database permissions by assigning Network Service to run both the HPSM service and the HPSM application pool.

If the service and the database are installed on separate computers, you must configure the correct permissions for the remote database, otherwise the HPSM service cannot login to the database and you might receive an error like the following:


Cannot open database "H ×
Not secure
~~https~~://jmetz10.auth.hpicorp.net:7637

Server Error in '/' Application.

Cannot open database "HPIPSC" requested by the login. The login failed.
Login failed for user 'NT AUTHORITY\NETWORK SERVICE'.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Cannot open database "HPIPSC" requested by the login. The login failed.
Login failed for user 'NT AUTHORITY\NETWORK SERVICE'.

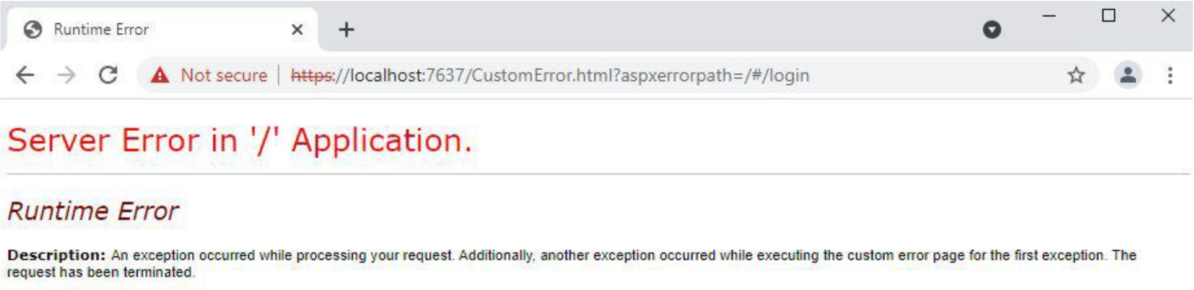
Source Error:

```
An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.
```

Stack Trace:

```
[SqlException (0x80131904): Cannot open database "HPIPSC" requested by the login. The login failed.
Login failed for user 'NT AUTHORITY\NETWORK SERVICE'.]
   System.Data.SqlClient.SqlInternalConnectionTds..ctor(DbConnectionPoolIdentity identity, SqlConnectionString connectionOptions, Sq
   System.Data.SqlClient.SqlConnectionFactory.CreateConnection(DbConnectionOptions options, DbConnectionPoolKey poolKey, Object pool
   System.Data.ProviderBase.DbConnectionFactory.CreatePooledConnection(DbConnectionPool pool, DbConnection owningObject, DbConnectio
   System.Data.ProviderBase.DbConnectionPool.CreateObject(DbConnection owningObject, DbConnectionOptions userOptions, DbConnectionInt
   System.Data.ProviderBase.DbConnectionPool.UserCreateRequest(DbConnection owningObject, DbConnectionOptions userOptions, DbConnect
   System.Data.ProviderBase.DbConnectionPool.TryGetConnection(DbConnection owningObject, UInt32 waitForMultipleObjectsTimeout, Boolea
   System.Data.ProviderBase.DbConnectionPool.TryGetConnection(DbConnection owningObject, TaskCompletionSource`1 retry, DbConnectionO
   System.Data.ProviderBase.DbConnectionFactory.TryGetConnection(DbConnection owningConnection, TaskCompletionSource`1 retry, DbConne
   System.Data.ProviderBase.DbConnectionInternal.TryOpenConnectionInternal(DbConnection outerConnection, DbConnectionFactory connect
   System.Data.ProviderBase.DbConnectionClosed.TryOpenConnection(DbConnection outerConnection, DbConnectionFactory connectionFactory,
   System.Data.SqlClient.SqlConnection.TryOpenInner(TaskCompletionSource`1 retry) +141
   System.Data.SqlClient.SqlConnection.TryOpen(TaskCompletionSource`1 retry) +362
   System.Data.SqlClient.SqlConnection.Open() +96
   NHibernate.Connection.DriverConnectionProvider.GetConnection() +112
   NHibernate.Tool.hbm2ddl.SuppliedConnectionProviderConnectionHelper.Prepare() +14
   NHibernate.Tool.hbm2ddl.SchemaMetadataUpdater.GetReservedWords(Dialect dialect, IConnectionHelper connectionHelper) +84
   NHibernate.Tool.hbm2ddl.SchemaMetadataUpdater.Update(ISessionFactory sessionFactory) +78
   NHibernate.Impl.SessionFactoryImpl..ctor(Configuration cfg, IMapping mapping, Settings settings, EventListeners listeners) +700
   NHibernate.Cfg.Configuration.BuildSessionFactory() +104
   DataObjects.DSSessionVariables.get_Instance() +376
```

If the HPSM service has been configured to run under a user or service account which has access to the database, you still might receive a server error, due to login problems of the HPSM application pool.


Runtime Error
Not secure
~~https~~://localhost:7637/CustomError.html?aspxerrorpath=/#/login

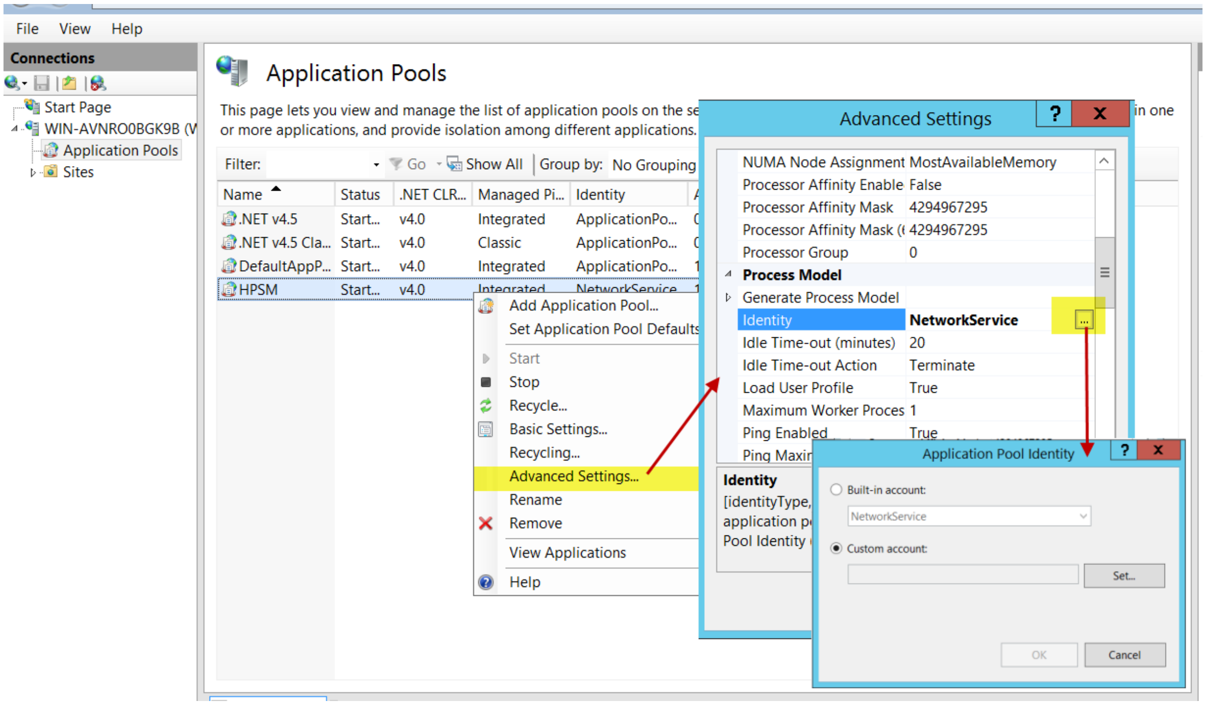
Server Error in '/' Application.

Runtime Error

Description: An exception occurred while processing your request. Additionally, another exception occurred while executing the custom error page for the first exception. The request has been terminated.

By default, the HPSM application pool will be configured with NetworkService, but this can be changed if desired to run under the same account as the HPSM service or by providing access to the database for the Network Service.

Open IIS, right-click the HPSM application pool, select **Advanced Settings**, click on **…** , select **Custom Account**, specify the account which should be used, and then select **OK**.



This page lets you view and manage the list of application pools on the se… or more applications, and provide isolation among different applications. … in one

Name	Status	.NET CLR...	Managed Pi...	Identity
.NET v4.5	Start...	v4.0	Integrated	ApplicationPo...
.NET v4.5 Cla...	Start...	v4.0	Classic	ApplicationPo...
DefaultAppP...	Start...	v4.0	Integrated	ApplicationPo...
HPSM	Start...	v4.0	Integrated	NetworkService

NUMA Node Assignment	MostAvailableMemory
Processor Affinity Enable	False
Processor Affinity Mask	4294967295
Processor Affinity Mask (6	4294967295
Processor Group	0
Process Model	
Generate Process Model	
Identity	**NetworkService**
Idle Time-out (minutes)	20
Idle Time-out Action	Terminate
Load User Profile	True
Maximum Worker Proces	1
Ping Enabled	True
Ping Maxir	

Identity
[identityType, application p… Pool Identity …

Built-in account: NetworkService

See the whitepaper titled "HP Security Manager - Using Microsoft® SQL Server" for more information about the required rights for a remote database. It is also possible that some IIS settings are not configured. Double check that all of the IIS settings were enabled as described in the "HP Security Manager Installation Guide".

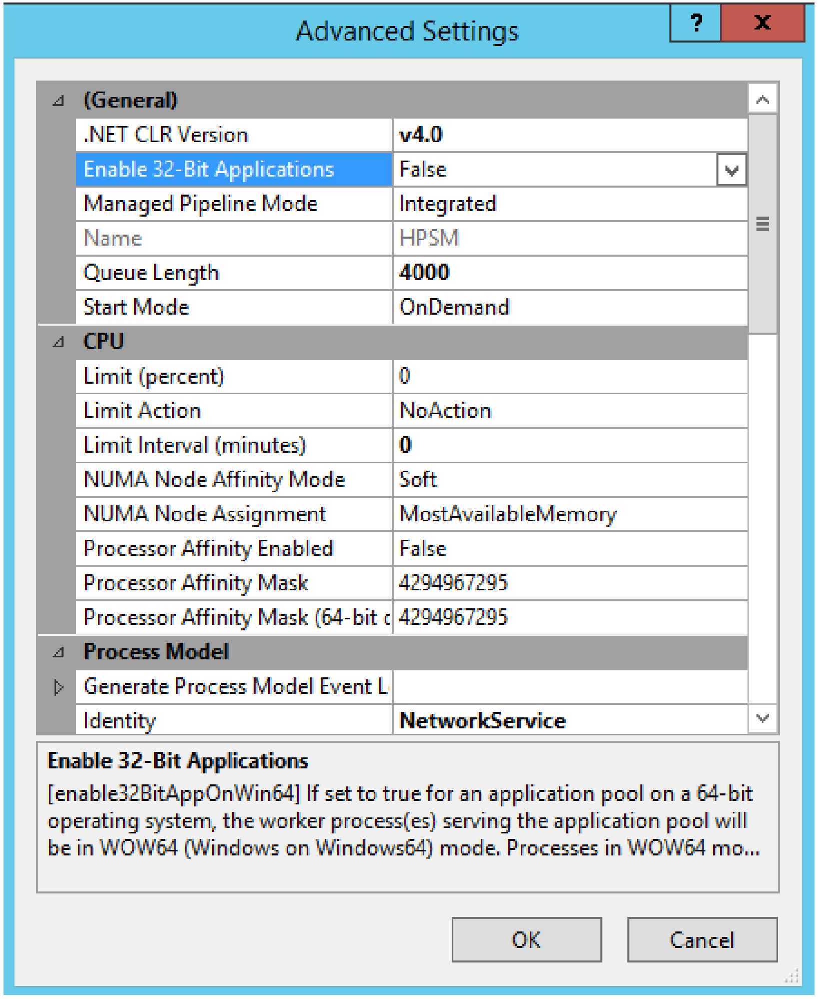
If the browser displays an error that it cannot read the web.config file, search the internet for more information on the error code.

32-Bit Applications not enabled for HPSM application pool

The Enable 32-bit Applications setting for the HPSM application pool may need to be toggled. To do this, follow these steps:

1. In IIS, select **Application Pools**, right-click **HPSM**, and then select **Advanced Settings** (or select **Advanced Settings** in the right -pane).

   The following screen displays:



(General)	
.NET CLR Version	**v4.0**
Enable 32-Bit Applications	False
Managed Pipeline Mode	Integrated
Name	HPSM
Queue Length	**4000**
Start Mode	OnDemand
CPU	
Limit (percent)	0
Limit Action	NoAction
Limit Interval (minutes)	**0**
NUMA Node Affinity Mode	Soft
NUMA Node Assignment	MostAvailableMemory
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Processor Affinity Mask (64-bit c	4294967295
Process Model	
Generate Process Model Event L	
Identity	**NetworkService**

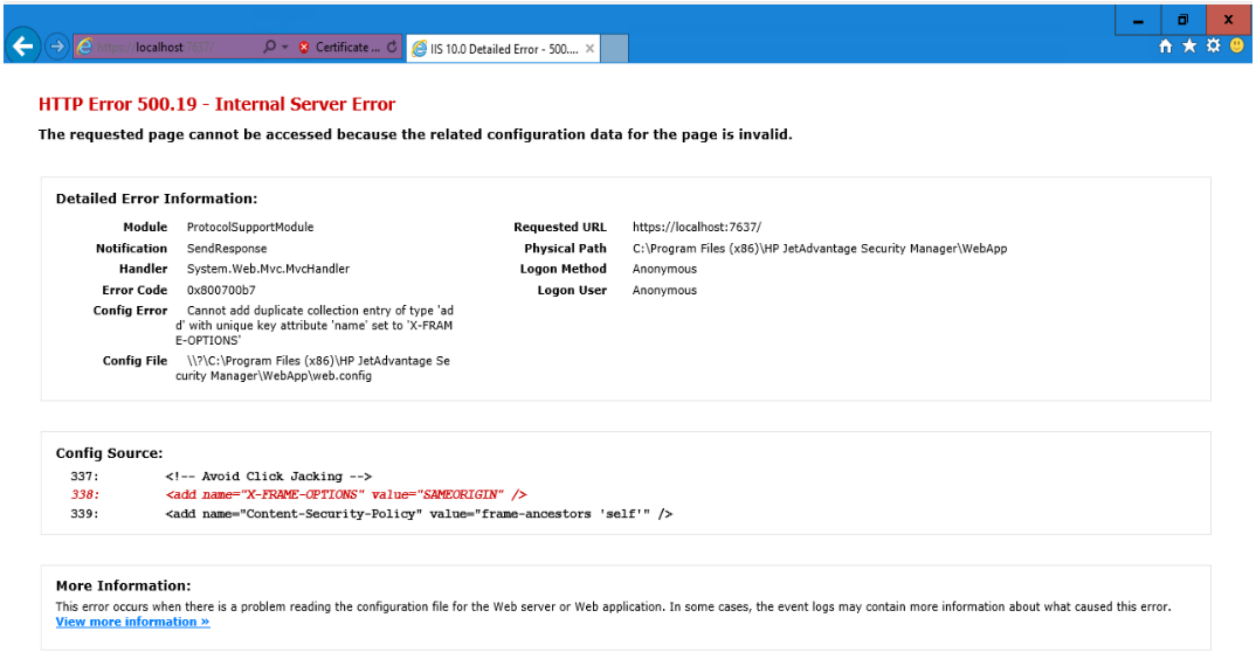
Enable 32-Bit Applications
[enable32BitAppOnWin64] If set to true for an application pool on a 64-bit operating system, the worker process(es) serving the application pool will be in WOW64 (Windows on Windows64) mode. Processes in WOW64 mo...

2. Change the setting for **Enable 32-bit Applications** from **False** to **True**.

HTTP 500.19 Internal Server Error with config source reference to X-Frame-Options

When running HPSM Application Pool on some systems, you might receive an HTTP 500.19 error with config source reference to X-Frame-Options.

Figure: HTTP 500.19 error received



HTTP Error 500.19 - Internal Server Error

The requested page cannot be accessed because the related configuration data for the page is invalid.

Detailed Error Information:

Module	ProtocolSupportModule	**Requested URL**	https://localhost:7637/
Notification	SendResponse	**Physical Path**	C:\Program Files (x86)\HP JetAdvantage Security Manager\WebApp
Handler	System.Web.Mvc.MvcHandler	**Logon Method**	Anonymous
Error Code	0x800700b7	**Logon User**	Anonymous
Config Error	Cannot add duplicate collection entry of type 'add' with unique key attribute 'name' set to 'X-FRAME-OPTIONS'		
Config File	\\?\C:\Program Files (x86)\HP JetAdvantage Security Manager\WebApp\web.config		

Config Source:

```
337:        <!-- Avoid Click Jacking -->
338:        <add name="X-FRAME-OPTIONS" value="SAMEORIGIN" />
339:        <add name="Content-Security-Policy" value="frame-ancestors 'self'" />
```

More Information:

This error occurs when there is a problem reading the configuration file for the Web server or Web application. In some cases, the event logs may contain more information about what caused this error.
View more information »

The Config Source shows in red information about X-FRAME-OPTIONS in line 338. During installation of HPSM, the installer configures the IIS settings for HPSM. It updated the applicationHost config file which is by default in the following location:

C:|Windows|System32|inetsrv|Config

For HPSM, the customHeaders section for the httpProtocol should be configured as the following:

```
<httpProtocol>
  <customHeaders>
    <clear />
    <add name="X-Powered-By" value="ASP.NET" />
  </customHeaders>
  <redirectHeaders>
    <clear />
  </redirectHeaders>
</httpProtocol>
```

Other customHeaders content should be removed. For example:

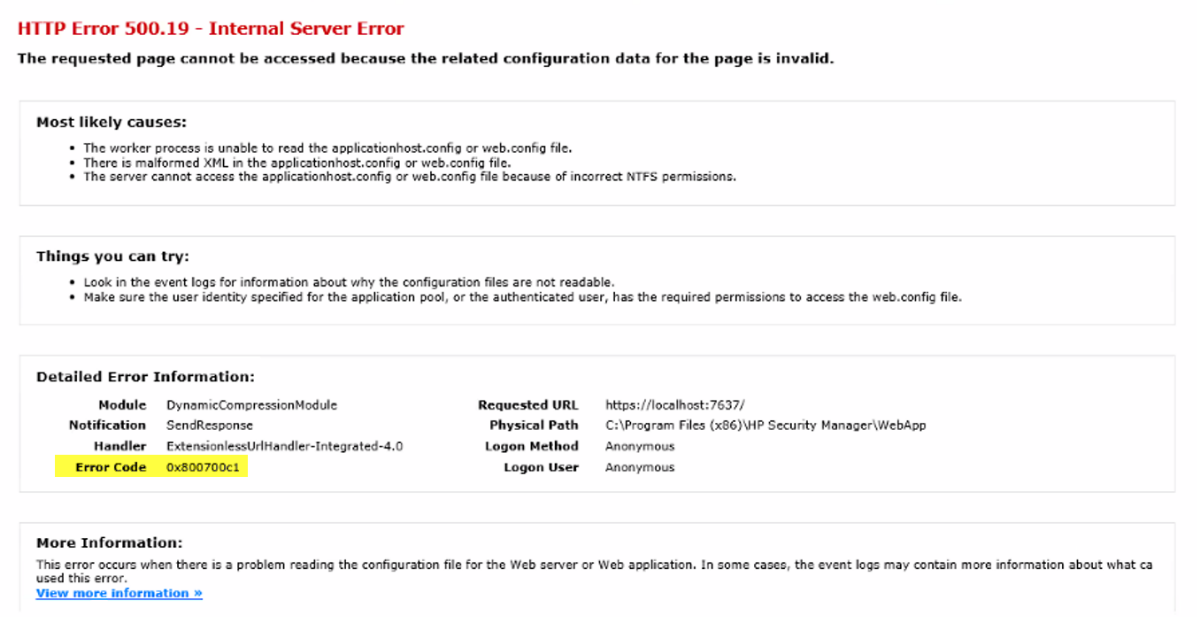
```
<add name="X-FRAME-OPTIONS" value="DENY" />
```

Before making any changes save a copy of the file and store it in a save location. After that remove, all special customHeaders add name sections, restart the HPSM application pool and restart the HP Security Manager service.

HTTP 500.19 Internal Server Error with error code 0x800700c1

When running HPSM Application Pool on some systems, you might receive an HTTP 500.19 error with error code 0x8000700c1.

Figure: HTTP Error 500.19 - Internal Server Error Error Code 0x800700c1.



HTTP Error 500.19 - Internal Server Error

The requested page cannot be accessed because the related configuration data for the page is invalid.

Most likely causes:

- The worker process is unable to read the applicationhost.config or web.config file.
- There is malformed XML in the applicationhost.config or web.config file.
- The server cannot access the applicationhost.config or web.config file because of incorrect NTFS permissions.

Things you can try:

- Look in the event logs for information about why the configuration files are not readable.
- Make sure the user identity specified for the application pool, or the authenticated user, has the required permissions to access the web.config file.

Detailed Error Information:

Module	DynamicCompressionModule	**Requested URL**	https://localhost:7637/
Notification	SendResponse	**Physical Path**	C:\Program Files (x86)\HP Security Manager\WebApp
Handler	ExtensionlessUrlHandler-Integrated-4.0	**Logon Method**	Anonymous
Error Code	0x800700c1	**Logon User**	Anonymous

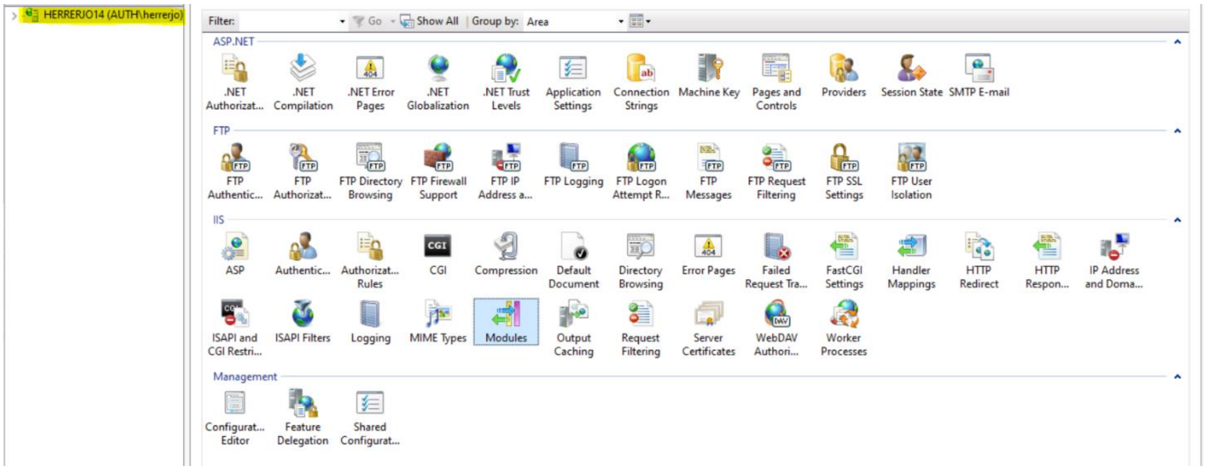
More Information:

This error occurs when there is a problem reading the configuration file for the Web server or Web application. In some cases, the event logs may contain more information about what ca used this error.

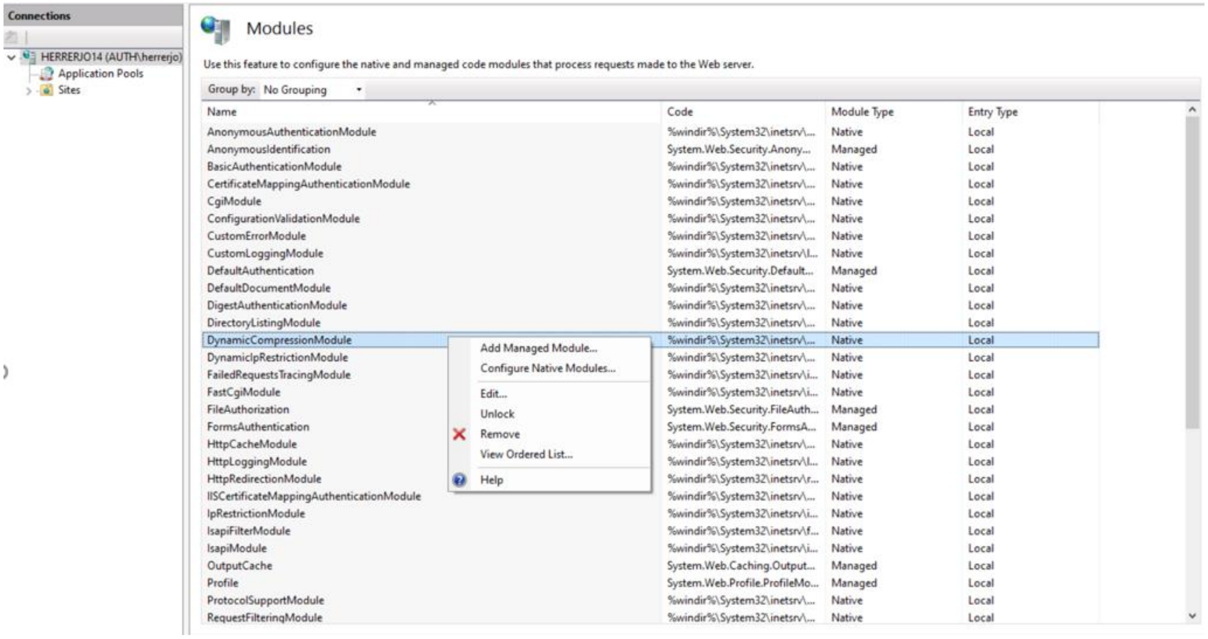
View more information »

Potential fix (it is possible that other IIS configuration settings are causing the same issue):

1. Open IIS (Internet Information Server).
2. Click on server module node at the top of the left navigation pane, select **Modules**, and then select **Open Feature** or double click **Modules**.



3. Right-click **DynamicCompressionModule** and select **Unlock**.



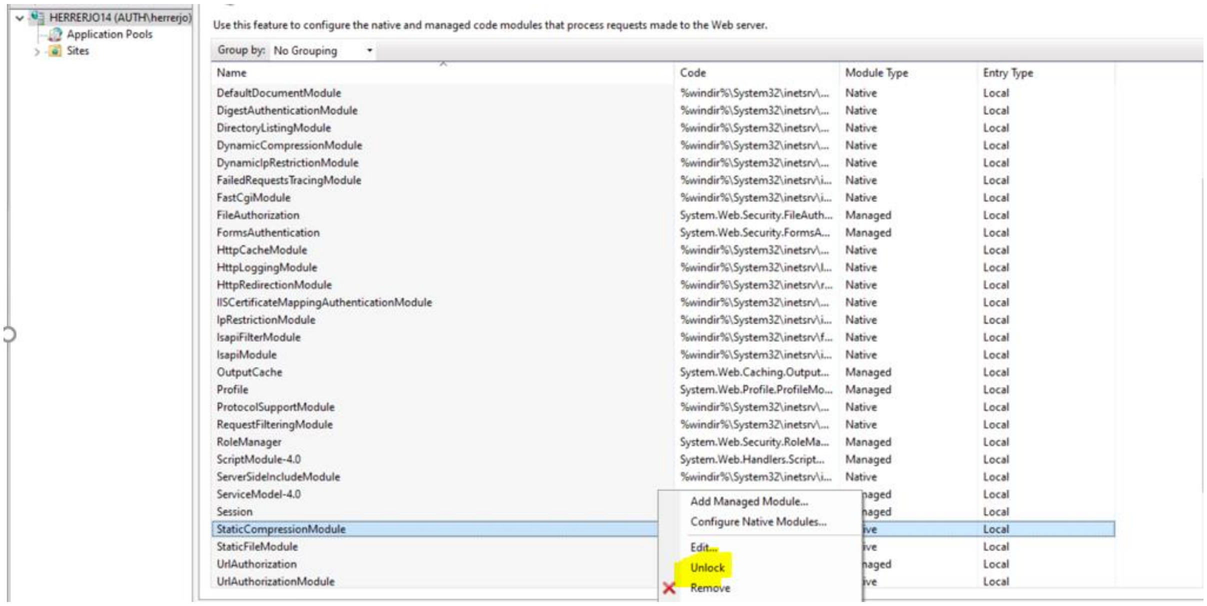
Modules

Use this feature to configure the native and managed code modules that process requests made to the Web server.

Group by: No Grouping

Name	Code	Module Type	Entry Type
AnonymousAuthenticationModule	%windir%\System32\inetsrv\...	Native	Local
AnonymousIdentification	System.Web.Security.Anony...	Managed	Local
BasicAuthenticationModule	%windir%\System32\inetsrv\...	Native	Local
CertificateMappingAuthenticationModule	%windir%\System32\inetsrv\...	Native	Local
CgiModule	%windir%\System32\inetsrv\...	Native	Local
ConfigurationValidationModule	%windir%\System32\inetsrv\...	Native	Local
CustomErrorModule	%windir%\System32\inetsrv\...	Native	Local
CustomLoggingModule	%windir%\System32\inetsrv\l...	Native	Local
DefaultAuthentication	System.Web.Security.Default...	Managed	Local
DefaultDocumentModule	%windir%\System32\inetsrv\...	Native	Local
DigestAuthenticationModule	%windir%\System32\inetsrv\...	Native	Local
DirectoryListingModule	%windir%\System32\inetsrv\...	Native	Local
DynamicCompressionModule	%windir%\System32\inetsrv\...	Native	Local
DynamicIpRestrictionModule	%windir%\System32\inetsrv\...	Native	Local
FailedRequestsTracingModule	%windir%\System32\inetsrv\i...	Native	Local
FastCgiModule	%windir%\System32\inetsrv\i...	Native	Local
FileAuthorization	System.Web.Security.FileAuth...	Managed	Local
FormsAuthentication	System.Web.Security.FormsA...	Managed	Local
HttpCacheModule	%windir%\System32\inetsrv\...	Native	Local
HttpLoggingModule	%windir%\System32\inetsrv\l...	Native	Local
HttpRedirectionModule	%windir%\System32\inetsrv\r...	Native	Local
IISCertificateMappingAuthenticationModule	%windir%\System32\inetsrv\...	Native	Local
IpRestrictionModule	%windir%\System32\inetsrv\i...	Native	Local
IsapiFilterModule	%windir%\System32\inetsrv\f...	Native	Local
IsapiModule	%windir%\System32\inetsrv\i...	Native	Local
OutputCache	System.Web.Caching.Output...	Managed	Local
Profile	System.Web.Profile.ProfileMo...	Managed	Local
ProtocolSupportModule	%windir%\System32\inetsrv\...	Native	Local
RequestFilteringModule	%windir%\System32\inetsrv\...	Native	Local

4. Right-click **StaticCompressionModule** and select **Unlock**.



Use this feature to configure the native and managed code modules that process requests made to the Web server.

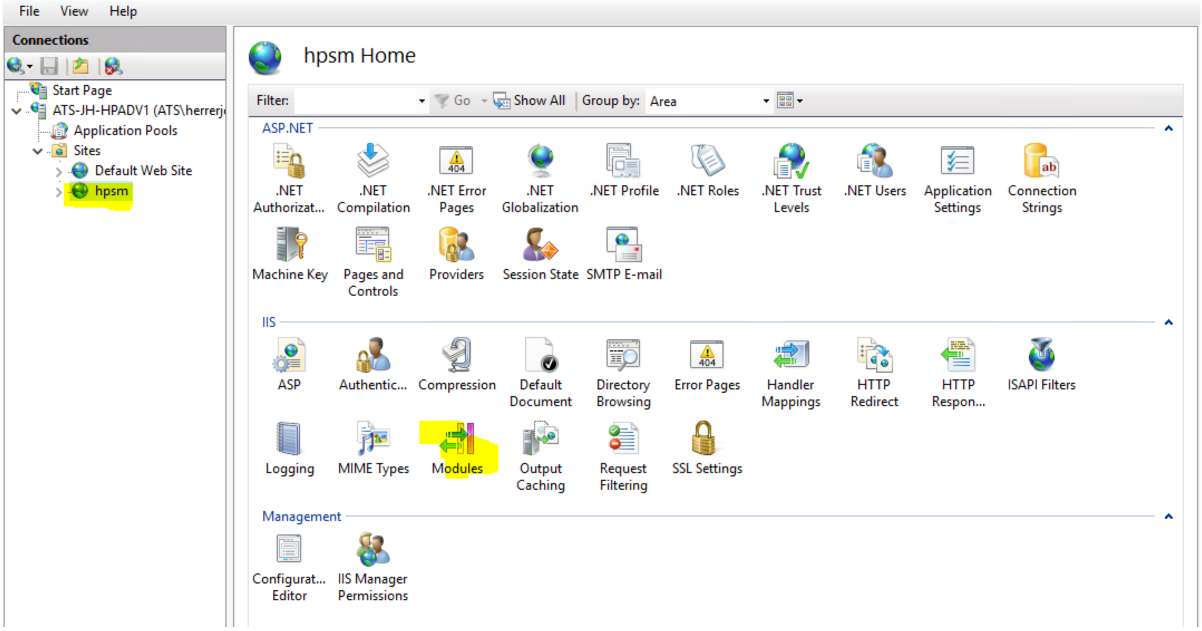
Group by: No Grouping

Name	Code	Module Type	Entry Type
DefaultDocumentModule	%windir%\System32\inetsrv\...	Native	Local
DigestAuthenticationModule	%windir%\System32\inetsrv\...	Native	Local
DirectoryListingModule	%windir%\System32\inetsrv\...	Native	Local
DynamicCompressionModule	%windir%\System32\inetsrv\...	Native	Local
DynamicIpRestrictionModule	%windir%\System32\inetsrv\...	Native	Local
FailedRequestsTracingModule	%windir%\System32\inetsrv\i...	Native	Local
FastCgiModule	%windir%\System32\inetsrv\i...	Native	Local
FileAuthorization	System.Web.Security.FileAuth...	Managed	Local
FormsAuthentication	System.Web.Security.FormsA...	Managed	Local
HttpCacheModule	%windir%\System32\inetsrv\...	Native	Local
HttpLoggingModule	%windir%\System32\inetsrv\l...	Native	Local
HttpRedirectionModule	%windir%\System32\inetsrv\r...	Native	Local
IISCertificateMappingAuthenticationModule	%windir%\System32\inetsrv\...	Native	Local
IpRestrictionModule	%windir%\System32\inetsrv\i...	Native	Local
IsapiFilterModule	%windir%\System32\inetsrv\f...	Native	Local
IsapiModule	%windir%\System32\inetsrv\i...	Native	Local
OutputCache	System.Web.Caching.Output...	Managed	Local
Profile	System.Web.Profile.ProfileMo...	Managed	Local
ProtocolSupportModule	%windir%\System32\inetsrv\...	Native	Local
RequestFilteringModule	%windir%\System32\inetsrv\...	Native	Local
RoleManager	System.Web.Security.RoleMa...	Managed	Local
ScriptModule-4.0	System.Web.Handlers.Script...	Managed	Local
ServerSideIncludeModule	%windir%\System32\inetsrv\i...	Native	Local
ServiceModel-4.0		naged	Local
Session		naged	Local
StaticCompressionModule		ive	Local
StaticFileModule		ive	Local
UrlAuthorization		naged	Local
UrlAuthorizationModule		ive	Local

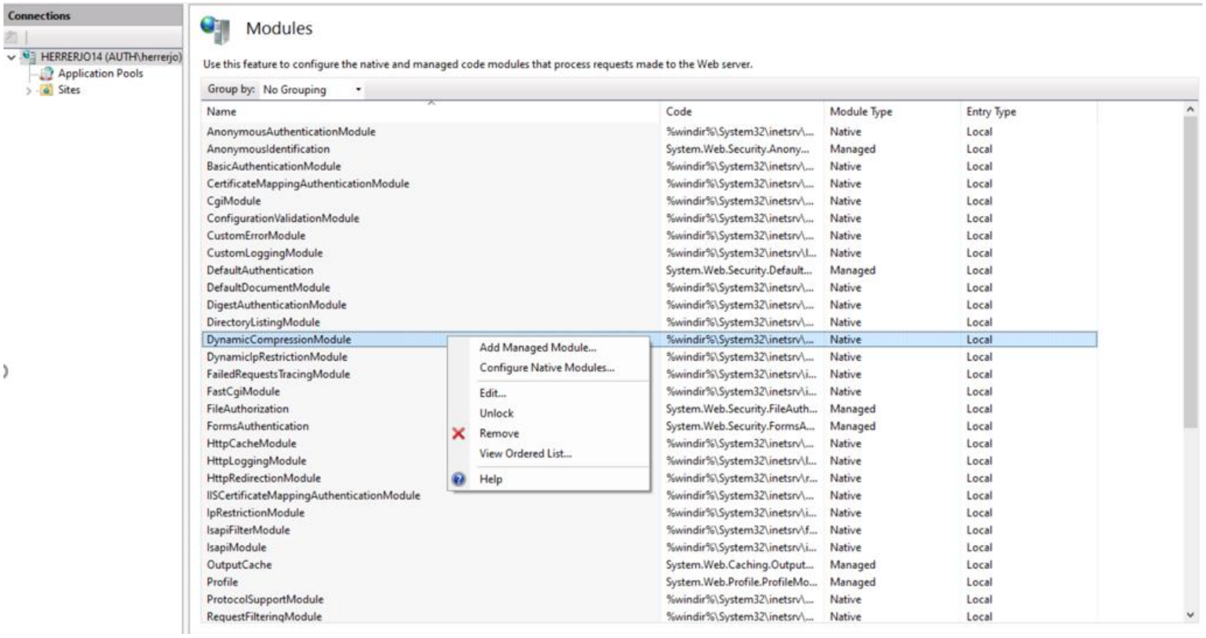
5. Expand Sites and select HPSM.

6. In the right pane in the IIS section , select "**Modules**" and select **“Open Feature”**, or double click the **Modules** option.

Figure: **Modules** option highlighted on HPSM Home screen



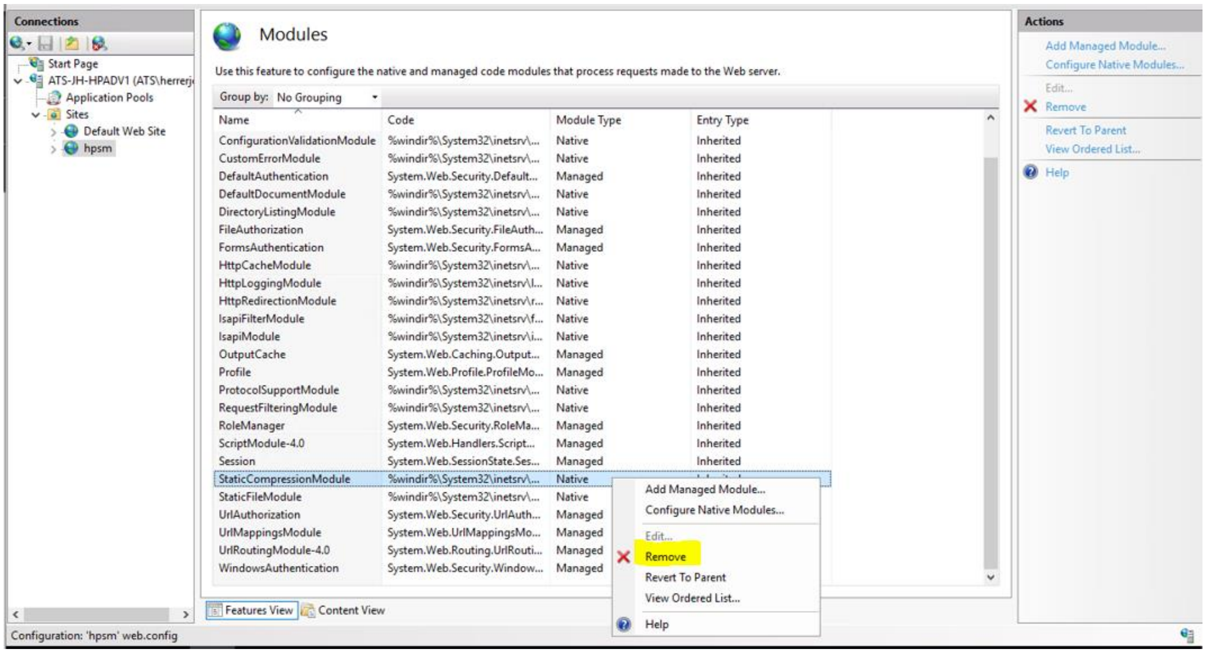
7. Right-click **DynamicCompressionModules** and select **Remove**.



Use this feature to configure the native and managed code modules that process requests made to the Web server.

Name	Code	Module Type	Entry Type
AnonymousAuthenticationModule	%windir%\System32\inetsrv\...	Native	Local
AnonymousIdentification	System.Web.Security.Anony...	Managed	Local
BasicAuthenticationModule	%windir%\System32\inetsrv\...	Native	Local
CertificateMappingAuthenticationModule	%windir%\System32\inetsrv\...	Native	Local
CgiModule	%windir%\System32\inetsrv\...	Native	Local
ConfigurationValidationModule	%windir%\System32\inetsrv\...	Native	Local
CustomErrorModule	%windir%\System32\inetsrv\...	Native	Local
CustomLoggingModule	%windir%\System32\inetsrv\l...	Native	Local
DefaultAuthentication	System.Web.Security.Default...	Managed	Local
DefaultDocumentModule	%windir%\System32\inetsrv\...	Native	Local
DigestAuthenticationModule	%windir%\System32\inetsrv\...	Native	Local
DirectoryListingModule	%windir%\System32\inetsrv\...	Native	Local
DynamicCompressionModule	%windir%\System32\inetsrv\...	Native	Local
DynamicIpRestrictionModule	%windir%\System32\inetsrv\...	Native	Local
FailedRequestsTracingModule	%windir%\System32\inetsrv\i...	Native	Local
FastCgiModule	%windir%\System32\inetsrv\i...	Native	Local
FileAuthorization	System.Web.Security.FileAuth...	Managed	Local
FormsAuthentication	System.Web.Security.FormsA...	Managed	Local
HttpCacheModule	%windir%\System32\inetsrv\...	Native	Local
HttpLoggingModule	%windir%\System32\inetsrv\l...	Native	Local
HttpRedirectionModule	%windir%\System32\inetsrv\r...	Native	Local
IISCertificateMappingAuthenticationModule	%windir%\System32\inetsrv\...	Native	Local
IpRestrictionModule	%windir%\System32\inetsrv\i...	Native	Local
IsapiFilterModule	%windir%\System32\inetsrv\f...	Native	Local
IsapiModule	%windir%\System32\inetsrv\i...	Native	Local
OutputCache	System.Web.Caching.Output...	Managed	Local
Profile	System.Web.Profile.ProfileMo...	Managed	Local
ProtocolSupportModule	%windir%\System32\inetsrv\...	Native	Local
RequestFilteringModule	%windir%\System32\inetsrv\...	Native	Local

8. Right-click **StaticCompressionModule** and select **Remove**.



Modules

Use this feature to configure the native and managed code modules that process requests made to the Web server.

Group by: No Grouping

Name	Code	Module Type	Entry Type
ConfigurationValidationModule	%windir%\System32\inetsrv\...	Native	Inherited
CustomErrorModule	%windir%\System32\inetsrv\...	Native	Inherited
DefaultAuthentication	System.Web.Security.Default...	Managed	Inherited
DefaultDocumentModule	%windir%\System32\inetsrv\...	Native	Inherited
DirectoryListingModule	%windir%\System32\inetsrv\...	Native	Inherited
FileAuthorization	System.Web.Security.FileAuth...	Managed	Inherited
FormsAuthentication	System.Web.Security.FormsA...	Managed	Inherited
HttpCacheModule	%windir%\System32\inetsrv\...	Native	Inherited
HttpLoggingModule	%windir%\System32\inetsrv\l...	Native	Inherited
HttpRedirectionModule	%windir%\System32\inetsrv\r...	Native	Inherited
IsapiFilterModule	%windir%\System32\inetsrv\f...	Native	Inherited
IsapiModule	%windir%\System32\inetsrv\i...	Native	Inherited
OutputCache	System.Web.Caching.Output...	Managed	Inherited
Profile	System.Web.Profile.ProfileMo...	Managed	Inherited
ProtocolSupportModule	%windir%\System32\inetsrv\...	Native	Inherited
RequestFilteringModule	%windir%\System32\inetsrv\...	Native	Inherited
RoleManager	System.Web.Security.RoleMa...	Managed	Inherited
ScriptModule-4.0	System.Web.Handlers.Script...	Managed	Inherited
Session	System.Web.SessionState.Ses...	Managed	Inherited
StaticCompressionModule	%windir%\System32\inetsrv\...	Native	
StaticFileModule	%windir%\System32\inetsrv\...	Native	
UrlAuthorization	System.Web.Security.UrlAuth...	Managed	
UrlMappingsModule	System.Web.UrlMappingsMo...	Managed	
UrlRoutingModule-4.0	System.Web.Routing.UrlRouti...	Managed	
WindowsAuthentication	System.Web.Security.Window...	Managed	

9. Restart the IIS.

As a non-admin user or service account (error 503)

When running HPSM Application Pool, if the service account is NOT a member of the local administrator group on the Security Manager server, additional steps are required to ensure the service account can access the service control manager like the Network Service can.

If these additional steps are not taken, the HPSM application pool will stop as soon as you try to open the HPSM web page, and a 503 error will likely be seen when attempting to launch Security Manager. The HPSMWeb.log in the directory *C:|Program Files (x86)|HP Security Manager|WebApp|log* and the Windows Event Viewer will contain errors indicating there are not sufficient rights to access service control manager:

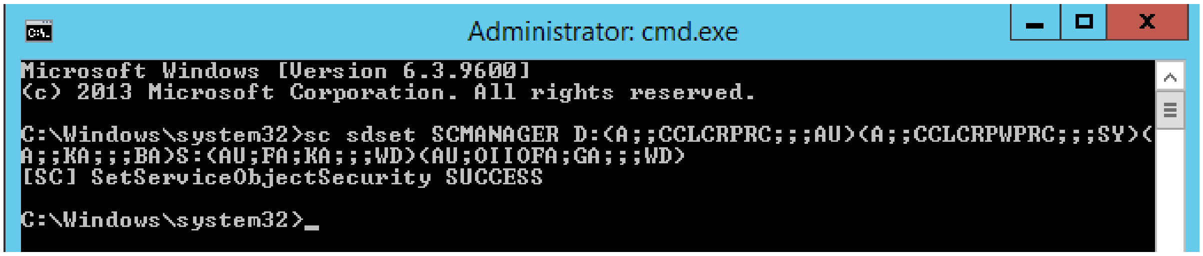
> <Data>HP JetAdvantage Security Manager: Unexpected Error Initializing - Shuting down: System.InvalidOperationException: Cannot open Service Control Manager on computer '.'. This operation might require other privileges. ---> System.ComponentModel.Win32Exception: Access is denied --- End of inner exception stack trace --- at System.ServiceProcess.ServiceController.GetDataBaseHandleWithAccess(String machineName, Int32 serviceControlManaqerAccess) at System.ServiceProcess.ServiceController.GetDataBaseHandleWithEnumerateAccess(String machineName) at System.ServiceProcess.ServiceController.GetServicesOfType(String machineName, Int32 serviceType) at System.ServiceProcess.ServiceController.GetServices() at LocksmithBusinessLogic.BizLogicMgr.ValidateProductAndDB() at LocksmithBusinessLogic.BizLogicMgr.Init()</Data>

By default, non-administrators cannot access the service control manager and cannot stop/start services.

To assign the rights needed for a non-admin account to access the service configuration manager, run the following from command prompt then restart the Security Manager service. This command provided privileges so that authenticated users can run the service control manager as required by Security Manager.

Open a command prompt as administrator, browse to *C:|Windows|System32*, and type the following command:

```
                    sc sdset SCMANAGER
   D:(A;;CCLCRPRC;;;AU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)S:(AU;FA;KA;;;WD)(A
   U;OIIOFA;GA;;;WD)
```



Administrator: cmd.exe

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>sc sdset SCMANAGER D:(A;;CCLCRPRC;;;AU)(A;;CCLCRPWPRC;;;SY)(
A;;KA;;;BA)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)
[SC] SetServiceObjectSecurity SUCCESS

C:\Windows\system32>_
```

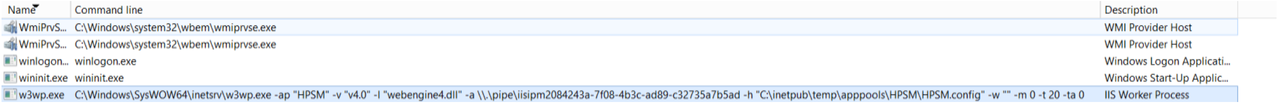
If successful, the line '[SC] SetServiceObjectSecurity SUCCESS' is displayed.

The final step is to make sure the service account is a member of the local IIS_USRS group.

Restart the Security Manager service, recycle the HPSM application pool, and you should be able to successfully open Security Manager.

When the HPSM application pool is running and the UI is launched, the process w3wp.exe will start. For each application pool inside IIS another w3wp.exe process will start.

When you add the column Command line in task manager you can see which process is used by which application pool.



Name	Command line	Description
WmiPrvS...	C:\Windows\system32\wbem\wmiprvse.exe	WMI Provider Host
WmiPrvS...	C:\Windows\system32\wbem\wmiprvse.exe	WMI Provider Host
winlogon...	winlogon.exe	Windows Logon Applicati...
wininit.exe	wininit.exe	Windows Start-Up Applic...
w3wp.exe	C:\Windows\SysWOW64\inetsrv\w3wp.exe -ap "HPSM" -v "v4.0" -l "webengine4.dll" -a \\.\pipe\iisipm2084243a-7f08-4b3c-ad89-c32735a7b5ad -h "C:\inetpub\temp\apppools\HPSM\HPSM.config" -w "" -m 0 -t 20 -ta 0	IIS Worker Process

In the command line column, you will see for the w3wp.exe process like:

> *C:|windows|SysWOW64|inetsrv|w3wp.exe* -ap "HPSM" -v "v4.0" -l "webengine4.dll" -a \\.a\pipe\iisipm324143214-2432424-sdfasfds- h "C:\inetpub\temp\apppools\HPSM\HPSM.config" -w – m 0 -t 20 -ta 0

For HPSM this also means that full access is required to the following file/path:
C:|Inetpub|temp|apppools|HPSM|HPSM.config.

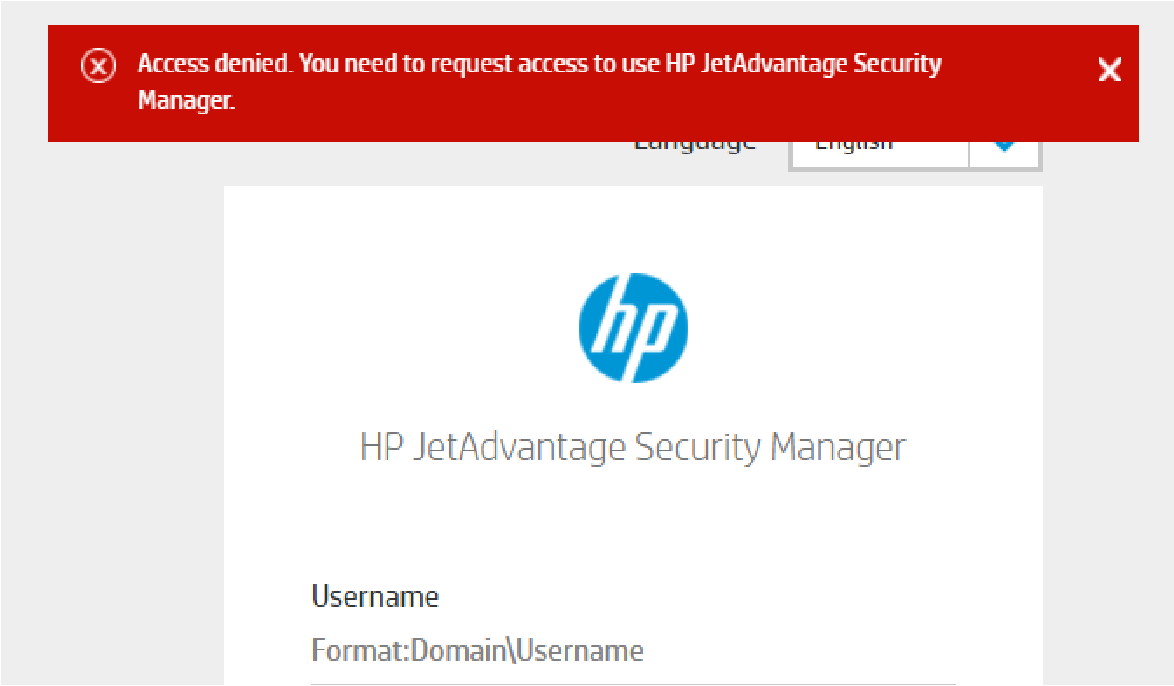
If the HPSM application pools is still crashing after trying to access the UI when running the HPSM application pool as a different user/service, then the account is most likely too restrictive. In that case try to run the default application of IIS as the same user/service. If the default application pool is also crashing when you try to access the default IIS homepage (http://localhost:80), then it confirms that the problem is outside of HPSM and caused by a too restrictive user or service account.

To resolve this issue, add the user/service account to the local administrators group.

Access Denied when trying to logon to HPSM

Users, even (local) Administrators might get an Access Denied when trying to logon to Security Manager.

Figure: **Access denied** error when trying to log in



Access denied. You need to request access to use HP JetAdvantage Security Manager.

Only users that are members of the HPIPSC group will have full access to the HP Security Manager and the specific user will have to be added to this group first.

Licensing Issues

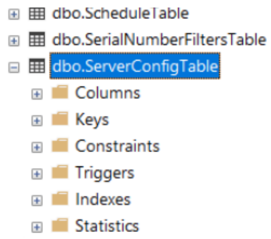
Licensing Issues in multi-homed environment: Failed to connect to licensing server

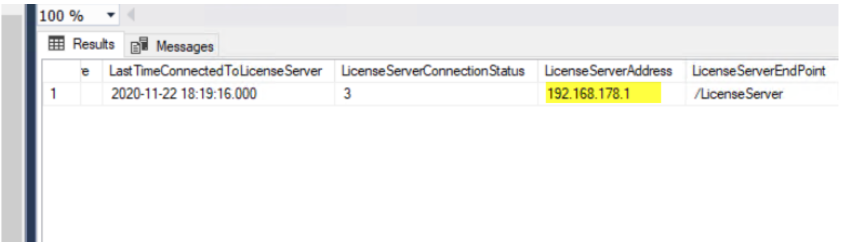
Issue

In a multi-homed server (several NICs installed). It is possible that the HPSM service tries to reach the HP Print License service on the wrong IP address/NIC with the result: Failed to connect to licensing server in the Dashboard screen and unable to add new licenses.

Perform the following steps to check if this is happening:

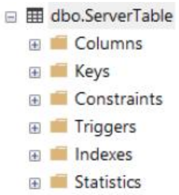
1. Retrieve the table DBO.ServerConfigTable (this contains one entry) and check for the LicenseServerAddress in this table.

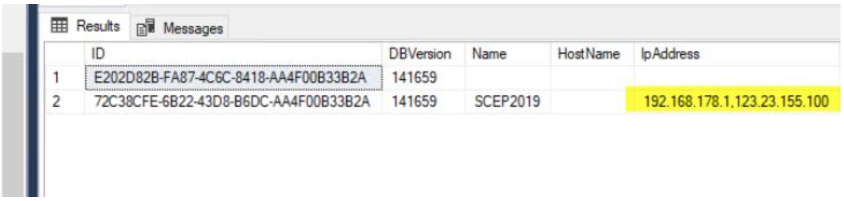




	e	LastTimeConnectedToLicenseServer	LicenseServerConnectionStatus	LicenseServerAddress	LicenseServerEndPoint
1		2020-11-22 18:19:16.000	3	192.168.178.1	/LicenseServer

2. Retrieve the table DBO.ServerTable and check which IP addresses are listed.





	ID	DBVersion	Name	HostName	IpAddress
1	E202D82B-FA87-4C6C-8418-AA4F00B33B2A	141659			
2	72C38CFE-6B22-43D8-B6DC-AA4F00B33B2A	141659	SCEP2019		192.168.178.1,123.23.155.100

If the second IP address in this table is used for communication with all the devices, then HPSM will not be able to communicate to the licensing server.

Solution

1. For every NIC , open the Control Panel, Network and Sharing Center and select Change Adapter Settings.
2. Right-click every Adapter/NIC.
3. Select **Internet Protocol Version 4 (TCP/IPv4)**.
4. Select **Properties**.
5. Select **Advanced** and disable **Automatic metric**.
6. Add a value for the Interface metric.
7. The interface which is used for communication with the devices should have the lowest number as lower number indicates higher priority.
8. Now restart the HP Security Manager service. During the service startup, HPSM will update the priority order in the DBO.ServerTable and update the DBO.ServerConfigTable accordingly.

NOTE: Changing the adapter order can also done in other ways, see for example: https://www.windowscentral.com/how-change-priority-order-network-adapters-windows-10

Licensing does not work when HPSM's hostname is changed after installation

If in the rare case the Security Manager server has obtained a new hostname, Flexera likely needs some help to reflect that change. Flexera refers to some keys in the windows registry related to server hostname.

The following error message in the HPSM Service log indicates an error while HPSM service tries to communicate with the Flexera Service. The line containing "GetLastFlexeraError" typically provides error information.

```
2021-05-25 13:54:13,478 ERROR Service   [License Task 5/25/21 01:54] - GetFeatureNames() - Unable
to get any features from Flexera. Retry 2
2021-05-25 13:54:14,494 ERROR Service   [License Task 5/25/21 01:54] - GetLicenseFeatures() -
Exception -  Attempted to read or write protected memory. This is often an indication that other
memory is corrupt. - Stacktrace -    at
HP.Print.License.CSharpWrapper.NativeMethods.HPGetLicenseFeaturelist(Int16 jobType, Int32
flag)__   at HP.Print.License.CSharpWrapper.Communication.GetLicenseFeatures(JobInfo job, Int32
searchFirst) in C:\Code\LS352\CSharpWrapper\Communication.cs:line 64
2021-05-25 13:54:14,494 ERROR Service   [License Task 5/25/21 01:54] - GetLastFlexeraError() - error
string is -  GetLastFlexeraError - Error string is - No socket connection to license server
manager._Feature:      IPSC_CMPS_License path:  27000@WIN-TEST;_FLEXnet Licensing error:-
7,10001_For further information, refer to the FLEXnet Licensing documentation,_available at
"www.flexerasoftware.com". - GetLastFlexeraError End
```

The error message "No socket connection to license server manager" indicates the following possibilities:

- Flexera service not running.
- HPSM Service's connection to Flexera service is blocked by a firewall.
- The registry entries telling HPSM Service where to connect to Flexera is not accessible, not present, corrupted, or incorrect (example change of hostname).

One option is to uninstall Security Manager, keep database and licenses intact, then reinstall Security Manager and point to the existing database. This would likely update the registry entries to the new hostname.

Another option involves editing the registry entries manually and restarting the services rather than a full uninstall/reinstall. The steps for this in HPSM 3.5 and older are different from the steps for HPSM 3.6 and newer.

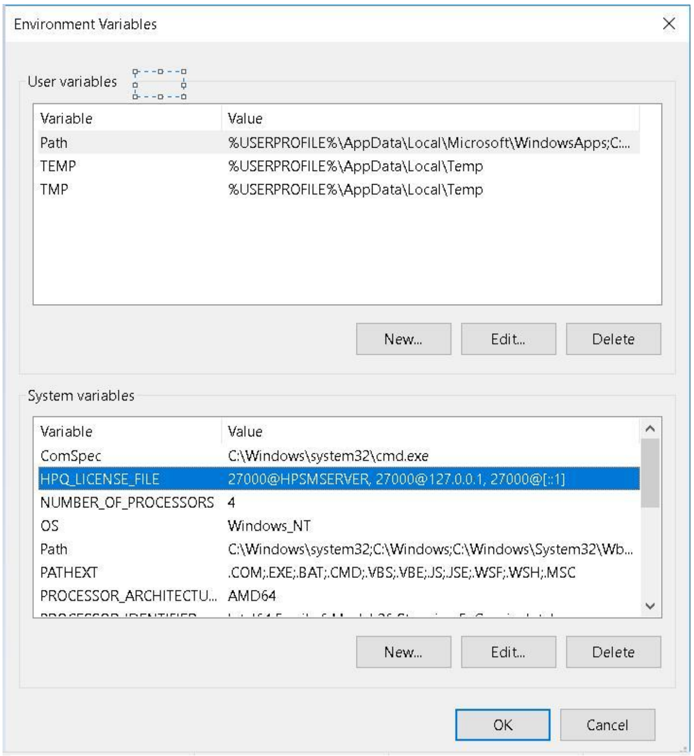
For HPSM 3.6 and newer

By default, HPSM 3.6 uses environment system variables for the variable HPQ_LICENSE_FILE instead of registry entries. The system variable also contains multiple values for IPv4 and IPv6 usage with the following value:

27000@<computername>,27000@127.0.0.1,27000@[::1]

Where <Computername> is the (host)name of the computer on which HPSM is running.

Figure: System variable HPQ_LICENSE_FILE



Variable	Value
Path	%USERPROFILE%\AppData\Local\Microsoft\WindowsApps;C:...
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

Variable	Value
ComSpec	C:\Windows\system32\cmd.exe
HPQ_LICENSE_FILE	27000@HPSMSERVER, 27000@127.0.0.1, 27000@[::1]
NUMBER_OF_PROCESSORS	4
OS	Windows_NT
Path	C:\Windows\system32;C:\Windows;C:\Windows\System32\Wb...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTU...	AMD64

When the HPSM hostname has been changed, the values for the HPQ_LICENSE_FILE system variable need to be changed accordingly. After this has been changed restart the HP Security Manager Service.

For HPSM 3.5 and older

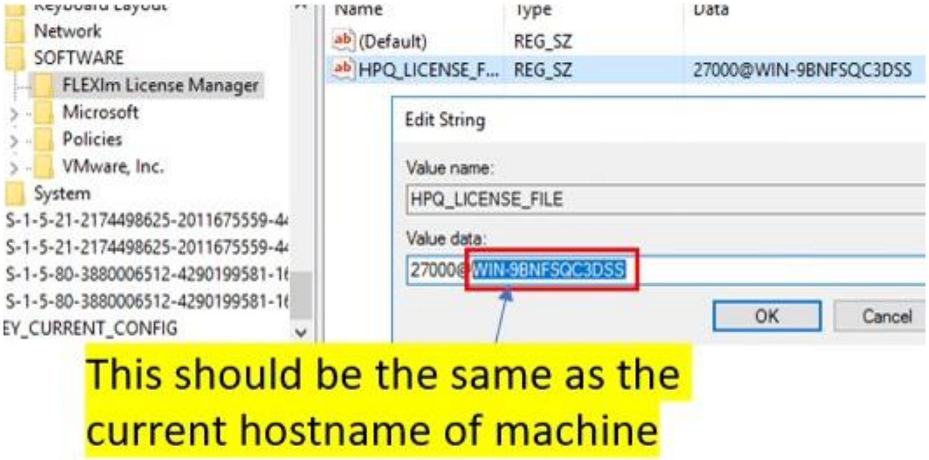
1. Stop the following services in this order:

- HP JetAdvantage Security Manager Service
- HP Print License Service
- Flexera Licensing Service

2. Open Registry Editor.

3. Find all the 'HPQ_LICENSE_FILE' keys in the registry and replace the values to reflect the new hostname (they will all have the old hostname referenced after the @ sign). There will be several keys in the registry for each machine and user account.

   Figure: Example of one of the HPQ_LICENSE_FILE entries in the registry



Value name: HPQ_LICENSE_FILE

Value data: 27000@WIN-9BNFSQC3DSS

This should be the same as the current hostname of machine

4. Delete license files under the following directory (do not delete DemoLicense file_ForStartup.lic).

   C:|ProgramData|HP|HP Print License Service|LicenseFiles

5. Delete All files under RecoveryXXX directory (do not delete the directory itself).

   C:|ProgramData|HP|HP Print License Service|RecoveryFile1 C:|ProgramData|HP|HP Print License Service|RecoveryFile2

6. Restart the services in the reverse order that you stopped them:

   - Flexera Licensing Service
   - HP Print License Service
   - HP JetAdvantage Security Manager Service

7. Check whether the HPSM server is working well with the demo license.

8. Install the issued license again.

'Insufficient licenses' error after nightly maintenance task with HPSM 3.6 or newer

If the message ‘insufficient’ licenses displays after the automatic nightly maintenance from HPSM, then do the following:

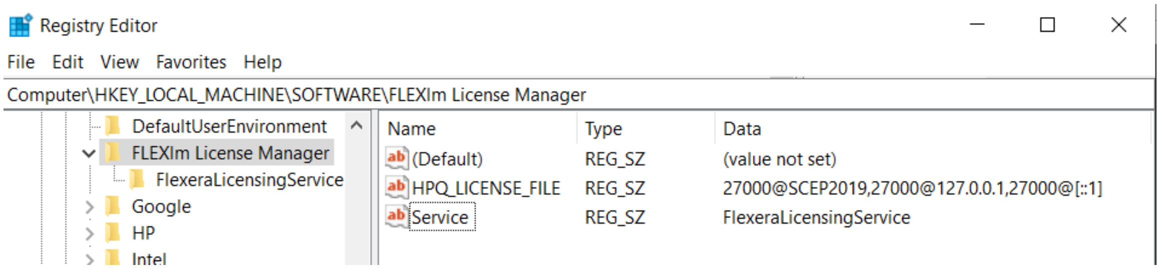
1. Remove the current system variable HPQ_LICENSE_FILE
2. Stop the following services in this order:
   - HP Security Manager Service
   - Flexera Licensing Service
3. Open Registry Editor and look for the following registry key:

   [HKEY_LOCAL_MACHINE\SOFTWARE\FLEXlm License Manager]

4. Create a new String Value with the name HPQ_LICENSE_FILE and the value where <Computername> is the (host)name of the computer on which HPSM is running:

   27000@<computername>,27000@127.0.0.1,27000@[::1]

   Figure: Computer is listed as the host name



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\FLEXlm License Manager

Name	Type	Data
(Default)	REG_SZ	(value not set)
HPQ_LICENSE_FILE	REG_SZ	27000@SCEP2019,27000@127.0.0.1,27000@[::1]
Service	REG_SZ	FlexeraLicensingService

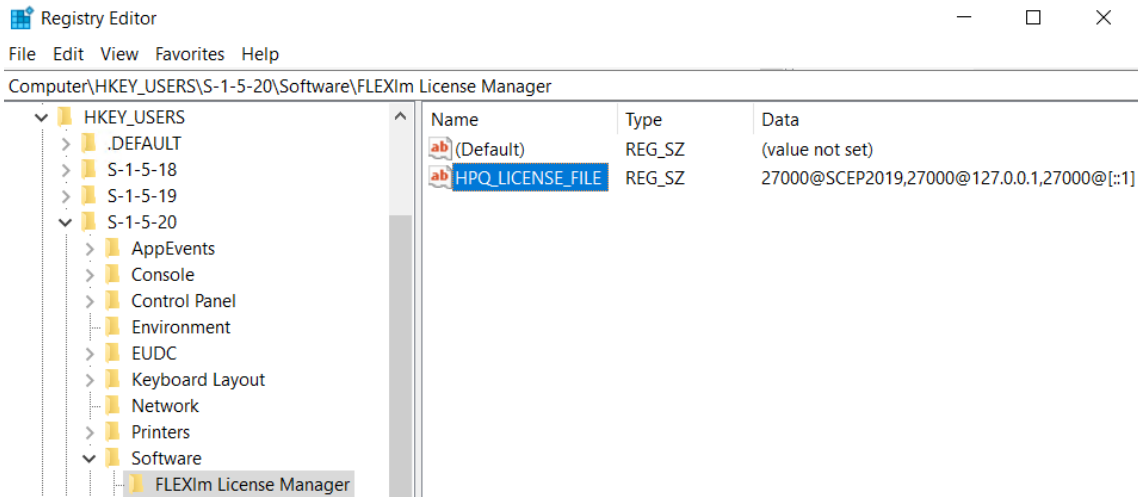
5. A similar entry must be made in the registry key for the user running the HPSM service. By default, this is the NETWORK service which has an SID of S-1-5-20. Look for the following registry key:

   [HKEY_USERS\S-1-5-20\Software\FLEXlm License Manager]

6. Create a new String Value under this key, with the string name HPQ_LICENSE_FILE and value where <Computername> is the (host)name of the computer on which HPSM is running:

   27000@<computername>,27000@127.0.0.1,27000@[::1]

   Figure: HPQ_LICENSE_FILE listed under FLEXlm License Manager registry key



Computer\HKEY_USERS\S-1-5-20\Software\FLEXlm License Manager

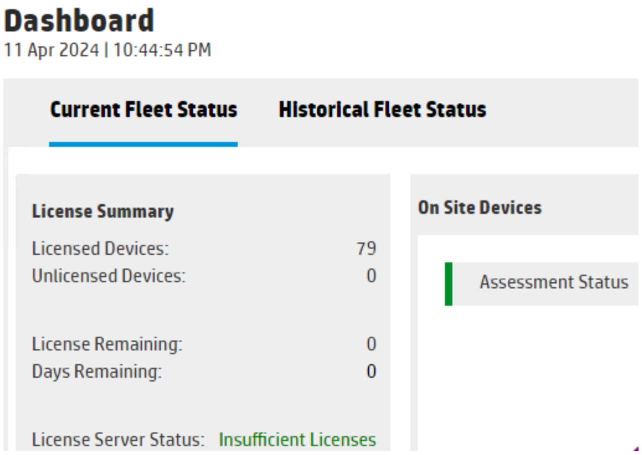
Name	Type	Data
(Default)	REG_SZ	(value not set)
HPQ_LICENSE_FILE	REG_SZ	27000@SCEP2019,27000@127.0.0.1,27000@[::1]

7. If HPSM service is configured to run under other user privileges, that’s specific user’s entry under HKEY_USERS must be modified.
8. Restart the services in the reverse order that you stopped them:
   - Flexera Licensing Service
   - HP Security Manager Service
9. Check whether the HPSM server is working well with the licenses.

   If the issue persists, reboot the server, and check again.

'Insufficient licenses' after upgrading to HPSM 3.10 or later

From HPSM 3.10 onwards, HPSM blocks the usage of all licenses when a duplicate license is detected in the folder: C:\ProgramData\HP\HPSM\LicenseFiles



Dashboard
11 Apr 2024 | 10:44:54 PM

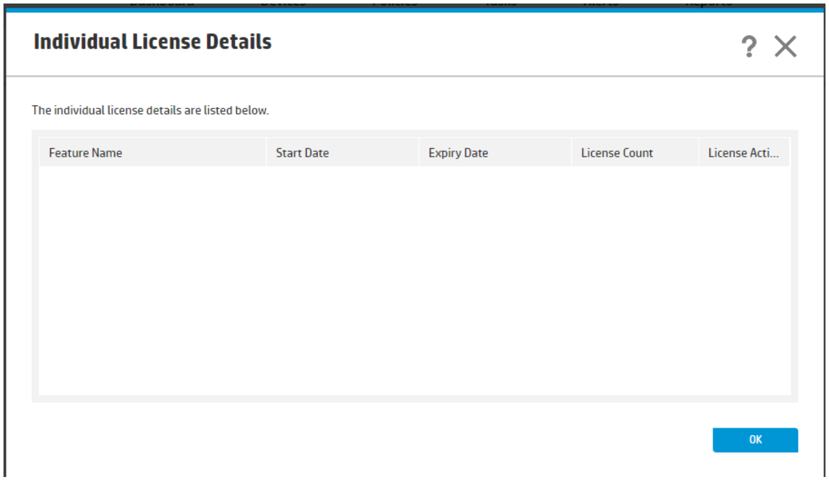
License Summary

Licensed Devices: 79
Unlicensed Devices: 0

License Remaining: 0
Days Remaining: 0

License Server Status: Insufficient Licenses

Under Settings, Licenses zero licenses are displayed. When clicking on View License Details, no information is displayed:



Individual License Details

The individual license details are listed below.

Feature Name	Start Date	Expiry Date	License Count	License Acti...

Solution:

1. Search CheckLicenseDuplication in the HPSM_service.log file to find which license file is duplicated (highlighted in yellow)

```
2024-04-09 14:06:02,016 INFO  Service   [License Task 4/9/24 02:06] -
Existing License in Folder: "00AE27A81D7E0E551A96F6EB738B_
     01000D9999CA5829DE54768B9764835E"
2024-04-09 14:06:02,016 INFO  Service   [License Task 4/9/24 02:06] -
Existing License in Folder: "0010FF9F8CB6C2CC792D73ADACCC_
     9A00643AD80B01D7E7729D8E5DAFECD4"
2024-04-09 14:06:02,016 INFO  Service   [License Task 4/9/24 02:06] -
Existing License in Folder: "00C409C1D64336C029596ED26BD8_
     AF00E2F416EBEBA935E52D14275D2C3E"
2024-04-09 14:06:02,016 ERROR Service   [License Task 4/9/24 02:06] -
LicenseWrapper.CheckLicenseDuplication: License :
"00EFEFA43EC385D06FD98DA1EF4B_  41008270CC7DB804E96281BE66F20B1D"
2024-04-09 14:06:02,016 DEBUG Service   [License Task 4/9/24 02:06] -
LicenseMgr.CheckOut
2024-04-09 14:06:02,016 DEBUG Service   [License Task 4/9/24 02:06] -
LicenseMgr.CheckOut #: 0
2024-04-09 14:06:02,016 DEBUG Service   [License Task 4/9/24 02:06] -
BizLogicMgrHelper -  GetDataSetCount returned: 9
2024-04-09 14:06:02,016 DEBUG Service   [License Task 4/9/24 02:06] -
LicenseWrapper.CheckOut for feature:  total # required: 9
```

```
2024-04-09 14:06:02,016 ERROR Service   [License Task 4/9/24 02:06] -
CheckOut() - Licenses Available - 0 - Seats Missing - 9 - Licenses
Assigned -0
2024-04-09 14:06:02,016 DEBUG Service   [License Task 4/9/24 02:06] -
LicenseWrapper.CheckOut numSeatsMissing: 9
2024-04-09 14:06:02,016 DEBUG Service   [License Task 4/9/24 02:06] -
LicenseMgr.UpdateCountAndStatus
2024-04-09 14:06:02,016 DEBUG Service   [License Task 4/9/24 02:06] -
BizLogicMgr - GetServerConfig
2024-04-09 14:06:02,031 DEBUG Service   [License Task 4/9/24 02:06] -
Method : DataProtection.Encrypt. Enter
2024-04-09 14:06:02,031 DEBUG Service   [License Task 4/9/24 02:06] -
License data:   -Feature:  -Expires in: 0 -# Assigned: 0 -# Available: 0
-# Total: 0 -Connection status ok: False -When:  -Feature:  -Feature:
12/31/99 11:59
```

2. Use the first number, in this case `00EFEFA43EC385D06FD98DA1EF4B`

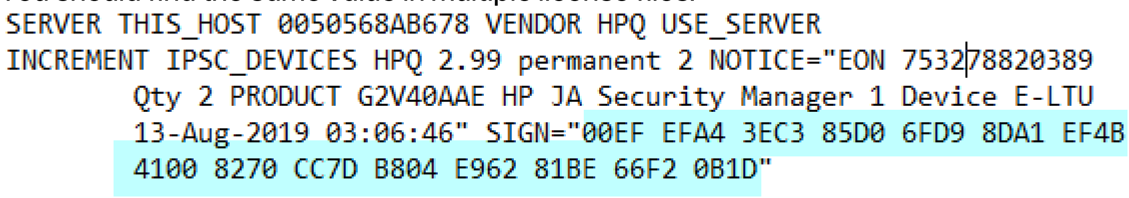
3. Add spaces to this after every 4th character, thus now it becomes

`00EF EFA4 3EC3 85D0 6FD9 8DA1 EF4B`

4. Now search for this value inside the license files in the directory:

C:\ProgramData\HP\HPSM\LicenseFiles

You should find the same value in multiple license files:



```
SERVER THIS_HOST 0050568AB678 VENDOR HPQ USE_SERVER
INCREMENT IPSC_DEVICES HPQ 2.99 permanent 2 NOTICE="EON 753278820389
        Qty 2 PRODUCT G2V40AAE HP JA Security Manager 1 Device E-LTU
        13-Aug-2019 03:06:46" SIGN="00EF EFA4 3EC3 85D0 6FD9 8DA1 EF4B
        4100 8270 CC7D B804 E962 81BE 66F2 0B1D"
```

5. Move the duplicate license files to a backup location.

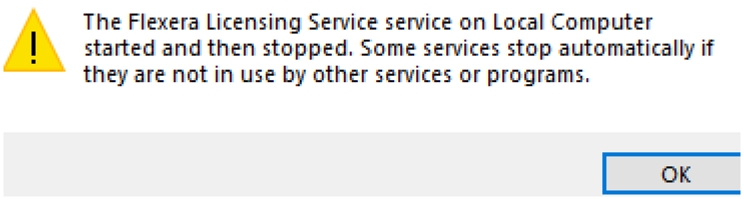
6. Stop HPSM service

7. Stop and restart flexera service

8. Restart HPSM service.

Flexera service Will Not Start (Flexera started and then stopped)

Shortly after starting the Flexera Service, you might see the following error message:



The Flexera Licensing Service service on Local Computer started and then stopped. Some services stop automatically if they are not in use by other services or programs.

This means that the account running the Flexera service does not have Full Control of the HPSM installation directory.

Solution

Go to the HPSM installation directory (Program Files (x86)\HP Security Manager) and provide Full Control to this directory for the account running the Flexera service.

‘Failed to retrieve the data’ error in the HPSM dashboard and zero licenses available

Whenever the error message “Failed to retrieve the data” in HPSM dashboard you need to check the **HPSMWeb.log** file in the directory \Program Files (x86)\HP Security Manager\WebApp\log for ERRORs. The following error might be listed in the log file:

```
020-11-16 13:45:04,560 INFO  Web  [71] - et=W2, controller=Licenses, action=Get,
httpresponsecode=InternalServerError, elapsed=60.525
2020-11-16 13:45:04,560 ERROR Web  System.ServiceModel.CommunicationObjectFaultedException:
The communication object, System.ServiceModel.Channels.ServiceChannel, cannot be used for
communication because it is in the Faulted state.
Server stack trace:
  at System.ServiceModel.Channels.CommunicationObject.Close(TimeSpan timeout)
  at System.ServiceModel.Channels.CommunicationObject.Close()
Exception rethrown at [0]:
  at System.Runtime.Remoting.Proxies.RealProxy.HandleReturnMessage(IMessage reqMsg, IMessage
retMsg)
```

The Flexera service might need more than 5 minutes to load all license files (if there is a high number of license files). This might be caused by a WCF timeout. By default this is set to 5 minutes.

Solution 1:
1. Stop HPSM service
2. Restart the hpsm application pool in IIS (internet information services).
3. Start HPSM service

Solution 2:
Step 1. Increased the clientTCPBindingOpenTimeout, clientTCPBindingSendTimeout, clientTCPBindingReceiveTimeout and clientTCPBindingCloseTimeout settings in the Web.config file and the HPSM_service.exe.config files to a higher value (for example 10 minutes for testing).

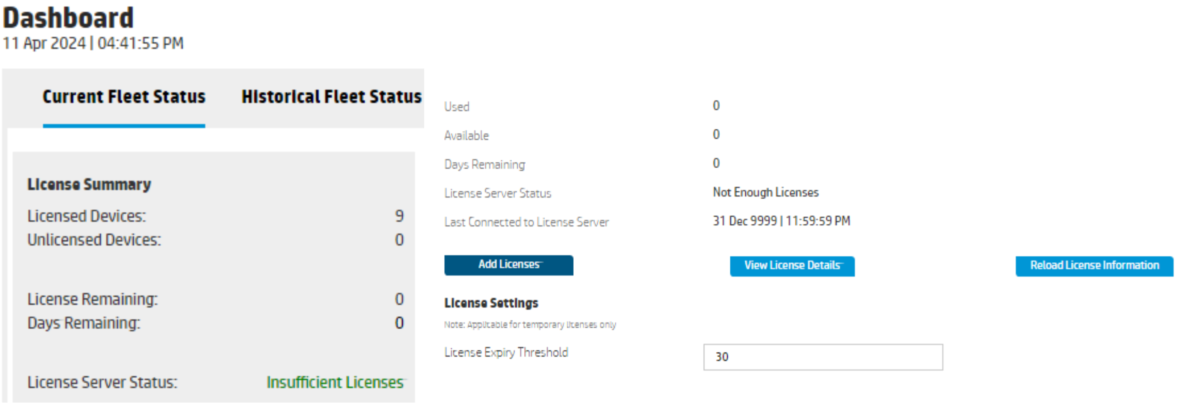
```
<!--ClientTCPBindingOpenTimeout : Increase the WCF timeout value to
open the WCF connection -->
    <add key="clientTCPBindingOpenTimeout" value="0:0:5:0" />
    <!--ClientTCPBindingSendTimeout : Increase the WCF timeout value
to send data in the WCF connection-->
    <add key="clientTCPBindingSendTimeout" value="0:0:5:0" />
    <!--ClientTCPBindingReceiveTimeout : Increase the WCF timeout
value to receive data in WCF connection-->
    <add key="clientTCPBindingReceiveTimeout" value="0:0:5:0" />
    <!--ClientTCPBindingCloseTimeout : Increase the WCF timeout
value to close the WCF connection-->
    <add key="clientTCPBindingCloseTimeout" value="0:0:5:0" />
```

NOTE: The following value requirements must be met:

- All values must have the same timeout
- The same values must be used in both Web.config and HPSM_service.config files
- Increasing the timeout causes UI to wait longer up-to the specific timeout, so it may be “busy,” until the request is completed or times out. So ideally, this should only be used if licensed features in UI, like creating blank policy is affected.

Step 2: Restart the HPSM application pool and then restart the HPSM service.

Insufficient Licenses in HPSM dashboard and zero licenses available with description of starting order of Flexera components



Dashboard
11 Apr 2024 | 04:41:55 PM

License Summary

Licensed Devices:	9
Unlicensed Devices:	0
License Remaining:	0
Days Remaining:	0
License Server Status:	Insufficient Licenses

Used	0
Available	0
Days Remaining	0
License Server Status	Not Enough Licenses
Last Connected to License Server	31 Dec 9999 | 11:59:59 PM

License Settings
Note: Applicable for temporary licenses only
License Expiry Threshold: 30

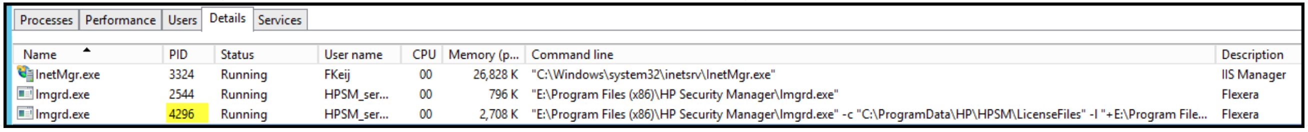
Check for the following error in the HPSMService.log

```
2024-04-11 16:40:01,123 ERROR Service   [License Task 4/11/24 04:39] -
GetLicenseFeatures() - Exception -  Attempted to read or write protected
memory. This is often an indication that other memory is corrupt. -
Stacktrace -    at
HP.Print.License.CSharpWrapper.NativeMethods.HPGetLicenseFeaturelist(Int1
6 jobType, Int32 flag)__    at
HP.Print.License.CSharpWrapper.Communication.GetLicenseFeatures(JobInfo
job, Int32 searchFirst)
2024-04-11 16:40:01,123 ERROR Service   [License Task 4/11/24 04:39] -
GetLastFlexeraError() - Fetch last error message from Flexera -
GetLastFlexeraError - Error string is - No socket connection to license
server manager._License path:  27000@WIN-AVNRO0BGK9B, 27000@127.0.0.1,
27000@[::1];_FlexNet Licensing error:-7,96 - GetLastFlexeraError End
2024-04-11 16:39:59,842 ERROR Service   [4] - GetFeatureNames() - Unable
to get any features from Flexera. Retry 3
```

The retry count will keep increasing. At the same time the Flexera.log might be ending with:

```
16:37:49 (lmgrd) pid 4296
16:37:49 (lmgrd) SLOG: Summary LOG statistics is enabled.
16:37:49 (lmgrd) Detecting other license server manager (lmgrd)
processes...
```

In the task manager you can see in the Details tab, that lmgrd.exe is listed twice:



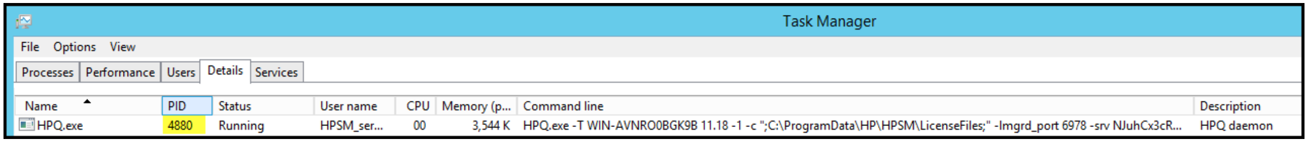
Name	PID	Status	User name	CPU	Memory (p...	Command line	Description
InetMgr.exe	3324	Running	FKeij	00	26,828 K	"C:\Windows\system32\inetsrv\InetMgr.exe"	IIS Manager
lmgrd.exe	2544	Running	HPSM_ser...	00	796 K	"E:\Program Files (x86)\HP Security Manager\lmgrd.exe"	Flexera
lmgrd.exe	4296	Running	HPSM_ser...	00	2,708 K	"E:\Program Files (x86)\HP Security Manager\lmgrd.exe" -c "C:\ProgramData\HP\HPSM\LicenseFiles" -l "+E:\Program File...	Flexera

This means that the Flexera service has not loaded all license information yet. Once all licenses have been loaded you will also see this loading process in the Flexera.log:

```
16:44:02 (lmgrd) License file(s):
C:\ProgramData\HP\HPSM\LicenseFiles\1.HP I-P Security_24260538_64.lic
C:\ProgramData\HP\HPSM\LicenseFiles\10.HP I-P Security_24261702.lic
C:\ProgramData\HP\HPSM\LicenseFiles\11.HP I-P Security_24261704.lic
C:\ProgramData\HP\HPSM\LicenseFiles\12.HP I-P Security_24261706.lic
C:\ProgramData\HP\HPSM\LicenseFiles\_DemoLicense_ForStartup.lic
```

HPSM will only be able to get the license count when the process HPQ.exe has been started.
This should be visible in the task manager and in the Flexera.log:

```
17:05:01 (lmgrd) Started HPQ (pid 4880)
```



Name	PID	Status	User name	CPU	Memory (p...	Command line	Description
HPQ.exe	4880	Running	HPSM_ser...	00	3,544 K	HPQ.exe -T WIN-AVNRO0BGK9B 11.18 -1 -c ";C:\ProgramData\HP\HPSM\LicenseFiles;" -lmgrd_port 6978 -srv NJuhCx3cR...	HPQ daemon

After HPQ has been started, click on another tab in HPSM and go back to the dashboard. The licenses should now be visible in the dashboard.

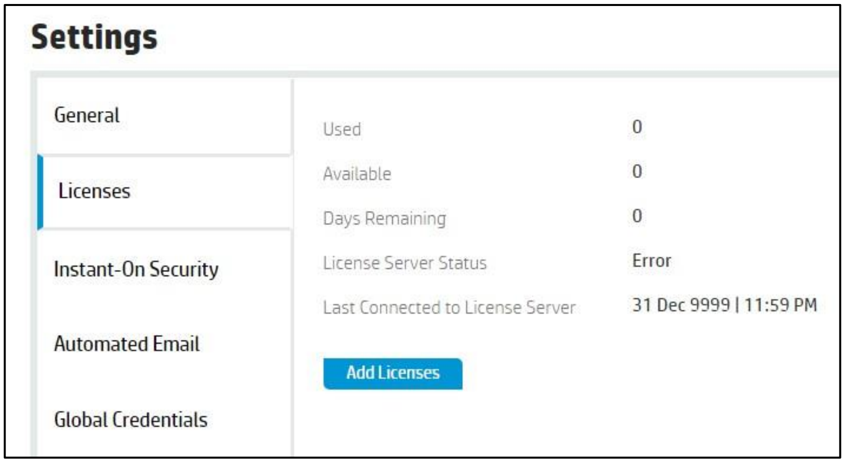
Mixing licenses limitations

Purchased licenses can be stacked, but mixing purchased with custom trial/evaluation licenses will usually generate errors. Examples include the following:

- Attempt to add a permanent license for 8000 devices with no expiration tied to mac address on top of a custom trial license that works on any machine: Failure - Cannot mix AnyHost and Mac Address hosts for IPSC_DEVICES.
- Attempt to add a permanent license for 8000 devices with no expiration tied to mac address over top of the demo license included in product: Success - IPSC_DEVICES replaces IPSC_CMPS.
- Attempt to add a permanent license for 8000 devices with no expiration tied to mac address over top of the downloaded 60-day trial license from the kiosk: Success - IPSC_DEVICES replaces IPSC_DEMO.
- Install downloaded 60-day trial license available on kiosk on top of demo license included in product: Success - IPSC_DEMO replaces IPSC_CMPS.
- Attempt to add another downloaded 60-day trial license from kiosk: Failure – cannot stack multiple IPSC_DEMO licenses.
- Attempt to add a custom trial license for 100 devices expiring Apr. 30 on top of default demo license included n product: Success, IPSC_DEVICES replaces IPSC_CMPS.
- Attempt to add another custom trial license for 550 devices expiring Aug 31 on top of another trial license: Success, added to existing 100 trial, but days remaining reflects first file read. Expired license is ignored. IPSC_DEVICES can stack together as long as all AnyHost.

Other Licensing Issues before HPSM 3.7

There are a couple of symptoms that would indicate something went wrong when applying the licenses. The License Server Status indicates Error instead of Success:



Used 0

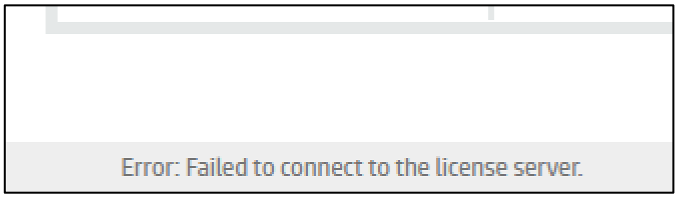
Available 0

Days Remaining 0

License Server Status Error

Last Connected to License Server 31 Dec 9999 | 11:59 PM

This may be accompanied by an error at the bottom of the page indicating "Error: Failed to connect to the license server."



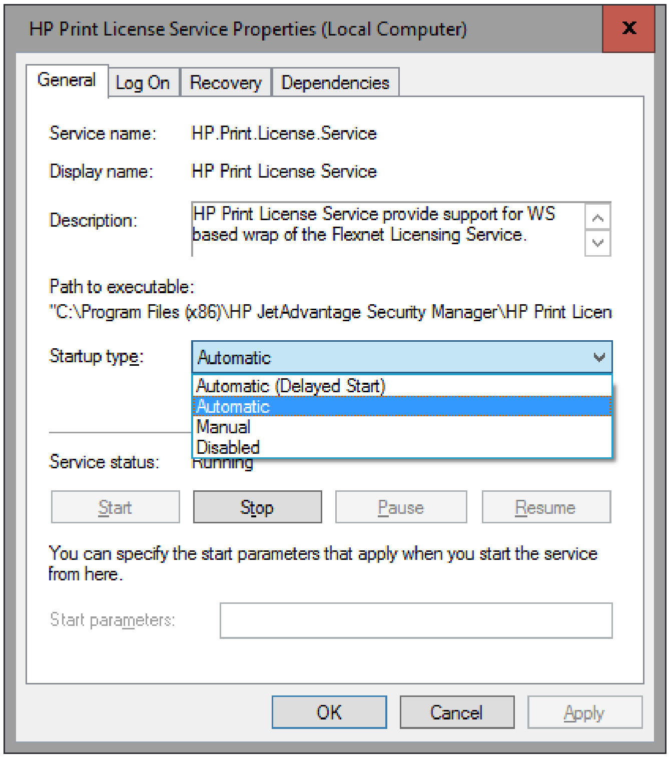
Error: Failed to connect to the license server.

Another sign of a problem occurs when attempting to Add Licenses Now, a failure screen displays indicating no licenses were added.

Here are some steps that can be followed to attempt to resolve these licensing issues:

1. Security Manager requires the proper startup of these 3 services.
    - Flexera Licensing Service
    - HP Print License Service
    - HP JetAdvantage Security Manager
2. You may need to stop and restart these services. Stop them in this order:
    - HP JetAdvantage Security Manager
    - HP Print License Service
    - Flexera Licensing Service
      Restart them in the reverse order:
    - Flexera Licensing Service
    - HP Print License Service
    - HP JetAdvantage Security Manager
3. Launch the UI.

The licensing process in Security Manager is handled by two services: Flexera and HP Print License service. The latter relies on the former working.



Service name: HP.Print.License.Service

Display name: HP Print License Service

Description: HP Print License Service provide support for WS based wrap of the Flexnet Licensing Service.

Path to executable:
"C:\Program Files (x86)\HP JetAdvantage Security Manager\HP Print Licen

Startup type: Automatic

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

There may be cases where the Flexera service cannot start because of reduced permissions on the service account it is using. Windows Event Viewer may indicate the service cannot start because of reduced permissions.

By default, the Flexera service runs under the Local Service account. If permissions are reduced on this account and cannot be increased, try running the service under another account with more permissions.

The services may also be starting up too slowly so that the later services cannot determine the initial services are started.

Try manually starting the services with a time break of perhaps 30 seconds in between. If this resolves the issue, a delay can be defined for the services when they automatically start.

Method one: Uninstall Security Manager

1. Make sure the uninstaller removes licenses.
2. Reinstall and add licenses.
3. When the uninstaller asks if you want to delete the database also, you can choose not to do so if you prefer to maintain all the devices, policies, and remediation data from the previous install.
4. Re-install Security Manager, point to the existing database, and then install the licenses.

Method two: Manually delete evaluation licenses
If you do not want to uninstall Security Manager, another technique for removing evaluation licenses is to manually delete them.

To do this, follow these steps:

1. Stop the services in this order:
   - HP JetAdvantage Security Manager service
   - HP Print License service
   - Flexera service
2. Delete the evaluation license file (do not delete the DemoLicense file) under:
   C:|ProgramData|HP|HP Print License Service|Licenses
3. Delete all recovery files (LSRecovery.xml) under the recovery directories (if present):
   C:|ProgramData|HP|HP Print License Service|RecoveryFile1
   C:|ProgramData|HP|HP Print License Service|RecoveryFile2
4. Reboot the HPSM server (in most cases restarting first Flexera service, then the Print License service and finally HP JetAdvantage Security Manager service, will not fix the licensing issue, a reboot is required in most situations).

If both services are running and issues still arise, there may license type conflicts such as trying to add purchased licenses alongside custom trial\evaluation licenses. Each license has unique parameters such as machine type, expiration date, and feature type. Some varieties cannot be mixed.

If problems still exist, there might be a port conflict. For example, Port 8888 needs to be open for the HP Print License service so check firewall and/or McAfee type firewall products. It might be easier to allow applications through the firewall instead of specific ports. Allow the following through Rules:

C:|Program Files (x86)| HP JetAdvantage Security Manager|HP Print License Service|lmgrd.exe
C:|Program Files (x86)| HP JetAdvantage Security Manager|HP Print License Service|HPQ.exe
C:|Program Files (x86)| HP JetAdvantage Security Manager|HP Print License Service|HP.Print.License.Host.WindowsService.exe

Even though Flexera and the HP Print License service are on the same machine, other products that use the HP Print License service may not have Flexera on the same machine. The HP Print License Service requires the dedication of this TCP Port and cannot be modified for alternative port assignment.

A successful use of port 8888 displays in the HPSM_Service.log file as follows:

```
2018-01-11 11:31:49,416 INFO Service      [License Task 1/11/18 11:31] - LicenseWrapper.Connect using
IPs : 15.25.250.161 : 15.25.250.161 device features ::devices version:   :host addr:
net.tcp://15.25.250.161:8888/LicensingService ok to LogErrors: True
```

An unsuccessful use of port 8888 displays in the HPSM_Service.log file as follows:

```
2015-04-07 11:15:27,146 ERROR Service - [License Task 4/7/15 11:15] - LicenseWrapper.Heartbeat -
(skipping) unexpected ERROR: System.ServiceModel.EndpointNotFoundException: Could not
connect to net.tcp://192.168.181.1:8888/LicensingService. The connection attempt lasted for a time
span of 00:00:21.0285341. TCP error code 10060: A connection attempt failed because the
connected party did not properly respond after a period, or established connection failed because
connected host has failed to respond 192.168.181.1:8888.
```

Other applications such as ePrint also use this HP Print License service but can use a different version that conflicts with the version used by Security Manager. For this reason, ePrint and Security Manager cannot coexist on the same machine. You may have to uninstall the existing HP Print License Service under Programs and Features or Add/Remove Programs and reinstall Security Manager to obtain the proper HP Print License Service.

Log files can indicate possible causes of the problem. Two log files exist for the license service:

C:|ProgramData|HP|HP Print License Service Files|Flexera.log C:|ProgramData|HP|HP

Print License Service Files|HPPLS.log

The Security Manager service log can also provide valuable information:

C:|Program Files (x86)| HP JetAdvantage Security Manager|log|HPHPSM_Service.log

For example:

```
2015-04-07 11:15:27,146 ERROR Service - [License Task 4/7/15 11:15] - LicenseWrapper.Heartbeat -
(skipping) unexpected ERROR: System.ServiceModel.EndpointNotFoundException: Could not
connect to net.tcp://192.168.181.1:8888/LicensingService. The connection attempt lasted for a time
span of 00:00:21.0285341. TCP error code 10060: A connection attempt failed because the
connected party did not properly respond after a period, or established connection failed because
connected host has failed to respond 192.168.181.1:8888.
```

A “Flexera call completed” message in the HPPLS log file indicates the issue is not related to the Flexera service.

A Winsock error usually means the service is having trouble opening a TCP socket. This might be network or firewall related, perhaps caused by a security app such as McAfee, etc.

The table below mentions possible error codes that may be seen in the Print License Service log file and a brief description of each.

Error Code	Description
0	Success.
-100	Something is wrong with the service. A security token mismatch between the client and the server or internal exceptions un- handled by the HPPLS.
-101	Null job handler.
-102	An invalid parameter is passed to any of the APIs.
-104	This corresponds to any exception that is thrown by HPPLS. The details of the exception are logged in the log file.
-105	A valid session is already present, and client tries to create another session.
-106	Either there are no features checked out and client tries to query for feature details or there is no feature available with the given name and version.
-107	An API is called with an empty session.
-108	Flexera server is not available.
-109	Flexera server is not responding.
-110	Some features that are passed to the API are invalid.
-111	Invalid file content.
-112	Token mismatch.
-113	Client does not exist.
-130	Flexera service is either not up & running or not ready to serve.

If Security Manager had been installed and the IP Address changed, that might cause issues as the HP Print License service would be trying to contact the Flexera service as seen in the HPPLS.log file:

net.tcp//Old IP Address:8888/LicensingService

An uninstall and reinstall of HPSM would solve this issue.

A purchased license file must be ordered with the exact match of the Security Manager server MAC address. The HP Print License manager will fail to operate properly without this exact match. If using VMWare, make sure the appropriate virtual adapter MAC address is used. The physical mac address of the NIC for the machine as seen under IPCONFIG is not the mac address of the VM.

Check the documentation of the VM vendor for instructions on how to find the mac address. VMWare also recommends a static MAC assignment to accommodate software licensing scenarios. If set to dynamic, it will not match the mac address in the license file any longer. Check the documentation of the VM vendor for instructions on how to set to static.

If the mac address in the license is not what Security Manager expects, there should be an error in the Flexera.log file found under C:\ProgramData\HP\HP Print License Service indicating what it read in the license file and what it expects for the correct mac address:

```
10:15:13 (HPQ) Wrong hostid on SERVER line for license file: 10:15:13 (HPQ)    C:\ProgramData\HP\HP
Print License Service\LicenseFiles\24092015101513_IPSC_DEVICES.lic
10:15:13 (HPQ) SERVER line says d8d38582501d, hostid is d8d38582501c 10:15:13 (HPQ) Invalid hostid
on SERVER line
10:15:13 (HPQ) Disabling 500 licenses from feature IPSC_DEVICES
```

If a trial/evaluation license installs fine but a purchased license does not install, it is likely that either the mac address is wrong in the license file or the license file itself is bad. A purchased license differs from a trial/evaluation license in that the purchased license only works on the machine where the mac address is provided. That mac address must match the mac address in use, and if running on a VM, the physical mac address for the machine is not the same as the mac address of the VM.

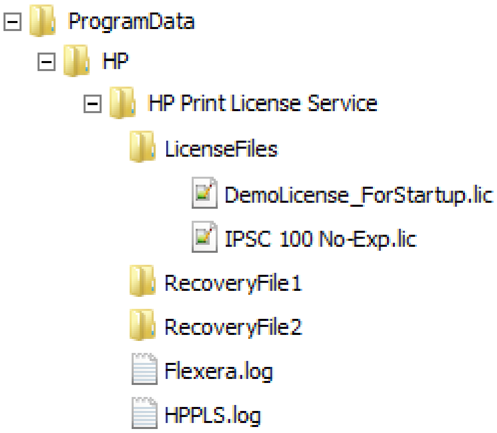
Second, it is possible that the license file itself is bad or corrupt, although rare. The feature name in the license file must be either IPSC_DEVICES or IPSC_DEMO. If it is HPSM_DEVICES, contact the licensing support team and request another license. When doing so, make sure to instruct them to generate a new license instead of re-sending the original license as they will not know the original license is bad unless you tell them.

The license has readable text in the first half and encrypted content (SIGN=xxxx …) in the latter half that matches the readable content in the first half. Content of license files SHOULD NOT be changed/edited at any time. Any edit to the readable content will no longer match the encrypted portion and the file will become corrupted and unusable. If "SIGN=0" in the latter half of the file, it is corrupt, and a new license file needs to be generated.

Make sure license files are present under:

C:|ProgramData|HP|HP Print License Service|LicenseFiles.

NOTE: By default, C:\ProgramData is a hidden folder. Either un-hide hidden folders to view this folder or type the folder name (C:\ProgramData) directly in the address bar.



```
⊟ ProgramData
  ⊟ HP
    ⊟ HP Print License Service
        LicenseFiles
            DemoLicense_ForStartup.lic
            IPSC 100 No-Exp.lic
        RecoveryFile1
        RecoveryFile2
        Flexera.log
        HPPLS.log
```

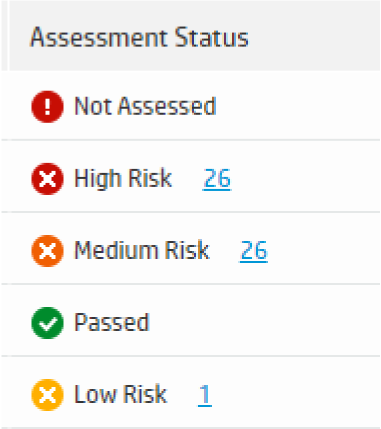
Device Status Errors and Credential Failures

It is important to understand how Security Manager interacts with devices to be able to troubleshoot issues such as credential failures or device status errors.

Security Manager uses a variety of techniques to manage different types of devices depending upon how features are exposed on the device.

- **SNMP** - Simple Network Management Protocol (SNMP) is used extensively in Security Manager for all types of devices, especially during a Verify task to determine status. SNMP is used to read from a device (SNMP GET REQ) or to write to a device (SNMP SET REQ). The packet contains one or more Object Identifiers (OID) that defines the item being read or configured. Security Manager supports both SNMPv1/SNMPv2, which is unencrypted, and SNMPv3, which is encrypted.

- **Web Services** - Web Services (WS*) is a SOAP-based protocol used mostly with HP FutureSmart devices. This communication uses port 7627. Security Manager communicates over HTTPS to ensure that all data is encrypted during the transmission.
- **LEDM** - For the configuration of some non-HP FutureSmart devices, Security Manager uses Low- end Data Model (LEDM). LEDM is based on the Representational State Transfer (REST) style architecture, which is a design that describes a simple interface for transmitting XML data over HTTP or HTTPS without an additional messaging layer. This configuration is done over HTTP or HTTPS depending on the device configuration and device firmware.
- **HTTP** ("screen scraping" or "web scraping) – Some features are not exposed through typical management protocols thus Security Manager resorts to performing what is referred to as "screen scraping" to use HTTP to read a page and extract settings.
- **DSMP** - DSMP is a proprietary protocol that Security Manager uses for some configuration options in the Digital Sending category for legacy HP Enterprise printers. DSMP is sent over HTTP.
- **PJL** - Security Manager may use Printer Job Language (PJL) to test the PJL Password on some devices.
- **CDM** - Security Manager uses a proprietary implementation of CDM only in version 3.1 and beyond to accommodate the "Secure by Default" initiative released in HP FutureSmart 4.5 firmware. CDM is sent over HTTPS.



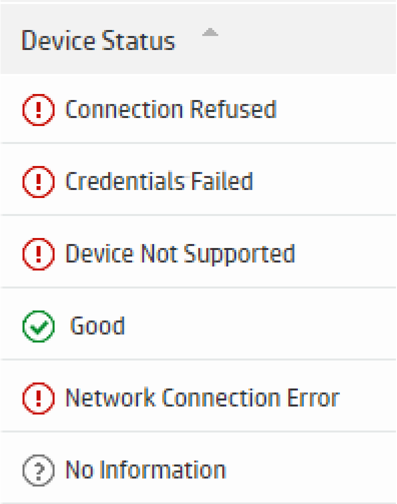
Assessment Status
! Not Assessed
✗ High Risk 26
✗ Medium Risk 26
✓ Passed
✗ Low Risk 1

The Assessment Status and is defined as follows

- Not assessed
- Assessed and all settings in compliance
- Assessed with only low risk items out of compliance
- Assessed with medium risk items (and possibly low) items out of compliance
- Assessed with high-risk items (and possibly low/medium) items out of compliance

It has nothing to do with the state or status of the device, it merely indicates which settings were in or out of compliance during the last assessment task.

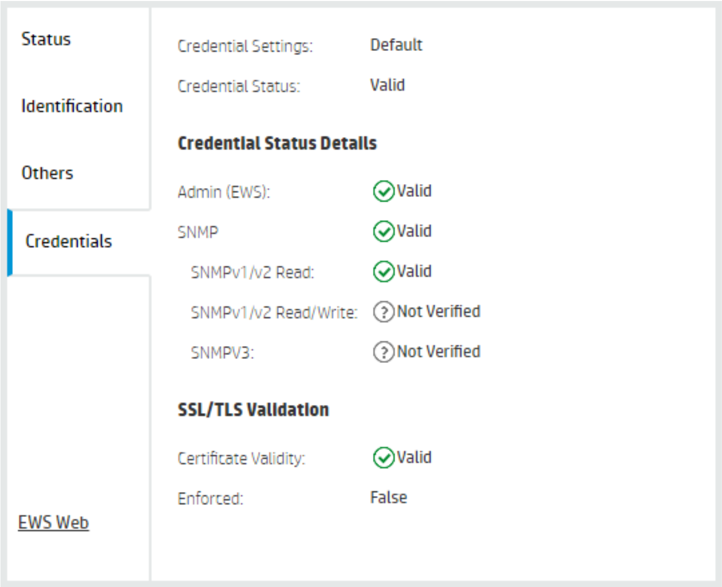
The Device Status column includes a visual icon to indicate Good (green check mark) or some sort of error (red x) indicating a problem. It also includes a textual description of the error as follows:



Device Status
❗ Connection Refused
❗ Credentials Failed
❗ Device Not Supported
✓ Good
❗ Network Connection Error
? No Information

- **Network Connection Error** - this error indicates an issue trying to communicate with a device over a specific protocol. Many times Security Manager is trying to securely connect to the device over SSL/TLS and cannot for some reason. Most common reasons for this error include the following:
  - No response from device on basic network communications such as ping. Device may be powered off or disconnected from network. Pings may be filtered at router or firewall.
  - Device responds to pings but does not respond to Web Services (WS*) queries.
  - Cannot browse to EWS page, perhaps EWS has been disabled.SSL/TLS handshake fails so transaction cannot be encrypted. Operating system controls the TLS versions in the handshake, not HPSM. Select the device and then select **Do Not Enforce SSL/TLS**.
  - Certificate has MD5 hash which Microsoft no longer supports, so SSL/TLS handshake is rejected. Right-click the device, select **Set SSL\TLS Enforcement**, and then select **Do Not Enforce** to temporarily fix. Now Verify again to see if state clears. If so, for a permanent solution, regenerate the self-signed certificate under EWS (might require newer Jetdirect firmware) to generate a new certificate with a supported hash.
  - ACL (Access Control List) blocking.
  - No certificate support, already set to not enforce SSL/TLS (grayed out).
  - Ports blocked, perhaps by firewall
  - Some cases have been reported whereby DAT indicates SNMPv1/v2 passes for Gets and Sets yet SNMPv3 cannot be enabled using SNMPv1/v2 and this error is generated. Often a second remediation will clear the error.

- **Connection Refused / Invalid Identity Certificate** - If Security Manager installed an identity certificate on the device, it tags it in the database to enforce trust for future communications.
    - Removed, expired, or revoked certificates.
    - Cannot connect to CRL (certificate revocation list) to check revocation.
- **Credentials Failed** - a mismatch occurred between what is stored in the database for the specific credential and what is on the device. Security Manager will always try what is stored in database first, then public/blank in case the credential was erased on the device, and finally any credential stored in the Global Credential Store. If all three attempts fail, Security Manager posts Credentials Failed as it needs proper credentials to communicate with the device.
    - SNMP behavior is to not respond to SNMP REQ packet when community name is wrong.
    - Older devices had two locations under EWS for Admin Password.



Credential Settings: Default

Credential Status: Valid

Credential Status Details

Admin (EWS):	✓ Valid
SNMP	✓ Valid
SNMPv1/v2 Read:	✓ Valid
SNMPv1/v2 Read/Write:	? Not Verified
SNMPV3:	? Not Verified

SSL/TLS Validation

Certificate Validity: ✓ Valid

Enforced: False

- **Device Not Supported** - device does not support enough security related items to be deemed supported by Security Manager. See “Supported Device List” whitepaper for a complete list of supported devices.
- **Error** - this is a rarely seen state that seems to occur on the devices that answer so little to queries that Security Manager deems it not manageable.
- **Hostname Resolution Error** - the hostname cannot be resolved. The DNS name server does not recognize the hostname being presented by Security Manager that previously represented the device.
- **License Required for Assessment** - not enough licenses are available, a license has not been assigned to the device yet.
- **No Information** - a Verify task has not yet been performed where Security Manager gathers a dozen or so attributes about the device and populates the columns. Adding a device will only perform a hostname lookup, but the device will remain in No Information status until a Verify is performed or an Assessment which begins with a Verify task.

Remember, browsing to EWS is strictly HTTP traffic. Security Manager and tools such as Web Jetadmin use WS*, LEDM, SNMP, DSMP, etc. to communicate to devices for the various settings depending upon how they are exposed for fleet management per device family.

For example, SNMP could be disabled on devices and not affect EWS browsing, but tools such as Web Jetadmin and Security Manager would be severely hampered as they would not be able to communicate with the device using a critical protocol.

Credential Management

It is common for both Web Jetadmin and Security Manager to be managing a fleet, and when one tool changes device credentials, the other tool indicates a credential failure until it too knows the credentials.

The best way to troubleshooting credential failures is to hone in on a single device, highlight one device and check the Properties by clicking on the device IP Address link. Normally for devices with no credential failure, the credentials will all be in a Valid state as seen to the right.

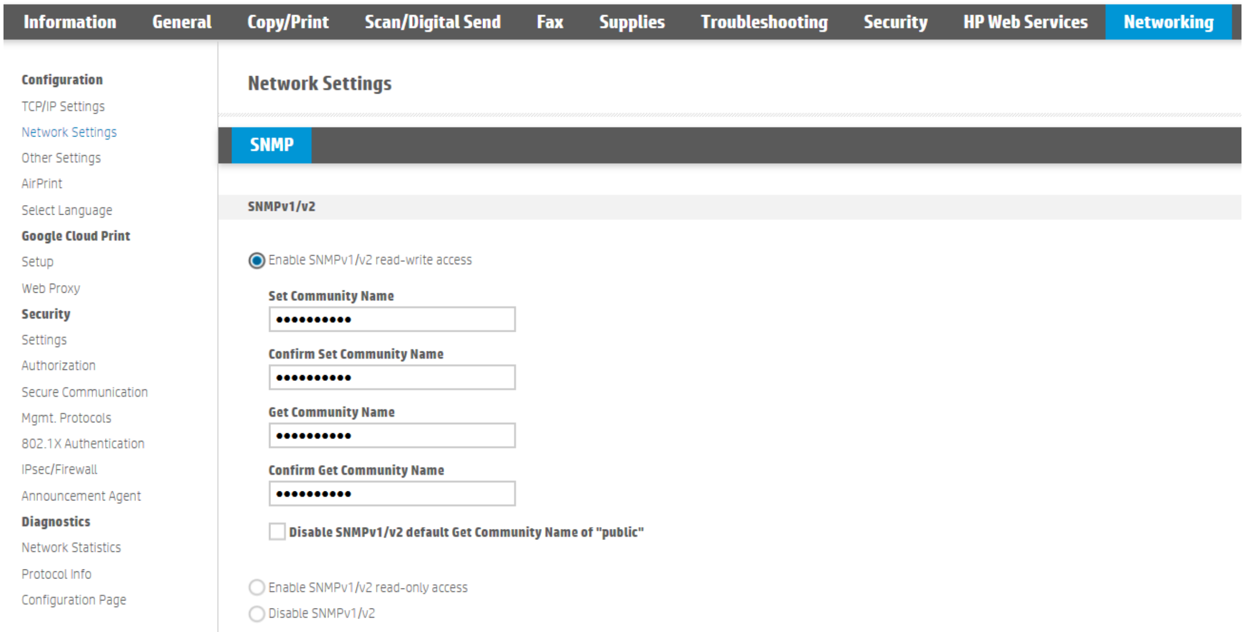
However, when the status indicates Credentials Failed, Security Manager does not know that credential to read and/or write settings that require that credential.

SNMP

SNMP v1/v2 credentials are broken into two types: Read and Read/Write.

These equate to the Get Community Name and Set Community Name under EWS. If there are no credentials entered for the **Get Community Name** in the EWS, and if the **Disable SNMP v1/v2 default Get Community Name of "public"** checkbox is not selected, the device is wide open to read information using SNMP with "public" used as the Community Name for an SNMP GET REQ packet.

This is not uncommon as very little if any sensitive data is passed thru Read attempts.



Network Settings

SNMP

SNMPv1/v2

● Enable SNMPv1/v2 read-write access

Set Community Name
••••••••••

Confirm Set Community Name
••••••••••

Get Community Name
••••••••••

Confirm Get Community Name
••••••••••

□ Disable SNMPv1/v2 default Get Community Name of "public"

○ Enable SNMPv1/v2 read-only access

○ Disable SNMPv1/v2

Starting with version 3.1, Security Manager checks both Set Community Name and a Get Community Name during a Verify task, and if fails, it will post a credential failure. If either an SNMP GET REQ or SNMP SET REQ packet receives no response, it is assumed a credential failure is present because devices will not respond if a Community Name does not match.

To resolve this situation, either clear the credentials on the device under EWS, or add the SNMP v1/v2 Read/write Community Name or the SNMP Write Community Name to the database (credential store) for the device by selecting it, clicking the Set Credentials icon, and then selecting Configure.

Admin (EWS) Password

If the Admin (EWS) Password is claiming Credentials Failed, this means that the test Security Manger performs to determine if an Admin (EWS) Password is present is failing. For HP FutureSmart devices, Security Manager will attempt to use web services to retrieve a system configuration page. Proper EWS credentials are required to retrieve such a page.

If the page is not returned, it is assumed the Admin (EWS) Password that Security Manager has stored for the device in the database or in the global store is incorrect. For older non-FutureSmart devices, an attempt is made over an HTTP request to retrieve the Security Status page under EWS. Again, if the page is not returned, it is assumed the Admin (EWS) Password that Security Manager has stored for the device in the database or in the global store is incorrect.

One technique to resolve this issue is to add the Admin (EWS) Password to the database (credential store) for the device by selecting it, clicking the Set Credentials icon, and then selecting Configure.

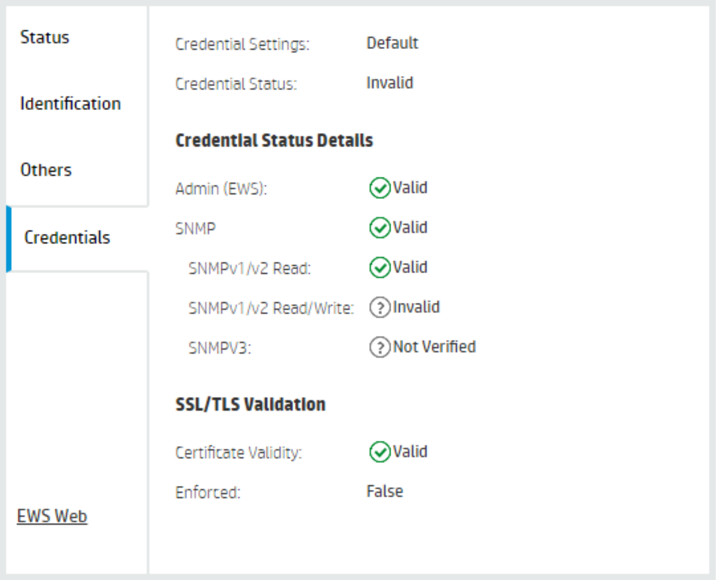
Another technique is to clear the Admin (EWS) Password under EWS, then right-click the device in HPSM and clear the credentials that are stored in the database under Set Credentials, Reset.

This ensures that Security Manager and the EWS match. Perform a Verify task and see if credentials failures are cleared. If it still claims credentials failed, try deleting the device and rediscovering.

Example of Check Credentials

Here is an example of a typical device interrogation of an HP FutureSmart device to check credentials.

During the Verify task, Security Manager starts by pinging the device. If there is no response to pings, a Network Communication Error status is posted.



Credential Settings: Default

Credential Status: Invalid

Credential Status Details

Admin (EWS): ✓ Valid

SNMP ✓ Valid

SNMPv1/v2 Read: ✓ Valid

SNMPv1/v2 Read/Write: ? Invalid

SNMPV3: ? Not Verified

SSL/TLS Validation

Certificate Validity: ✓ Valid

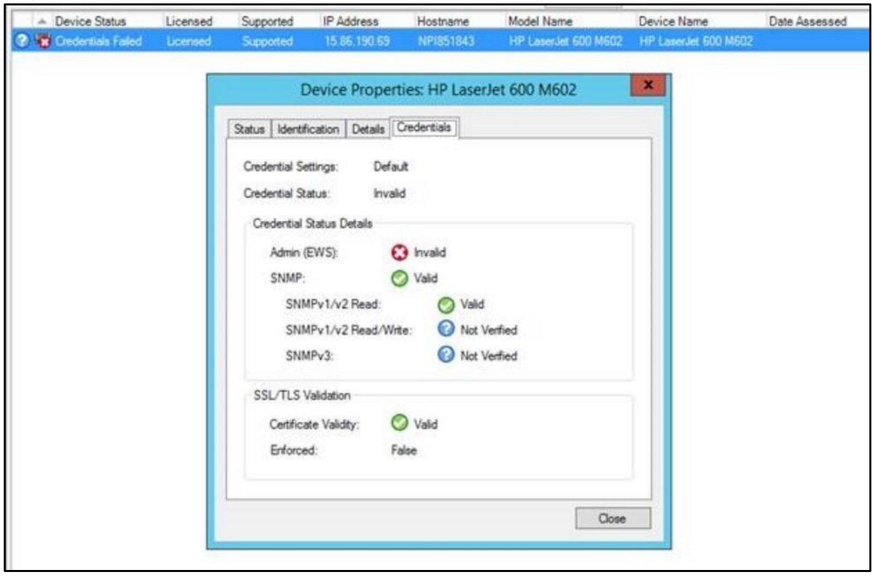
Enforced: False

- If pings are successful, there are several SNMP GET REQ packets sent with various OIDs to retrieve basic device information.
- If the OIDs receive no response, Security Manager makes an educated guess that the SNMP credentials are wrong since that would be the exact behavior if the Community Names do not match, and the device still responds to pings.

Therefore, a Credentials Failed status is posted blaming the SNMP Read Community Name. The remaining transactions are secure ones over port 443 and port 7627 using to attempt to retrieve an endpoint called SystemConfiguration over web services.

If that fails, there will be several indications in log files that it failed, and the status will indicate Credentials Failed as seen below blaming the Admin (EWS) Password because you must know the correct Admin (EWS) Password to retrieve the information via Web services:

Figure: Device Properties, Credentials tab



Device Status	Licensed	Supported	IP Address	Hostname	Model Name	Device Name	Date Assessed
Credentials Failed	Licensed	Supported	15.86.190.69	NPI851843	HP LaserJet 600 M602	HP LaserJet 600 M602	

Device Properties: HP LaserJet 600 M602

Credential Settings: Default
Credential Status: Invalid

Credential Status Details
Admin (EWS): ✗ Invalid
SNMP: ✓ Valid
SNMPv1/v2 Read: ✓ Valid
SNMPv1/v2 Read/Write: ? Not Verified
SNMPv3: ? Not Verified

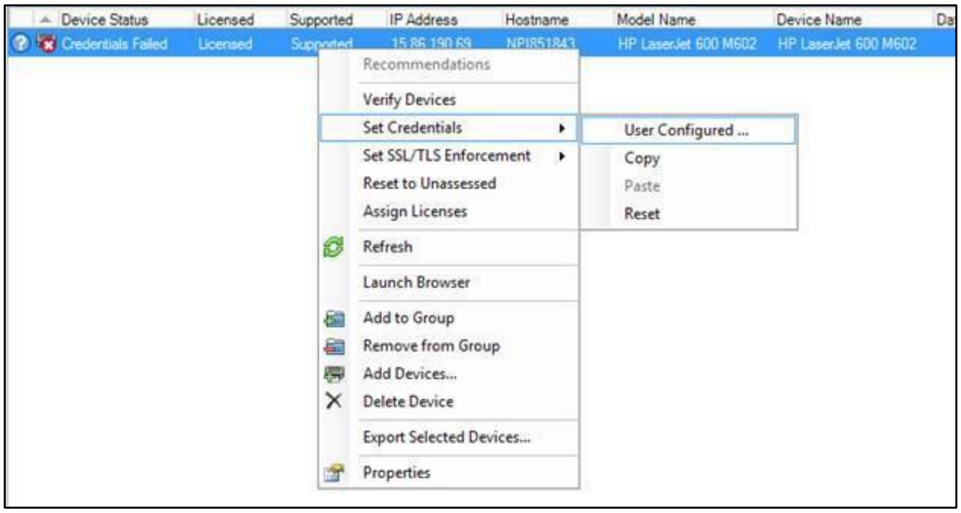
SSL/TLS Validation
Certificate Validity: ✓ Valid
Enforced: False

The EapNetworkLib.log file contains statements indicating the request was forbidden, for example:

```
15:32:47,213 ERROR EapNetworkLib [28]-
EapNetworkLib.EapUnauthorizedAccessException: XmlRest.Get(NPI851843,
/systemconfiguration, 0) failed. HTTP status code: Forbidden ---> System.Net.WebException: The
remote server returned an error: (403) Forbidden.
```

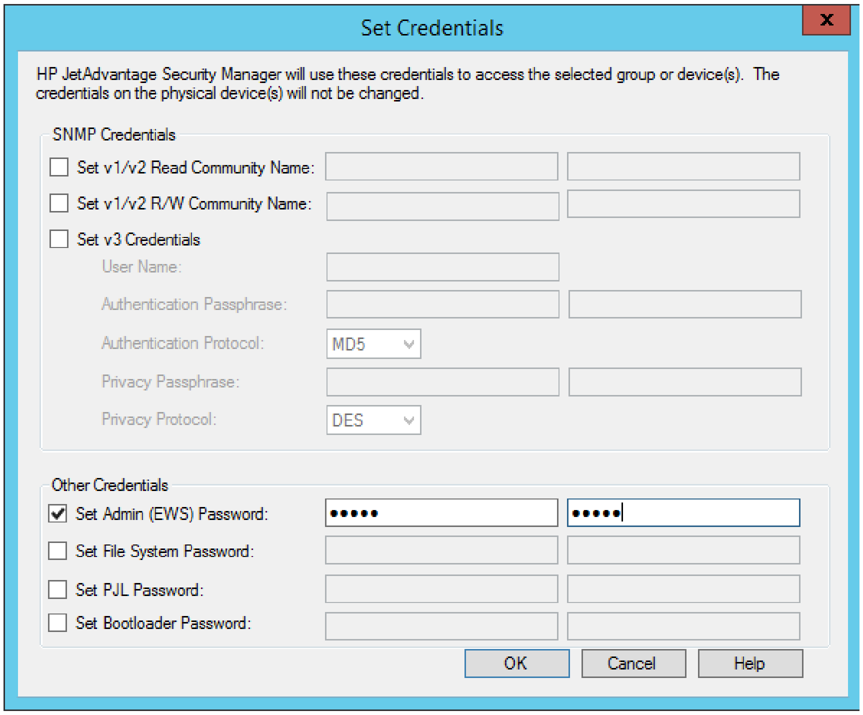
If you try to access the device EWS, it should only show the Information tab unless you login and provide the correct Admin (EWS) Password if an Admin (EWS) Password is set.

If one is set and you can successfully login to EWS by entering it, that same Admin (EWS) Password can be manually entered into the Security Manager database for the device by right clicking the device and then adding it:



Device Status	Licensed	Supported	IP Address	Hostname	Model Name	Device Name	Da
Credentials Failed	Licensed	Supported	15.86.190.69	NPI851843	HP LaserJet 600 M602	HP LaserJet 600 M602	

Figure: Typing the Admin EWS Credentials



Set Credentials

HP JetAdvantage Security Manager will use these credentials to access the selected group or device(s). The credentials on the physical device(s) will not be changed.

SNMP Credentials

☐ Set v1/v2 Read Community Name:

☐ Set v1/v2 R/W Community Name:

☐ Set v3 Credentials

User Name:

Authentication Passphrase:

Authentication Protocol: MD5

Privacy Passphrase:

Privacy Protocol: DES

Other Credentials

☑ Set Admin (EWS) Password: ●●●●● ●●●●●

☐ Set File System Password:

☐ Set PJL Password:

☐ Set Bootloader Password:

Now a verify task should succeed because the password matches the device.

Device Communication Log Files

If failures still cannot be resolved for SNMP Community Names or Admin (EWS) Password, view the log files for more information. Log files are stored under C:\Program Files (x86)\HP Security Manager\logs.

The three log files containing the most valuable troubleshooting data include:

- HPSM_Service.log – contains data regarding HPSM service and actions it performs
- EapNetworkLib.log – contains data regarding network traffic to devices
- EapDeviceLib.log – contains data specific to device settings

The EapNetworkLib.log file contains statements such as below that either the SystemConfiguration endpoint cannot be retrieved, or the Security Status page cannot be returned for Admin (EWS) Password issues. It also contains statements that SNMP GET REQ or SNMP SET REQ attempts were not returned for SNMP credential issues.

Example Admin (EWS) password failure for HP FutureSmart device:

> Exception message=XmlRest.Get(15.86.190.69, /systemconfiguration, 0) failed. HTTP status code: Forbidden, inner exception message=The remote server returned an error: (403) Forbidden.

Example Admin (EWS) password failure for non-FutureSmart device:

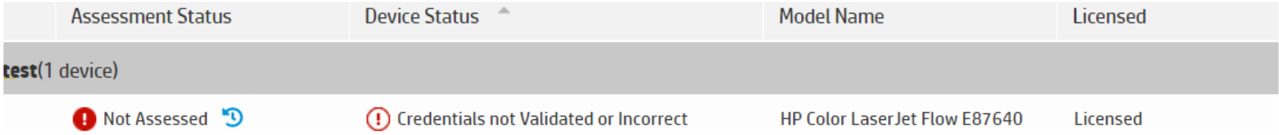
```
15:52:04,451 WARN        EapNetworkLib [4]        - Exception
message=Web.Get(15.86.190.170,https://15.86.190.170:443/hp/jetdirect/s ecurity_status.html,0)
failed. HTTP status code: Unauthorized, inner exception message. The remote server returned an
error: (401) Unauthorized.
```

Example SNMP Set Community Name failure for non-FutureSmart device:

> Exception message=Snmp.Set(15.86.190.69,1 varbind(s)) timed out., inner exception message=No response was received from the agent. Timeout is set to 30000 milliseconds.

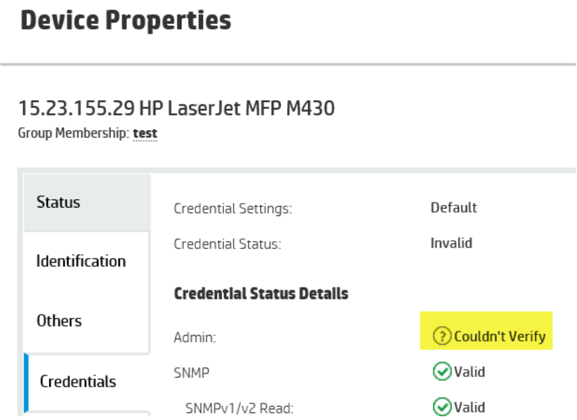
Credentials not Validated or Incorrect

One status that might display is “Credentials not Validated or Incorrect”.



Assessment Status	Device Status	Model Name	Licensed
test(1 device)			
! Not Assessed	! Credentials not Validated or Incorrect	HP Color LaserJet Flow E87640	Licensed

When clicking on the IP address and selecting the Credentials section, HPSM will display a status of **Couldn’t Verify** for the Admin credentials.



Device Properties

15.23.155.29 HP LaserJet MFP M430

Group Membership: test

Credential Settings: Default

Credential Status: Invalid

Credential Status Details

Admin: ? Couldn't Verify

SNMP ✓ Valid

SNMPv1/v2 Read: ✓ Valid

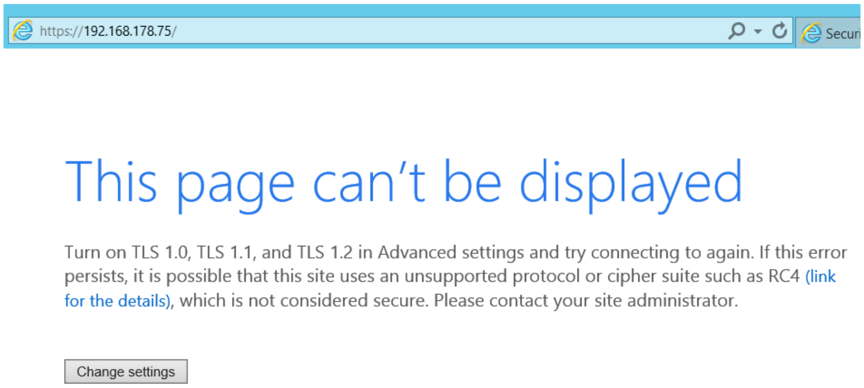
In the EAPNetworkLib.log the following error might be present:

```
2021-10-14 11:00:36,938 ERROR EapNetworkLib [94]  - uid=_dd999c08fa2f_192.168.178.75, Aggregate exception=[type=IOException:message=Authentication failed because the remote party has closed the transport stream.]
2021-10-14 11:00:36,938 ERROR EapNetworkLib [94]  - uid=_dd999c08fa2f_192.168.178.75, Exception message=XmlRest.Get(192.168.178.75, /systemconfiguration, 0) Caught a WebException communicating with address=192.168.178.75 Exception of type 'EapNetworkLib.EapWebException' was thrown. , inner exception message=Exception of type 'EapNetworkLib.EapWebException' was thrown.
```

In the EapDeviceLib.log the following error might also be present when it was an instant-on announcement:

```
2021-10-14 15:44:13,936 ERROR Pipeline [4]  - uid=_ef385274a315_15.23.155.27, Pipeline.Execute(): Network connection refused, address=15.23.155.27
```

When trying to open the EWS page with Internet Explorer (IE) directly from the HPSM server you might receive the error ‘This page can’t be displayed’:



This page can’t be displayed

Turn on TLS 1.0, TLS 1.1, and TLS 1.2 in Advanced settings and try connecting to again. If this error persists, it is possible that this site uses an unsupported protocol or cipher suite such as RC4 (link for the details), which is not considered secure. Please contact your site administrator.

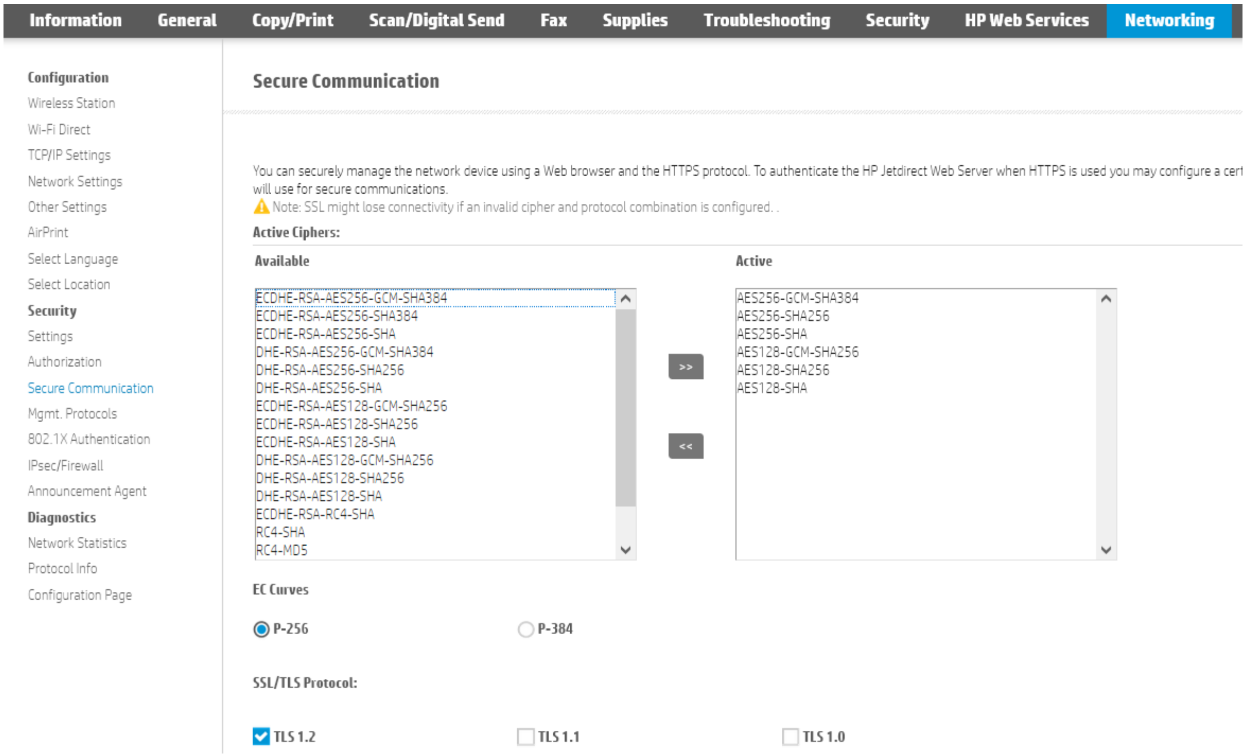
This error message indicates a mismatch of TLS and ciphers between the server/IE and the device.

When the EWS page of the device can be displayed successfully in IE from the HPSM server, then HPSM should be able to return a device status of Good.

When trying to open the EWS page with Chrome from the HPSM server, the printer might get displayed correctly.

HPSM uses the same cypher settings as IE and the OS. Chrome seems to bypass some of those settings.

On HP FutureSmart devices the active ciphers and TLS settings are displayed on the **Networking** tab under the **Secure Communication** menu.



Secure Communication

You can securely manage the network device using a Web browser and the HTTPS protocol. To authenticate the HP Jetdirect Web Server when HTTPS is used you may configure a cert will use for secure communications.

⚠ Note: SSL might lose connectivity if an invalid cipher and protocol combination is configured. .

Active Ciphers:

Available

ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384
ECDHE-RSA-AES256-SHA
DHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-SHA256
DHE-RSA-AES256-SHA
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256
ECDHE-RSA-AES128-SHA
DHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA
ECDHE-RSA-RC4-SHA
RC4-SHA
RC4-MD5

Active

AES256-GCM-SHA384
AES256-SHA256
AES256-SHA
AES128-GCM-SHA256
AES128-SHA256
AES128-SHA

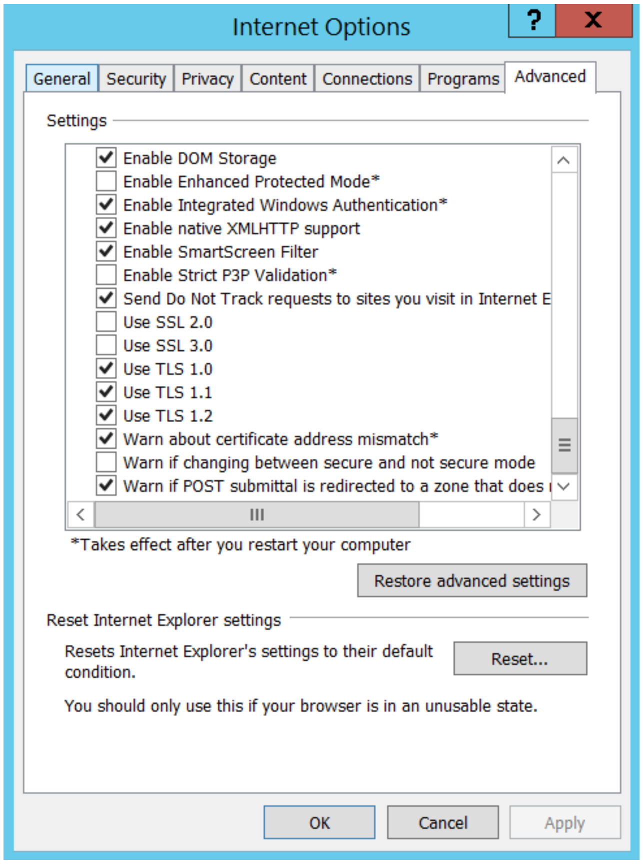
EC Curves

● P-256 ○ P-384

SSL/TLS Protocol:

☑ TLS 1.2 □ TLS 1.1 □ TLS 1.0

In IE, open Internet Options, and select the **Advanced** tab to view or edit the SSL and TLS selections:



Settings

- ☑ Enable DOM Storage
- □ Enable Enhanced Protected Mode*
- ☑ Enable Integrated Windows Authentication*
- ☑ Enable native XMLHTTP support
- ☑ Enable SmartScreen Filter
- □ Enable Strict P3P Validation*
- ☑ Send Do Not Track requests to sites you visit in Internet E
- □ Use SSL 2.0
- □ Use SSL 3.0
- ☑ Use TLS 1.0
- ☑ Use TLS 1.1
- ☑ Use TLS 1.2
- ☑ Warn about certificate address mismatch*
- □ Warn if changing between secure and not secure mode
- ☑ Warn if POST submittal is redirected to a zone that does i

*Takes effect after you restart your computer

Reset Internet Explorer settings

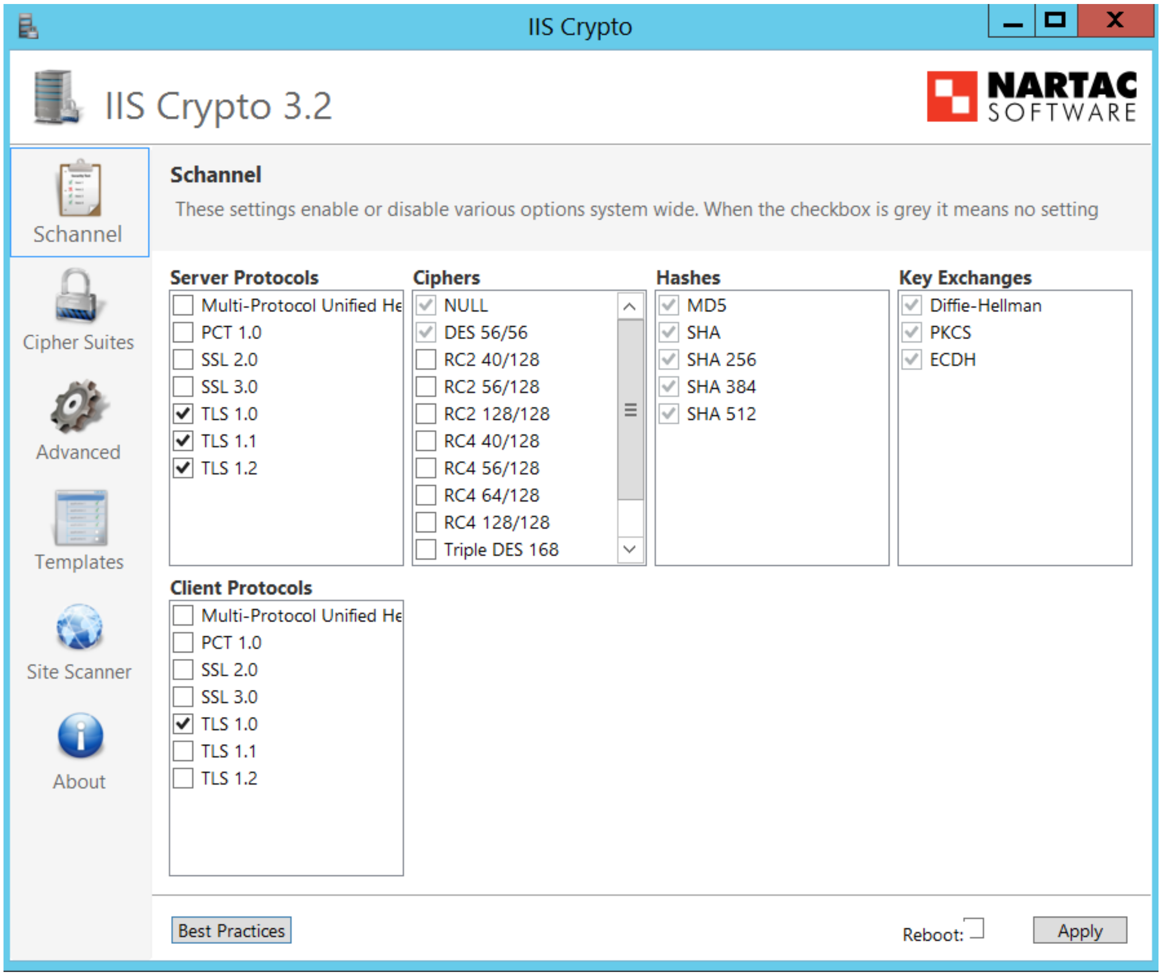
Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

However, If the ciphers are not enabled in the OS, then they cannot be enabled via IE. The OS SChannel and cipher suites are controlled by the Schannel registry settings and possible group policy settings:

HKLM SYSTEM|CurrentControlSet|Control|SecurityProviders|SCHANNEL

With IIS Crypto, see https://www.nartac.com/Products/IISCrypto/Download, you can easily visualize the settings.



Schannel

These settings enable or disable various options system wide. When the checkbox is grey it means no setting

Server Protocols

- □ Multi-Protocol Unified He
- □ PCT 1.0
- □ SSL 2.0
- □ SSL 3.0
- ☑ TLS 1.0
- ☑ TLS 1.1
- ☑ TLS 1.2

Ciphers

- ☑ NULL
- ☑ DES 56/56
- □ RC2 40/128
- □ RC2 56/128
- □ RC2 128/128
- □ RC4 40/128
- □ RC4 56/128
- □ RC4 64/128
- □ RC4 128/128
- □ Triple DES 168

Hashes

- ☑ MD5
- ☑ SHA
- ☑ SHA 256
- ☑ SHA 384
- ☑ SHA 512

Key Exchanges

- ☑ Diffie-Hellman
- ☑ PKCS
- ☑ ECDH

Client Protocols

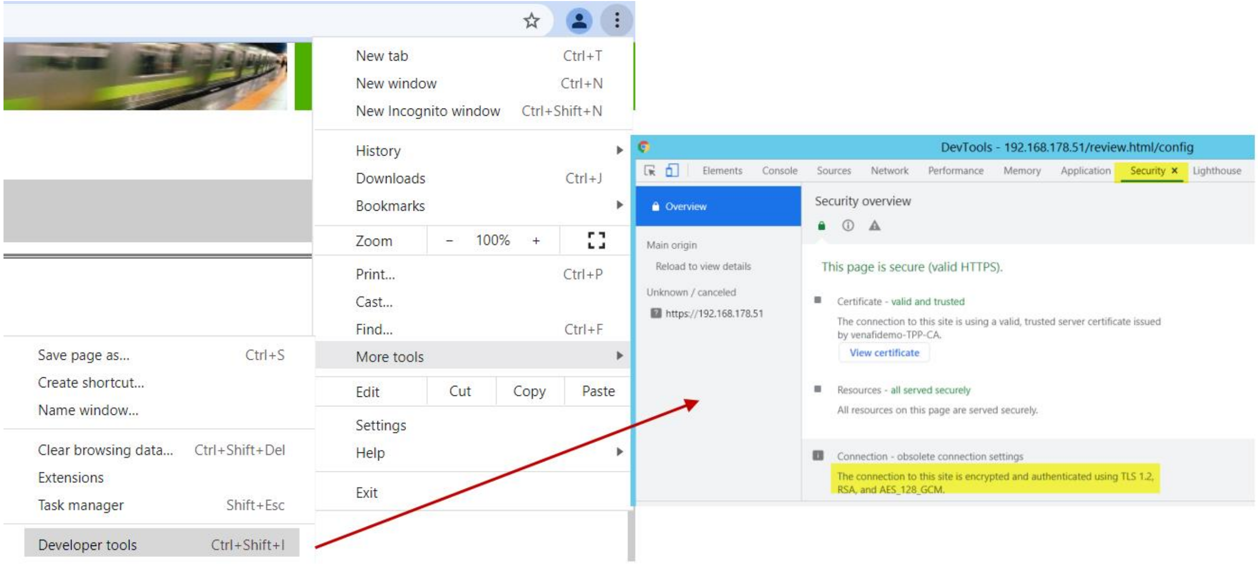
- □ Multi-Protocol Unified He
- □ PCT 1.0
- □ SSL 2.0
- □ SSL 3.0
- ☑ TLS 1.0
- □ TLS 1.1
- □ TLS 1.2

Reboot: □

For successful EWS password validation there must be a match between the OS settings and device settings for the SSL/TLS Protocols and the Active Ciphers on the device.

NOTE: OS changes for the SSL/TLS protocol and Ciphers require a server reboot.

It is also possible to check in a browser which Protocol and Cipher is used when communication is successful. For Chrome, click the 3 dots in the upper right corner, select **More tools**, **Developer Tools**, **Security**.



Security overview

This page is secure (valid HTTPS).

Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by venafidemo-TPP-CA.

Resources - all served securely

All resources on this page are served securely.

Connection - obsolete connection settings

The connection to this site is encrypted and authenticated using TLS 1.2, RSA, and AES_128_GCM.

Hanging or Slow Tasks

If a task is started but never seems to complete or takes an extraordinary time to complete, there may very well be a valid reason or some configuration options to try to improve performance.

Hung Tasks vs. Slow Tasks

It is important to determine if the task is hung forever and will never complete or if it is taking much longer than expected to complete.

First, try the same policy on a few devices to see if it completes. Also, try an extremely simple task on the fleet to see if a setting in the policy might be responsible for the delay or hang. You want to narrow down settings and/or devices to see if they are causing a task to be slow or hung. Versions of Security Manager prior to 3.0.1 had known issues where certain items in a policy could cause a task to hang indefinitely.

For example, setting that required web scraping to assess/remediate relied upon a Microsoft library to perform the HTTP transaction. Some servers had Microsoft libraries installed that would not permit performing this HTTP transaction. Security Manager 3.0.1 starting using a third-party library to perform these transactions that eliminated the hang.

Security Manager relies on a shared library called Microsoft.MSHTML.dll to perform queries on devices using a technique referred to as "web scraping" to manage the features. Older devices rely on this technique more than newer HP FutureSmart devices. Typically, this file is already present in the Global Assembly Cache (GAC), and if so, Security Manager will use the file loaded in GAC. If the file is not present in GAC, Security Manager will load a copy of this file.

Issues may arise where functionality of this file is not working or is blocked by browser settings, for example. One such setting is a browser setting called "Run antimalware software on ActiveX controls" under the Security tab that will block the usage of this dll. If so, there is a possibility that a task relying on this .dll file to perform managing of a feature may hang as there is never a return to the query. Security Manager 3.1 uses a newer third-party library to perform web scraping to alleviate this issue on these unique servers that block the usage of the MS library.

If tasks are still hanging, deleting the task under the Tasks tab will not stop all the devices from being assessed/remediated. The devices are still tagged in the database as not complete and will start again if the service is restarted, for example. You will have to wait for incomplete devices to run their course.

Credential Failed or Network Connection Error Impacting Performance

Devices in a Credentials Failed or Network Connection Error status can cause extreme delays in completing tasks. Try to run the task again without devices in this state. If it completes in a more reasonable amount of time, Security Manager 3.1 offers some timeout and threading settings that can be configured to help lessen to negative performance impact of devices in such a state.

These settings can be controlled using configuration items in the HPSM_Service.exe.config file. If the server has the power, increasing the threads and decreasing the timeouts can substantially reduce the time it takes to complete tasks. In the list below several change suggestions are listed. If performance or behavior is worse after making those changes, then you need to revert the changes.

To change these parameters, open the following file in a test editor:

C:|Program Files (x86)|HP Security Manager|HPSM_config.exe.config

Edit the following entries, save changes, and restart the Security Manager service.

```
<add key="snmpRequestTimeout" value="30000"
```

Value is in milliseconds (30s) – amount of time to wait for responses to SNMP packets

Change suggestion: In most environments you can set this to 2000

```
<add key="verificationSnmpRequestTimeout" value="2000"
```

Value is in milliseconds (2s) – amount of time to wait for SNMP responses during a Verify task

```
<add key="timeBetweenEapRetry" value="5000"
```

Value is in milliseconds (5s) – time to wait between retries on SNMP packets

Change suggestion: in most environments you can set this to 2000

```
<add key="eapRetryLimit" value="2"
```

Number of retries if a device fails to respond for a request

Change suggestion: Limit the retries to 1

```
<add key="eapAdminCredentialRetryDelay" value="500" />
```

This setting is suggested when there are devices ending up in Inconclusive or Admin credentials Failed

```
<add key="eapMaxThreadCount" value="100”
```

Total number of active threads to devices

HPSM 3.6.1 and older was ignoring the configured value.

HPSM 3.7 and newer will be using the actual configured value. It is therefore recommended to start with 100. Check performance and after that increase and validate if this improves the performance.

```
<add key="maxNumberTasks" value="10"
```

Number of tasks that can be open simultaneously. This means that Security Manager will either have 10 child tasks of 25 devices each open at a time for Verification and Assessment, or 10 tasks of one device each During Instant-On, Remediation and Credential retry.

Change suggestion: increase this to 50.

```
<add key="numberDevicesInEAPTaskCheckpointInterval" value="25"
```

This only applies to verification and assessment/remediation tasks, it means 25 devices will be present in each child task.

Change suggestion: increase this to 50.

```
<add key= “caManagerMaxThreadCount" value="100"
```

Number of devices at a time when a request is sent to CA manager to provide certificate remediations.

Change suggestion: increase this to 200.

Slow device remediation, EWS Password not verified, ping and SNMP are working fine

Sometimes there are some issues accessing the EWS page of the device or accessing the device over port 7637 while ping and SNMP are working fine. This can cause major delays while trying to remediate those devices.

For every config item which uses web services, the default time out of 60 seconds will be used. From HPSM 3.6 onwards this timeout is configurable in EapNetworkLib.dll.config.

Recommendation is to change this timeout to 20 seconds and monitor if this brings indeed faster assessment and remediation.

1. Open the EapNetworkLib.dll.config file
2. Change the value for the httpTimeout to for example 20 seconds
3. Restart the HPSM service
4. Monitor the performance and make further adjustments if needed.

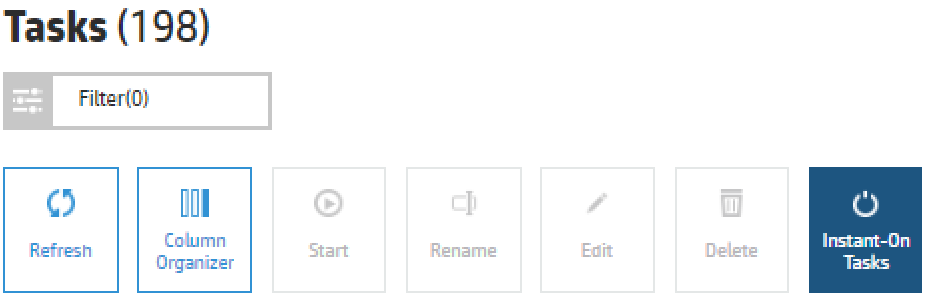
Performance Impact of Instant-On Remediations

A high volume of Instant-On automatic remediations occurring in the background will absolutely affect performance. It is possible there are a few devices causing such a high volume, or it might be devices are sending announcements for legitimate reasons and the server can only handle so many tasks.

If many of the messages are coming from one device, it might be because a faulty device is operating from the network and coming back again, or that devices are constantly rebooting for some reason. Try eliminating such devices if suspicions arise, they may be responsible for the bulk of Instant-On remediations.

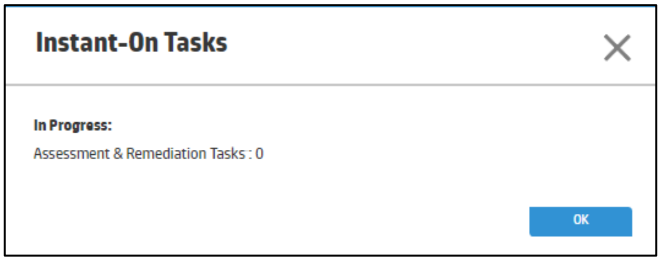
You can also try turning off Instant-On completely in Security Manager, at least temporarily to see if it is the contributing factor of the hangs/delays.

View the number of active Instant-On assessments under the **Tasks** tab by selecting **Instant-On Tasks**:



Instant-On announcements are processed immediately (i.e adding of the devices), but the action of performing the assessment/remediation task is scheduled.

These display as one task at a time for each device, and Security Manager processes a maximum of 10 Instant-On remediation tasks at a time.



Instant-On Tasks

In Progress:

Assessment & Remediation Tasks : 0

This number of maximum tasks at a time can be controlled using a configuration item in the HPSM_Service.exe.config file found under

\Program Files (x86)\HP Security Manager

```
<add key="eapMaxThreadCount" value="100" />
<add key="maxNumberTasks" value="10" />
<add key="numberDevicesInEAPTaskCheckpointInterval" value="25" />
<add key="caManagerMaxThreadCount" value="100" />
```

Change “maxNumberTasks” from a value of “10” to as much higher value to see if it makes a difference.

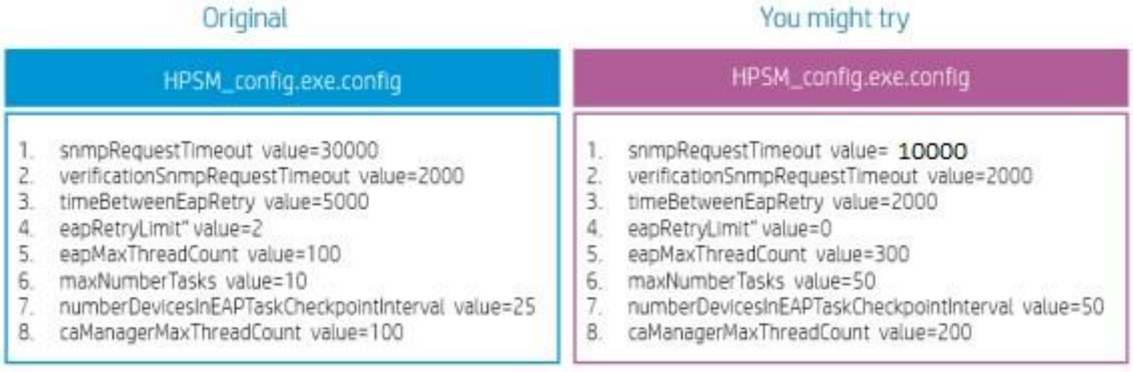
The threading for scheduled tasks can also be increased here. By default, each parent task is broken into child tasks of 25 devices each. This number can be increased to increase the performance by changing ="numberDevicesInEAPTaskCheckpointInterval" to a higher number.

It may boil down to if the fleet is exceptionally large and Instant-On seems to be consuming the bulk of the bandwidth, a separate server may be required to process the Instant-On tasks. This will allow for the “instant” remediation benefit of Instant-On in cases where a device is cold reset, for example.

However, it will not compromise the ability of the scheduled tasks to keep the entire fleet in compliance if running on a separate server.

One other possible cause of hanging tasks includes the Email Summary Reports feature. Assess/remediate tasks run forever if an invalid email address is configured in automated output. In such a case, tasks should be canceled manually, and the correct email address should be configured in settings.

Suggestions for improving performance are provided below but certainly not limited to these values. This may take some trial and error. For example, setting eapRetryLImit=0 can shave approximately 24s off total assess/remediation time per device.



Original	You might try
HPSM_config.exe.config	HPSM_config.exe.config
1. snmpRequestTimeout value=30000	1. snmpRequestTimeout value= 10000
2. verificationSnmpRequestTimeout value=2000	2. verificationSnmpRequestTimeout value=2000
3. timeBetweenEapRetry value=5000	3. timeBetweenEapRetry value=2000
4. eapRetryLimit" value=2	4. eapRetryLimit" value=0
5. eapMaxThreadCount value=100	5. eapMaxThreadCount value=300
6. maxNumberTasks value=10	6. maxNumberTasks value=50
7. numberDevicesInEAPTaskCheckpointInterval value=25	7. numberDevicesInEAPTaskCheckpointInterval value=50
8. caManagerMaxThreadCount value=100	8. caManagerMaxThreadCount value=200

Slow performance and reaching max SQL connection pool with Timeouts in HPSM_service.log

Issue: when HPSM needs to handle lots of instant on requests and scheduled tasks, it will need a lot of SQL connections. By default HPSM is using an SQL connection pool for 100 simultaneous connections and a SQL timeout of 60 seconds. When this is not enough timeouts will occur, as you can see in the following entries from the HPSM_service.log file.

```
2023-06-07 07:25:08,410 WARN  NHibernate.Util.ADOExceptionReporter  [7855] -
System.InvalidOperationException: Timeout expired.  The timeout period
elapsed prior to obtaining a connection from the pool.  This may have
occurred because all pooled connections were in use and max pool size
was reached.__   at
System.Data.ProviderBase.DbConnectionFactory.TryGetConnection(DbConnect
ion owningConnection, TaskCompletionSource`1 retry, DbConnectionOptions
userOptions, DbConnectionInternal oldConnection, DbConnectionInternal&
connection)__   at
System.Data.ProviderBase.DbConnectionInternal.TryOpenConnectionInternal
(DbConnection outerConnection, DbConnectionFactory connectionFactory,
TaskCompletionSource`1 retry, DbConnectionOptions userOptions)__   at
System.Data.SqlClient.SqlConnection.TryOpenInner(TaskCompletionSource`1
retry)__   at
System.Data.SqlClient.SqlConnection.TryOpen(TaskCompletionSource`1
retry)__   at System.Data.SqlClient.SqlConnection.Open()__   at
NHibernate.Connection.DriverConnectionProvider.GetConnection()__   at
NHibernate.AdoNet.ConnectionManager.GetConnection()__   at
NHibernate.AdoNet.AbstractBatcher.Prepare(IDbCommand cmd)
2023-06-07 07:25:09,684 ERROR NHibernate.Util.ADOExceptionReporter
[5367] - Timeout expired.  The timeout period elapsed prior to
obtaining a connection from the pool.  This may have occurred because
all pooled connections were in use and max pool size was reached.
```

Solution: increase the SQL connection pool for Nhibernate and SQL database connection in the HPSM_service.exe.config file and the Web.config file and restart. Steps:

1. Open the HPSM_service.exe.config file and the Web.config file.

2. Search for the following entries and add Max Pool Size=200 at the end of the connection string

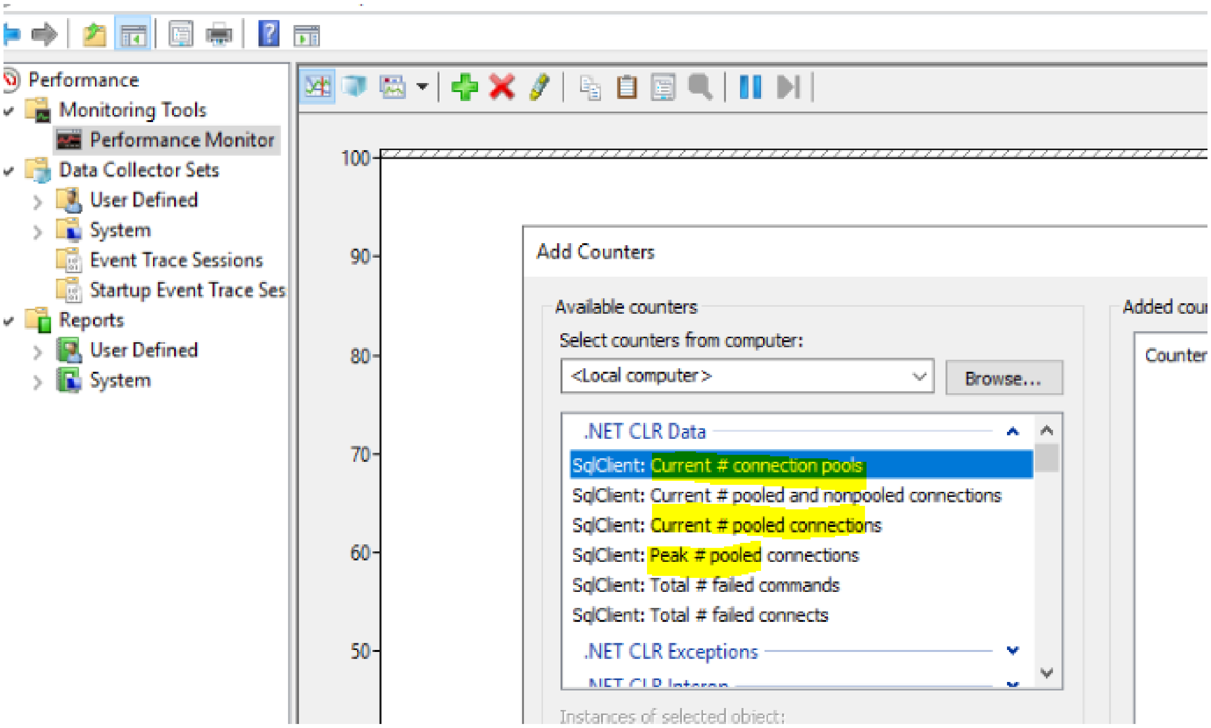
```
<add key="dbConnection" value="Server=(local)\SQLEXPRESS2022;initial
catalog=HPIPSC;Integrated Security=SSPI;Connection Timeout=30;Max Pool
Size=200" />

<add key="dbMasterConnection"
value="Server=(local)\SQLEXPRESS2022;initial catalog=master;Integrated
Security=SSPI;Connection Timeout=30;Max Pool Size=200" />

<property name=
"connection.connection_string">Server=(local)\SQLEXPRESS2022; initial
catalog=HPIPSC;Integrated Security=SSPI;Max Pool Size=200</property>
<property name="command_timeout">60</property>
```

3. Save the changes
4. Stop HPSM service, stop the HPSM application pool
5. Start HPSM application pool
6. Start HPSM service.

Note: if the SQL timeout is not listed in the keys **dbConnection** and **dbMasterConnection**, then it will be using the default timeout of 30 seconds. Besides those sql timeouts there are also a few other SQL timeouts defined in the config files:

```
<!--SqlQueryTimeout: Sql query timeout in seconds.  0 indicates no
limit (an attempt to execute a command will wait indefinitely), if any
invalid value is given,Recommended value is 300 will be taken-->
<add key="SqlQueryTimeout" value="300" />

<!--MaintenanceTaskQueryTimeout: Maintenance task query timeout in
seconds.  0 indicates no limit (an attempt to execute a command will
wait indefinitely), if any invalid value is given, Recommended value is
600 will be taken-->
<add key="MaintenanceTaskQueryTimeout" value="600" />

<session-factory name="NHibernate.Test">
<property name="command_timeout">60</property>
```

Note: it's possible to monitor the actual sql connection pool with Performance Monitor:
Start **Performance Monitor**
Click on **Performance Monitor** under Monitoring Tools in the left pane
Right-mouse click on the graph in the right pane and select **Add Counters**
Double click on **.NET CLR Data**
Add the desired SqlClient counters, see screenshot.


Performance
Monitoring Tools
Performance Monitor
Data Collector Sets
User Defined
System
Event Trace Sessions
Startup Event Trace Ses
Reports
User Defined
System
100
90
80
70
60
50
Add Counters
Available counters
Select counters from computer:
<Local computer>
Browse...
.NET CLR Data
SqlClient: Current # connection pools
SqlClient: Current # pooled and nonpooled connections
SqlClient: Current # pooled connections
SqlClient: Peak # pooled connections
SqlClient: Total # failed commands
SqlClient: Total # failed connects
.NET CLR Exceptions
.NET CLR Interop
Instances of selected object:
Added cou
Counter

It's also possible to run a query on the SQL server to see the current active number of connections. Open SQL Server Management Studio, connect to the instance and select New Query. Add the following query:

```
SELECT COUNT(*) AS ConnectionCount
FROM sys.sysprocesses sp
JOIN sys.databases db ON sp.dbid = db.database_id
WHERE db.name = 'HPIPSC'
```

Hit **Execute**

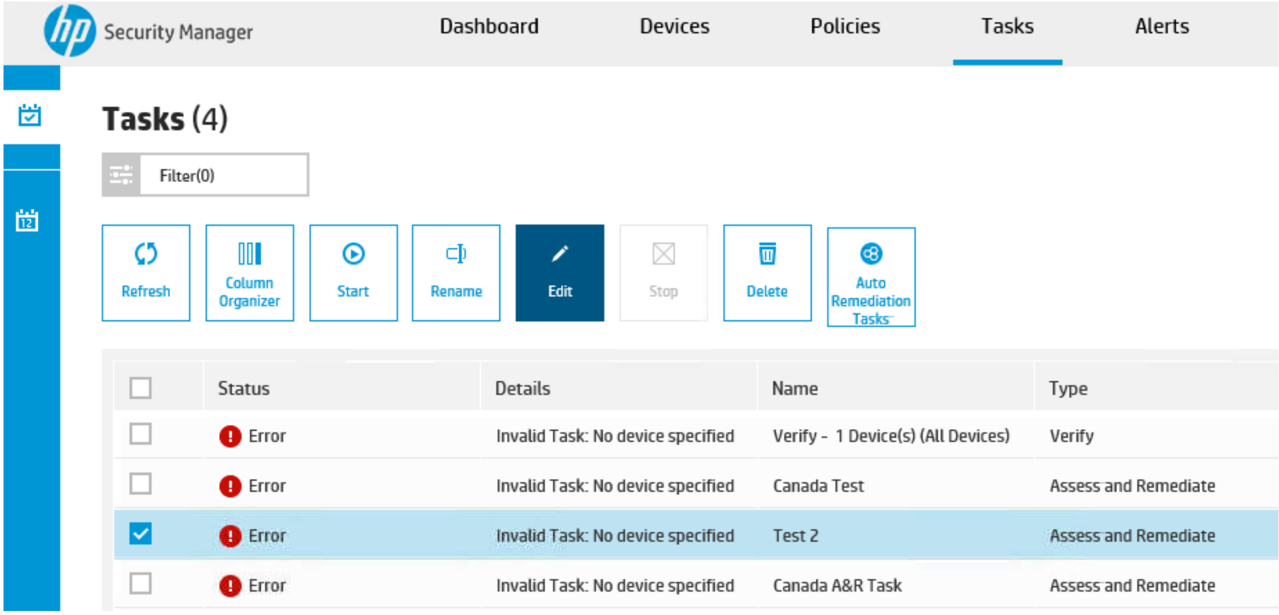
Note: this only displays the current number of connections and can be used to check the number of connections when HPSM UI is slow.

Upgrade Issues

'Invalid Task: No device specified' after upgrading to HPSM 3.7

After upgrade to HPSM 3.7 tasks might not run and end-up with error Invalid Task; no device specified.

Figure: Errors listed on the Tasks tab of HPSM



Tasks (4)

	Status	Details	Name	Type
□	Error	Invalid Task: No device specified	Verify - 1 Device(s) (All Devices)	Verify
□	Error	Invalid Task: No device specified	Canada Test	Assess and Remediate
☑	Error	Invalid Task: No device specified	Test 2	Assess and Remediate
□	Error	Invalid Task: No device specified	Canada A&R Task	Assess and Remediate

The HPSM_service.log file is containing errors, such as Cannot find data type UDT_DeviceId and Could not find stored procedure ‘HPIPSC.DBO.spDeleteSingleTask.

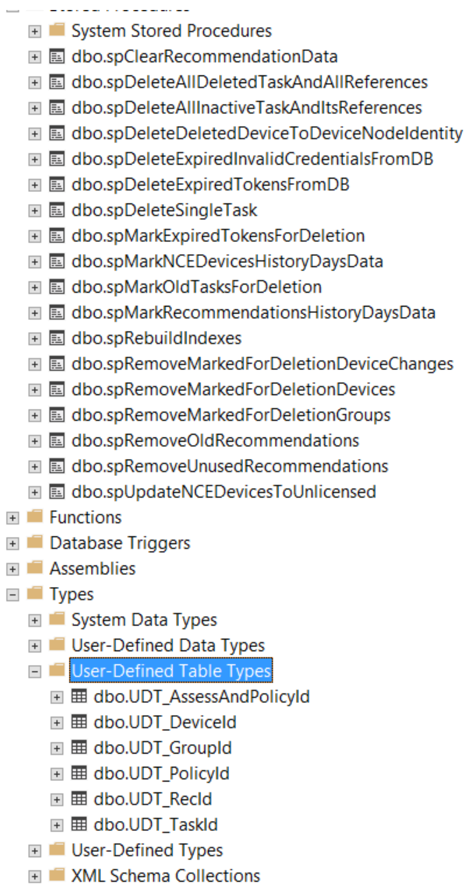
See following examples:

```
2022-02-16 11:59:22,611 DEBUG Service   [5] -
CheckAndMaybeThrowDBConnectionOrFullException: System.Data.SqlClient.SqlException
(0x80131904): Column, parameter, or variable @T_DeviceIds. : Cannot find data type
UDT_DeviceId.__   at System.Data.SqlClient.SqlConnection.OnError(SqlException exception,
Boolean breakConnection, Action`1 wrapCloseInAction)__   at
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject
stateObj, Boolean callerHasConnectionLock, Boolean asyncClose)__   at
System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand
cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler,
TdsParserStateObject stateObj, Boolean& dataReady)__   at
System.Data.SqlClient.SqlDataReader.TryConsumeMetaData()__   at
System.Data.SqlClient.SqlDataReader.get_MetaData()__   at
System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior
runBehavior, String resetOptionsString, Boolean isInternal, Boolean
forDescribeParameterEncryption, Boolean shouldCacheForAlwaysEncrypted)__   at
System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior,
RunBehavior runBehavior, Boolean returnStream, Boolean async, Int32 timeout, Task& task,
Boolean asyncWrite, Boolean inRetry, SqlDataReader ds, Boolean
describeParameterEncryptionRequest)__   at
System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior,
RunBehavior runBehavior, Boolean returnStream, String method, TaskCompletionSource`1
completion, Int32 timeout, Task& task, Boolean& usedCache, Boolean asyncWrite, Boolean
inRetry)__   at System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior
cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method)__   at
System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String
method)__   at System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[]
datatables, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command,
CommandBehavior behavior)__   at System.Data.Common.DbDataAdapter.Fill(DataSet
dataSet, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command,
CommandBehavior behavior)__   at System.Data.Common.DbDataAdapter.Fill(DataSet
dataSet, String srcTable)__   at
LocksmithBusinessLogic.BizLogicMgrHelper.GetDeviceDataSet(QueryFilter q, Boolean
includeAllDevices, Boolean onlyReturnRecCount, LSGroupVO
group)__ClientConnectionId:8b38d659-bb01-481c-99e1-ce44e49af760__Error
Number:351,State:3,Class:16
```

This means that the stored procedures and User-Defined Table Types were not created correctly during the upgrade to 3.7.

The following figure shows how it should look after a successful upgrade to version 3.7:

Figure: User-Defined Table Types created correctly and listed under Types



```
⊟ Stored Procedures
   ⊞ System Stored Procedures
   ⊞ dbo.spClearRecommendationData
   ⊞ dbo.spDeleteAllDeletedTaskAndAllReferences
   ⊞ dbo.spDeleteAllInactiveTaskAndItsReferences
   ⊞ dbo.spDeleteDeletedDeviceToDeviceNodeIdentity
   ⊞ dbo.spDeleteExpiredInvalidCredentialsFromDB
   ⊞ dbo.spDeleteExpiredTokensFromDB
   ⊞ dbo.spDeleteSingleTask
   ⊞ dbo.spMarkExpiredTokensForDeletion
   ⊞ dbo.spMarkNCEDevicesHistoryDaysData
   ⊞ dbo.spMarkOldTasksForDeletion
   ⊞ dbo.spMarkRecommendationsHistoryDaysData
   ⊞ dbo.spRebuildIndexes
   ⊞ dbo.spRemoveMarkedForDeletionDeviceChanges
   ⊞ dbo.spRemoveMarkedForDeletionDevices
   ⊞ dbo.spRemoveMarkedForDeletionGroups
   ⊞ dbo.spRemoveOldRecommendations
   ⊞ dbo.spRemoveUnusedRecommendations
   ⊞ dbo.spUpdateNCEDevicesToUnlicensed
⊞ Functions
⊞ Database Triggers
⊞ Assemblies
⊟ Types
   ⊞ System Data Types
   ⊞ User-Defined Data Types
   ⊟ User-Defined Table Types
      ⊞ dbo.UDT_AssessAndPolicyId
      ⊞ dbo.UDT_DeviceId
      ⊞ dbo.UDT_GroupId
      ⊞ dbo.UDT_PolicyId
      ⊞ dbo.UDT_RecId
      ⊞ dbo.UDT_TaskId
   ⊞ User-Defined Types
   ⊞ XML Schema Collections
```

If the user who has been running the SQL upgrade commands did have a default database other than DBO, then this issue would occur.

Solution

Upgrade to HPSM 3.7.1.

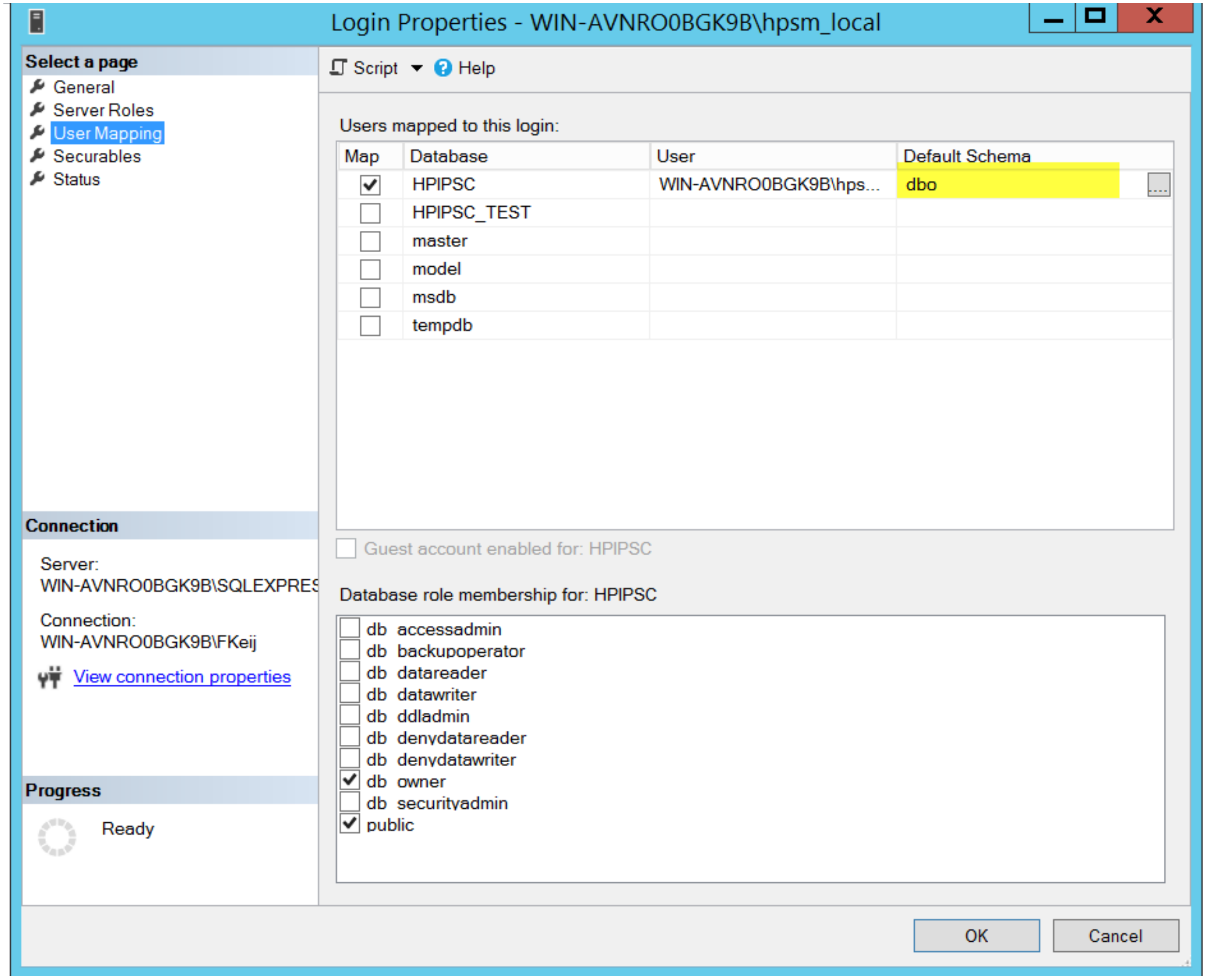
Or

Obtain the updated InstallSQLScripts_3.7VersionC.zip and re-run the InstallOrUpgradeRemoteDb.bat file to create the missing stored procedures and the missing User-defined table types.

Workaround

Change the default schema for the user running the SQL upgrade to DBO and re-run the InstallSQLScripts.

Figure: ‘dbo’ is listed as the default schema in Login Properties under User Mapping



Login Properties - WIN-AVNRO0BGK9B\hpsm_local

Users mapped to this login:

Map	Database	User	Default Schema
☑	HPIPSC	WIN-AVNRO0BGK9B\hps...	dbo
□	HPIPSC_TEST		
□	master		
□	model		
□	msdb		
□	tempdb		

□ Guest account enabled for: HPIPSC

Database role membership for: HPIPSC

□ db accessadmin
□ db backupoperator
□ db datareader
□ db datawriter
□ db ddladmin
□ db denydatareader
□ db denydatawriter
☑ db owner
□ db securityadmin
☑ public

Connection

Server:
WIN-AVNRO0BGK9B\SQLEXPRES

Connection:
WIN-AVNRO0BGK9B\FKeij

Progress

Ready

Web page not displayed, hangs, or Invalid Column name error after upgrading to HPSM 3.7

In some situations, the HPSM UI will not display, the web page will not open, and/or the browser hangs with a spinning icon while waiting to load the UI.

An ‘Invalid Column name’ error is listed in the HPSM_service.log file after upgrading to 3.7:

```
2 022-02-09 15:44:20,899 ERROR NHibernate.AdoNet.AbstractBatcher
System.Data.SqlClient.SqlException (0x80131904): Invalid column name
'RemoveLicenseAlone'.__   at System.Data.SqlClient.SqlConnection
```

The new column "RemoveLicenseAlone" in the Server.config table has not been created.
If you look at the UpgradeDbSchemaVer15to16.sql, you will find the following steps for this:

```
GO
PRINT
'=============================================================================='
```

```
PRINT 'Add and Update RemoveLicenseAlone in ServerConfigTable'
PRINT
'=============================================================================='
GO
IF NOT EXISTS(SELECT 1 FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME =
'ServerConfigTable' AND COLUMN_NAME = 'RemoveLicenseAlone')
 BEGIN
 DECLARE @SQL NVARCHAR(MAX) = N'';
 SET @SQL += N'
 ALTER TABLE ServerConfigTable ADD RemoveLicenseAlone BIT NOT NULL DEFAULT 0'
 PRINT @SQL
 EXECUTE(@SQL)
 END;
```

The execution of the part failed during the upgrade process. Therefore, it is required to run the following sql commands to create the missing table (this can be done from SQL Management Studio):

```
IF NOT EXISTS(SELECT 1 FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME =
'ServerConfigTable' AND COLUMN_NAME = 'RemoveLicenseAlone')
 BEGIN
 DECLARE @SQL NVARCHAR(MAX) = N'';
 SET @SQL += N'
 ALTER TABLE ServerConfigTable ADD RemoveLicenseAlone BIT NOT NULL DEFAULT 0'
```

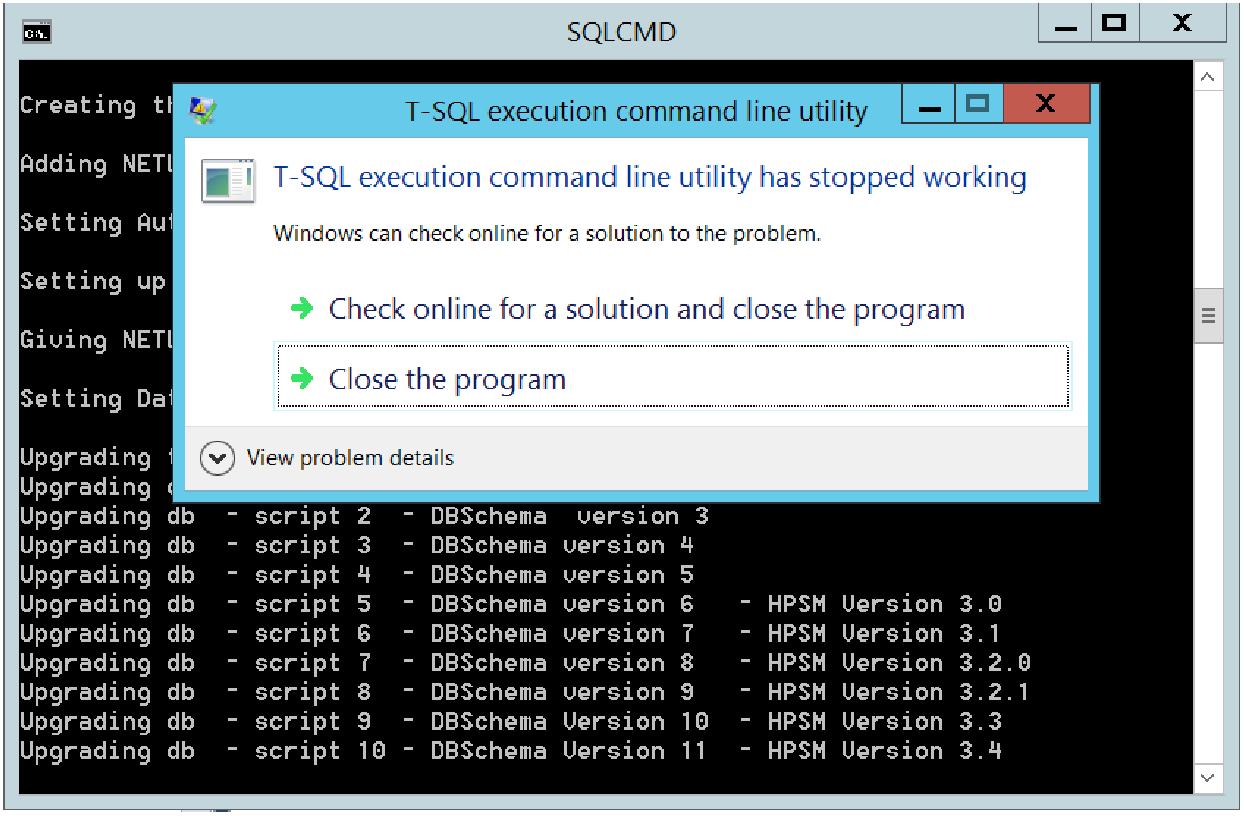
After making the change to the table, restart the HPSM service.

T-SQL Execution command line utility has stopped working error

While running the InstallOrUpgraderemoteDB.bat you might experience an SQLCMD crash, where the following error is displayed:

T-SQL Execution command line utility stopped working

Figure: “T-SQL Execution command line utility stopped working” error during InstallSqlScripts



```
Creating th

Adding NETI

Setting Aut

Setting up

Giving NETI

Setting Dat

Upgrading i
Upgrading c
Upgrading db  - script 2  - DBSchema  version 3
Upgrading db  - script 3  - DBSchema version 4
Upgrading db  - script 4  - DBSchema version 5
Upgrading db  - script 5  - DBSchema version 6   - HPSM Version 3.0
Upgrading db  - script 6  - DBSchema version 7   - HPSM Version 3.1
Upgrading db  - script 7  - DBSchema version 8   - HPSM Version 3.2.0
Upgrading db  - script 8  - DBSchema version 9   - HPSM Version 3.2.1
Upgrading db  - script 9  - DBSchema Version 10  - HPSM Version 3.3
Upgrading db  - script 10 - DBSchema Version 11  - HPSM Version 3.4
```

T-SQL execution command line utility

T-SQL execution command line utility has stopped working

Windows can check online for a solution to the problem.

➔ Check online for a solution and close the program

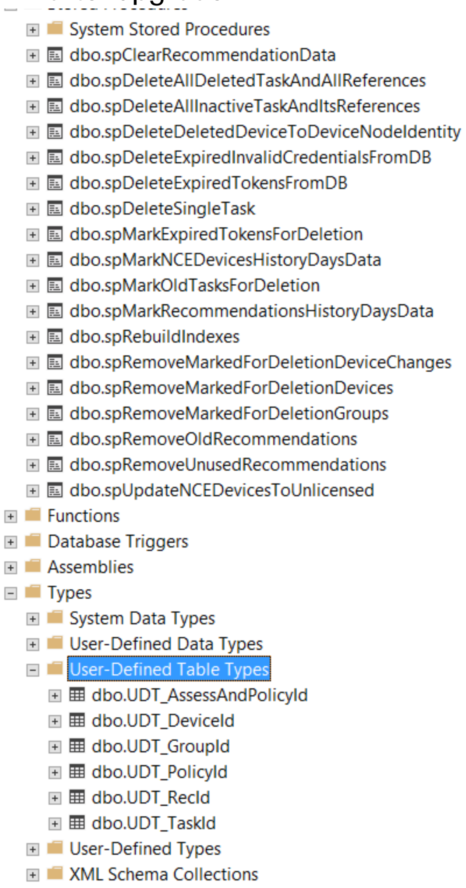
➔ Close the program

View problem details

Solution

After clicking **Close the program** the InstallOrUpgradeRemoteDb.bat will continue to run, but one or more stored procedures might be missing.

1. Make sure the following Stored Procedures and User-defined table types have been installed after upgrade:



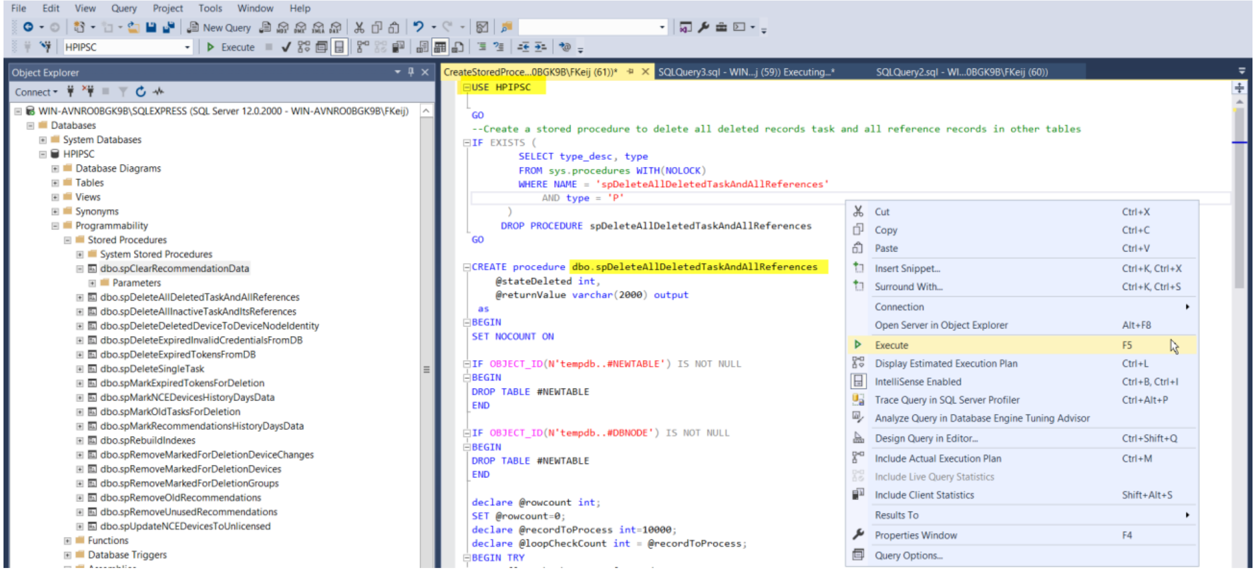
```
⊞ System Stored Procedures
⊞ dbo.spClearRecommendationData
⊞ dbo.spDeleteAllDeletedTaskAndAllReferences
⊞ dbo.spDeleteAllInactiveTaskAndItsReferences
⊞ dbo.spDeleteDeletedDeviceToDeviceNodeIdentity
⊞ dbo.spDeleteExpiredInvalidCredentialsFromDB
⊞ dbo.spDeleteExpiredTokensFromDB
⊞ dbo.spDeleteSingleTask
⊞ dbo.spMarkExpiredTokensForDeletion
⊞ dbo.spMarkNCEDevicesHistoryDaysData
⊞ dbo.spMarkOldTasksForDeletion
⊞ dbo.spMarkRecommendationsHistoryDaysData
⊞ dbo.spRebuildIndexes
⊞ dbo.spRemoveMarkedForDeletionDeviceChanges
⊞ dbo.spRemoveMarkedForDeletionDevices
⊞ dbo.spRemoveMarkedForDeletionGroups
⊞ dbo.spRemoveOldRecommendations
⊞ dbo.spRemoveUnusedRecommendations
⊞ dbo.spUpdateNCEDevicesToUnlicensed
⊞ Functions
⊞ Database Triggers
⊞ Assemblies
⊟ Types
  ⊞ System Data Types
  ⊞ User-Defined Data Types
  ⊟ User-Defined Table Types
    ⊞ dbo.UDT_AssessAndPolicyId
    ⊞ dbo.UDT_DeviceId
    ⊞ dbo.UDT_GroupId
    ⊞ dbo.UDT_PolicyId
    ⊞ dbo.UDT_RecId
    ⊞ dbo.UDT_TaskId
  ⊞ User-Defined Types
  ⊞ XML Schema Collections
```

2. If a stored procedure is missing, double click the sql command in the InstallScripts.zip file, for example: CreateStoredProcedure_DeleteAllDeletedTasksAndReferencedRecords.sql
   This will open the sql command in SQL Server Management Studio.

   NOTE: You can also open the sql command in Notepad and copy and paste the command in SQL Server Management Studio.

3. Change the USE $(DBNAME) into the actual database name (USE HPIPSC, for example).

4. Right-click and select **Execute.**


File
Edit
View
Query
Project
Tools
Window
Help
New Query
Execute
HPIPSC
Object Explorer
Connect
WIN-AVNROOBGK9B\SQLEXPRESS (SQL Server 12.0.2000 - WIN-AVNROOBGK9B\FKeij)
Databases
System Databases
HPIPSC
Database Diagrams
Tables
Views
Synonyms
Programmability
Stored Procedures
System Stored Procedures
dbo.spClearRecommendationData
Parameters
dbo.spDeleteAllDeletedTaskAndAllReferences
dbo.spDeleteAllInactiveTaskAndItsReferences
dbo.spDeleteDeletedDeviceToDeviceNodeIdentity
dbo.spDeleteExpiredInvalidCredentialsFromDB
dbo.spDeleteExpiredTokensFromDB
dbo.spDeleteSingleTask
dbo.spMarkExpiredTokensForDeletion
dbo.spMarkNCEDevicesHistoryDaysData
dbo.spMarkOldTasksForDeletion
dbo.spMarkRecommendationsHistoryDaysData
dbo.spRebuildIndexes
dbo.spRemoveMarkedForDeletionDeviceChanges
dbo.spRemoveMarkedForDeletionDevices
dbo.spRemoveMarkedForDeletionGroups
dbo.spRemoveOldRecommendations
dbo.spRemoveUnusedRecommendations
dbo.spUpdateNCEDevicesToUnlicensed
Functions
Database Triggers
CreateStoredProce...0BGK9B\FKeij (61))*
SQLQuery3.sql - WIN...j (59)) Executing...*
SQLQuery2.sql - WI...0BGK9B\FKeij (60))
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Insert Snippet... Ctrl+K, Ctrl+X
Surround With... Ctrl+K, Ctrl+S
Connection
Open Server in Object Explorer Alt+F8
Execute F5
Display Estimated Execution Plan Ctrl+L
IntelliSense Enabled Ctrl+B, Ctrl+I
Trace Query in SQL Server Profiler Ctrl+Alt+P
Analyze Query in Database Engine Tuning Advisor
Design Query in Editor... Ctrl+Shift+Q
Include Actual Execution Plan Ctrl+M
Include Live Query Statistics
Include Client Statistics Shift+Alt+S
Results To
Properties Window F4
Query Options...

```
USE HPIPSC

GO
--Create a stored procedure to delete all deleted records task and all reference records in other tables
IF EXISTS (
        SELECT type_desc, type
        FROM sys.procedures WITH(NOLOCK)
        WHERE NAME = 'spDeleteAllDeletedTaskAndAllReferences'
            AND type = 'P'
      )
     DROP PROCEDURE spDeleteAllDeletedTaskAndAllReferences
GO

CREATE procedure dbo.spDeleteAllDeletedTaskAndAllReferences
    @stateDeleted int,
    @returnValue varchar(2000) output
 as
BEGIN
SET NOCOUNT ON

IF OBJECT_ID(N'tempdb..#NEWTABLE') IS NOT NULL
BEGIN
DROP TABLE #NEWTABLE
END

IF OBJECT_ID(N'tempdb..#DBNODE') IS NOT NULL
BEGIN
DROP TABLE #NEWTABLE
END

declare @rowcount int;
SET @rowcount=0;
declare @recordToProcess int=10000;
declare @loopCheckCount int = @recordToProcess;
BEGIN TRY
```

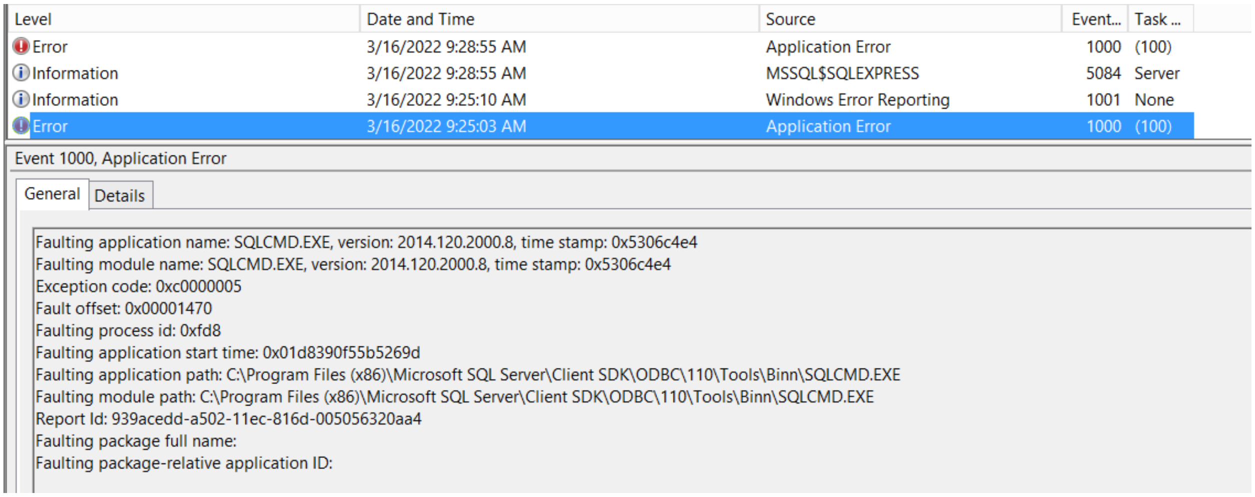
The missing stored procedure should be created.

If it is still not created, you must continue with the steps provided in the solution described in the section "HPSM service stopping automatically after upgrading to HPSM 3.7 or HPSM 3.7.1 with ERROR Invalid column in HPSM_service.log".

Application Error in Event log while executing the InstallSqlScripts

In the event log (under Windows Logs, Application) the following error is displayed while executing the InstallSqlScripts:

Application Error with event 1000



Level	Date and Time	Source	Event...	Task ...
Error	3/16/2022 9:28:55 AM	Application Error	1000	(100)
Information	3/16/2022 9:28:55 AM	MSSQL$SQLEXPRESS	5084	Server
Information	3/16/2022 9:25:10 AM	Windows Error Reporting	1001	None
Error	3/16/2022 9:25:03 AM	Application Error	1000	(100)

Event 1000, Application Error

```
Faulting application name: SQLCMD.EXE, version: 2014.120.2000.8, time stamp: 0x5306c4e4
Faulting module name: SQLCMD.EXE, version: 2014.120.2000.8, time stamp: 0x5306c4e4
Exception code: 0xc0000005
Fault offset: 0x00001470
Faulting process id: 0xfd8
Faulting application start time: 0x01d8390f55b5269d
Faulting application path: C:\Program Files (x86)\Microsoft SQL Server\Client SDK\ODBC\110\Tools\Binn\SQLCMD.EXE
Faulting module path: C:\Program Files (x86)\Microsoft SQL Server\Client SDK\ODBC\110\Tools\Binn\SQLCMD.EXE
Report Id: 939acedd-a502-11ec-816d-005056320aa4
Faulting package full name:
Faulting package-relative application ID:
```

Solution

Follow the same solution steps provided for *T-SQL Execution command line utility has stopped working error.*

HPSM service stops, http Error 503 in browser, and Invalid column error after upgrading

When the HPSM service is stopping automatically and an http Error 503 is returned in the browser after upgrading from HPSM 3.5 to a newer HPSM version (3.6, 3.6.1, 3.7, or 3.7.1), an “Invalid column name error” displays in the HPSM_service.log file:

```
2022-03-08 21:18:02,058 ERROR NHibernate.AdoNet.AbstractBatcher
System.Data.SqlClient.SqlException (0x80131904): Invalid column name
'RemoveLicenseAlone'.__ at System.Data.SqlClient.SqlConnection.OnError(SqlException
exception, Boolean breakConnection, Action`1 wrapCloseInAction)__ at
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject
stateObj, Boolean callerHasConnectionLock, Boolean asyncClose)__ at
System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand
cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler,
TdsParserStateObject stateObj, Boolean& dataReady)__ at
System.Data.SqlClient.SqlDataReader.TryConsumeMetaData()__ at
System.Data.SqlClient.SqlDataReader.get_MetaData()__ at
System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior
runBehavior, String resetOptionsString, Boolean isInternal, Boolean
forDescribeParameterEncryption, Boolean shouldCacheForAlwaysEncrypted)__ at
System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior,
RunBehavior runBehavior, Boolean returnStream, Boolean async, Int32 timeout, Task& task,
Boolean asyncWrite, Boolean inRetry, SqlDataReader ds, Boolean
describeParameterEncryptionRequest)__ at
System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior,
RunBehavior runBehavior, Boolean returnStream, String method, TaskCompletionSource`1
completion, Int32 timeout, Task& task, Boolean& usedCache, Boolean asyncWrite, Boolean
inRetry)__ at System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior
cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method)__ at
System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String
method)__ at NHibernate.AdoNet.AbstractBatcher.ExecuteReader(IDbCommand
cmd)_ClientConnectionId:ca4ef007-8d35-4077-957c-5ed4ec981bce_Error
Number:207,State:1,Class:16
```

This means that the column ‘RemoveLicenseAlone’ has not been created in the ServerConfigTable during upgrade.

Solution when using HPSM 3.7.1
Run the installSQLscripts manually. You can run the HPSM installer to extract the InstallSQLscripts or you can find them in the HPSM root installation directory, such as:

C:|Program Files (x86)|HP Security Manager|

Unzip the file and re-run the InstallOrUpgradeRemoteDB.bat file, see the readme inside the InstallSQLscripts for further details.

NOTE: This only seems to happen when using SQL 2012 or older in combination with HPSM 3.5 installed on d:\ or e:\ drive and default schema not set to DBO during upgrade of HPSM.

Restart the HPSM application pool and start the HPSM service after making this change to the table.

Solution when using HPSM 3.7

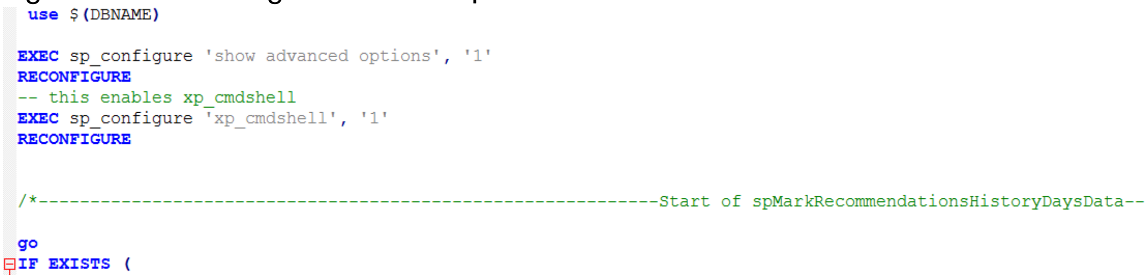
When using HPSM 3.7, you must obtain the InstallSQLScriptsC from HPSM support. To do this, use one of the following methods:

NOTE: Both methods will create the missing column RemoveLicenseAlone in the ServerConfig table.

Method One

1. Unzip the file.
2. Re-run the *InstallOrUpgradeRemoteDB.bat* file.
   NOTE: For instructions, see the Readme inside the InstallSQLscripts.
3. If the issue persists, make the following additional changes to the scripts:
   a. Unzip the InstallSQLScripts.zip (or InstallSQLScriptsC.zip when using 3.7.0):
   b. Open the file CreateStoredProcedure_MaintenanceTasks.sql with Notepad.
   c. Add the following commands to the second line of the file:
      EXEC sp_configure 'show advanced options', '1'
      RECONFIGURE
      -- this enables xp_cmdshell
      EXEC sp_configure 'xp_cmdshell', '1'
      RECONFIGURE

      Figure: Correct configuration in Notepad



```
 use $(DBNAME)

EXEC sp_configure 'show advanced options', '1'
RECONFIGURE
-- this enables xp_cmdshell
EXEC sp_configure 'xp_cmdshell', '1'
RECONFIGURE


/*------------------------------------------------------------Start of spMarkRecommendationsHistoryDaysData--

go
IF EXISTS (
```

4. Save the changes.
5. Re-run the *InstallOrUpgradeRemoteDB.bat* file again.
   NOTE: The syntax for this batch file is described in the corresponding Readme_InstallSqlScripts.zip.
6. Restart the HPSM application pool and start the HPSM service after making this change.

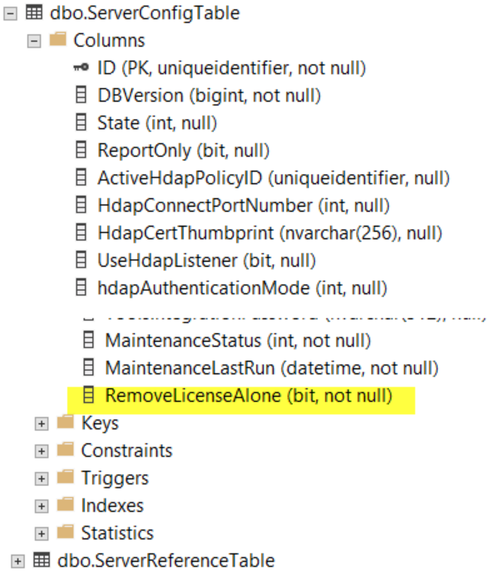
Method Two

1. Run the following sql command from SQL Management studio when using a database called HPIPSC:

```
use HPIPSC
IF NOT EXISTS(SELECT 1 FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME =
'ServerConfigTable' AND COLUMN_NAME = 'RemoveLicenseAlone')
 BEGIN
 DECLARE @SQL NVARCHAR(MAX) = N'';
 SET @SQL += N'
 ALTER TABLE ServerConfigTable ADD RemoveLicenseAlone BIT NOT NULL DEFAULT 0'
 PRINT @SQL
 EXECUTE(@SQL)
 END;
```

2. Restart the HPSM application pool and start the HPSM service after making this change to the table. The missing column RemoveLicenseAlone is listed in the ServerConfig table.

Figure: ServerConfig table with the RemoveLicenseAlone column listed

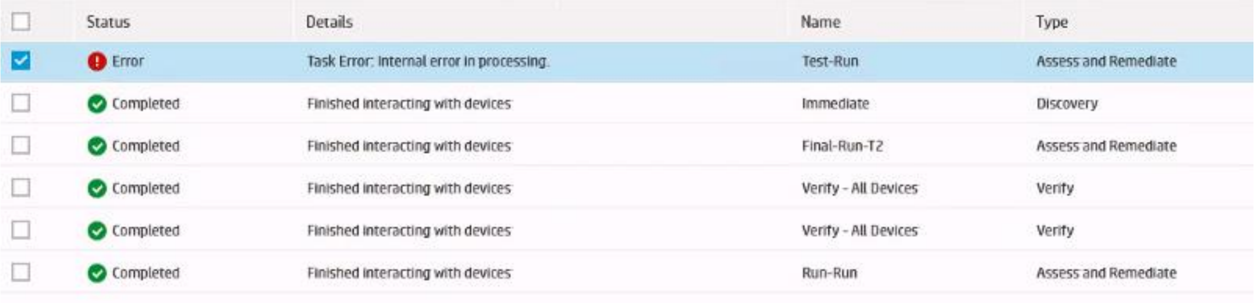


⊟ dbo.ServerConfigTable
- ⊟ Columns
  - ID (PK, uniqueidentifier, not null)
  - DBVersion (bigint, not null)
  - State (int, null)
  - ReportOnly (bit, null)
  - ActiveHdapPolicyID (uniqueidentifier, null)
  - HdapConnectPortNumber (int, null)
  - HdapCertThumbprint (nvarchar(256), null)
  - UseHdapListener (bit, null)
  - hdapAuthenticationMode (int, null)
  - MaintenanceStatus (int, not null)
  - MaintenanceLastRun (datetime, not null)
  - RemoveLicenseAlone (bit, not null)
- ⊞ Keys
- ⊞ Constraints
- ⊞ Triggers
- ⊞ Indexes
- ⊞ Statistics

⊞ dbo.ServerReferenceTable

Task Error: Internal error in processing when re-running a task after upgrading to HPSM 3.8 and/or unable to complete a new task.

Immediately after upgrading to HPSM 3.8, it's possible that you cannot re-run a task. As it will end up with Task Error. See screenshot:



□	Status	Details	Name	Type
☑	Error	Task Error: Internal error in processing.	Test-Run	Assess and Remediate
□	Completed	Finished interacting with devices	Immediate	Discovery
□	Completed	Finished interacting with devices	Final-Run-T2	Assess and Remediate
□	Completed	Finished interacting with devices	Verify - All Devices	Verify
□	Completed	Finished interacting with devices	Verify - All Devices	Verify
□	Completed	Finished interacting with devices	Run-Run	Assess and Remediate

When creating a new task, the newly created task will never complete and cannot be stopped from the UI.

Instant on announcements cannot be handled by HPSM.

In the HPSM_service.log file you might see Nhibernate ERRORS:

2022-07-05 10:58:50,860 ERROR NHibernate.AdoNet.AbstractBatcher System.Data.SqlClient.SqlException (0x80131904): Invalid Column name 'LastSuccessfulAutoEWSPasswordResetOn'.__

2022-07-05 10:58:51,095 ERROR NHibernate.Util.ADOExceptionReporter [3] - Invalid column name ‘LastSuccessfulAutoEWSPasswordResetOn’.

In the InstantOn.log you might see ERRORS like:
2022-07-05 12:19:50,689 ERROR InstantOn [4] - DirectSSLListenerTask: LocksmithCore.ExceptionPackagerHdap: Unable to find or create a device__ bei LocksmithBusinessLogic.PackagerNAP.ProcessDeviceDiscoveryReturnDevice(DeviceIdentity deviceIdentity, Boolean& newDeviceWasCreated)__ bei TaskManager.DirectSSLListenerTask.DoWork(Object data)

Both issues are caused by the fact fact that the column LastSuccessfulAutoEWSPasswordResetOn in the dbo.deviceTable was not created during upgrade.

Solution:
(re)run the InstallOrUpgradeRemoteDB.bat from the InstallSqlScripts.zip file to create the missing column in the database.
Note: the InstallSqlScripts are located in the directory Program Files (x86)\HP Security Manager
Restart he HPSM service.
If the task still fails:

- Stop the HP Security Manager service
- Run the following SQL script from SQL Management Studio (change HPIPSC into a different database in case it’s named differently:

```
USE HPIPSC

GO
IF NOT EXISTS(SELECT 1 FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME =
'DeviceTable' AND
  (COLUMN_NAME = 'LastSuccessfulAutoEWSPasswordResetOn'))
BEGIN
  DECLARE @SQL NVARCHAR(MAX) = N'';
  SET @SQL += N'
  ALTER TABLE dbo.DeviceTable
  ADD  LastSuccessfulAutoEWSPasswordResetOn datetime NOT NULL DEFAULT
CONVERT(DATETIME, ''9999-12-31 23:59:59.000'')'
  PRINT @SQL
  EXECUTE(@SQL)
END;
GO
```

- Restart HPSM Security Manager service

Task Error: After upgrading to HPSM 3.10 some tasks end up in Task Error

When running a task with a policy which has been upgraded to 3.10 and which contains an ID certificate, you might see the following error in the HPSM_service.log file:

```
2023-07-24 03:31:40,024 ERROR Data
PolicyFramework.LocksmithPolicyException: : Duplicate resource id's
found in policy. Can't resolve reference: PLSanOptions
Line 4183: 2023-07-24 03:31:40,024 ERROR Service [6] - AssessmentTask:
Task Error:
{0}: Duplicate resource id's found in policy. Can't resolve reference:
PLSanOptions at
```

```
PolicyFramework.PolicyResourceManager.GetResource(String
resourceName)__ at
PolicyFramework.PolicyResourceManager.GetResource(ItemId itemId)__ at
PolicyFramework.Policy.IsActiveInstance(ItemId itemIdentity)__ at
PolicyFramework.Policy.GetControlValue(ItemId id,
PolicyControlValueType type)__ at
AssessmentRemediation.AssessmentParser.IsActive(ItemId identity,
List`1& returnedPolicyIds)__ at
AssessmentRemediation.AssessmentParser.GetActivePolicyItem(String
itemName, List`1& retPolItem)__ at
AssessmentRemediation.AssessmentParser.CreateAssessmentItems()__ at
AssessmentRemediation.Assessment..ctor(Policy policy)__ at
AssessmentRemediation.AssessmentTask.ExecuteTask()
2023-07-24 03:31:40,024 ERROR Service [6] - Warning - Truncated DB
string object - TaskBase - ErrorMessage -orginal: AssessmentTask: Task
Error: {0}
```

Solution: create a new policy with exactly the same values and run the task with the new policy.

Additional information: the policy was not upgraded correctly. A root cause was never found as the original DB (before upgrade) was no longer available when this issue was reported.

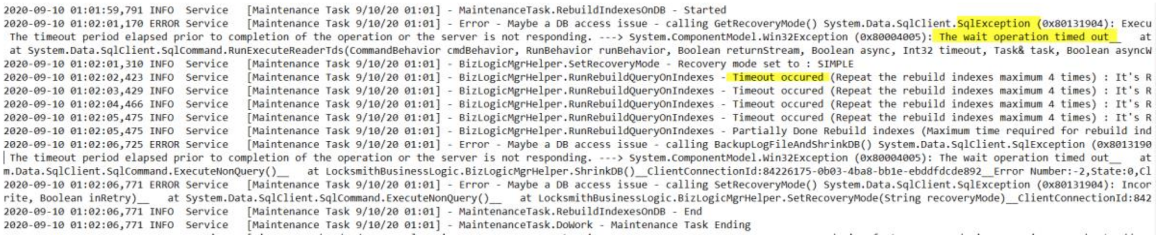
Growing Database and Nightly Maintenance failing

Growing Database and Nightly Maintenance failing (3.6.1 and older)

The HPSM inbuild maintenance starts at 01.00 AM.

If the database keeps growing (for example over 10GB), then you need to verify if the nightly maintenance is being executed correctly. To do this, follow these steps:

1. Check the HPSM_service.log file for any errors that indicate the nightly maintenance is failing. For example, an SQL timeout might occur.
   NOTE: Some information is only logged as INFO not as ERROR.



```
2020-09-10 01:01:59,791 INFO  Service   [Maintenance Task 9/10/20 01:01] - MaintenanceTask.RebuildIndexesOnDB - Started
2020-09-10 01:02:01,170 ERROR Service   [Maintenance Task 9/10/20 01:01] - Error - Maybe a DB access issue - calling GetRecoveryMode() System.Data.SqlClient.SqlException (0x80131904): Execu
 The timeout period elapsed prior to completion of the operation or the server is not responding. ---> System.ComponentModel.Win32Exception (0x80004005): The wait operation timed out__   at
 at System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async, Int32 timeout, Task& task, Boolean asyncW
2020-09-10 01:02:01,310 INFO  Service   [Maintenance Task 9/10/20 01:01] - BizLogicMgrHelper.SetRecoveryMode - Recovery mode set to : SIMPLE
2020-09-10 01:02:02,423 INFO  Service   [Maintenance Task 9/10/20 01:01] - BizLogicMgrHelper.RunRebuildQueryOnIndexes - Timeout occured (Repeat the rebuild indexes maximum 4 times) : It's R
2020-09-10 01:02:03,429 INFO  Service   [Maintenance Task 9/10/20 01:01] - BizLogicMgrHelper.RunRebuildQueryOnIndexes - Timeout occured (Repeat the rebuild indexes maximum 4 times) : It's R
2020-09-10 01:02:04,466 INFO  Service   [Maintenance Task 9/10/20 01:01] - BizLogicMgrHelper.RunRebuildQueryOnIndexes - Timeout occured (Repeat the rebuild indexes maximum 4 times) : It's R
2020-09-10 01:02:05,475 INFO  Service   [Maintenance Task 9/10/20 01:01] - BizLogicMgrHelper.RunRebuildQueryOnIndexes - Timeout occured (Repeat the rebuild indexes maximum 4 times) : It's R
2020-09-10 01:02:05,475 INFO  Service   [Maintenance Task 9/10/20 01:01] - BizLogicMgrHelper.RunRebuildQueryOnIndexes - Partially Done Rebuild indexes (Maximum time required for rebuild ind
2020-09-10 01:02:06,725 ERROR Service   [Maintenance Task 9/10/20 01:01] - Error - Maybe a DB access issue - calling BackupLogFileAndShrinkDB() System.Data.SqlClient.SqlException (0x8013190
 The timeout period elapsed prior to completion of the operation or the server is not responding. ---> System.ComponentModel.Win32Exception (0x80004005): The wait operation timed out__   at
m.Data.SqlClient.SqlCommand.ExecuteNonQuery()__   at LocksmithBusinessLogic.BizLogicMgrHelper.ShrinkDB()__ClientConnectionId:84226175-0b03-4ba8-bb1e-ebddfdcde892__Error Number:-2,State:0,Cl
2020-09-10 01:02:06,771 ERROR Service   [Maintenance Task 9/10/20 01:01] - Error - Maybe a DB access issue - calling SetRecoveryMode() System.Data.SqlClient.SqlException (0x80131904): Incor
rite, Boolean inRetry)__   at System.Data.SqlClient.SqlCommand.ExecuteNonQuery()__   at LocksmithBusinessLogic.BizLogicMgrHelper.SetRecoveryMode(String recoveryMode)__ClientConnectionId:842
2020-09-10 01:02:06,771 INFO  Service   [Maintenance Task 9/10/20 01:01] - MaintenanceTask.RebuildIndexesOnDB - End
2020-09-10 01:02:06,771 INFO  Service   [Maintenance Task 9/10/20 01:01] - MaintenanceTask.DoWork - Maintenance Task Ending
```

2. Configure the timeout value. From 3.5 onwards this can be configured with the configuration parameter in the HPSM_Service.exe.config file:
   NOTE: The default timeout for the maintenance task is 30 minutes.

   <add key="ClearOldRecommendationTasksMaxDuration" value="30" />

3. After making changes, restart the HPSM service (required).

Because it is unknown which timeout is required, it is better to remove the old data with a script from SQL Management Studio to prevent timeouts.

To do this, follow these steps:

1. Stop the HPSM service.
2. Execute the following script:

```
DECLARE @X INT=1;

WAY:

SELECT TOP 10000 * into #NEWTABLE FROM
(SELECT  rec.ID AS recID, rToret.KEY_ID as rToretID, rt.ID AS rtID,  rvt.ID  as rvtID, rTorv.ID AS
rTorvID,
rTorat.KEY_ID AS rToratKEY_ID, rat.ID AS ratID, av.ID AS avID, raTop.ID AS raTopID
FROM DBO.RecommendationTable rec
LEFT OUTER JOIN DBO.RecToReasonsTable rToret ON rToret.KEY_ID = rec.ID
LEFT OUTER JOIN DBO.ReasonTable rt ON rt.ID = rToret.Reason
LEFT OUTER JOIN DBO.ReasonToReasonValuesTable rTorv ON  rTorv.ID = rt.ID
LEFT OUTER JOIN DBO.ReasonValueTable rvt ON rvt.ID = rTorv.ReasonValue_ID
LEFT OUTER JOIN DBO.RecToRecommendationActionsTable rTorat ON rTorat.KEY_ID = rec.ID
LEFT OUTER JOIN DBO.RecommendationActionTable rat ON rat.ID =
rTorat.RecommendationAction
LEFT OUTER JOIN DBO.AssessmentValueTable av ON av.ID = rat.ActionValue_REF
LEFT OUTER JOIN DBO.RecActionsToParametersTable raTop ON raTop.ID = rat.ID

where   rec.AssessmentAndPolicyUniqueID NOT IN ( select distinct
dal.assessmentAndPolicyUniqueID as uniqueID from  DBO.DeviceAssessmentLogTable dal
where dal.State = 2 )) as Sub1

--select count (*) from #NEWTABLE

DELETE a FROM  DBO.RecToRecommendationActionsTable  a INNER JOIN #NEWTABLE B ON
a.KEY_ID= B.rToratKEY_ID
DELETE a FROM  DBO.RecToReasonsTable a inner join #NEWTABLE B on a.KEY_ID = B.rToretID
DELETE a FROM  DBO.RecommendationTable a inner join #NEWTABLE B on a.ID = B.recID

DELETE a FROM  DBO.ReasonToReasonValuesTable a inner join #NEWTABLE B on a.ID =
B.rTorvID
DELETE a FROM  DBO.ReasonTable a inner join #NEWTABLE B on a.ID = B.rtID

DELETE a FROM  DBO.ReasonValueTable a inner join #NEWTABLE B on a.ID = B.rvtID
DELETE a FROM  DBO.RecActionsToParametersTable a inner join #NEWTABLE B on a.ID =
B.raTopID
DELETE a FROM  DBO.RecommendationActionTable a inner join #NEWTABLE B on a.ID =
B.ratID
DELETE a FROM  DBO.AssessmentValueTable a inner join #NEWTABLE B on a.ID = B.avID

SET @X = (select count (*) from #NEWTABLE)

drop table #NEWTABLE

IF @X=10000 GOTO WAY;
```

3. If needed, shrink the database with the following command:
   EXEC sp_configure DBCC Shrinkdatabase ('HPIPSC')
   NOTE: After the script has been completed, there might be a lot of empty space in the HPSM database. The space which the database needs will be a few GB smaller.

4. Restart the HPSM service.

From this point onwards the nightly maintenance should be finished within the default timeout of 30 minutes.

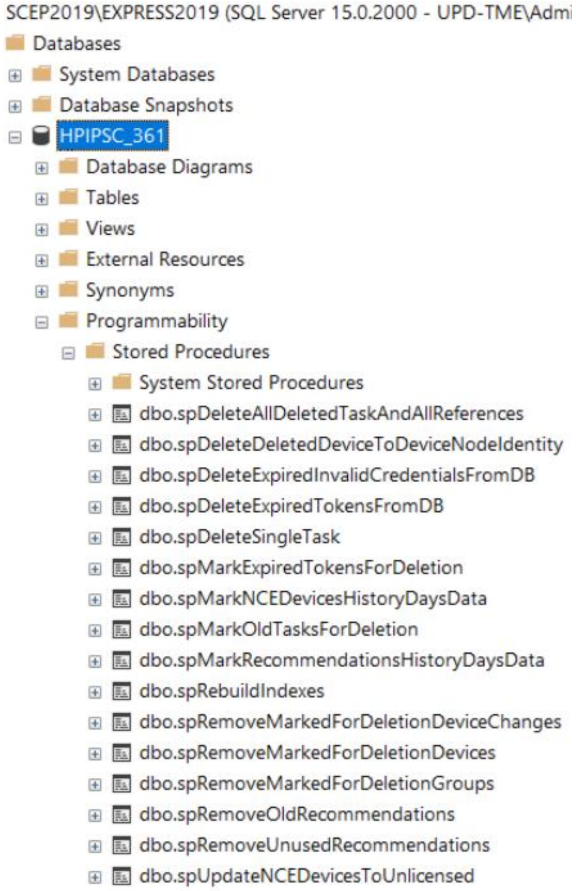
Growing Database and Nightly Maintenance failing (3.7 and newer)

After upgrade to 3.7, the nightly maintenance might fail and the Maintenance.log file contains errors about missing procedures.

For example, the following error indicates that the stored procedure called spRemoveOldRecommendations is missing from the SQL database.

```
2022-01-27 01:01:01,855 ERROR MaintenanceTask   - RemoveOldRecommendation :
SqlException occured - Could not find stored procedure 'spRemoveOldRecommendations'
```

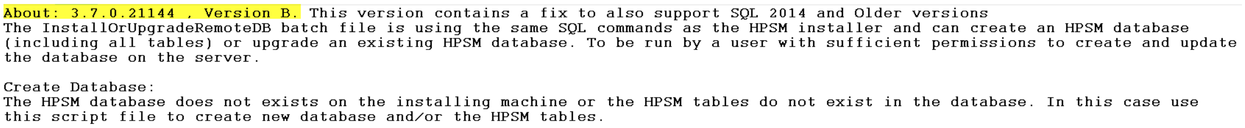
With SQL Management studio you can see all the stored procedures.



```
SCEP2019\EXPRESS2019 (SQL Server 15.0.2000 - UPD-TME\Admi
Databases
⊞ System Databases
⊞ Database Snapshots
⊟ HPIPSC_361
    ⊞ Database Diagrams
    ⊞ Tables
    ⊞ Views
    ⊞ External Resources
    ⊞ Synonyms
    ⊟ Programmability
        ⊟ Stored Procedures
            ⊞ System Stored Procedures
            ⊞ dbo.spDeleteAllDeletedTaskAndAllReferences
            ⊞ dbo.spDeleteDeletedDeviceToDeviceNodeIdentity
            ⊞ dbo.spDeleteExpiredInvalidCredentialsFromDB
            ⊞ dbo.spDeleteExpiredTokensFromDB
            ⊞ dbo.spDeleteSingleTask
            ⊞ dbo.spMarkExpiredTokensForDeletion
            ⊞ dbo.spMarkNCEDevicesHistoryDaysData
            ⊞ dbo.spMarkOldTasksForDeletion
            ⊞ dbo.spMarkRecommendationsHistoryDaysData
            ⊞ dbo.spRebuildIndexes
            ⊞ dbo.spRemoveMarkedForDeletionDeviceChanges
            ⊞ dbo.spRemoveMarkedForDeletionDevices
            ⊞ dbo.spRemoveMarkedForDeletionGroups
            ⊞ dbo.spRemoveOldRecommendations
            ⊞ dbo.spRemoveUnusedRecommendations
            ⊞ dbo.spUpdateNCEDevicesToUnlicensed
```

If one or more stored procedures are missing, then this might be caused by the original upgrade/InstallSQLscripts of HPSM which uses a command which is only supported from SQL 2016 onwards.

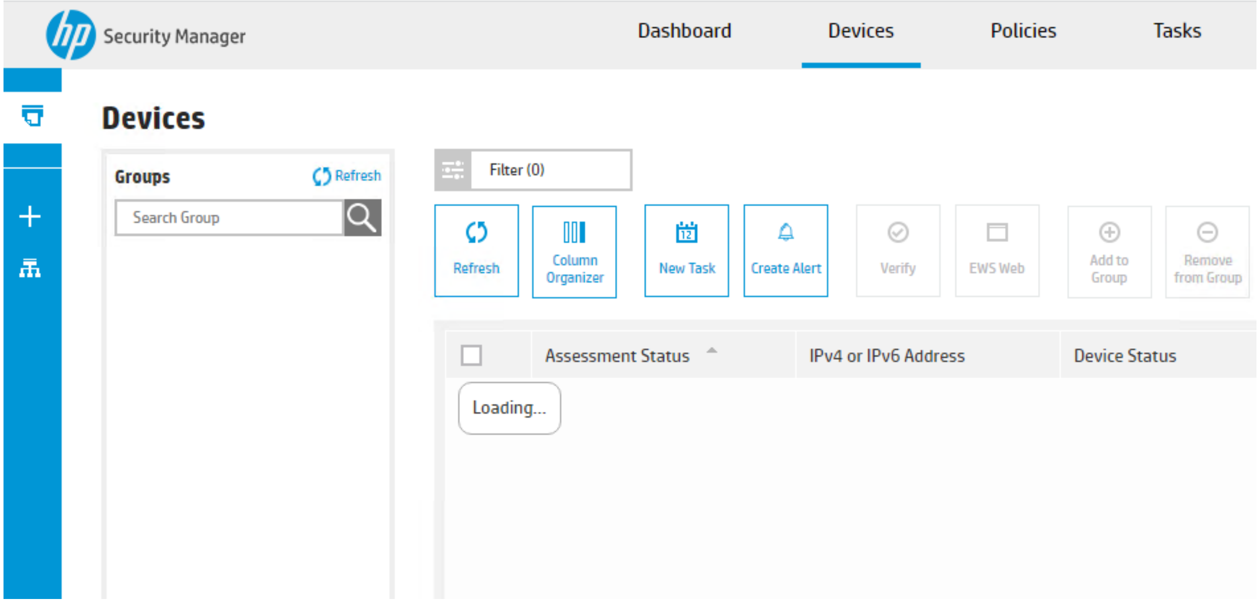
The fixed scripts have been updated to support also older versions of SQL. The updated readme_InstallSQLScripts contains the following version information:



```
About: 3.7.0.21144 , Version B. This version contains a fix to also support SQL 2014 and Older versions
The InstallOrUpgradeRemoteDB batch file is using the same SQL commands as the HPSM installer and can create an HPSM database
(including all tables) or upgrade an existing HPSM database. To be run by a user with sufficient permissions to create and update
the database on the server.

Create Database:
The HPSM database does not exists on the installing machine or the HPSM tables do not exist in the database. In this case use
this script file to create new database and/or the HPSM tables.
```

Devices tab shows "Loading..." and is not showing any devices or groups after upgrade

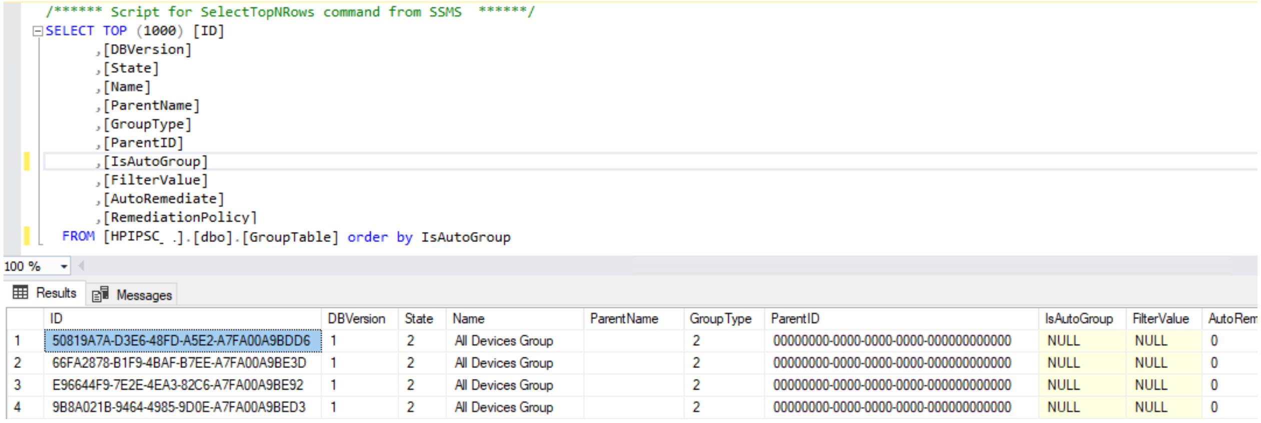
After upgrading it's possible that the dashboard shows the correct number of devices, but on the devices screen, the UI remains at Loading. See screenshot.



In the HPSM_service.log file you can find the following similar error:

```
2022-11-03 21:11:59,849 ERROR Service   [38] -
ScheduledTaskMgr.Unregister - Unexpected Error:
System.InvalidCastException: Object cannot be cast from DBNull to
other types.__   at
System.DBNull.System.IConvertible.ToBoolean(IFormatProvider
provider)__   at
LocksmithBusinessLogic.BizLogicMgr.GetAllGroupRecordsAlone()__   at
LocksmithBusinessLogic.DashBoard.DashBoardManager.ExtractSnapShotDetai
lsFromDS(DataSet dsSnapShotList, DataSet notSupportedSnapShotList)__
at LocksmithBusinessLogic.DashBoard.DashBoardManager.SaveSnapShot()__
at
TaskManager.ScheduleTaskManager.CheckParentStateAndRemoveIfAppropriate
(Guid impactedParentID, Boolean forceDBCheck, String msg, Boolean
propagateStatusMsgAndStateToParent, TaskStatus finalTaskStatus)__   at
TaskManager.ScheduleTaskManager.UnregisterInstanceOnly(WorkerTaskState
wts_toUnReg, String msg, Boolean propagateStatusMsgToParent,
TaskStatus finalTaskStatus)__   at
TaskManager.ScheduleTaskManager.Unregister(WorkerTaskState
workerTaskState, String msg, Boolean propagateStatusMsgToParent,
TaskStatus finalTaskStatus)
```

This behavior is caused by the fact that there are multiple entries in the DB with All Devices Groups with a value of NULL for the IsAutoGroup value. See screenshot.



```
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP (1000) [ID]
      ,[DBVersion]
      ,[State]
      ,[Name]
      ,[ParentName]
      ,[GroupType]
      ,[ParentID]
      ,[IsAutoGroup]
      ,[FilterValue]
      ,[AutoRemediate]
      ,[RemediationPolicy]
  FROM [HPIPSC_ .].[dbo].[GroupTable] order by IsAutoGroup
```

	ID	DBVersion	State	Name	ParentName	GroupType	ParentID	IsAutoGroup	FilterValue	AutoRem
1	50819A7A-D3E6-48FD-A5E2-A7FA00A9BDD6	1	2	All Devices Group		2	00000000-0000-0000-0000-000000000000	NULL	NULL	0
2	66FA2878-B1F9-4BAF-B7EE-A7FA00A9BE3D	1	2	All Devices Group		2	00000000-0000-0000-0000-000000000000	NULL	NULL	0
3	E96644F9-7E2E-4EA3-82C6-A7FA00A9BE92	1	2	All Devices Group		2	00000000-0000-0000-0000-000000000000	NULL	NULL	0
4	9B8A021B-9464-4985-9D0E-A7FA00A9BED3	1	2	All Devices Group		2	00000000-0000-0000-0000-000000000000	NULL	NULL	0

There should only be one entry in this table for the All Devices Group with a value of zero for IsAutoGroup.

To remove the incorrect entries from the table, please run the following script:

```
USE %DBNAME%  -- Replace %DBNAME% with Database name

-- Delete records from GroupTable where IsAutoGroup is NULL
Delete from [dbo].[GroupTable] where IsAutoGroup is NULL
```

Note: This issue has originally been seen after upgrading from 3.6.1 to 3.8 on a database which already contained the incorrect entries in 3.6.1. The root cause of the incorrect entries is unknown. The only way to resolve this issue is by removing the incorrect entries.

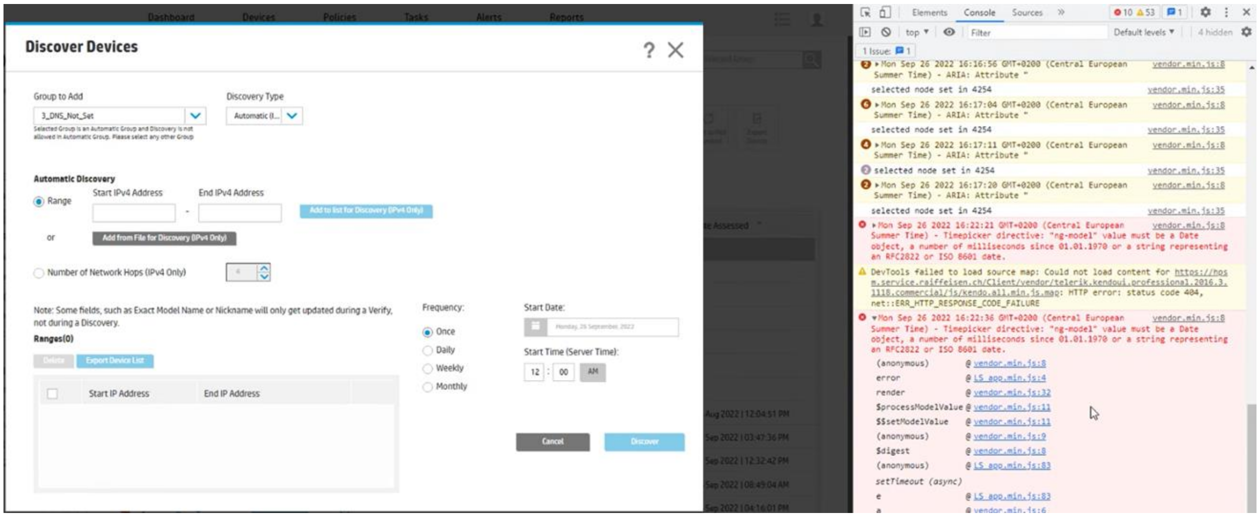
After upgrading to HPSM 3.8 the Start Time of a newly created task is always showing 12:00AM

When creating a new task on a server with localized settings, it's possible that the Server Time cannot be fetched by HPSM 3.8. The UI will in that case always display 12:00 AM as the starting time of the new task.

When you run Chrome in developer mode (F12), you can also see the error message, like

```
(Central European Summer Time) Timepicker directive: "ng-model" value
must be a a Date object, a number of milliseconds since 01.01.1970 or
a string representing an RFC2822 or ISO 8601 date.
```

See screenshot:



Discover Devices

Group to Add: 3_DNS_Not_Set

Selected Group is an Automatic Group and Discovery is not allowed in Automatic Group. Please select any other Group

Discovery Type: Automatic (I...

Automatic Discovery

● Range Start IPv4 Address - End IPv4 Address [Add to list for Discovery (IPv4 Only)]

or [Add from File for Discovery (IPv4 Only)]

○ Number of Network Hops (IPv4 Only) 4

Note: Some fields, such as Exact Model Name or Nickname will only get updated during a Verify, not during a Discovery.

Ranges(0)

[Delete] [Export Device List]

□	Start IP Address	End IP Address

Frequency:
● Once
○ Daily
○ Weekly
○ Monthly

Start Date: Monday, 26 September 2022

Start Time (Server Time): 12 : 00 AM

[Cancel] [Discover]

```
▸Mon Sep 26 2022 16:16:56 GMT+0200 (Central European       vendor.min.js:8
Summer Time) - ARIA: Attribute "
selected node set in 4254                                  vendor.min.js:35
▸Mon Sep 26 2022 16:17:04 GMT+0200 (Central European       vendor.min.js:8
Summer Time) - ARIA: Attribute "
selected node set in 4254                                  vendor.min.js:35
▸Mon Sep 26 2022 16:17:11 GMT+0200 (Central European       vendor.min.js:8
Summer Time) - ARIA: Attribute "
selected node set in 4254                                  vendor.min.js:35
▸Mon Sep 26 2022 16:17:20 GMT+0200 (Central European       vendor.min.js:8
Summer Time) - ARIA: Attribute "
selected node set in 4254                                  vendor.min.js:35
▸Mon Sep 26 2022 16:22:21 GMT+0200 (Central European       vendor.min.js:8
Summer Time) - Timepicker directive: "ng-model" value must be a Date
object, a number of milliseconds since 01.01.1970 or a string representing
an RFC2822 or ISO 8601 date.
DevTools failed to load source map: Could not load content for https://hos
m.service.raiffeisen.ch/Client/vendor/telerik.kendoui.professional.2016.3.
1118.commercial/js/kendo.all.min.js.map: HTTP error: status code 404,
net::ERR_HTTP_RESPONSE_CODE_FAILURE
▾Mon Sep 26 2022 16:22:36 GMT+0200 (Central European       vendor.min.js:8
Summer Time) - Timepicker directive: "ng-model" value must be a Date
object, a number of milliseconds since 01.01.1970 or a string representing
an RFC2822 or ISO 8601 date.
  (anonymous)        @ vendor.min.js:8
  error              @ LS_app.min.js:4
  render             @ vendor.min.js:32
  $processModelValue @ vendor.min.js:11
  $$setModelValue    @ vendor.min.js:11
  (anonymous)        @ vendor.min.js:9
  $digest            @ vendor.min.js:8
  (anonymous)        @ LS_app.min.js:83
  setTimeout (async)
  e                  @ LS_app.min.js:83
  a                  @ vendor.min.js:6
```

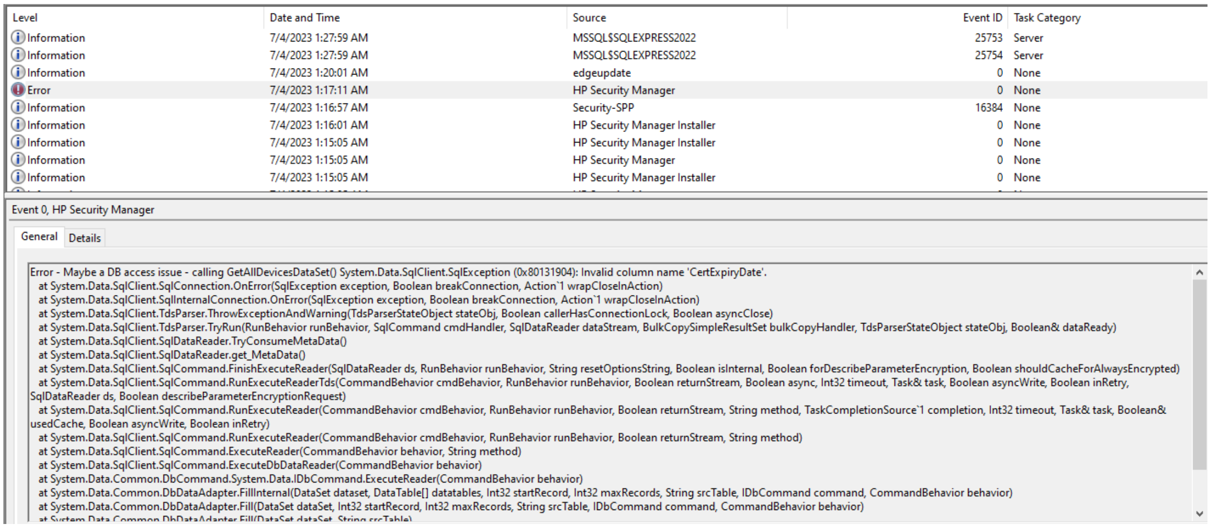
Resolution: Upgrade to HPSM 3.9 or higher.

Workaound: Configure the HPSM server to use US settings (Region settings and language settings)for Welcome Screen and new User Accounts.

After upgrading to HPSM 3.10 zero devices are displayed in the UI and the event viewer shows and error with CertExpiryDate in the description and/or Certificate Expiry Date column missing

Issue 1: after upgrade to HPSM 3.10 and logging into HPSM there are zero devices displayed. In the Windows event viewer, you can see a HP Security Manager error with event ID 0 and the following description:

```
Error - Maybe a DB access issue - calling GetAllDevicesDataSet()
System.Data.SqlClient.SqlException (0x80131904): Invalid column name
'CertExpiryDate'.
```



Level	Date and Time	Source	Event ID	Task Category
Information	7/4/2023 1:27:59 AM	MSSQL$SQLEXPRESS2022	25753	Server
Information	7/4/2023 1:27:59 AM	MSSQL$SQLEXPRESS2022	25754	Server
Information	7/4/2023 1:20:01 AM	edgeupdate	0	None
Error	7/4/2023 1:17:11 AM	HP Security Manager	0	None
Information	7/4/2023 1:16:57 AM	Security-SPP	16384	None
Information	7/4/2023 1:16:01 AM	HP Security Manager Installer	0	None
Information	7/4/2023 1:15:05 AM	HP Security Manager Installer	0	None
Information	7/4/2023 1:15:05 AM	HP Security Manager	0	None
Information	7/4/2023 1:15:05 AM	HP Security Manager Installer	0	None

Event 0, HP Security Manager

```
Error - Maybe a DB access issue - calling GetAllDevicesDataSet() System.Data.SqlClient.SqlException (0x80131904): Invalid column name 'CertExpiryDate'.
   at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)
   at System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction)
   at System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose)
   at System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj, Boolean& dataReady)
   at System.Data.SqlClient.SqlDataReader.TryConsumeMetaData()
   at System.Data.SqlClient.SqlDataReader.get_MetaData()
   at System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString, Boolean isInternal, Boolean forDescribeParameterEncryption, Boolean shouldCacheForAlwaysEncrypted)
   at System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async, Int32 timeout, Task& task, Boolean asyncWrite, Boolean inRetry,
SqlDataReader ds, Boolean describeParameterEncryptionRequest)
   at System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method, TaskCompletionSource`1 completion, Int32 timeout, Task& task, Boolean&
usedCache, Boolean asyncWrite, Boolean inRetry)
   at System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method)
   at System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String method)
   at System.Data.SqlClient.SqlCommand.ExecuteDbDataReader(CommandBehavior behavior)
   at System.Data.Common.DbCommand.System.Data.IDbCommand.ExecuteReader(CommandBehavior behavior)
   at System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior)
   at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior)
   at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, String srcTable)
```

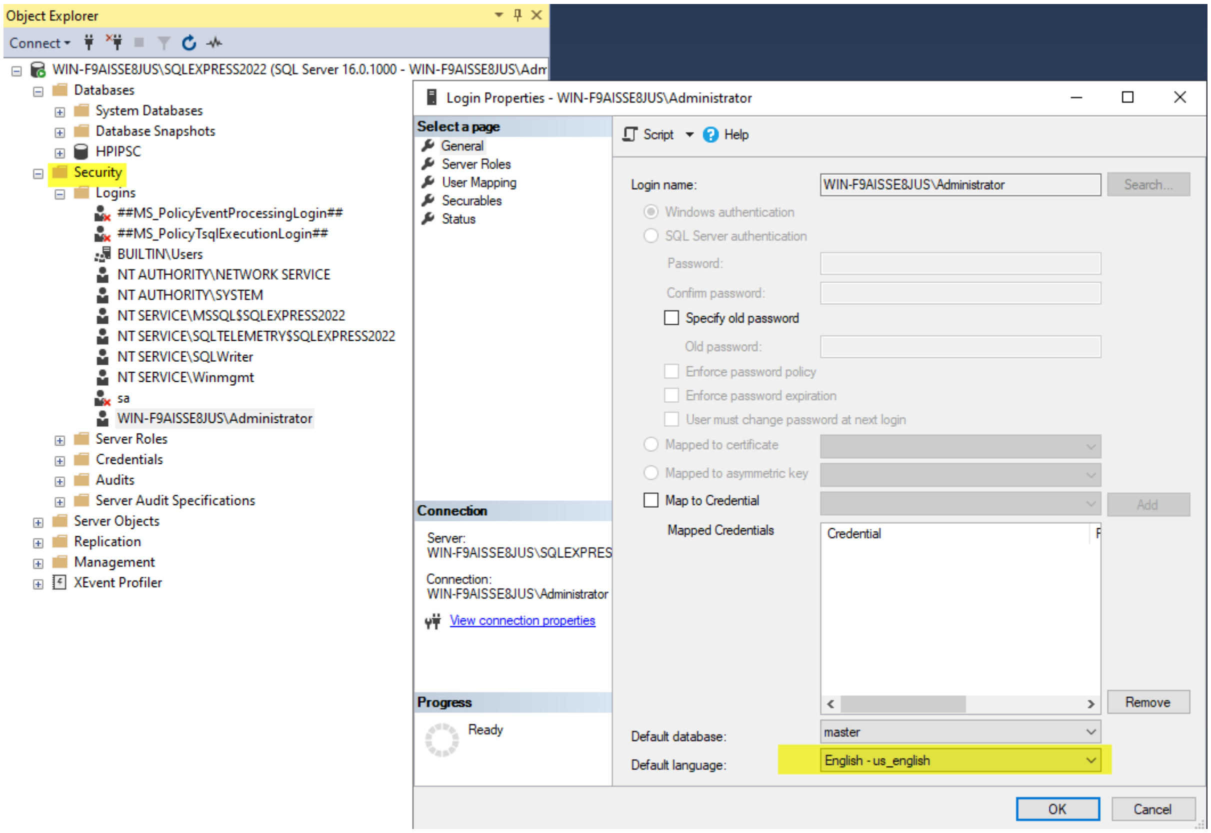
Issue 2: after upgrade to HPSM 3.10 and logging into HPSM you cannot see the column option Certificate Expiry Date when clicking on Column Organizer
I

Additional information:
When upgrading to HPSM 3.10 a new column called CertExpiryDate should get added to the dbo.DeviceTable. If the column CertExpiryDate is missing, then zero devices will be displayed in the UI (while in fact all the devices are still listed in the DB). When you re-run the InstallSQLscripts, you can see the following error in the InstallOrUpgradeRemoteDB21.log:

```
  ALTER TABLE dbo.DeviceTable
  ADD  CertExpiryDate datetime NOT NULL DEFAULT CONVERT(DATETIME,
'9999-12-31 23:59:59.000')
Msg 242, Level 16, State 3, Server gbrdsm050001522\BAR_SQLVIRT_DEV,
Line 2
The conversion of a varchar data type to a datetime data type resulted
in an out-of-range value.
Msg 1750, Level 16, State 1, Server gbrdsm050001522\BAR_SQLVIRT_DEV,
Line 2
Could not create constraint or index. See previous errors.
```

Solution:
There are two ways to get the missing column.
Method 1:

1. Open SQL Server Management Studio
2. Expand Security for the instance running HPSM database
3. Expand the Logins
4. Right-mouse click on the user running the SQL installation scripts and select **Properties**
5. Change the default Language to English -us_English as shown in the following screenshot:


Object Explorer
Connect
WIN-F9AISSE8JUS\SQLEXPRESS2022 (SQL Server 16.0.1000 - WIN-F9AISSE8JUS\Adm
Databases
System Databases
Database Snapshots
HPIPSC
Security
Logins
##MS_PolicyEventProcessingLogin##
##MS_PolicyTsqlExecutionLogin##
BUILTIN\Users
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
NT SERVICE\MSSQL$SQLEXPRESS2022
NT SERVICE\SQLTELEMETRY$SQLEXPRESS2022
NT SERVICE\SQLWriter
NT SERVICE\Winmgmt
sa
WIN-F9AISSE8JUS\Administrator
Server Roles
Credentials
Audits
Server Audit Specifications
Server Objects
Replication
Management
XEvent Profiler
Login Properties - WIN-F9AISSE8JUS\Administrator
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Search...
Connection
View connection properties
Progress
Ready
Add
Remove
OK
Cancel

Login name: WIN-F9AISSE8JUS\Administrator
● Windows authentication
○ SQL Server authentication
Password:
Confirm password:
□ Specify old password
Old password:
□ Enforce password policy
□ Enforce password expiration
□ User must change password at next login
○ Mapped to certificate
○ Mapped to asymmetric key
□ Map to Credential
Mapped Credentials | Credential

Server:
WIN-F9AISSE8JUS\SQLEXPRES

Connection:
WIN-F9AISSE8JUS\Administrator

Default database: master
Default language: English - us_english

6. Click on **Ok**
7. Close SQL Server Management Studio.
8. Now you can re-run the InstallSQLScripts with the account which was just changed.

Note: The InstallSQLScripts.zip are in the root directory of HPSM. Unpack the scripts, open a command prompt with administrator rights and run InstallOrUpgradeRemoteDB.bat (required syntax in corresponding help file and will be displayed when executing the bat file without any further options.

9. Refresh the Devices screen in HPSM and the devices will now be displayed.
10. As an alternative to step 8, you can also reopen SQL Server Management Studio with the following next steps:
    - open the UpgradeDbSchemaVer21to22.sql from the InstallSQLScripts
    - change on the first line:
      `USE $(DBNAME) into USE` HPIPSC (or whatever the actual databasename is)
    - Click on Execute
    - Refresh the Devices screen in HPSM and the devices will now be displayed.

Method 2:
With this method the SQL user configuration remains the same.

1. Execute the following SQL commands in SQL Management Studio (in the example below the database name is HPIPSC):

```
USE HPIPSC

PRINT
'==============================================================================
'
PRINT 'Add CertExpiryDate Column in DeviceTable'
PRINT
'==============================================================================
'
GO
IF NOT EXISTS(SELECT 1 FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME =
'DeviceTable' AND (COLUMN_NAME = 'CertExpiryDate'))
BEGIN
  DECLARE @SQL NVARCHAR(MAX) = N'';
  SET @SQL += N'
  ALTER TABLE dbo.DeviceTable
  ADD  CertExpiryDate datetime NOT NULL DEFAULT CONVERT(DATETIME, ''9999-12-31
23:59:59.000'',120)'
  PRINT @SQL
 EXECUTE(@SQL)
END;
GO
```

Note: 120 is used for the format 'yyyy-mm-dd hh:mm:ss'

2. Refresh the Devices screen in HPSM and the devices will now be displayed.

When you click on Column Organizer, the column option Certificate Expiry Date should also be displayed. If this is not displayed, remove all cached data in Chrome:
Go to **Settings**,
Privacy and Security
Clear Browsing data,
Select Time Range: **All time**

Select **Browsing history**, **Cookies and other site data** and **Cached images and files**.
Click on **Clear Data**

After re-logging into HPSM the column should now be displayed.

Certificate Installation Failures

Certificate installation fails on HP DesignJet Z9

HPSM can generate a CSR on behalf of the device (CSR source set to HPSM) or can retrieve the CSR from the device, if the device supports this process. As this is not supported by the HP DesignJet Z9, you almost must select the CSR source as HPSM for ID certificate installations on this device.
In the EAPDeviceLib.log you can see the following error when using device as source:

```
2020-06-18 11:47:29,192 DEBUG Pipeline [5]  - uid=_a738e1943df8_10.10.10.119, Exception while converting
certificate to X509Certificate
```

The input is not a valid Base-64 string as it contains a non-base 64 character, more than two padding characters, or an illegal character among the padding characters.

Certificate installation issues with Microsoft CA

Troubleshooting certificate installation failures is no different than troubleshooting most configuration issues. The typical scenarios can cause failures such as name resolution issues, network connectivity issues, traffic blocked by firewall, permissions, device issues, etc.

Security Manager uses DCOM over RPC to submit requests to the CA and retrieve certificates, like workstations do for auto-enrollment of certificates. Remote Procedure Call (RPC) is a mechanism that allows Windows processes to communicate with one another, either between a client and server across a network or within a single system. Numerous built-in Windows components utilize RPC. RPC uses dynamic ports for communication between systems, but a static port (TCP port 135) must also be used as a starting point for communication. The RPC endpoint mapper listens on this static port.

In a typical RPC session, a client contacts a server's endpoint mapper on TCP port 135 and requests the dynamic port number assigned to a particular service. The server responds with the IP address and port number that the service registered with RPC when it started, and the client then contacts the service on that IP address and port.

If the RPC server is unavailable, errors will occur indicating the certificate was not installed. Many other reasons can cause a certificate to not install. For example, the RPC server's name may be resolving to the wrong IP address, resulting in the client contacting the wrong server or attempting to contact an IP address not currently in use. Alternatively, the server's name may not be resolving at all. A firewall or other security application on the server, or a network firewall appliance between the client and server, may be preventing traffic from reaching the server on TCP port 135. The client may be unable to reach the server at all due to a general network problem.

The following troubleshooting steps should help to resolve these issues.

1. Check the policy settings again for accuracy.
    a. Check especially the Certificate Authority Server and Certificate Authority settings.
    b. Ping the server by name from the client to verify that the name resolves to the correct IP address.
    c. If it does not, verify that the client and server are both using the correct DNS servers, which must be inside the domain and will typically be domain controllers.
    d. Try an IP Address instead of a hostname for the server in case the hostname is not resolving.
    e. Check whether the Key Length or Signature Algorithm values in the policy are not supported by the device either as a value that can be created in a CSR if Jetdirect is chosen as source or as a value in the certificate itself.
2. Check the Certificate Authority settings again to ensure that the account running the HPSM service has the rights to submit requests to the CA.
   NOTE: By default, the Network Service account runs the HPSM service, and Network Service manifest itself remotely as the machine name (machine$).

3. Check the CA Template settings again.
    a. Make syre the account running the HPSM service has the rights for Read and Enroll and that Authenticated Users has Read permissions.
    b. Make sure **Submit in Request** is selected in the template settings under the **Subject Name** tab. If not, then certificate will be created for the Security Manager server and not the printer.

4. Make sure the Security Manager server is on the same domain as the CA server.
   NOTE: If the CA server is on a different domain as the HPSM server, and no trust relationship exists between the domains, an error will display claiming the template does not exist. Even though the template clearly exists, templates must be published into Active Directory for clients to use them, and the lack of trust relationship will prevent Security Manager from seeing the template.

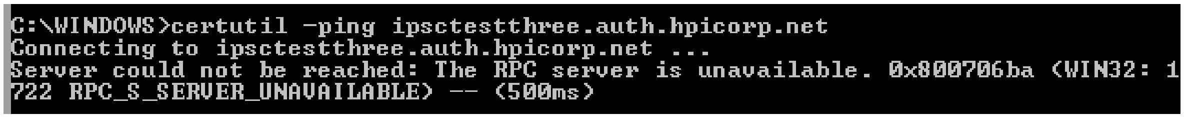
5. Check firewall settings for any ports being blocked, and if the firewall is enabled on the Security Manager server, make sure traffic on TCP port 135 is allowed to pass.
   NOTE: Security Manager uses DCOM over RPC, like workstations do for auto-enrollment of certificates, and DCOM uses port 135 for certificate enrollment. If workstations are successfully auto-enrolling for certificates, it can be reasonably assumed the CA server firewall is not blocking port 135.

The certutil tool can simulate the behavior Security Manager performs to submit a request and retrieve a certificate by checking for the port being blocked or not:

certutil -ping “CA server”

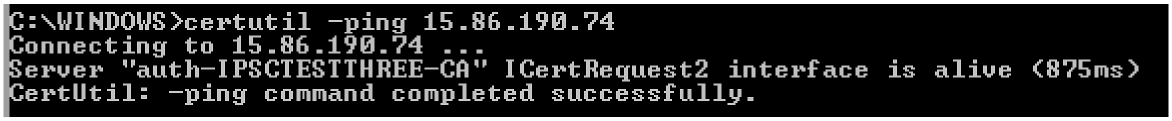
Examples of an unsuccessful attempt to connect to a non-resolvable FQDN and a successful attempt to the IP Address:

- The PortQry command-line utility or PortQryui.exe user interface utility (both downloadable from Microsoft, for example: https://www.microsoft.com/en-us/download/details.aspx?id=24009) can be used to test connectivity from the client to the server and determine which ports are open on the server. It includes support for RPC and can be used to determine which services have dynamic ports registered with RPC and which specific ports they use.



```
C:\WINDOWS>certutil -ping ipsctestthree.auth.hpicorp.net
Connecting to ipsctestthree.auth.hpicorp.net ...
Server could not be reached: The RPC server is unavailable. 0x800706ba (WIN32: 1
722 RPC_S_SERVER_UNAVAILABLE) -- (500ms)
```

- If workstations are also having issues auto-enrolling for certificates, then the standard troubleshooting steps for resolving RPC Server Unavailable errors may apply. For example, ensuring that the RPC service us running, the Authenticated Users group is in the “Certificate Service DCOM Access” group, **Enable Distributed COM on this computer** is selected in the Default Properties tab, etc.



```
C:\WINDOWS>certutil -ping 15.86.190.74
Connecting to 15.86.190.74 ...
Server "auth-IPSCTESTTHREE-CA" ICertRequest2 interface is alive (875ms)
CertUtil: -ping command completed successfully.
```

Certificate installation issues with SCEP

Workflow for SCEP

When a SCEP server is used with a SCEP challenge password, then you should first see int the log file, that the SCEP challenge password is requested (GetOneTimePassword) and obtained.

```
2021-04-09 16:26:43,506 DEBUG Scep   [5] - Scep::GetOneTimePassword(): called
2021-04-09 16:26:43,568 DEBUG Scep   [5] - Scep::SendRequest(): GET
https://Testserver.cloudshare.com/vedscep/mscep_admin
2021-04-09 16:26:46,814 DEBUG Scep   [5] - Scep::SendRequest(): Server returned status code
OK (OK)
2021-04-09 16:26:46,830 DEBUG Scep   [5] - Scep::SendRequest(): payload size: 2514
2021-04-09 16:26:46,830 DEBUG Scep   [5] - Scep::SendRequest(): MIME content type: text/html
2021-04-09 16:26:46,830 DEBUG Scep   [5] - --- BEGIN ndes_admin RESPONSE ---
__?<HTML><Head><Meta HTTP-Equiv="Content-Type" Content="text/html; charset=UTF-
8"><Title>Network Device Enrollment Service</Title></Head><Body BgColor=#FFFFFF><Font
ID=locPageFont Face="Arial"><Table Border=0 CellSpacing=0 CellPadding=4 Width=100%
BgColor=#008080><TR><TD><Font ID=locPageTitleFont Face="Arial" Size=-1
Color=#FFFFFF><LocID ID=locMSCertSrv>Network Device Enrollment
Service</LocID></Font></TD></TR></Table><P ID=locPageTitle> Network Device Enrollment
Service allows you to obtain certificates for routers or other network devices using the Simple
Certificate Enrollment Protocol (SCEP). </P><P> To complete certificate enrollment for your
network device you will need the following information: <P> The thumbprint (hash value) for the
CA certificate is: <B> 89AF30A1 77B4BA20 7B9E07FD F77643D9 </B> <P> The enrollment
challenge password is: <B> 365603DA91776E62 </B> <P> This password can be used only once
and will expire within 60 minutes. <P> Each enrollment requires a new challenge password. You
can refresh this web page to obtain a new challenge password. </P> <P ID=locPageDesc> For
more information see  <A HREF=http://go.microsoft.com/fwlink/?LinkId=67852>Using Network
Device Enrollment Service </A>. </P> <P></Font></Body></HTML> __--- END ndes_admin
RESPONSE ---
2021-04-09 16:26:46,877 DEBUG Scep   [5] - Scep::GetOneTimePassword(): Extracted ndes
challenge: 365603DA91776E62
```

Now HPSM can send the actual request:

```
2021-04-09 16:26:46,877 INFO  Scep   [5] - Generating CSR
2021-04-09 16:26:46,892 DEBUG Scep   [5] - Scep::CreateSubjectName(): Created Subject Name
: CN = Printer1.usa.CompanyXXX, O = XXX, OU = MPS, L = Low, ST = New York, C = US
2021-04-09 16:26:47,455 INFO  Scep   [5] - Getting CA Certificates from SCEP Server
2021-04-09 16:26:47,455 DEBUG Scep   [5] - Scep::GetCACert() called
2021-04-09 16:26:47,455 DEBUG Scep   [5] - Scep::SendRequest(): GET
https://testserver.cloudshare.com/vedscep/mscep/?operation=GetCACert&message=ignore
2021-04-09 16:26:48,064 DEBUG Scep   [5] - Scep::SendRequest(): Server returned status code
OK (OK)
2021-04-09 16:26:48,064 DEBUG Scep   [5] - Scep::SendRequest(): payload size: 2378
2021-04-09 16:26:48,064 DEBUG Scep   [5] - Scep::SendRequest(): MIME content type:
application/x-x509-ca-ra-cert
2021-04-09 16:26:48,080 DEBUG Scep   [5] - Scep::GetCACert(): Received 2 CA/RA certificates
2021-04-09 16:26:48,095 INFO  Scep   [5] - Submit SCEP Request to SCEP Server
2021-04-09 16:26:48,095 DEBUG Scep   [5] - Scep::SubmitToScep(): called
2021-04-09 16:26:48,264 DEBUG Scep   [5] - Scep::CreateSubjectName(): Created Subject Name
: CN = printer1.usa.CompanyXXX, O = XXX, OU = MPS, L = Low, ST = New York, C = US
2021-04-09 16:26:48,264 DEBUG Scep   [5] - Scep::SubmitToScep(): Selected SignatureAlgorithm
: SHA256
2021-04-09 16:26:48,592 DEBUG Scep   [5] - Scep::SendRequest(): GET
https://uvo1pum39esurtb5qe9.env.cloudshare.com/vedscep/mscep/?operation=PKIOperation
```

```
&message=MIINNgYJKoZIhvcNAQcCoIINJzCCDSMCAQExCzAJBgUrDgMCGgUAMIIGtwY ---
removed further details for readability of log file—
2021-04-09 16:26:50,304 DEBUG Scep   [5] - Scep::SendRequest(): Server returned status code
OK (OK)
2021-04-09 16:26:50,304 DEBUG Scep   [5] - Scep::SendRequest(): payload size: 1202
2021-04-09 16:26:50,304 DEBUG Scep   [5] - Scep::SendRequest(): MIME content type:
application/x-pki-message
2021-04-09 16:26:50,304 DEBUG Scep   [5] - Scep::SubmitToScep(): Received PKCS7 Response
Packet
```

After this there is not much detail available about a potential error in the SCEP.log while generating the certificate. In fact, the SCEP server only reports pkiStatus: 0 (successful), PkiStatus: 3 (pending) or PkiStatus: 2 (failed) for the certificate generation.

Example of PKIStatus 3 in the HPCM.log:

```
2021-04-09 16:26:50,382 DEBUG Scep   [5] - Scep::SubmitToScep(): pkiStatus:3 (Pending) failInfo:
(none)
This is followed by a polling request.
2021-04-09 16:26:50,382 INFO  Scep   [5] - Scep::SubmitToScep(): PKIStatus is3. Certificate Signing
Request pending. Poll to get the certificate
As polling is done by HPSM, it should be followed by a success message as well.
```

Example of success response 0 in the HPCM.log (can be seen with and without :)

```
2020-09-30 15:19:51,442 DEBUG Scep   [4] - Scep::SubmitToScep(): pkiStatus:0 (Success) failInfo:
(none)
```

Example of failure 3 in HPCM.log:

```
2021-09-28 16:51:06,990 ERROR HPCM   [28] - SCEPConnector: Errow while Enroll: PKIStatus is 2.
Error while signing the certifica
```

When an error 2 is reported, then additional tools will have to be used to find out why the process failed on the SCEP server. Check the windows event viewer on the SCEP server, when this error occurs. Also check if there are any logs available in the SCEP server, which might explain the actual error message.

ASN1 bad tag in HPSM_service.log file using HPSM 3.7.0 or 3.7.1 and Microsoft NDES (SCEP)

When using NDES (Microsoft implementation of SCEP), the ID certificate installation will fail with HPSM 3.7 and 3.7.1 with the following error message in the HPSM_service.log file:

```
2022-03-23 14:52:23,477 ERROR Service [26] - PKI Provider Web Access Restriction Error.
Exception: HP.HPCM.Contract.Exception.BadRequestException: ASN1 bad tag value met.____ at
HP.HPCM.ScepConnector.SCEPConnector.Enroll(CertificateEnrollData certificateEnrollData)
at HP.HPCM.Provider.ProviderHandler.ExecuteEnroll(String providerName,
CertificateEnrollData certData)__ at HP.HPCM.HPCMService.Execute(CertificateEnrollData
request)
```

In the event viewer from the NDES server you might see the following error:

```
- <EventData Name="EVENT_MSCEP_FAIL_TO_DECRYPT_INNER">
```

```
<Data Name="ErrorCode">0x80090005</Data>
<Data Name="ErrorMessage">BadData.</Data>
```

Solution

Upgrade to HPSM 3.8 or obtain new dll's for HPSM 3.7.1 from HPSM support.

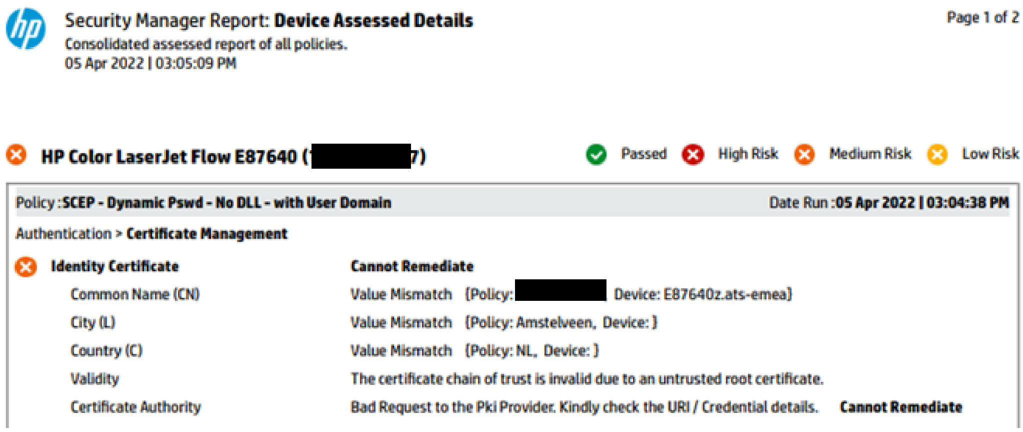
'Bad Request to the Pki Provider' or Cannot Remediate when using dynamic passwords

Issue

When using Microsoft SCEP (NDES) ID, the certificate installation might fail. In the Assessment report the following error will be listed:

Bad Request to the PKi Provider. Kindly check the UI/Credential details. Cannot Remediate.

Figure: "Bad Request to the PKi Provider...." Error listed



Security Manager Report: **Device Assessed Details**
Consolidated assessed report of all policies.
05 Apr 2022 | 03:05:09 PM

Page 1 of 2

✗ **HP Color LaserJet Flow E87640 ([redacted]7)**

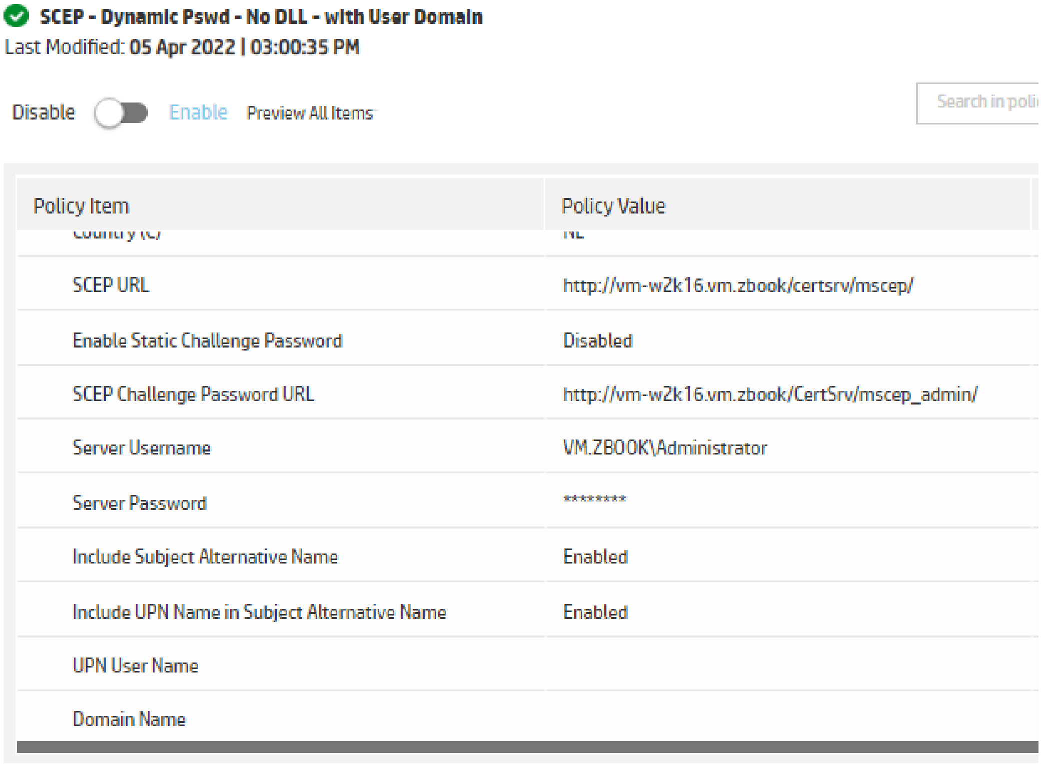
✓ Passed ✗ High Risk ✗ Medium Risk ✗ Low Risk

Policy :**SCEP - Dynamic Pswd - No DLL - with User Domain**   Date Run :**05 Apr 2022 | 03:04:38 PM**

Authentication > **Certificate Management**

✗ **Identity Certificate**	**Cannot Remediate**
Common Name (CN)	Value Mismatch (Policy: [redacted] Device: E87640z.ats-emea)
City (L)	Value Mismatch (Policy: Amstelveen, Device:)
Country (C)	Value Mismatch (Policy: NL, Device:)
Validity	The certificate chain of trust is invalid due to an untrusted root certificate.
Certificate Authority	Bad Request to the Pki Provider. Kindly check the URI / Credential details. **Cannot Remediate**

First check the credentials, SCEP URL and SCEP challenge password URL in the policy.



SCEP - Dynamic Pswd - No DLL - with User Domain

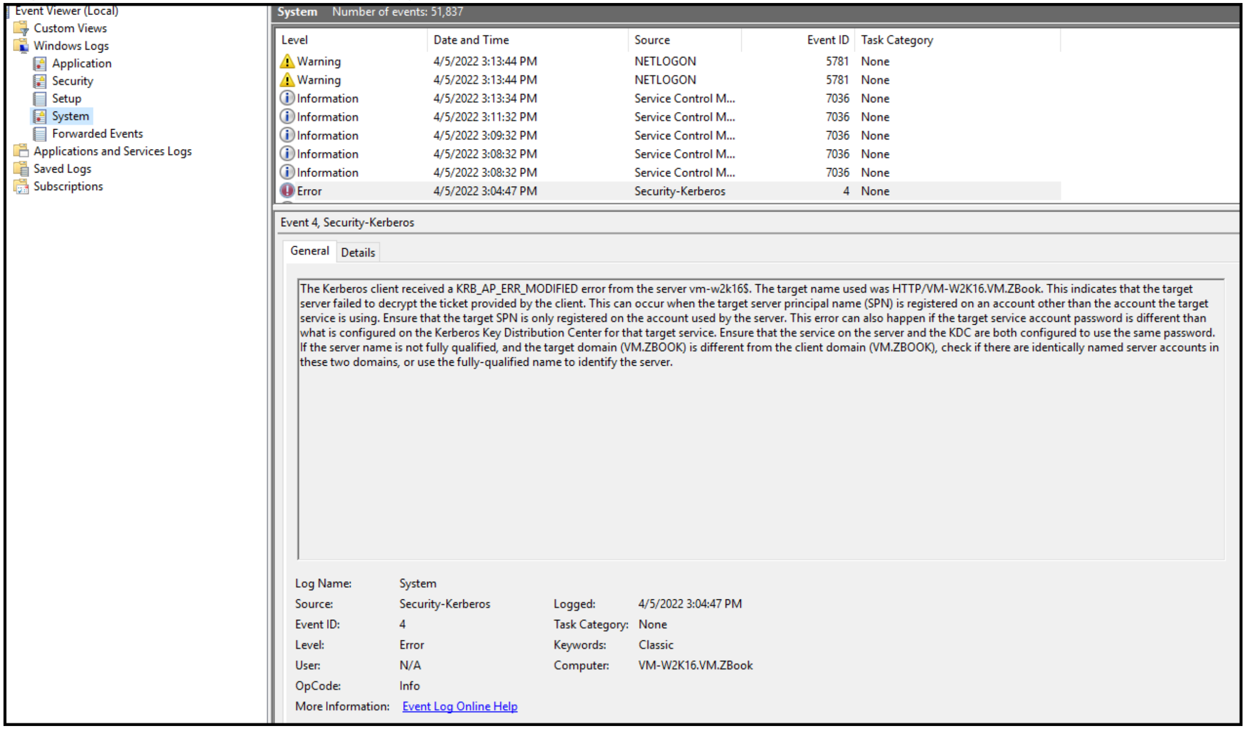
Last Modified: **05 Apr 2022 | 03:00:35 PM**

Policy Item	Policy Value
Country (C)	NL
SCEP URL	http://vm-w2k16.vm.zbook/certsrv/mscep/
Enable Static Challenge Password	Disabled
SCEP Challenge Password URL	http://vm-w2k16.vm.zbook/CertSrv/mscep_admin/
Server Username	VM.ZBOOK\Administrator
Server Password	********
Include Subject Alternative Name	Enabled
Include UPN Name in Subject Alternative Name	Enabled
UPN User Name	
Domain Name	

If the URLs and username and password are correct, then additional information should be checked.

Check in the event viewer system log if there is an event ID 4.

Figure: Event Viewer, System log where an **Event 4** is listed



System Number of events: 51,837

Level	Date and Time	Source	Event ID	Task Category
Warning	4/5/2022 3:13:44 PM	NETLOGON	5781	None
Warning	4/5/2022 3:13:44 PM	NETLOGON	5781	None
Information	4/5/2022 3:13:34 PM	Service Control M...	7036	None
Information	4/5/2022 3:11:32 PM	Service Control M...	7036	None
Information	4/5/2022 3:09:32 PM	Service Control M...	7036	None
Information	4/5/2022 3:08:32 PM	Service Control M...	7036	None
Information	4/5/2022 3:08:32 PM	Service Control M...	7036	None
Error	4/5/2022 3:04:47 PM	Security-Kerberos	4	None

Event 4, Security-Kerberos

The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server vm-w2k16$. The target name used was HTTP/VM-W2K16.VM.ZBook. This indicates that the target server failed to decrypt the ticket provided by the client. This can occur when the target server principal name (SPN) is registered on an account other than the account the target service is using. Ensure that the target SPN is only registered on the account used by the server. This error can also happen if the target service account password is different than what is configured on the Kerberos Key Distribution Center for that target service. Ensure that the service on the server and the KDC are both configured to use the same password. If the server name is not fully qualified, and the target domain (VM.ZBOOK) is different from the client domain (VM.ZBOOK), check if there are identically named server accounts in these two domains, or use the fully-qualified name to identify the server.

Log Name:	System		
Source:	Security-Kerberos	Logged:	4/5/2022 3:04:47 PM
Event ID:	4	Task Category:	None
Level:	Error	Keywords:	Classic
User:	N/A	Computer:	VM-W2K16.VM.ZBook
OpCode:	Info		
More Information:	Event Log Online Help		

Text from General section in EventID 4: The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server vm-w2k16$. The target name used was HTTP/VM-W2K16.VM.ZBook. This indicates that the target server failed to decrypt the ticket provided by the client. This can occur when the target server principal name (SPN) is registered on an account other than the account the target service is using. Ensure that the target SPN is only registered on the account used by the server.

This error can also happen if the target service account password is different than what is configured on the Kerberos Key Distribution Center for that target service. Ensure that the service on the server and the KDC are both configured to use the same password. If the server name is not fully qualified, and the target domain (VM.ZBOOK) is different from the client domain (VM.ZBOOK), check if there are identically named server accounts in these two domains or use the fully qualified name to identify the server.

Here you already see that there is something wrong with the account (SPN) being used in the policy.

In the **HPSM Service Log** you will find the same information as in the assessment report:

```
Line 563: 2022-04-05 15:04:51,246 ERROR Service   [17] - PKI Provider Web Access Restriction
Error. Exception: HP.HPCM.Contract.Exception.BadRequestException: BadRequest__   at
HP.HPCM.ScepConnector.SCEPConnector.Enroll(CertificateEnrollData certificateEnrollData)
at HP.HPCM.Provider.ProviderHandler.ExecuteEnroll(String providerName,
CertificateEnrollData certData)__   at HP.HPCM.HPCMService.Execute(CertificateEnrollData
request)
```

In the SCEP Log, you will find some additional information to an unauthorized action:

```
2022-04-05 15:04:46,756 DEBUG Scep  [4] - SCEP::SendRequest(): GET http://vm-
w2k16.vm.zbook/CertSrv/mscep_admin/
2022-04-05 15:04:47,055 ERROR Scep  [4] - SCEP::SendRequest(): Exception
System.AggregateException: One or more errors occurred. --->
System.Net.Http.HttpRequestException: An error occurred while sending the request. --->
System.Net.WebException: The remote server returned an error: (401) Unauthorized. --->
System.ComponentModel.Win32Exception: The target principal name is incorrect__  at
System.Net.NTAuthentication.GetOutgoingBlob(Byte[] incomingBlob, Boolean throwOnError,
SecurityStatus& statusCode)__  at System.Net.NTAuthentication.GetOutgoingBlob(String
incomingBlob)__  at System.Net.NegotiateClient.DoAuthenticate(String challenge,
WebRequest webRequest, ICredentials credentials, Boolean preAuthenticate)__  at
System.Net.NegotiateClient.Authenticate(String challenge, WebRequest webRequest,
ICredentials credentials)__  at System.Net.AuthenticationManagerDefault.Authenticate(String
challenge, WebRequest request, ICredentials credentials)__  at
System.Net.AuthenticationState.AttemptAuthenticate(HttpWebRequest httpWebRequest,
ICredentials authInfo)__  at System.Net.HttpWebRequest.CheckResubmitForAuth()__  at
System.Net.HttpWebRequest.CheckResubmit(Exception& e, Boolean& disableUpload)__  ---
End of inner exception stack trace ---__  at
System.Net.HttpWebRequest.EndGetResponse(IAsyncResult asyncResult)__  at
System.Net.Http.HttpClientHandler.GetResponseCallback(IAsyncResult ar)__  --- End of inner
exception stack trace ---__  --- End of inner exception stack trace ---__  at
System.Threading.Tasks.Task`1.GetResultCore(Boolean waitCompletionNotification)__  at
ScepClient.Scep.SendRequest(Uri requestUri, String method, Byte[] request_body, String
request_content_type, List`1 add_headers)__---> (Inner Exception #0)
System.Net.Http.HttpRequestException: An error occurred while sending the request. --->
System.Net.WebException: The remote server returned an error: (401) Unauthorized. --->
System.ComponentModel.Win32Exception: The target principal name is incorrect__  at
System.Net.NTAuthentication.GetOutgoingBlob(Byte[] incomingBlob, Boolean throwOnError,
SecurityStatus& statusCode)__  at System.Net.NTAuthentication.GetOutgoingBlob(String
incomingBlob)__  at System.Net.NegotiateClient.DoAuthenticate(String challenge,
WebRequest webRequest, ICredentials credentials, Boolean preAuthenticate)__  at
System.Net.NegotiateClient.Authenticate(String challenge, WebRequest webRequest,
ICredentials credentials)__  at System.Net.AuthenticationManagerDefault.Authenticate(String
challenge, WebRequest request, ICredentials credentials)__  at
System.Net.AuthenticationState.AttemptAuthenticate(HttpWebRequest httpWebRequest,
ICredentials authInfo)__  at System.Net.HttpWebRequest.CheckResubmitForAuth()__  at
System.Net.HttpWebRequest.CheckResubmit(Exception& e, Boolean& disableUpload)__  ---
End of inner exception stack trace ---__  at
System.Net.HttpWebRequest.EndGetResponse(IAsyncResult asyncResult)__  at
System.Net.Http.HttpClientHandler.GetResponseCallback(IAsyncResult ar)__  --- End of inner
exception stack trace ---<---__
2022-04-05 15:04:47,055 ERROR Scep  [4] - SCEP::GetOneTimePassword() failed; StatusCode:
BadRequest (The remote server returned an error: (401) Unauthorized.)
2022-04-05 15:04:47,055 DEBUG Scep  [4] - SCEP::GetOneTimePassword(): failed; no regex
match
2022-04-05 15:04:47,055 DEBUG Scep  [4] - SCEP : Challenge Password :
2022-04-05 15:04:47,055 ERROR Scep  [4] - SCEP::Enroll(): Could not retrieve Challenge
password from SCEP Server due to :BadRequest
```

Solution
From a command prompt with admin privileges, delete the SPN for the useraccount used in the HPSM policy. This can be done with the setspn -U -D command, example:
setspn -U -D http/VM-W2K16.VM.ZBOOK administrator

The command prompt will confirm that the unregistration was successful:

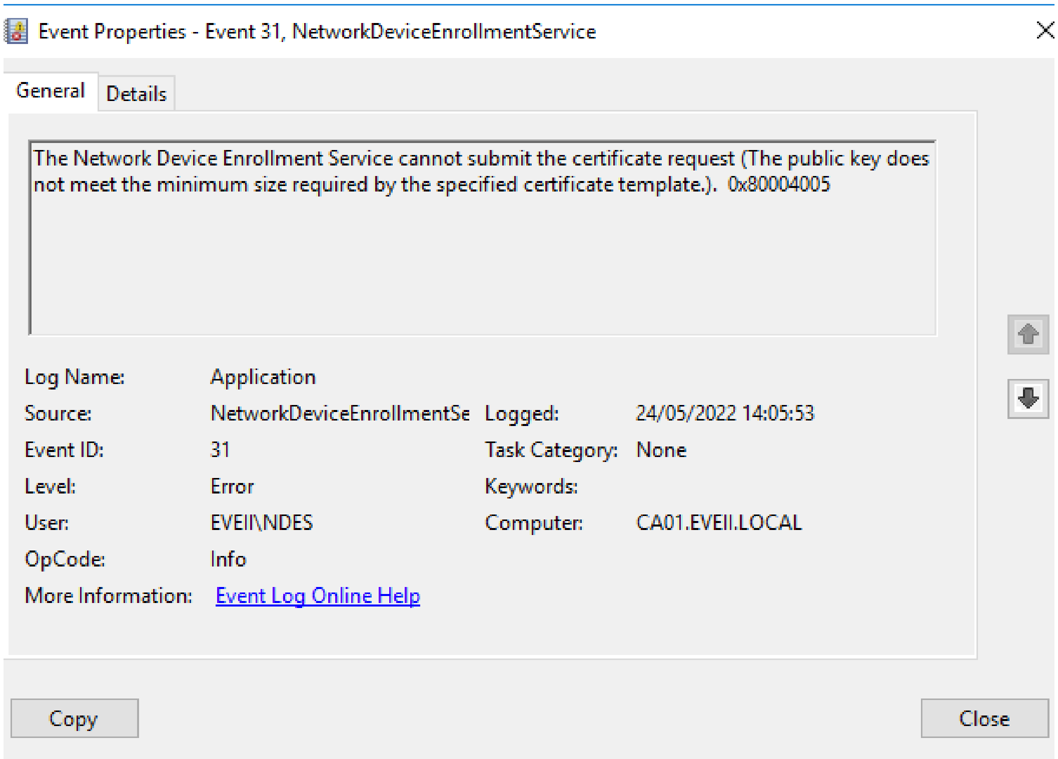
```
Unregistering ServicePrincipalNames for CN=Administrator,CN=Users,DC=VM,DC=ZBook
    http/VM-W2K16.VM.ZBOOK
Updated object
```

Microsoft SCEP fails and InternalServerError in Scep.log

HPSM 3.6.1/3.7/3.7.1 is hardcoding the public key length to 2048 key length. If the public key length in the CA template is higher, then the request will fail. The only indication about the key length is in the system log file *from the SCEP server.*

In the Scep.log file you can find the following error:

```
2022-03-17 17:37:12,887 DEBUG Scep   [24] - SCEP::SendRequest(): GET
https://svpt1qiknc002.bcpcorp.dev/CertSrv/mscep_admin/
2022-03-17 17:37:13,449 DEBUG Scep   [24] - SCEP::SendRequest(): Server returned status code
InternalServerError (Internal Server Error)
```



The Network Device Enrollment Service cannot submit the certificate request (The public key does not meet the minimum size required by the specified certificate template.). 0x80004005

Log Name: Application
Source: NetworkDeviceEnrollmentSe
Logged: 24/05/2022 14:05:53
Event ID: 31
Task Category: None
Level: Error
Keywords:
User: EVEII\NDES
Computer: CA01.EVEII.LOCAL
OpCode: Info
More Information: Event Log Online Help

Solution
Upgrade to HPSM 3.8.

Workaround

Obtain the HP.HPCM.ScepClient.dll and HP.HPCM.ScepConnector.dll from HPSM 3.6 and install those in HPSM 3.7.1.

1. Stop the HPSM service.
2. Open the "C:\Program Files (x86)\HP Security Manager\PkiProviders" directory.
3. Rename the "HP.HPCM.ScepClient.dll" file to "HP.HPCM.ScepClient.dll.old".
4. Rename the "HP.HPCM.ScepConnector.dll" file to "HP.HPCM.ScepConnector.dll.old".
5. Copy the 3.6.0 dll's to the directory location.
6. Restart the HPSM service.

NOTE: The scep dll's from 3.8 cannot be used with older HPSM versions.

Sectigo SCEP fails when the intermediate CA certificate is in X.509 format while HPSM 3.8 and older is expecting CMS format

Background information:

As per the RFC8894 (SCEP Protocol) two CA formats are supported for the CA configuration.

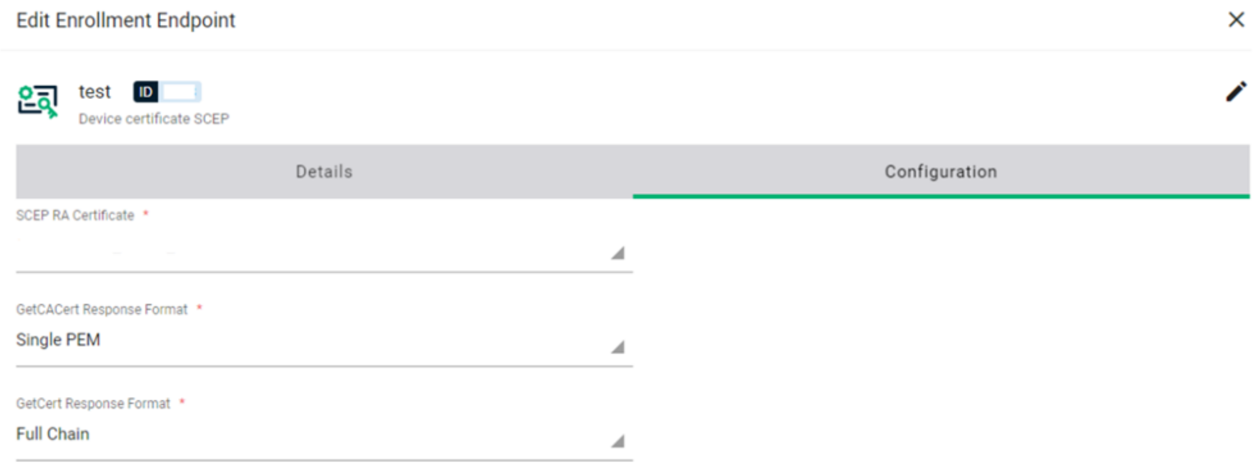
If the CA does not have any intermediate CA certificates, the response consists of a single X.509 CA certificate. The response will have a Content-Type of "application/x-x509-ca-cert".
If the CA has intermediate CA certificates, the response consists of a degenerate certificates-only CMS SignedData message (Section 3.4) containing the certificates, with the intermediate CA certificate(s) as the leaf certificate(s). The response will have a Content-Type of "application/x-x509-ca-ra-cert"
Ref: https://www.rfc-editor.org/rfc/rfc8894.html#section-4.2.1.1
The SCEP operation GetCACert can respond x-x509-ca-cert or x-x509-ca-ra-cert based on their CA design. HPSM 3.8 and older only accepts x-x509-ca-ra-cert, and HPSM 3.9 also handles/accepts x-x509-ca-cert format.

In the SCEP log from 3.7.0 (not visible in 3.8 logs) you can see the CA request:

```
2022-08-24 18:41:54,880 DEBUG Scep [24] - SCEP::SendRequest(): MIME
content type: application/x-x509-ca-cert
```

Workaround for HPSM 3.8 and older by changing the GetCACert Response Format from Sectigo:
Change the Sectigo CA response. This can be done per Sectigo profile to set per SCEP Endpoint the GetCACert Response Format.

Login to SCM and select Enrollment> SCEP
Select the SCEP endpoint that was created, click on the **Edit** button
Select Configuration tab (see screenshot)



Edit Enrollment Endpoint

test ID

Device certificate SCEP

SCEP RA Certificate *

GetCACert Response Format *

Single PEM

GetCert Response Format *

Full Chain

Now you can change GetCACert Response Format from **Single PEM** into **Chain in CMS**
The GetCert Response Format can be changed from **Single Certificate** to **Full Chain**

Solution: Upgrade to HPSM 3.9

Could not retrieve Challenge password from the SCEP Server in Scep.log and questions marks in the logged RESPONSE

Could not retrieve Challenge password from the SCEP Server in Scep.log and questions marks in the logged RESPONSE

In some cases the response from the SCEP server with the SCEP challenge password cannot be decoded by HPSM. In the Scep.log file you can see:

```
2023-09-12 16:59:39,281 DEBUG Scep   [21] - --- BEGIN ndes_admin RESPONSE ---
__??????????????????????=?????????????????????????????????????????????????????
?????????????4????????????????????????????????????????????????4?????????4?????
???????????????/????????????????????4?????????????????????????????????????????
?4????????????????????????????????????????????????????????????????????????????
?????????????????????????????????????????????›????????????????????????????????
????????????????????????????????????????›?????????????????????????????????????
??????`?????????????????????7???????????5????????????????????7????????????????
??????????????????†???????????????????????????????????????????????????????????
?????__--- END ndes_admin RESPONSE ---
2023-09-12 16:59:39,296 DEBUG Scep   [21] - SCEP::GetOneTimePassword():
failed; no regex match
2023-09-12 16:59:39,296 DEBUG Scep   [21] - SCEP : Challenge Password :
2023-09-12 16:59:39,296 ERROR Scep   [21] - SCEP::Enroll(): Could not retrieve
Challenge password from SCEP Server
```

This happens with HPSM 3.10 and older using the default SCEP plugin. The default SCEP plugin cannot handle a UTF-8 SCEP challenge response.
Solution: obtain updated SCEP dll's for HP Security Manager 3.10 or upgrade to at least 3.11 when this version becomes available.

Could not retrieve Challenge password from the SCEP Server in Scep.log and when the challenge password is visible in the SCEP.log

HPSM expects a hexadecimal SCEP challenge password and is checking if the SCEP challenge password contains characters A-F and numerical values 0-9. If this is not the case, then the provided password cannot be used by HPSM and in the scep.log file you will see the error message: Could not retrieve Challenge password from SCEP server.

```
2023-09-13 11:52:13,574 DEBUG Scep   [26] - --- BEGIN ndes_admin RESPONSE ---
__?<HTML><Head><Meta HTTP-Equiv="Content-Type" Content="text/html;
charset=UTF-8"><Title>Network Device Enrollment Service</Title></Head><Body
BgColor=#FFFFFF><Font ID=locPageFont Face="Arial"><Table Border=0
CellSpacing=0 CellPadding=4 Width=100% BgColor=#008080><TR><TD><Font
ID=locPageTitleFont Face="Arial" Size=-1 Color=#FFFFFF><LocID
ID=locMSCertSrv>Network Device Enrollment
Service</LocID></Font></TD></TR></Table><P ID=locPageTitle> Network Device
Enrollment Service allows you to obtain certificates for routers or other
network devices using the Simple Certificate Enrollment Protocol (SCEP).
</P><P> To complete certificate enrollment for your network device you will
need the following information: <P> The thumbprint (hash value) for the CA
certificate is: <B> BAF35B6A FE7855C1 B7BA39E8 5CB180C1 </B> <P> The
enrollment challenge password is: <B> U6IMNIIRMK5V </B> <P> This password can
be used only once and will expire within 45 minutes. <P> Each enrollment
requires a new challenge password. You can refresh this web page to obtain a
new challenge password. </P> <P ID=locPageDesc> For more information see  <A
HREF=http://go.microsoft.com/fwlink/?LinkId=67852>Using Network Device
Enrollment Service </A>. </P> <P></Font></Body></HTML>__--- END ndes_admin
RESPONSE ---
2023-09-13 11:52:13,590 DEBUG Scep   [26] - SCEP::GetOneTimePassword():
failed; no regex match
2023-09-13 11:52:13,590 DEBUG Scep   [26] - SCEP : Challenge Password :
2023-09-13 11:52:13,590 ERROR Scep   [26] - SCEP::Enroll(): Could not retrieve
Challenge password from SCEP Server
```

Solution: change the configuration on the SCEP server to generate Hexadecimall SCEP challenge passwords.

Incorrect Certificate Authority Server or CA server down/unreachable

Check the HPCM.log file in the directory:

C:|Program Files (x86)|HP Security Manager|log

It might have errors like the following:

2020-04-10 12:30:14,536 ERROR HPCM [7] - Error while retreiving Provider: The constructor to deserialize an object of type 'HP.HPCM.Contract.Exception.ServerUnavailableException' was not found.. 2020-04-10 12:30:14,537 ERROR HPCM [7] - Error while Enrolling Certificate for Request 8d680a79-af7b-411e-9ffc-0e4ea9c98da8. Exception : The constructor to deserialize an object of type 'HP.HPCM.Contract.Exception.ServerUnavailableException' was not found. StackTrace : at HP.HPCM.Provider.ProviderHandler.ExecuteEnroll(String providerName, CertificateEnrollData certData) at HP.HPCM.HPCMService.Execute(CertificateEnrollData request)

Check the HPCM.log file in the directory:

C:|Program Files (x86)|HP Security Manager|PkiProviders|log

It might list errors like the following:

```
2020-04-10 12:30:14,508 ERROR HPCM System.Runtime.InteropServices.COMException
(0x800706BA): The RPC server is unavailable. (Exception from HRESULT: 0x800706BA)at
NETcertcli.CCertRequestClass.Submit(Int32 Flags, String strRequest, String strAttributes, String
strConfig)at
HPCMMicrosoftPKI.MicrosoftPKICertificateBase.SubmitCertRequestAndGetCertificate (String
request, String certificateServer, Int32 certFormat, String attribute, String& certificate, Int32&
requestId) at HPCMMicrosoftPKI.MicrosoftPKICertificateBase.GetJetdirectIdentityCertUsingJetdi
rectRequest(String certificateServer, String csr, String templateName, String& signedCertificate,
Int32& requestId, String& certRequest) [7] - The certificate server is unavailable: [2008R2-DC-
TME.wrong\upd-tme2008r2-dc-tme-ca]

This could be because that certificate server name is not a valid computer name, or it cannot be
accessed. 2020-04-14 10:21:32,873 ERROR HPCM [26] - Failure in Connecting to the Certificate
Server, Server UnavailableHP.HPCM.Contract.Exception.ServerUnavailableException: The
certificate server is unavailable: [2008r2-dc-tem\UPD-TME-2008R2-DC-TME.wrong]

This could be because that certificate server name is not a valid computer name, or it cannot be
accessed. ---> System.Runtime.InteropServices.COMException: The RPC server is unavailable.
(Exception from HRESULT: 0x800706BA) at NETcertcli.CCertRequestClass.Submit(Int32 Flags,
String strRequest, String strAttributes, String strConfig) at
HPCMMicrosoftPKI.MicrosoftPKICertificateBase.SubmitCertRequestAndGetCertificate (String
request, String certificateServer, Int32 certFormat, String attribute, String& certificate, Int32&
requestId)at HPCMMicrosoftPKI.MicrosoftPKICertificateBase.GetJetdirectIdentityCertUsingJetdi
rectRequest(String certificateServer, String csr, String templateName, String& signedCertificate,
Int32& requestId, String& certRequest) --- End of inner exception stack trace --- at
HPCMMicrosoftPKI.MicrosoftPKICertificateBase.GetJetdirectIdentityCertUsingJetdi
rectRequest(String certificateServer, String csr, String templateName, String& signedCertificate,
Int32& requestId, String& certRequest) at
HPCMMicrosoftPKI.MicrosoftPKICertificateBase.EnrollCertificate(CertificateEnrol lData
certificateEnrollData, Boolean isMicrosoftSA, CertificateEnrollResult& result)at
HPCMMicrosoftPKI.MicrosoftEnterprisePKI.Enroll(CertificateEnrollData certificateEnrollData) cert
```

Incorrect Certificate Authority Name in policy

Check the HPCM.log in the directory:

C:|Program Files (x86)|HP Security Manager|log

```
2020-04-10 12:11:20,386 ERROR HPCM [5] - Error while retreiving Provider: The constructor to
deserialize an object of type 'HP.HPCM.Contract.Exception.CertificateAuthorityNameException'
was not found.. 2020-04-10 12:11:20,386 ERROR HPCM [5] - Error while Enrolling Certificate for
Request 3b6aac52-4565-449b-a3d2-5b9d4c318bc2. Exception : The constructor to deserialize an
object of type 'HP.HPCM.Contract.Exception.CertificateAuthorityNameException' was not found.
StackTrace : at HP.HPCM.Provider.ProviderHandler.ExecuteEnroll(String providerName,
CertificateEnrollData certData) at HP.HPCM.HPCMService.Execute(CertificateEnrollData request)
```

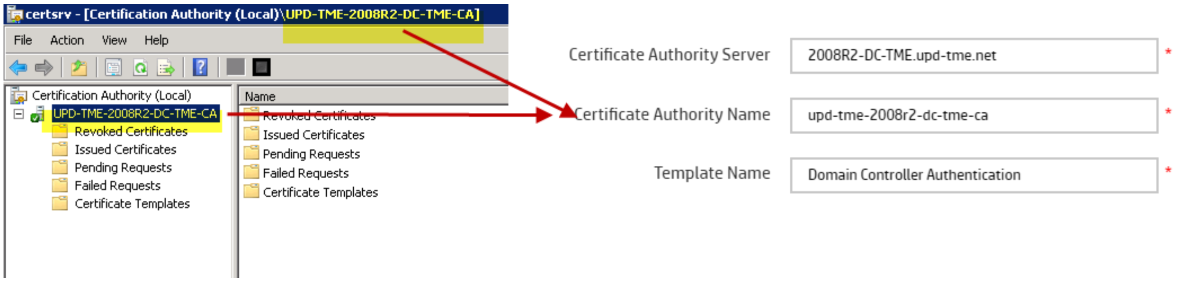
Check the HPCM.log in the directory:

C:|Program Files (x86)|HP Security Manager|PkiProviders|log

It might have errors like the following:

```
2020-04-10 12:46:11,738 ERROR HPCM [5] - Failure in fetching the
CertificateHP.HPCM.Contract.Exception.CertificateAuthorityNameException: The Certificate
Authority part of the certificate server is invalid: [2008R2-DCTME\upd-tme-2008r2-dc-tme-ca] --->
System.ArgumentException: Value does not fall within the expected range. at
NETcertcli.CCertRequestClass.RetrievePending(Int32 RequestId, String strConfig)at
HPCMMicrosoftPKI.MicrosoftPKICertificateBase.CheckPendingCertRequest(Int32 requestId, String
certificateServer, Int32 certFormat, String& certificate)at
HPCMMicrosoftPKI.MicrosoftPKICertificateBase.RetrievePendingCertificateJetdirec tCsr(String
certificateServer, Int32 requestId, String& signedCertificateString) --- End of inner exception stack
trace --- at HPCMMicrosoftPKI.MicrosoftPKICertificateBase.RetrievePendingCertificateJetdirec
tCsr(String certificateServer, Int32 requestId, String& 45 signedCertificateString)at
HPCMMicrosoftPKI.MicrosoftPKICertificateBase.EnrollCertificate(CertificateEnrol lData
certificateEnrollData, Boolean isMicrosoftSA, CertificateEnrollResult& result)at
HPCMMicrosoftPKI.MicrosoftEnterprisePKI.Enroll(CertificateEnrollData certificateEnrollData)
```

NOTE: There are no errors in the file ../WebApp/log?HPCM.log. This error happens when the CA server which is specified in the ID certificate is not valid or when the CA is not available.



Certificate Authority Server: 2008R2-DC-TME.upd-tme.net *

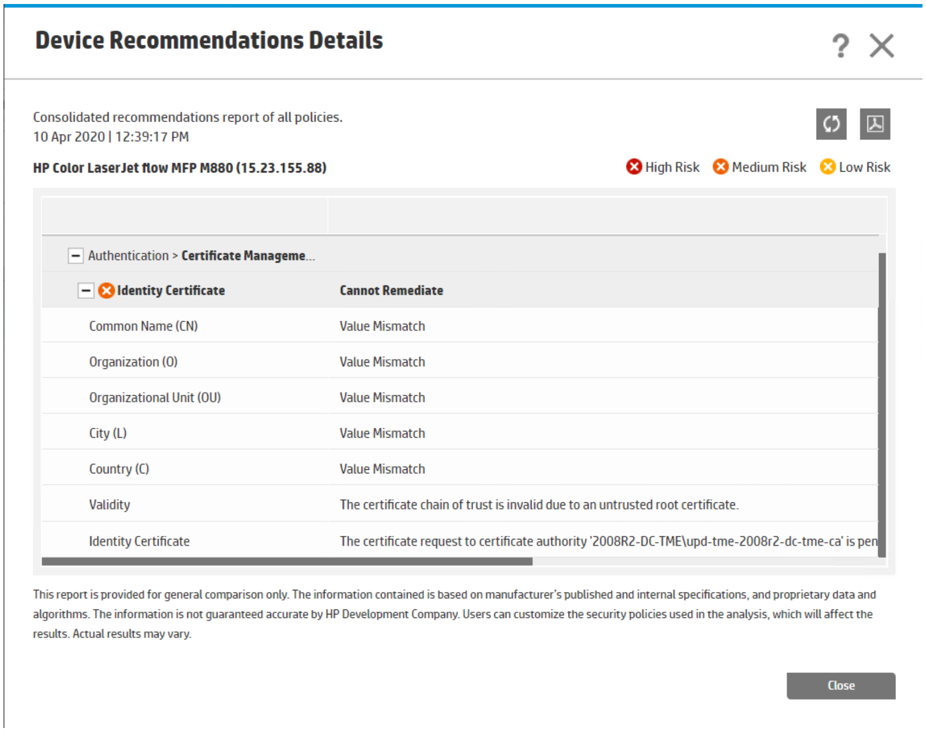
Certificate Authority Name: upd-tme-2008r2-dc-tme-ca *

Template Name: Domain Controller Authentication *

CA server is configured to require manual approval of the request

In some situations, you might see the following error message:

The certificate request to certificate authority 'AuthorityName' is pending.



Device Recommendations Details

Consolidated recommendations report of all policies.
10 Apr 2020 | 12:39:17 PM

HP Color LaserJet flow MFP M880 (15.23.155.88)

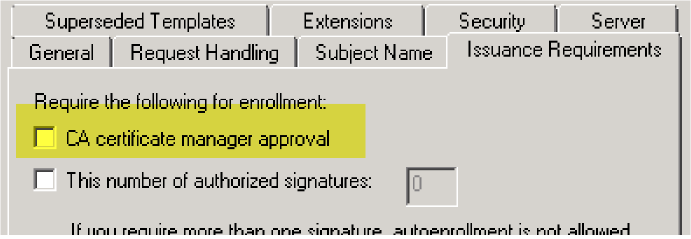
⊗ High Risk ⊗ Medium Risk ⊗ Low Risk

⊟ Authentication > **Certificate Manageme...**	
⊟ ⊗ **Identity Certificate**	**Cannot Remediate**
Common Name (CN)	Value Mismatch
Organization (O)	Value Mismatch
Organizational Unit (OU)	Value Mismatch
City (L)	Value Mismatch
Country (C)	Value Mismatch
Validity	The certificate chain of trust is invalid due to an untrusted root certificate.
Identity Certificate	The certificate request to certificate authority '2008R2-DC-TME\upd-tme-2008r2-dc-tme-ca' is pen

This report is provided for general comparison only. The information contained is based on manufacturer's published and internal specifications, and proprietary data and algorithms. The information is not guaranteed accurate by HP Development Company. Users can customize the security policies used in the analysis, which will affect the results. Actual results may vary.

Figure: Identity Certificate error listed under Device Recommendations

Check on the CA server if the request is listed under Pending Requests and validate that the checkbox for CA certificate manager approval has been deselected for the CA certificate which is used in the policy.



Require the following for enrollment:

□ CA certificate manager approval

□ This number of authorized signatures: 0

If you require more than one signature, autoenrollment is not allowed.

The Template Name in the policy for the certificate template is incorrect

Check the HPCM.log file in the directory:

C:|Program Files (x86)|HP Security Manager|log

Entries like the following might be listed in the log file:

```
2020-04-14 10:30:09,076 DEBUG HPCM [4] - DoEnroll : Request - b7a69e45-c89f-4880-bafe-
5141256a5837 2020-04-14 10:30:10,173 INFO HPCM [4] - ParseCertResponse : PkiProviderName -
MSEnterprise ; Status - Pending ; Request ID - b7a69e45-c89f-4880-bafe-5141256a5837 Check
the HPCM.log file in the directory: C:\Program Files (x86)\HP Security Manager\PkiProviders\log
```

Entries like the following might be listed in the log file:

```
2020-04-14 10:30:09,076 DEBUG HPCM [4] - DoEnroll : Request - b7a69e45-c89f-4880-bafe-
5141256a5837
```

Check the HPSM_service.log file in the directory:

C:|Program Files (x86)|HP Security Manager|PkiProviders|log

Entries like the following might be listed in the log file:

```
2020-04-14 10:30:14,075 DEBUG Service [4] - HPCMEventManager calling callback for Request
ID: b7a69e45-c89f-4880-bafe-5141256a5837
```

Check the HPSM_service.log file in the directory:

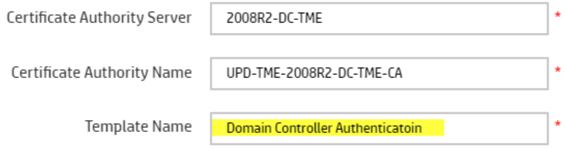
C:|Program Files (x86)|HP Security Manager|PkiProviders|log

Entries like the following might be listed in the log file:

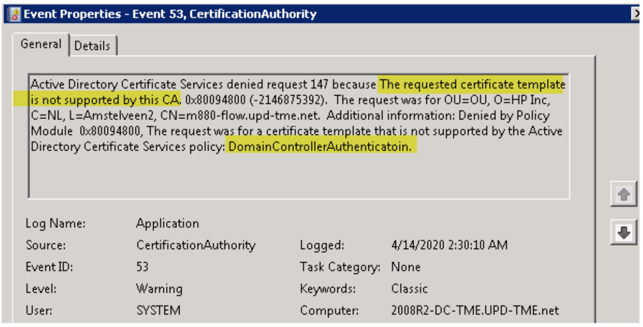
```
2020-04-14 10:30:14,075 DEBUG Service [22] - HPCMMangerResponseManager Dequeue
b7a69e45-c89f-4880-bafe-5141256a5837

2020-04-14 10:30:14,075 DEBUG Service [22] –

HPCMMangerResponseManager Dequeue - b7a69e45-c89f-4880-bafe5141256a5837 Status
is: Pending

2020-04-14 10:30:14,075 DEBUG Service [22] - recommendation state: = SuggestedCannotFix
```

On the CA server, you can find the following Warning in the event viewer event ID 53) or in the Failed Requests list from the CA:

Active Directory Certificate Services denied request 147 because The requested certificate template is not supported by this CA. 0x80094800 (-2146875392). The request was for OU=OU, O=HP Inc, C=NL, L=Amstelveen2, CN=m880-flow.updtme.net. Additional information: Denied by Policy Module 0x80094800, The 47 request was for a certificate template that is not supported by the Active Directory Certificate Services policy: DomainControllerAuthenticatoin.



Certificate Authority Server	2008R2-DC-TME *
Certificate Authority Name	UPD-TME-2008R2-DC-TME-CA *
Template Name	Domain Controller Authenticatoin *



Active Directory Certificate Services denied request 147 because The requested certificate template is not supported by this CA. 0x80094800 (-2146875392). The request was for OU=OU, O=HP Inc, C=NL, L=Amstelveen2, CN=m880-flow.upd-tme.net. Additional information: Denied by Policy Module 0x80094800, The request was for a certificate template that is not supported by the Active Directory Certificate Services policy: DomainControllerAuthenticatoin.

Log Name:	Application		
Source:	CertificationAuthority	Logged:	4/14/2020 2:30:10 AM
Event ID:	53	Task Category:	None
Level:	Warning	Keywords:	Classic
User:	SYSTEM	Computer:	2008R2-DC-TME.UPD-TME.net

In this example, the Template Name had a typo: Authenticatoin instead of Authentication. Comparing log files with a successful enrollment.

When an enrollment is successful you should see in the HPCM.log file:

```
2020-04-14 16:28:45,925 DEBUG HPCM [30] - DoEnroll : Request - 09a561fb-263a4b6e-ac41-
58ad50df812f 2020-04-14 16:28:46,515 INFO HPCM [30] - ParseCertResponse :
PkiProviderName - MSEnterprise ; Status - Success ; Request ID - -58ad50df812f
```

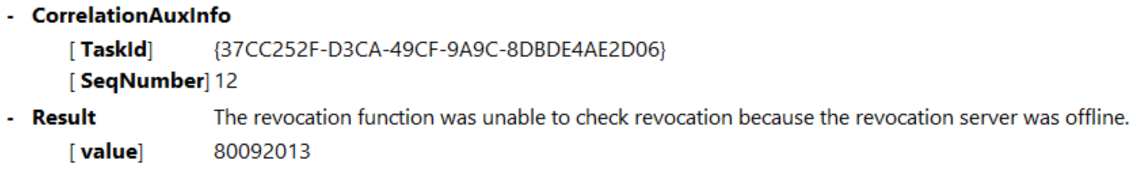
Invalid ID certificate when CRL is unreachable

If the printer does have a valid certificate and HPSM cannot contact obtain the CRL (Certificate Revocation List) from the issuing CA then HPSM will display Invalid Certificate. In the HPSM service log file this will also be visible. Example:

```
2023-09-2808:31:48,956 INFO Service [49] -
AssessmentItemIdentityCert.Assess - Device IP : 10.110.29.19 - Status :
The online certificate revocation list (CRL) that the certificate relies
on is currently offline.
2023-09-2808:32:24,068 INFO Service [57] -
HPCMResponseManager.HandleException- Device IP : 10.110.29.19 - Policy
Item : Certificate Authority - Status : It is not possible to determine
whether the certificate has been revoked. This can be due to the
certificate revocation list (CRL) being offline or unavailable.
```

HPSM is asking the OS if a certificate has been revoked and you will not be able to see in the HPSM_Service.log file which CRL is unreachable.

In the Windows Event Viewer you can also enable CAPI2 logging, which will provide similar information about a unreachable CRL. CAPI2 logging can be enabled in the event viewer under **Applications and Services**, **Microsoft**, **Windows**, **CAPI2**, **Operations** with an **Enable Log** option on the right site.



- **CorrelationAuxInfo**
  - [**TaskId**] {37CC252F-D3CA-49CF-9A9C-8DBDE4AE2D06}
  - [**SeqNumber**] 12
- **Result** The revocation function was unable to check revocation because the revocation server was offline.
  - [**value**] 80092013

In a network trace you will be able to see which CRL is not reachable (for example HTTP 404 Not Found when the CRL is published via http). Verify that all certification authorities in the chain have valid CRLs published. When a Microsoft CA is used, this can be done with certutil.

Open a command prompt with administrator rights and use the following command:

certutil.exe -URL http://URL.crl

where URL.crl is the actual URL of the CRL.

Example:

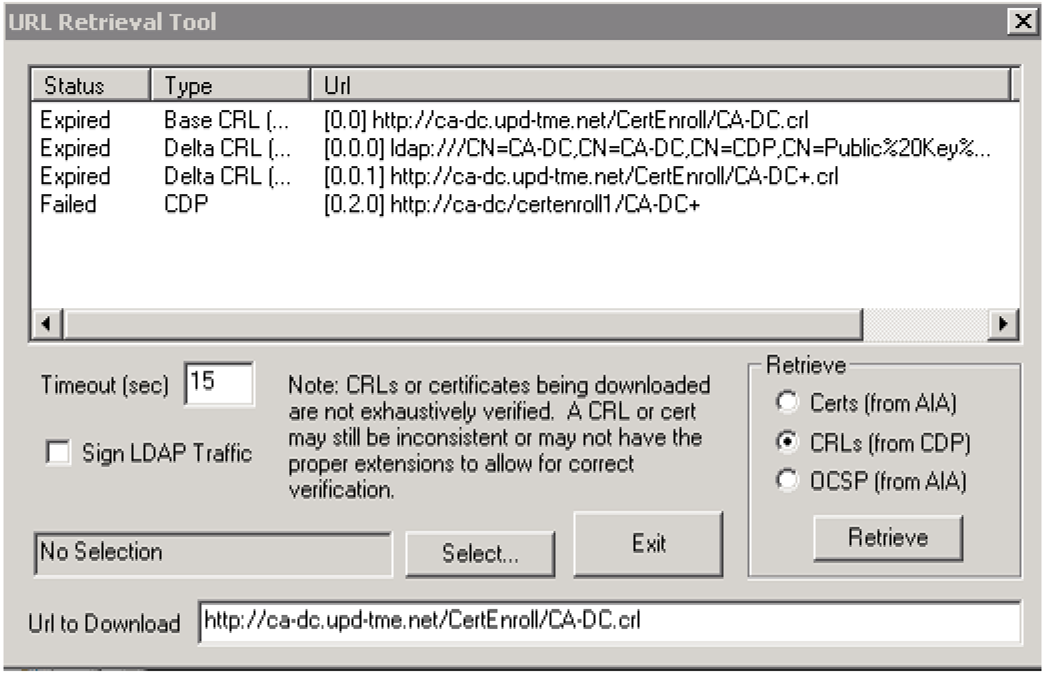
certutil.exe -URL http://ca-dc.upd-tme.net/CertEnroll/CA-DC.crl

This will open the URL Retrieval Tool.

Click **Retrieve** in the URL Retrieval Tool to see the actual status of the CRL’s.

In the following figure you can see that the CDP is not accessible (which means that certificates cannot be validated by HPSM).

Figure: CDP Status is listed as Failed in the URL Retrieval Tool



URL Retrieval Tool

Status	Type	Url
Expired	Base CRL (...	[0.0] http://ca-dc.upd-tme.net/CertEnroll/CA-DC.crl
Expired	Delta CRL (...	[0.0.0] ldap:///CN=CA-DC,CN=CA-DC,CN=CDP,CN=Public%20Key%...
Expired	Delta CRL (...	[0.0.1] http://ca-dc.upd-tme.net/CertEnroll/CA-DC+.crl
Failed	CDP	[0.2.0] http://ca-dc/certenroll1/CA-DC+

Timeout (sec) 15

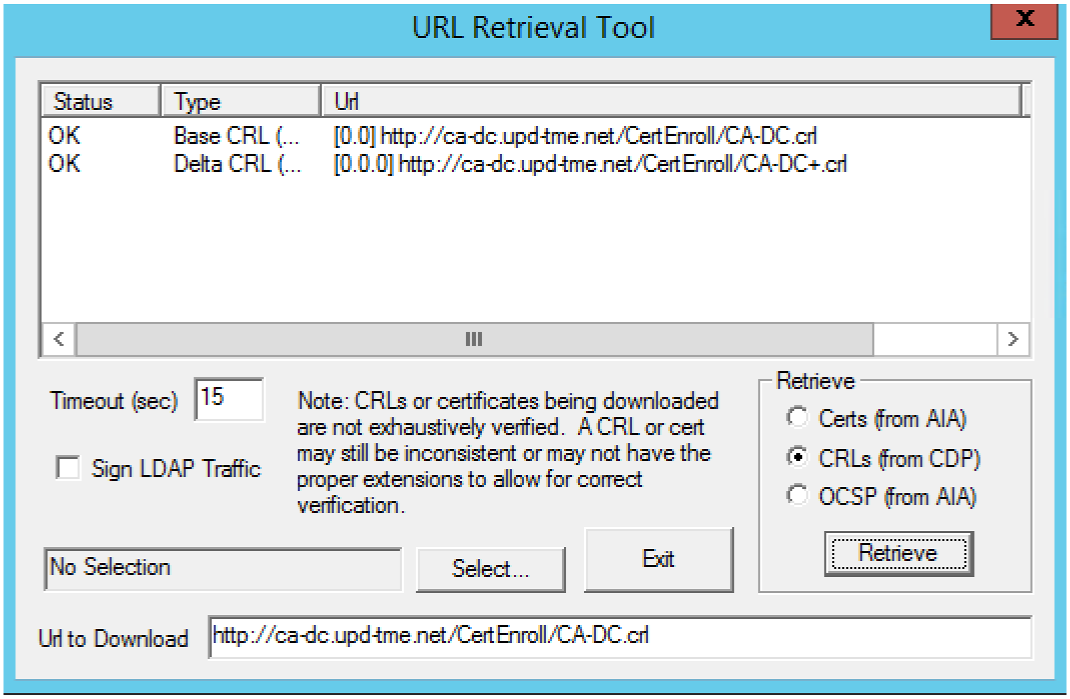
□ Sign LDAP Traffic

Note: CRLs or certificates being downloaded are not exhaustively verified. A CRL or cert may still be inconsistent or may not have the proper extensions to allow for correct verification.

Retrieve
○ Certs (from AIA)
● CRLs (from CDP)
○ OCSP (from AIA)

Url to Download http://ca-dc.upd-tme.net/CertEnroll/CA-DC.crl

When there are no issues with the CRL's, the Status should display as OK:



URL Retrieval Tool

Status	Type	Url
OK	Base CRL (...	[0.0] http://ca-dc.upd-tme.net/CertEnroll/CA-DC.crl
OK	Delta CRL (...	[0.0.0] http://ca-dc.upd-tme.net/CertEnroll/CA-DC+.crl

Timeout (sec) 15

□ Sign LDAP Traffic

Note: CRLs or certificates being downloaded are not exhaustively verified. A CRL or cert may still be inconsistent or may not have the proper extensions to allow for correct verification.

Retrieve
○ Certs (from AIA)
● CRLs (from CDP)
○ OCSP (from AIA)

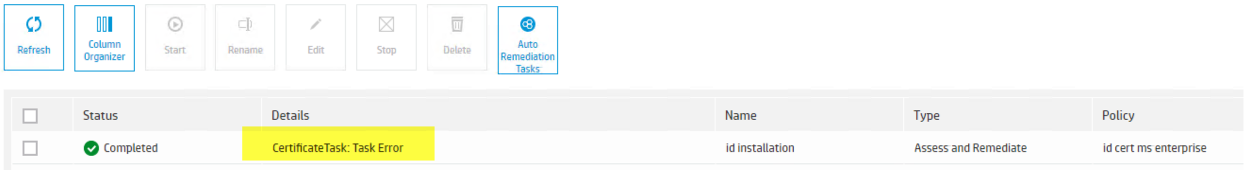
Url to Download http://ca-dc.upd-tme.net/CertEnroll/CA-DC.crl

With the above example the CRL is reachable and accessible with an administrative account. The account running HPSM service must have access to the same information.

CertificateTask: Task Error (HPSM 3.8) when using RSA with SHA1

Signature

Issue: After running a certificate remediation task it's possible that the task ends up with Task Error. See screenshot:



□	Status	Details	Name	Type	Policy
□	✓ Completed	CertificateTask: Task Error	id installation	Assess and Remediate	id cert ms enterprise

Additional information:
In the HPSM_service.log you can find the following error:

```
2022-07-04 15:53:46,162 ERROR Service   [22] - Warning - Truncated DB
string object - TaskBase - ErrorMessage -orginal: Certificate Task:
Task Error: {0}Internal error in processing'SHA1' is not a known hash
algorithm.__Parameter name: hashAlgorithm__Actual value was SHA1.   at
System.Security.Cryptography.X509Certificates.RSAPkcs1X509SignatureGen
erator.GetSignatureAlgorithmIdentifier(HashAlgorithmName
hashAlgorithm)__   at
System.Security.Cryptography.X509Certificates.Pkcs10CertificationReque
stInfo.ToPkcs10Request(X509SignatureGenerator signatureGenerator,
HashAlgorithmName hashAlgorithm)__   at
AssessmentRemediation.HPCMRequest.SubmitRequest(Task task,
Dictionary`2 policyItems, Guid& hpcmRequestId)__   at
AssessmentRemediation.CertificateTask.ExecuteTask()
```

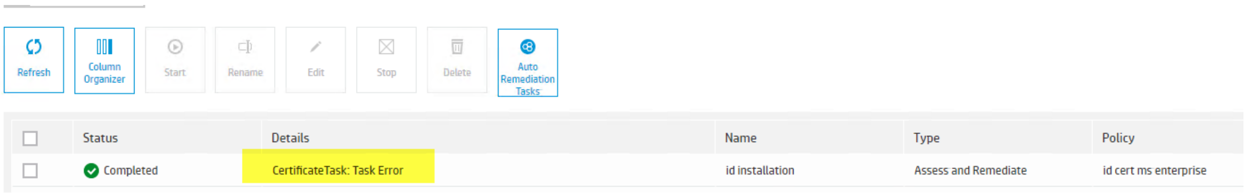
This means that the policy is configured with the **Certificate Request Signature** of SHA-1 and the **Certificate Signing Request (CSR) Source** is set to HPSM.
SHA-1 is weak algorithm and from HPSM 3.8 onwards it's no longer supported when using the CSR as HPSM.

Solution:
Select a stronger signature algorithm in the HPSM policy.

Note: It's possible to change the CSR source to device and still remediate the ID certificate, but this removes the option to add SAN information in the request and the usage of weak algorithm is not recommended.

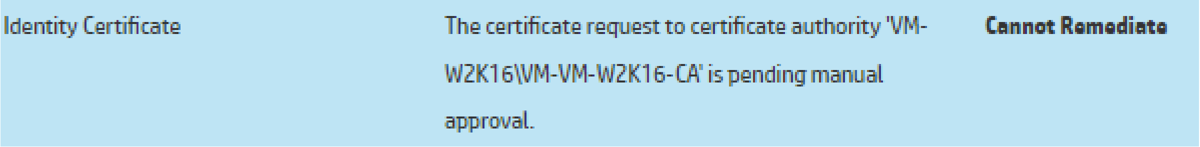
CertificateTask: Task Error (HPSM 3.8) when using ECDSA with Key Length P-256

Issue: After running a certificate remediation task it's possible that the task ends up with Task Error. See screenshot:



□	Status	Details	Name	Type	Policy
□	✓ Completed	CertificateTask: Task Error	id installation	Assess and Remediate	id cert ms enterprise

When you click on the device to look at the remediation details you can see that it looks like the certificate is pending manual approval:



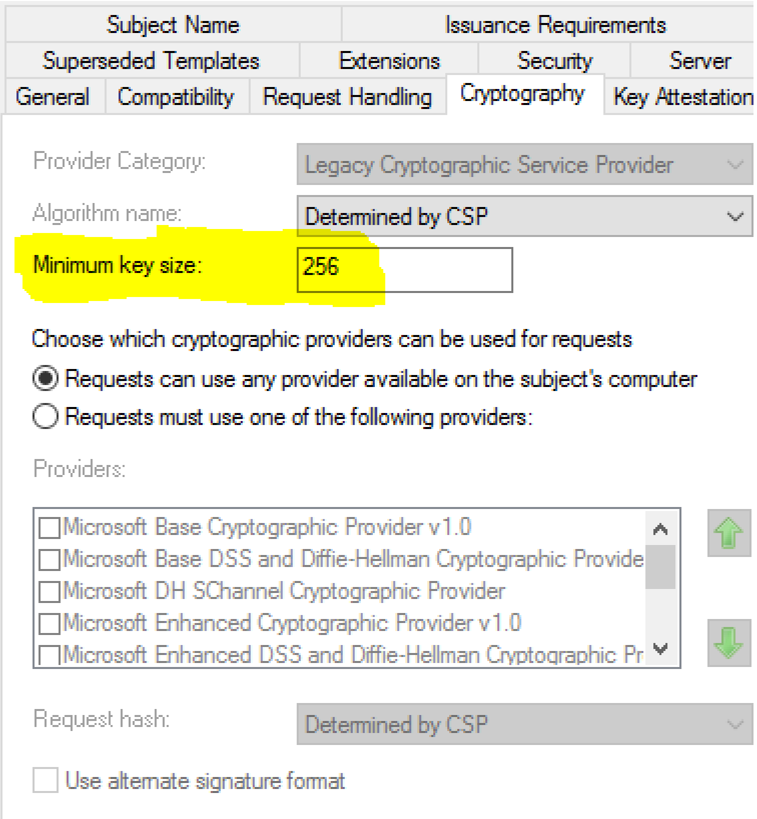
Identity Certificate	The certificate request to certificate authority 'VM-W2K16\VM-VM-W2K16-CA' is pending manual approval.	**Cannot Remediate**

On the CA server the certificate is in the Failed Requests with the following error message: "Active Directory Certificate Services denied request 143 because the public key does not meet the minimum size required by the specified certificate template. 0x80094811 (-2146875375 CERTSRV_E_KEY_LENGTH). The request was for CN=10.23.155.80, OU=ATS-EMEA, O=HP Inc, L=Amstelveen, S=NH, C=NL. Additional information: Denied by Policy Module"

Additional information:
This can occur when the policy in HPSM has been configured with the ECDSA Encryption Key and a Key Length of P-256, while the ID template on the CA server is set to a higher minimum encryption.

Solution:
The ID certificate template which is used needs to be configured with a minimum key length of 256.
Go to the CA server
Right click on **Certificate Templates** and select **Manage.**
Double click on the template which is used in the HPSM policy
Select the tab **Cryptography**
Set the **Minimum key size** to 256.

See screenshot below of a Windows 2016 Enterprise CA server. Note, the Cryptographic settings might have slightly different options depending on the actual OS version.



Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 256

Choose which cryptographic providers can be used for requests

● Requests can use any provider available on the subject's computer

○ Requests must use one of the following providers:

Providers:

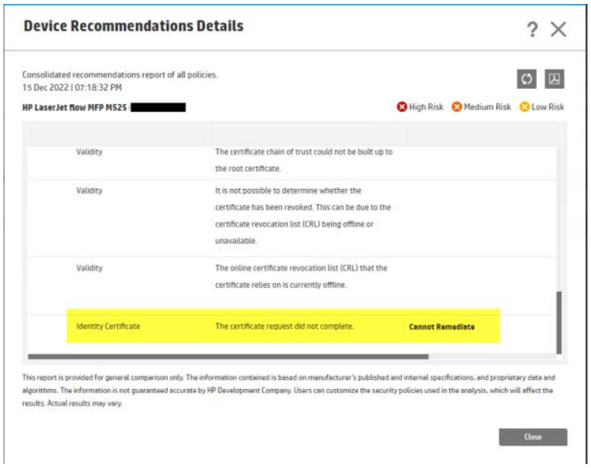
□ Microsoft Base Cryptographic Provider v1.0
□ Microsoft Base DSS and Diffie-Hellman Cryptographic Provide
□ Microsoft DH SChannel Cryptographic Provider
□ Microsoft Enhanced Cryptographic Provider v1.0
□ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr

Request hash: Determined by CSP

□ Use alternate signature format

HPSM fails to install ID certificate (Cannot Remediate) and access denied in logs, while ID certificate did get issued by CA server

HPSM can display Medium risk for ID certificate remediation and Cannot Remediate in the device recommendations screen. In some cases the status might even change into: “Unable to communicate” with the Device.



Consolidated recommendations report of all policies.
15 Dec 2022 | 07:18:32 PM

HP LaserJet flow MFP M525 [redacted]

Validity	The certificate chain of trust could not be built up to the root certificate.	
Validity	It is not possible to determine whether the certificate has been revoked. This can be due to the certificate revocation list (CRL) being offline or unavailable.	
Validity	The online certificate revocation list (CRL) that the certificate relies on is currently offline.	
Identity Certificate	The certificate request did not complete.	Cannot Remediate

This report is provided for general comparison only. The information contained is based on manufacturer's published and internal specifications, and proprietary data and algorithms. The information is not guaranteed accurate by HP Development Company. Users can customize the security policies used in the analysis, which will affect the results. Actual results may vary.

This might mean that HPSM was able to retrieve an ID certificate from a CA but HPSM was unable to install the certificate on the device.

Enable debug mode and check the EAPDeviceLib.log. An error and debug statement like the following might be listed:

```
2020-04-01 09:04:14,007 DEBUG Pipeline [36] -
uid=_95c5978c54dd_10.133.227.46, Exception while converting
certificate to X509Certificate Access denied.
2020-04-01 09:04:14,007 ERROR Pipeline [36] -
uid=_95c5978c54dd_10.133.227.46, Pipeline execution halted due to
step failure, address=10.133.227.46, failed
step=PipelineStepGetCertificateKeyLength, failed
transform=InstallIDCert, failed with step
```

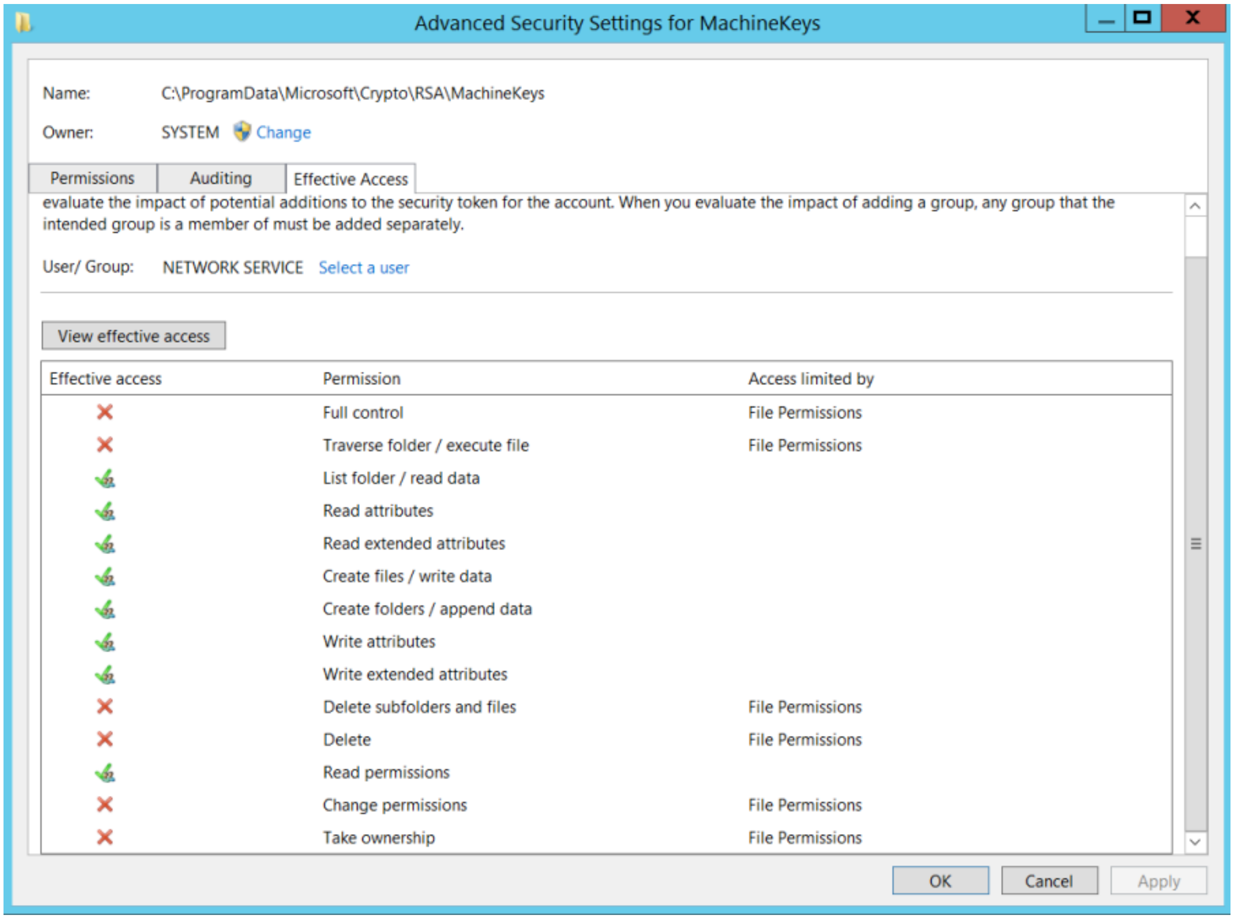
The HPCM.log file might have a similar error:

```
2022-12-15 00:21:19,472 ERROR Service   [21] -
HPCMMangerResponseManager.ProcessAsyncHPCMResponse - Unexpected
exception: System.Security.Cryptography.CryptographicException: Access
is denied.____   at
System.Security.Cryptography.CryptographicException.ThrowCryptographicE
xception(Int32 hr)__   at
System.Security.Cryptography.Utils._GenerateKey(SafeProvHandle hProv,
Int32 algid, CspProviderFlags flags, Int32 keySize, SafeKeyHandle&
hKey)__   at
System.Security.Cryptography.Utils.GetKeyPairHelper(CspAlgorithmType
keyType, CspParameters parameters, Boolean randomKeyContainer, Int32
dwKeySize, SafeProvHandle& safeProvHandle, SafeKeyHandle&
safeKeyHandle)__   at
System.Security.Cryptography.RSACryptoServiceProvider.GetKeyPair()__
at System.Security.Cryptography.RSACryptoServiceProvider..ctor(Int32
dwKeySize, CspParameters parameters, Boolean useDefaultKeySize)__   at
CertificateServices.CertificateUtil.CopyPrivateKey(X509Certificate2
cert, AsymmetricAlgorithm PrivateKey, String Password)__   at
AssessmentRemediation.HPCMResponseManager.ProcessHPCMResponse(Task
task, HPCMResultEventArgs hpcmResultEventArgs)__   at
AssessmentRemediation.HPCMResponseManager.ProcessAsyncHPCMResponse(Task
task, Guid HPCMRequestId)
```

If these messages are displayed in the log, then HPSM is missing READ access for the following directory:

C:|ProgramData|Microsoft|Crypto|RSA|MachineKeys

Provide at least READ access to NT Authority\System (if HP Security Manager service is running as network service).



Name: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys

Owner: SYSTEM

evaluate the impact of potential additions to the security token for the account. When you evaluate the impact of adding a group, any group that the intended group is a member of must be added separately.

User/ Group: NETWORK SERVICE

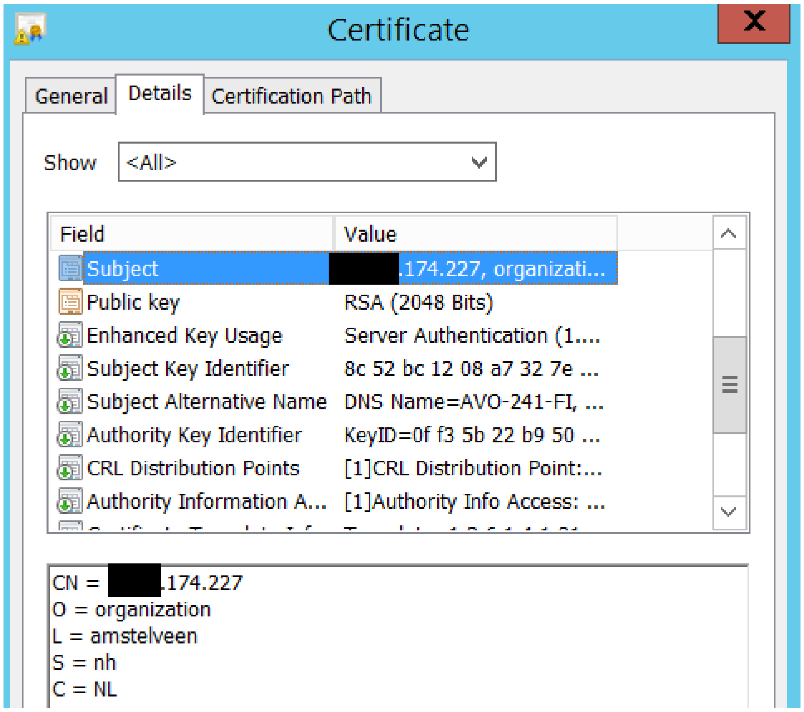
Effective access	Permission	Access limited by
✗	Full control	File Permissions
✗	Traverse folder / execute file	File Permissions
✓	List folder / read data	
✓	Read attributes	
✓	Read extended attributes	
✓	Create files / write data	
✓	Create folders / append data	
✓	Write attributes	
✓	Write extended attributes	
✗	Delete subfolders and files	File Permissions
✗	Delete	File Permissions
✓	Read permissions	
✗	Change permissions	File Permissions
✗	Take ownership	File Permissions

After making the changes, re-run the task.

CN value lists the IP address of the printer instead of the DNS name

Normally, the CN value contains the hostname of the device, but sometimes the IP address is listed in the certificate and the Issued To field.

Figure: Example of IP address listed

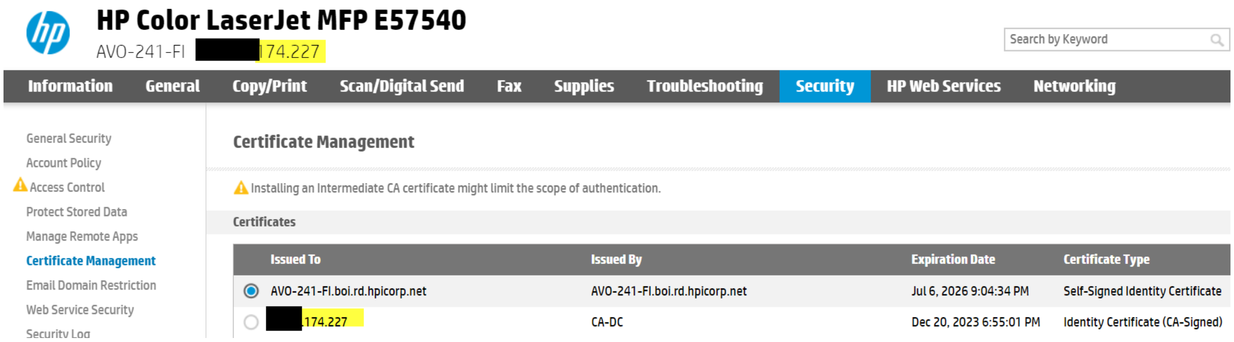


Show <All>

Field	Value
Subject	[redacted].174.227, organizati...
Public key	RSA (2048 Bits)
Enhanced Key Usage	Server Authentication (1....
Subject Key Identifier	8c 52 bc 12 08 a7 32 7e ...
Subject Alternative Name	DNS Name=AVO-241-FI, ...
Authority Key Identifier	KeyID=0f f3 5b 22 b9 50 ...
CRL Distribution Points	[1]CRL Distribution Point:...
Authority Information A...	[1]Authority Info Access: ...

CN = [redacted].174.227
O = organization
L = amstelveen
S = nh
C = NL

In the EWS, the IP address is also listed in the **Issued To** field.



Certificate Management

⚠ Installing an Intermediate CA certificate might limit the scope of authentication.

Certificates

	Issued To	Issued By	Expiration Date	Certificate Type
●	AVO-241-FI.boi.rd.hpicorp.net	AVO-241-FI.boi.rd.hpicorp.net	Jul 6, 2026 9:04:34 PM	Self-Signed Identity Certificate
○	[redacted]174.227	CA-DC	Dec 20, 2023 6:55:01 PM	Identity Certificate (CA-Signed)

This happens when the IP address of the printer cannot be resolved. For printers in remote subnets HPSM is relying on the correct DNS entries for the device. For printers in local subnets (same subnet as HPSM), alternative resolution method can be used as well.

To fix this problem, the correct DNS (forward and reverse lookup) entries for the printer must be created on the DNS server. After this has been setup correctly, the printer needs to be assessed and remediated with the ID certificate policy.

Certificate Installation Failures with Zebra devices

The precious section with Certificate Installation Failures is also applicable to Zebra devices. For certificate management with Zebra device LinkOS 6.2 or higher is required.

HPSM can only install certificates on Zebra devices, it cannot assess the installed certificates. HPSM will still try to retrieve details such as CertCAExpiryDate, CertCASerialNumber. This will fail and in the EAP log file you will always see errors like the following:

```
2021-05-31 22:32:40,206 ERROR Pipeline [17]  - uid=_26e8b1343ca1_10.10.10.15, Pipeline execution
halted due to step failure, address=10.10.10.15, failed step=PipelineStepSetError, failed
```

transform=ReturnNotAvailable, failed with step result=

These errors do not impact the CertDeviceCA and CerDeviceIdentity operations to install (CA and ID) certificates.

As it is only possible to install one ID certificate and one CA certificate on Zebra devices, there is a special workflow for those devices in HPSM. It's not possible to see remotely or in the EWS which ID certificate or CA certificate has been installed. That is also the reason that HPSM can only remediate ID and CA certificates on these devices. You can only check in the EWS if a CA or ID certificate has been installed.

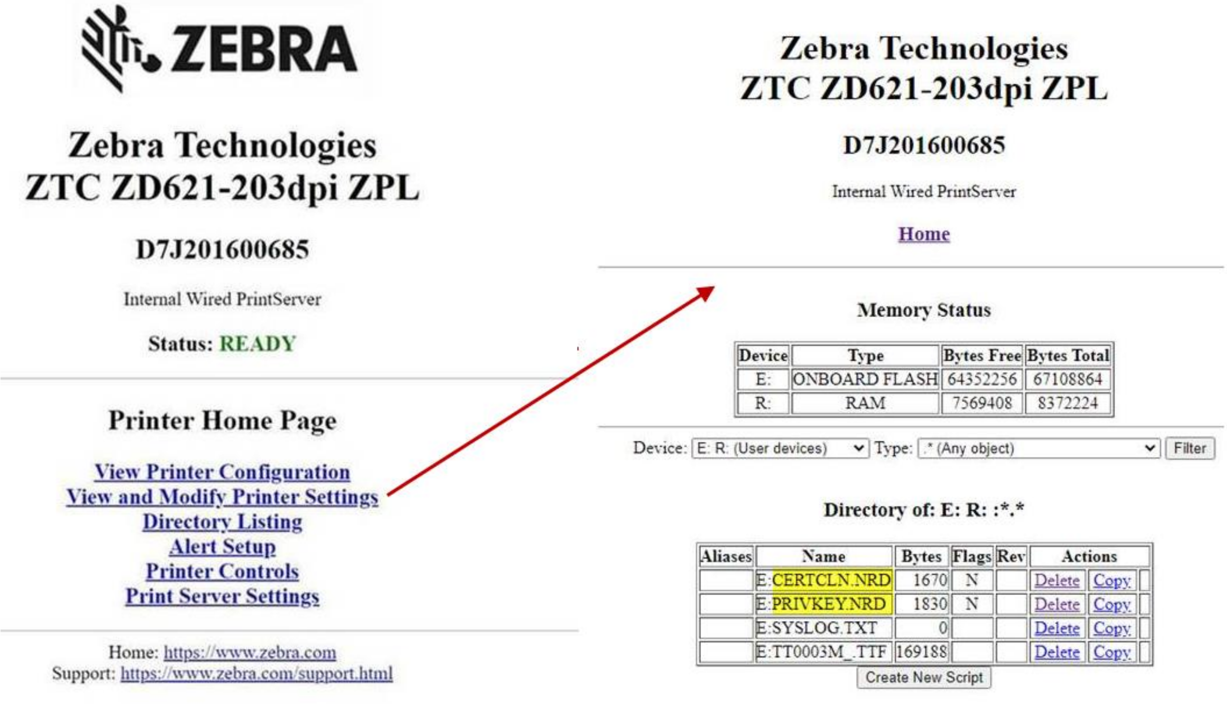
Therefore, HPSM performs the following simplified steps for installing a certificate on a Zebra device during the ID/CA remediation process.

- HPSM removes the certificate from the Zebra device. This means removing the PRIVKEY.NRD, CERTCLN.NRD for ID certificate installation and removing the CACERTSV.NRD for CA certificate installation.
- HPSM installs the certificate on the Zebra device
- HPSM checks if the certificate has been installed correctly on the Zebra device. This means checking if the files PRIVKEY.NRD, CERTCLN.NRD are present for an ID certificate and the file CACERTSV.NRD should be present after a CA certificate installation.

In the EAPDeviceLib.log file you can follow the steps for when debug logging is enabled.

In the EWS of a Zebra device you can also see the certificate files. Open the EWS of the device and select **Directory Listing.** If an ID and/or CA certificate is installed, you should now see the corresponding NRD files.

Figure: NRD files listed



ZEBRA

Zebra Technologies
ZTC ZD621-203dpi ZPL

D7J201600685

Internal Wired PrintServer

Status: READY

Printer Home Page

View Printer Configuration
View and Modify Printer Settings
Directory Listing
Alert Setup
Printer Controls
Print Server Settings

Home: https://www.zebra.com
Support: https://www.zebra.com/support.html

Zebra Technologies
ZTC ZD621-203dpi ZPL

D7J201600685

Internal Wired PrintServer

Home

Memory Status

Device	Type	Bytes Free	Bytes Total
E:	ONBOARD FLASH	64352256	67108864
R:	RAM	7569408	8372224

Device: E: R: (User devices) Type: .* (Any object) Filter

Directory of: E: R: :*.*

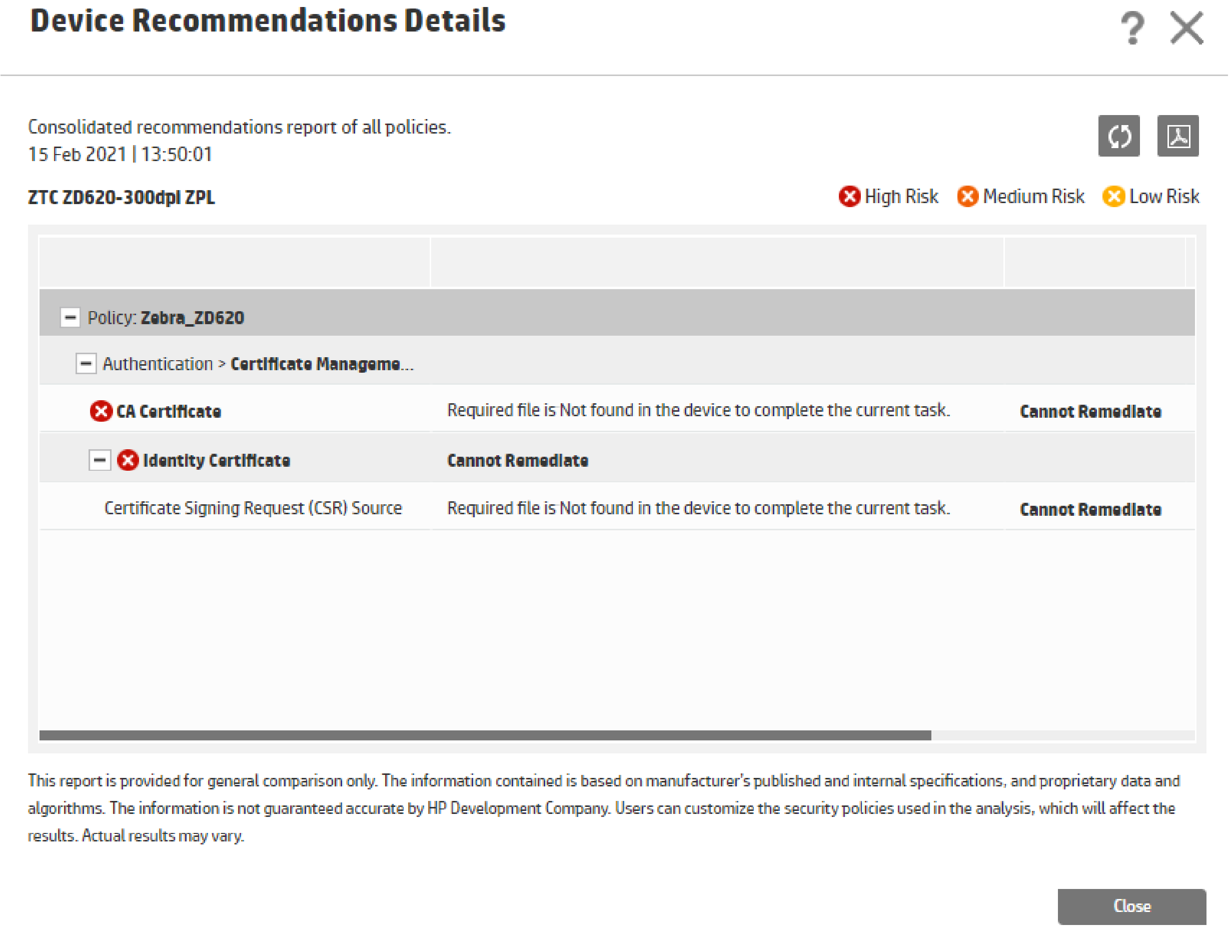
Aliases	Name	Bytes	Flags	Rev	Actions		
	E:CERTCLN.NRD	1670	N		Delete	Copy	
	E:PRIVKEY.NRD	1830	N		Delete	Copy	
	E:SYSLOG.TXT	0			Delete	Copy	
	E:TT0003M_.TTF	169188			Delete	Copy	

Create New Script

If you cannot **Delete** the certificate files via the EWS, then most likely HPSM will not be able to delete those files either. See also step 4 under Resolving Zebra Device Issues.

Cannot Remediate (Required file is not found in the device)

A **Cannot Remediate** error such as **Required file is not found in the device to complete the current task** is received.



Device Recommendations Details

Consolidated recommendations report of all policies.
15 Feb 2021 | 13:50:01

ZTC ZD620-300dpi ZPL

✖ High Risk ✖ Medium Risk ✖ Low Risk

− Policy: **Zebra_ZD620**		
− Authentication > **Certificate Manageme...**		
✖ **CA Certificate**	Required file is Not found in the device to complete the current task.	**Cannot Remediate**
− ✖ **Identity Certificate**	**Cannot Remediate**	
Certificate Signing Request (CSR) Source	Required file is Not found in the device to complete the current task.	**Cannot Remediate**

This report is provided for general comparison only. The information contained is based on manufacturer's published and internal specifications, and proprietary data and algorithms. The information is not guaranteed accurate by HP Development Company. Users can customize the security policies used in the analysis, which will affect the results. Actual results may vary.

With debug logging enabled for the EAP* files, you will see more details in the EAPDeviceLib.log file.
Most likely you will find the following error message after the upload of the certificate has been completed:

```
2021-02-15 16:22:27,319 INFO  Pipeline [3]  - uid=_6de01642251b_10.129.255.170, Completed Upload Certificate. Reset Network
2021-02-15 16:22:27,334 INFO  Pipeline [3]  - uid=_6de01642251b_10.129.255.170, Delaying 35000 millis
2021-02-15 16:23:02,338 INFO  Pipeline [3]  - uid=_6de01642251b_10.129.255.170, Verifying  PRIVKEY.NRD
2021-02-15 16:23:02,338 INFO  Pipeline [3]  - uid=_6de01642251b_10.129.255.170, Verify installed files
2021-02-15 16:23:02,338 INFO  Pipeline [3]  - uid=_6de01642251b_10.129.255.170, Connecting to Printer
2021-02-15 16:23:02,338 INFO  Pipeline [3]  - uid=_6de01642251b_10.129.255.170, Connection Opened. List Files
2021-02-15 16:23:07,370 ERROR Pipeline [3]  - uid=_6de01642251b_10.129.255.170, Error while listing files: No files found.
```

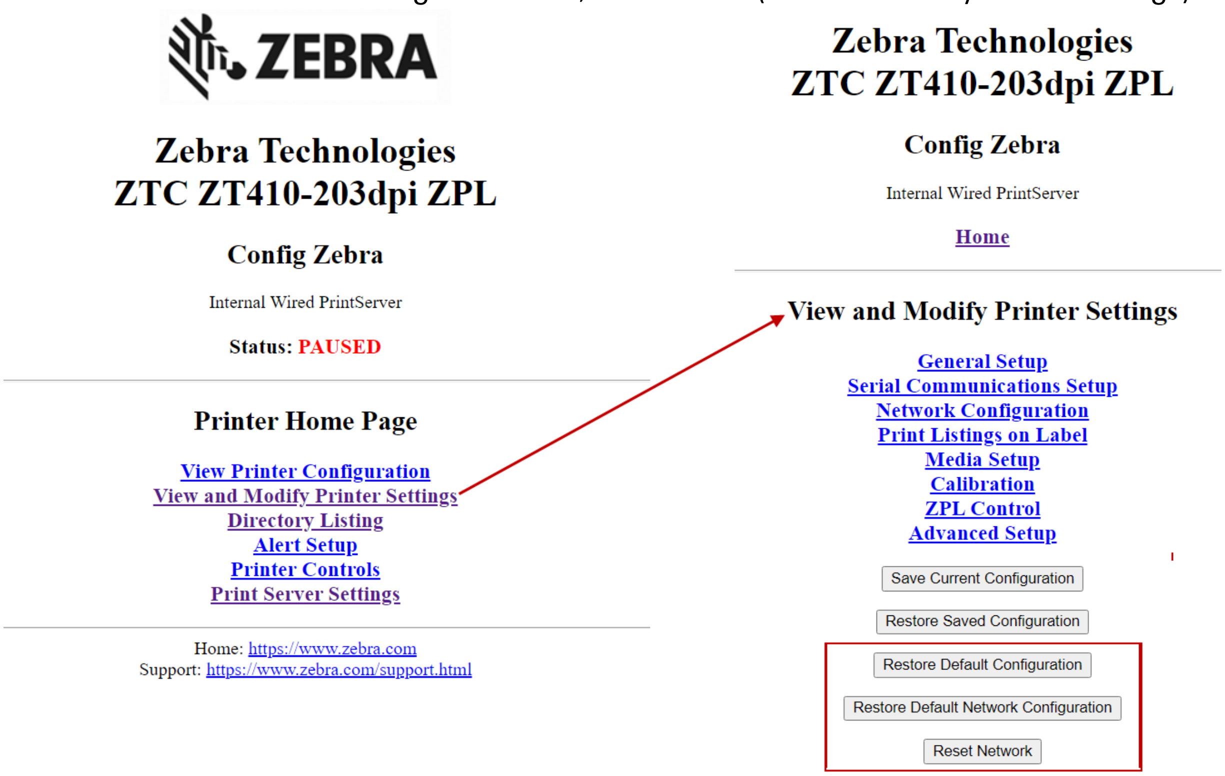
This means that HPSM was able to upload the certificate to the device, but for an unknown reason the certificate was not installed on the device.

Resolving Zebra device certificate issues

The following options can be tried to resolve this device specific issue:

1. Reset the printer to default conditions. To do this, use one of the following two methods:
   - The printer control panel. For instructions, go to Zebra support: https://supportcommunity.zebra.com/s/article/Defaulting-the-ZT400-and-ZT600-Printer-with-color-touch-panel-to-Factory-Settings?language=en_US, OR
   - The Embedded Web Server (EWS) under View and Modify Printer Settings.

2. Reset the network settings. To do this, use the EWS (View and Modify Printer Settings).



Zebra Technologies
ZTC ZT410-203dpi ZPL

Config Zebra

Internal Wired PrintServer

Status: PAUSED

Printer Home Page

View Printer Configuration
View and Modify Printer Settings
Directory Listing
Alert Setup
Printer Controls
Print Server Settings

Home: https://www.zebra.com
Support: https://www.zebra.com/support.html

Zebra Technologies
ZTC ZT410-203dpi ZPL

Config Zebra

Internal Wired PrintServer

View and Modify Printer Settings

General Setup
Serial Communications Setup
Network Configuration
Print Listings on Label
Media Setup
Calibration
ZPL Control
Advanced Setup
Save Current Configuration
Restore Saved Configuration
Restore Default Configuration
Restore Default Network Configuration
Reset Network

3. Update the firmware to Link-OS 6.3 or newer, or reinstall current firmware in the printer.

4. Remove old certificates manually, if HP SM cannot remove them or if this cannot be removed via the EWS use the Zebra Setup Utilities, go to Zebra support: https://www.zebra.com/us/en/support-downloads/printer-software/printer-setup-utilities.html.

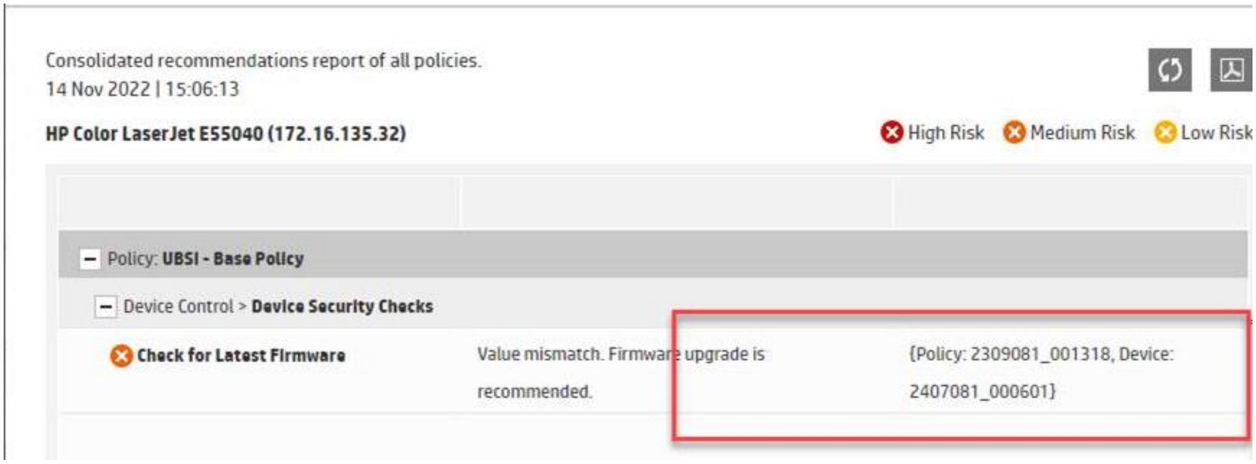
5. If steps 1-4 do not solve the issue, provide an "allcv" report of the printer to check the printer settings.
6. After completing this step, send this information as a TXT file to Zebra support so Zebra can examine that information further.
   Go to Zebra support: https://www.zebra.com/us/en/support-downloads/knowledge-articles/printer-fails-to-respond-to-allcv-or-other-lengthy-data-request-using-the-zsu.html.

Miscellaneous

HPSM is recommending a firmware downgrade after a firmware

assessment of the HP Color LaserJet E55040

ISSUE: After performing a firmware assessment of the HP Color LaserJet E55040 HPSM is recommending a firmware downgrade instead of a firmware upgrade. The next screenshot shows an example of this.



Consolidated recommendations report of all policies.
14 Nov 2022 | 15:06:13

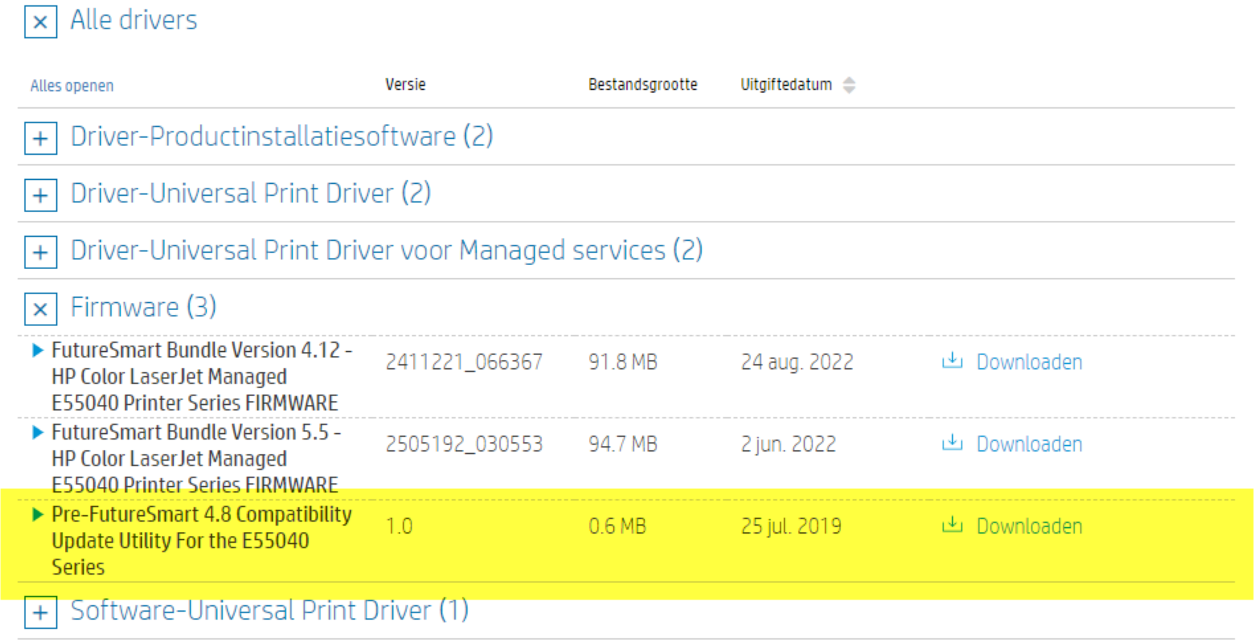
HP Color LaserJet E55040 (172.16.135.32)

− Policy: **UBSI - Base Policy**

− Device Control > **Device Security Checks**

Check for Latest Firmware	Value mismatch. Firmware upgrade is recommended.	{Policy: 2309081_001318, Device: 2407081_000601}

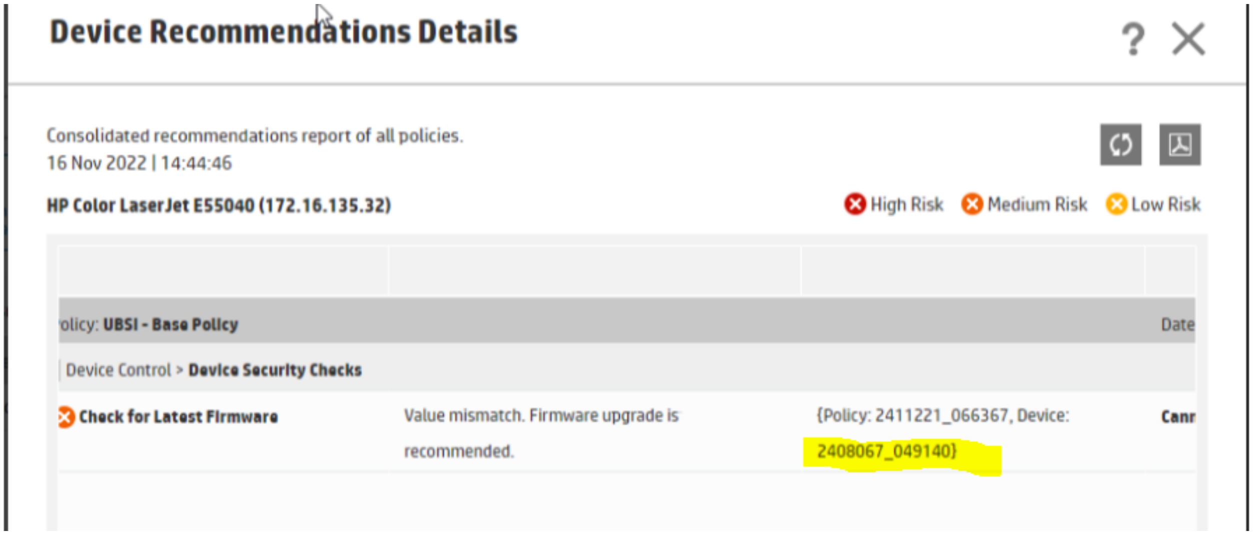
SOLUTION: Run the Pre-Futuresmart 4.8 Compatibility Update Utility for the E55040 Series. This can be found on the support pages for this model on hp.com.



☒ Alle drivers

Alles openen	Versie	Bestandsgrootte	Uitgiftedatum	
⊞ Driver-Productinstallatiesoftware (2)				
⊞ Driver-Universal Print Driver (2)				
⊞ Driver-Universal Print Driver voor Managed services (2)				
☒ Firmware (3)				
▶ FutureSmart Bundle Version 4.12 - HP Color LaserJet Managed E55040 Printer Series FIRMWARE	2411221_066367	91.8 MB	24 aug. 2022	Downloaden
▶ FutureSmart Bundle Version 5.5 - HP Color LaserJet Managed E55040 Printer Series FIRMWARE	2505192_030553	94.7 MB	2 jun. 2022	Downloaden
▶ Pre-FutureSmart 4.8 Compatibility Update Utility For the E55040 Series	1.0	0.6 MB	25 jul. 2019	Downloaden
⊞ Software-Universal Print Driver (1)				

A new assessment after running this utility will now show the expected results:



Device Recommendations Details

Consolidated recommendations report of all policies.
16 Nov 2022 | 14:44:46

HP Color LaserJet E55040 (172.16.135.32)

'olicy: **UBSI - Base Policy** Date

Device Control > **Device Security Checks**

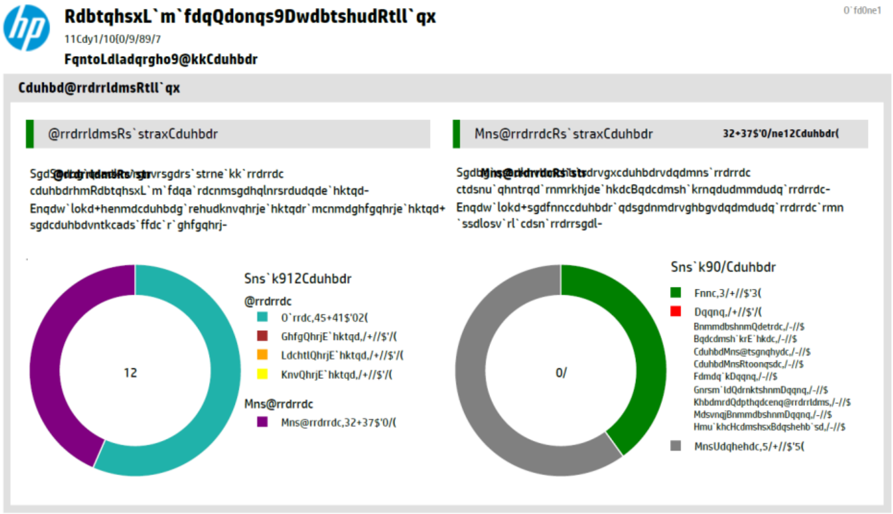
Check for Latest Firmware	Value mismatch. Firmware upgrade is recommended.	{Policy: 2411221_066367, Device: 2408067_049140}	**Canr**

Background information: Before running this firmware compatibility utility HP, the device was identified by HPSM as a device which could use the same firmware as the HP Color LaserJet M552.

Exported Reports Are Showing Garbage/Unreadable Text

In rare cases it is possible that the exported HPSM reports (delivered via email) are unreadable.

Figure: Exported HPSM reports are unreadable



RdbtqhsxL`m`fdqQdonqs9DwdbtshudRtll`qx
11Cdy1/10{0/9/89/7
FqntoLdladqrgho9@kkCduhbdr

0`fd0ne1

Cduhbd@rrdrrldmsRtll`qx

@rrdrrldmsRs`straxCduhbdr

Sgd@rdrrldmsRs`strvrsgdrs`strne`kk`rrdrrdc cduhbdrhmRdbtqhsxL`m`fdqa`rdcnmsgdhqlnrsrdudqde`hktqd- Enqdw`lokd+henmdcduhbdg`rehudknvqhrje`hktqdr`mcnmdghfgqhrje`hktqd+ sgdcduhbdvntkcads`ffdc`r`ghfgqhrj-

Mns@rrdrrdcRs`straxCduhbdr **32+37$'0/ne12Cduhbdr(**

SgdMns@rrdrrdcRs`stsdrvgxcduhbdrvdqdmns`rrdrrdc ctdsnu`qhntrqd`rnmrkhjde`hkdcBqdcdmsh`krnqdudmmdudq`rrdrrdc- Enqdw`lokd+sgdfnnccduhbdr`qdsgdnmdrvghbgvdqdmdudq`rrdrrdc`rmn `ssdlosv`rl`cdsn`rrdrrsgdl-

When the same report is generated in the HPSM UI, the report is displayed correctly.

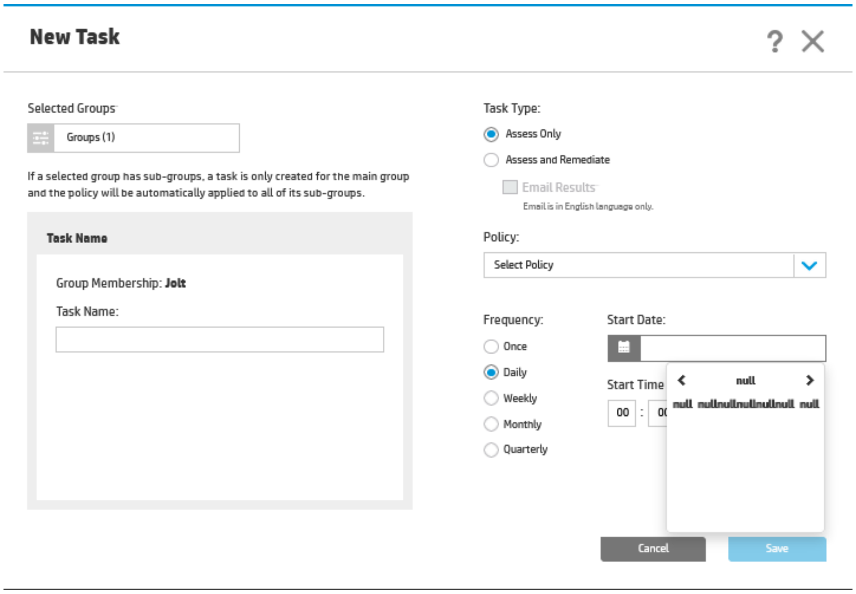
This issue can be resolved by (re)installing the fonts which are shipped with HPSM. The fonts are in the following location:

C:|Program Files (x86)|HP Security Manager|Resources|fonts

Double click on the font and then click the **Install** button, or right-click the Font and select **Install**.

Unable to select a date when creating a task (null visible)

Issue:
When you try to create a task you might be unable to select a date as the calender is not displayed correctly. Instead the word null is displayed multiple times.
See screenshot:



New Task

Selected Groups

Groups (1)

If a selected group has sub-groups, a task is only created for the main group and the policy will be automatically applied to all of its sub-groups.

Task Name

Group Membership: **Jolt**

Task Name:

Task Type:

● Assess Only

○ Assess and Remediate

□ Email Results

Email is in English language only.

Policy:

Select Policy

Frequency:

○ Once

● Daily

○ Weekly

○ Monthly

○ Quarterly

Start Date:

Start Time

00 : 00

null

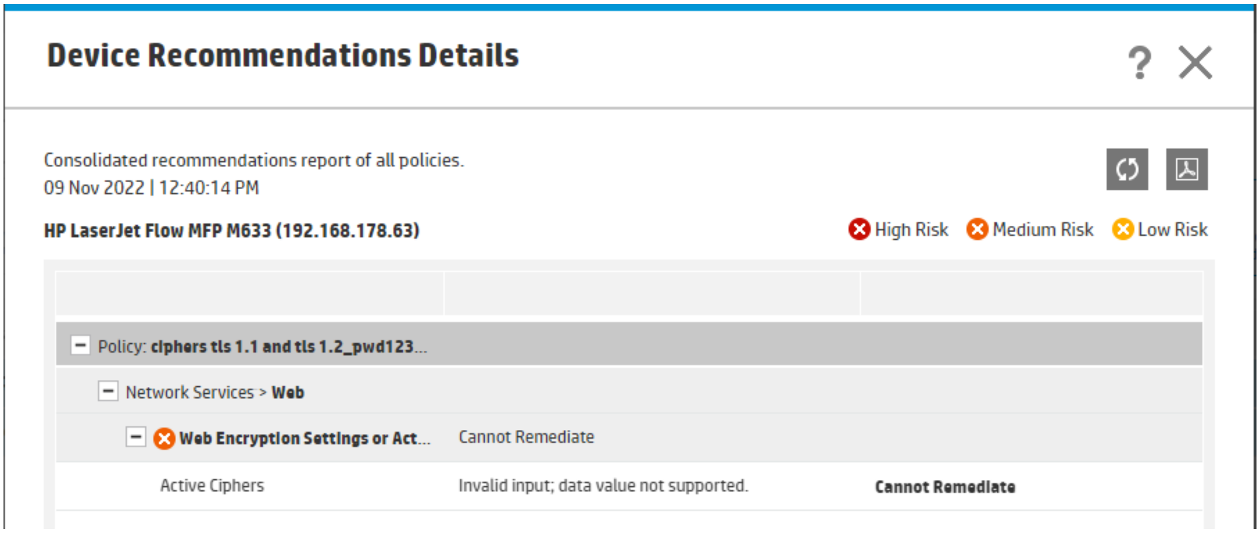
null nullnullnullnullnull null

Additional information:
This can happen when using Firefox browser or when using IE on a localized Windows 2019 server. Firefox is not officially supported with HPSM and Microsoft retired IE out of support in June 2022.

Solution:
Use another supported browser: Edge or Chrome.

Cannot Remediate Web Encryption or Active Ciphers (Invalid input; data value not supported)

In some situations, HPSM 3.8 and older is unable to remediate cipher settings on devices which have a different cipher configuration.
The remediation result will show: Invalid input, see screenshot.



Consolidated recommendations report of all policies.
09 Nov 2022 | 12:40:14 PM

HP LaserJet Flow MFP M633 (192.168.178.63)

⊟ Policy: ciphers tls 1.1 and tls 1.2_pwd123...		
⊟ Network Services > Web		
⊟ ⊗ Web Encryption Settings or Act...	Cannot Remediate	
Active Ciphers	Invalid input; data value not supported.	Cannot Remediate

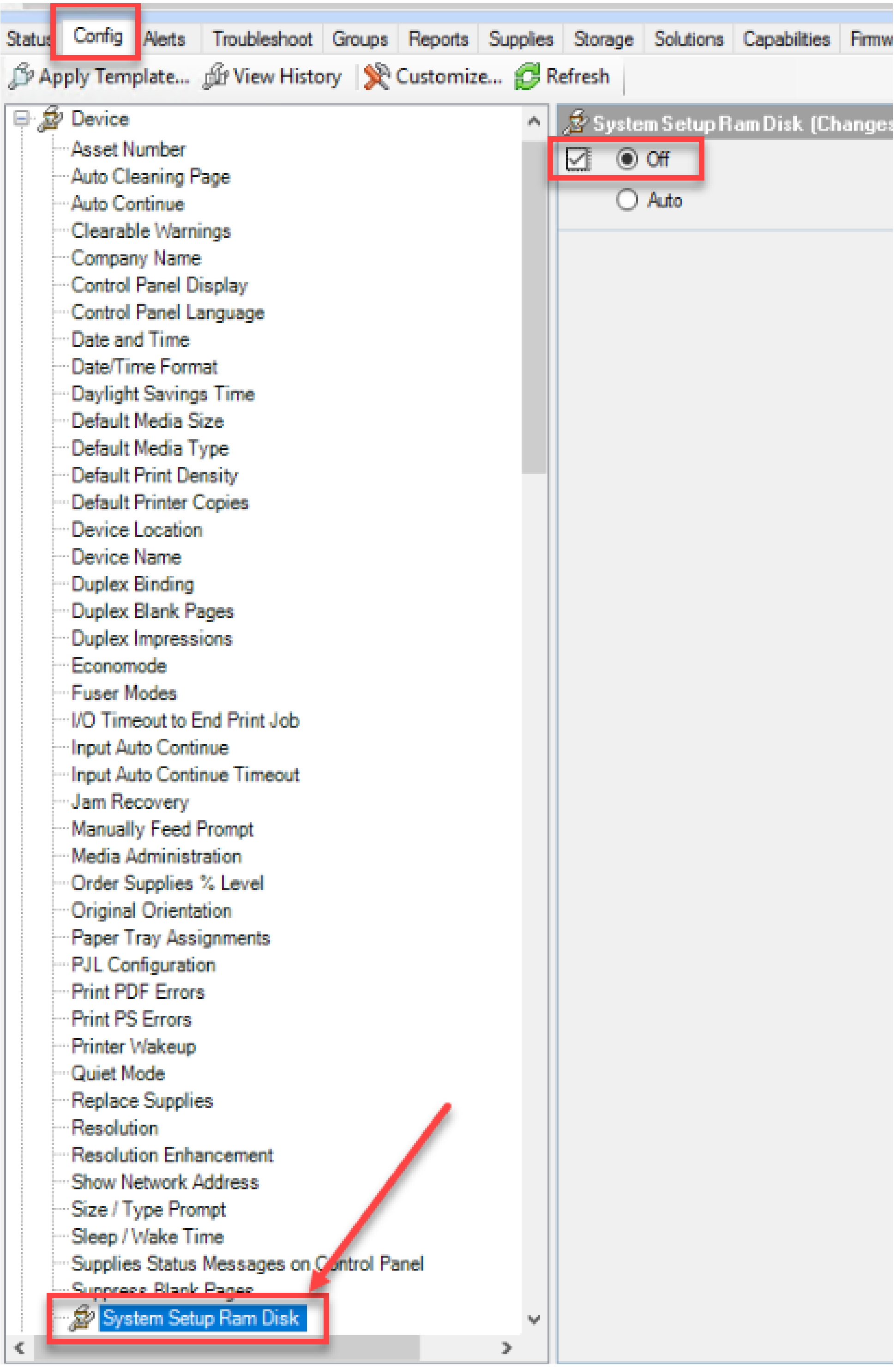
Root cause: HPSM 3.8 and older is not always configuring the TLS and ciphers with one command.
Solution:
Upgrade to HPSM 3.9

HPSM always displaying Medium Risk for File Erase Mode on some legacy HP devices, such as HP LaserJet P3010

Issue: When running an assessment and remediation task with a policy with File Erase Mode (with the option ignore when not supported), HPSM might report Medium risk on some legacy HP LaserJet device, even if those devices do not have a hard disk installed.

Solution:
Disable the RAM disk on the legacy HP Laser Jet devices and re-run the assessment.
The RAM disk can be disabled with HP WebJetadmin or directly in the EWS of the device.

In HP Web Jetadmin this option can be found by expanding **Device** category and selecting System Setup Ram Disk. See screenshot:

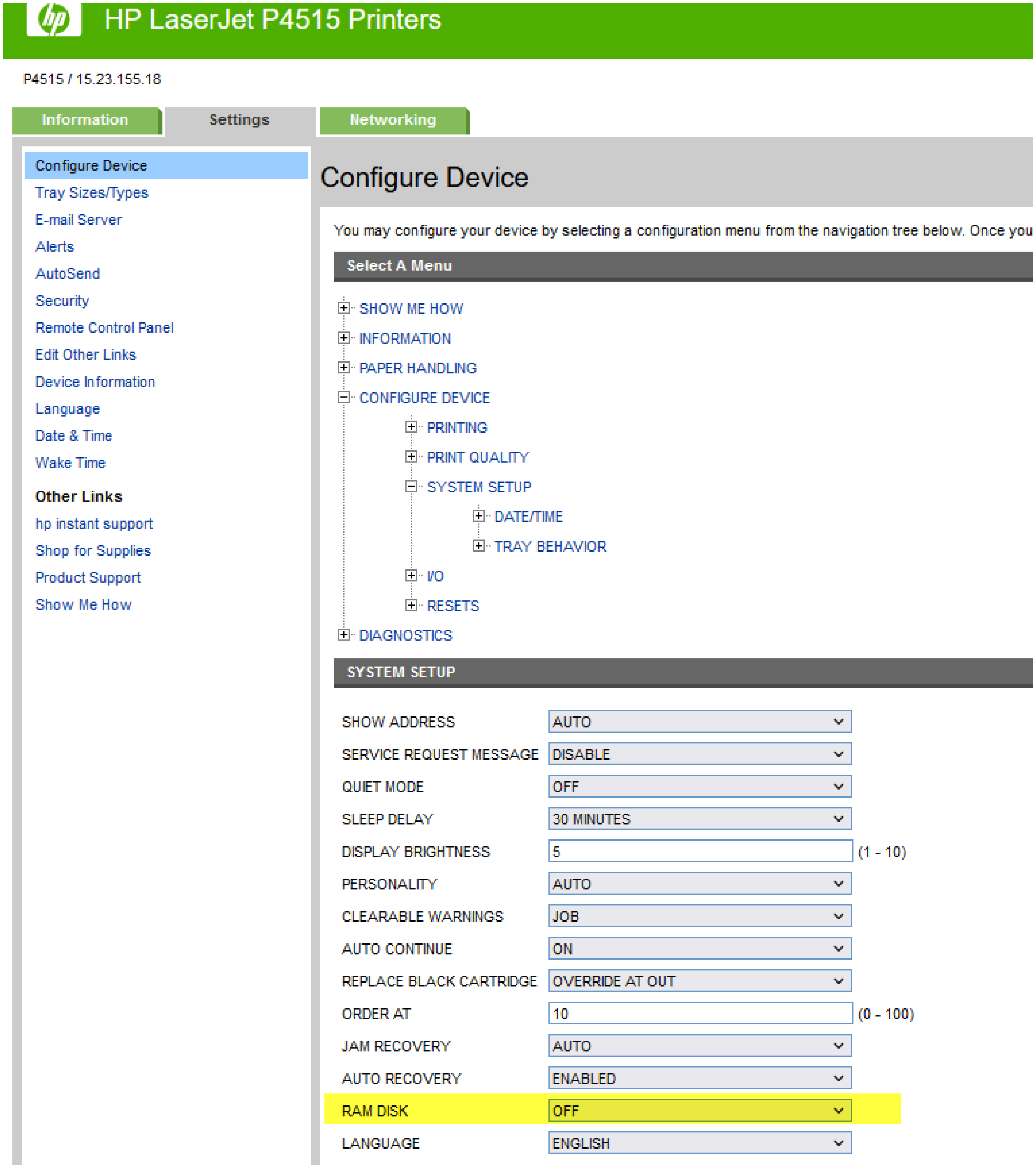


System Setup Ram Disk (Change

☑ ● Off

○ Auto

In the EWS of a device this can be found on the **Settings** tab, Configure Device, System Setup. Change the option RAM Disk to Off and click on **Apply.**



Configure Device

You may configure your device by selecting a configuration menu from the navigation tree below. Once you

SYSTEM SETUP

SHOW ADDRESS	AUTO	
SERVICE REQUEST MESSAGE	DISABLE	
QUIET MODE	OFF	
SLEEP DELAY	30 MINUTES	
DISPLAY BRIGHTNESS	5	(1 - 10)
PERSONALITY	AUTO	
CLEARABLE WARNINGS	JOB	
AUTO CONTINUE	ON	
REPLACE BLACK CARTRIDGE	OVERRIDE AT OUT	
ORDER AT	10	(0 - 100)
JAM RECOVERY	AUTO	
AUTO RECOVERY	ENABLED	
RAM DISK	OFF	
LANGUAGE	ENGLISH	

HPSM is unable to communicate over SNMPv3 with some legacy HP Laserjet devices

Issue: After configuring the SNMPv3 credentials of some legacy devices via the EWS and disabling SNMPv1/v2, HPSM cannot communicate with the device over SNMPv3

Solution: Configure the SNMPv3 credentials of the device with HPSM instead of the EWS. Disable initially SNMPv3 on the device and enable SNMPv1v2 via the EWS. Now remediate the device with an HPSM policy with the desired SNMP settings (v1 and v3).

Background information (SNMPv3 passphrases versus keys)

The HP EWS management interface allows access to many device settings. Both device and HP Jetdirect management settings can be viewed and adjusted from HP EWS. While you might expect these to be identical to the settings found in the HPSM configuration interface, this is not always the case for some legacy devices. For example, HP EWS might show SNMPv3 credentials as hexadecimal keys, while HPSM always has credentials configured with passphrases. This is a significant difference. HP does not recommend managing SNMPv3 from both interfaces on the same device.

Best practices: Configure the SNMPv3 settings of the (legacy) devices with HPSM and use the Global Credentials feature to ensure that HPSM has enough information to discover your SNMPv3-protected devices.

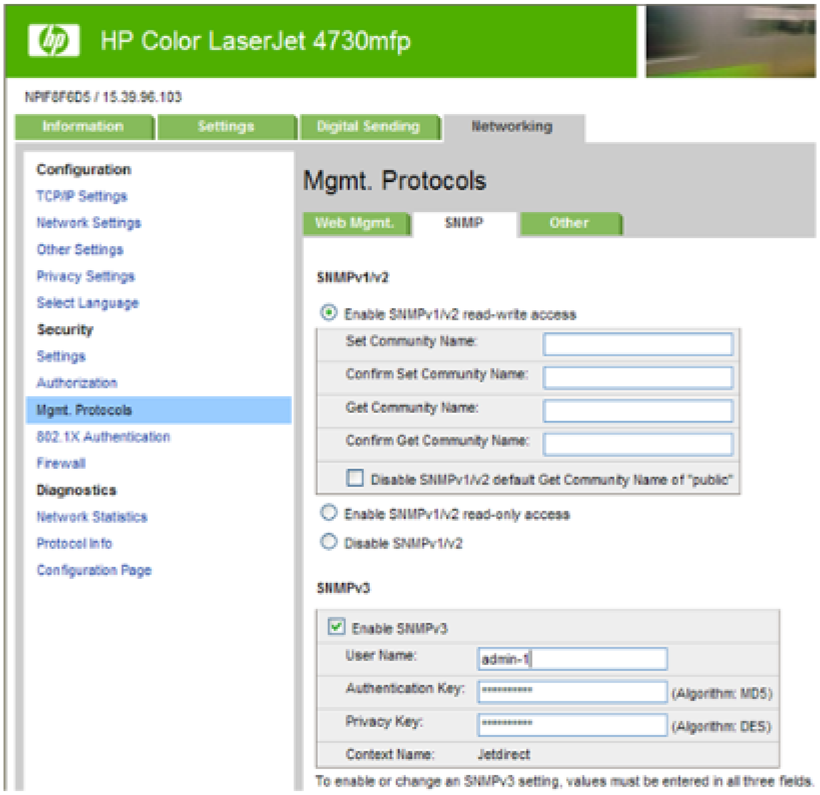
When the SNMPv3 credential is configured from HPSM with a policy, the policy contains a username and two passphrases to the interface. The passphrases are designed with human usability in mind and can be simple, easy-to-remember strings of letters and/or numbers. (example oncewasasmallcat) When HPSM sets up the device for SNMPv3 security, it transposes that phrase into a hex key using a hash technique of MD5 or DES, depending on the phrase. So, while HPSM allows the user to work with friendly passphrases, the SNMPv3 communication between HP Jetdirect and HPSM uses very cryptic strings that prevent tampering with devices and data.

Best practices: If HPSM is initially used to configure SNMPv3 on devices, HPSM should be used instead of HP EWS (a must for some legacy devices). Administrators can continue to use HP EWS as a management interface with the exception of SNMPv3 settings.

Some legacy HP EWS interfaces require the user to enter hexadecimal keys rather than passphrases. For security reasons, it does not disclose the key values that are currently stored on the device. This means it is extremely difficult to manage SNMPv3 credentials from both HP EWS and HPSM. Therefore, HPSM should be the primary tool for managing a fleet, that contains older legacy devices. HP highly recommends that you use HPSM exclusively for managing SNMPv3 settings as well.

Note: HP Web Jetadmin can also be used to configure the SNMPv3 settings on those legacy devices.

Example of EWS of a legacy device which requires SNMPv3 keys instead of SNMPv3 passphrases:



Mgmt. Protocols

SNMPv1/v2

● Enable SNMPv1/v2 read-write access

Set Community Name:	
Confirm Set Community Name:	
Get Community Name:	
Confirm Get Community Name:	

□ Disable SNMPv1/v2 default Get Community Name of "public"

○ Enable SNMPv1/v2 read-only access

○ Disable SNMPv1/v2

SNMPv3

☑ Enable SNMPv3

User Name:	admin-1	
Authentication Key:	***********	(Algorithm: MD5)
Privacy Key:	***********	(Algorithm: DES)
Context Name:	Jetdirect	

To enable or change an SNMPv3 setting, values must be entered in all three fields.

Note: Some legacy devices, like HP LaserJet P4515, seem to offer passphrases. However, the devices are not using the same encryption as HPSM and communication over SNMPv3 is only possible when SNMPv3 has been configures with HPSM or WJA.

Missing hostname for a device even when nslookup provides a response

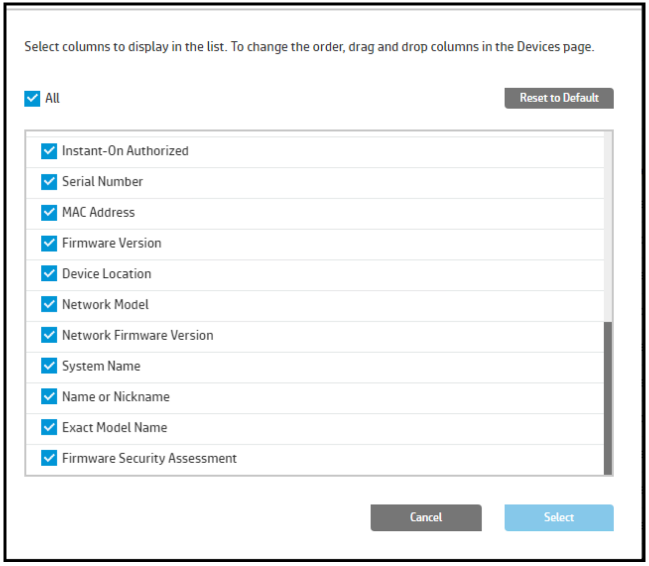
Before HPSM is displaying a value in the Host Name column it performs lookup and reverse lookup. This information needs to match, other wise HPSM will not consider any of this as valid information and display an empty value for the Host Name.
HPSM is asking the operating system via .net to perform a name resolution and revers lookup. You can test this with an nslookup and reverse nslookup, which is normally matching the OS behavior:
Nslookup <PrinterIp>
This should provide an answer like PrinterHostname.com
Now perform a lookup:
Nslookup <Printerhostname.com>

If you get a response to both queries and they match, then HPSM should be displaying the hostname of the device in the UI.

Note: name resolution for devices in the local subnet can also be done with other methods by the OS.

Column “Certificate Expiry Date” is missing in HPSM UI

Issue: HPSM 3.10 introduced the column Certificate Expiry Date. Sometime this column is not listed in the list of columns, even when using HPSM 3.10 or later. See screenshot:



Select columns to display in the list. To change the order, drag and drop columns in the Devices page.

☑ All

☑ Instant-On Authorized
☑ Serial Number
☑ MAC Address
☑ Firmware Version
☑ Device Location
☑ Network Model
☑ Network Firmware Version
☑ System Name
☑ Name or Nickname
☑ Exact Model Name
☑ Firmware Security Assessment

Solution: Clear the cache of the browser and reload HPSM in the browser.

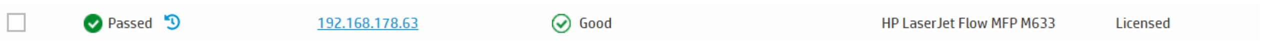
HPSM_service.log file errors

CryptographicException error or ‘Padding is invalid and cannot be removed’ error

CryptographicException errors such as A ‘Padding is invalid and cannot be removed’ error are listed in the HPSM_service.log file:

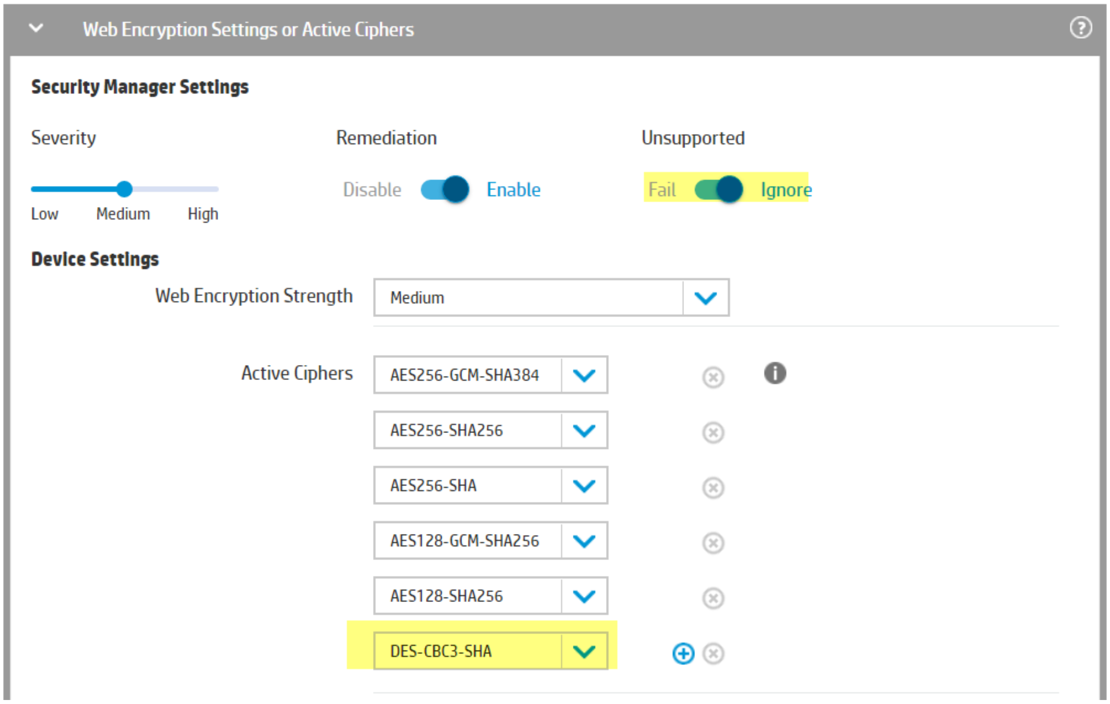
```
2022-03-17 14:52:32,386 ERROR Service
System.Security.Cryptography.CryptographicException: Padding is invalid and cannot be
removed.__  at System.Security.Cryptography.CapiSymmetricAlgorithm.DepadBlock(Byte[]
block, Int32 offset, Int32 count)__  at
System.Security.Cryptography.CapiSymmetricAlgorithm.TransformFinalBlock(Byte[]
inputBuffer, Int32 inputOffset, Int32 inputCount)__  at
System.Security.Cryptography.CryptoStream.Read(Byte[] buffer, Int32 offset, Int32 count)__
at LocksmithCore.DataProtection.Decrypt(Byte[] keyBytes, Byte[] bytestoBeDecrypted)__  at
LocksmithCore.DataProtection.Decrypt(String cipherText, String passPhrase, String saltValue)
 [4] - Error while Decrypting :
```

This means that HPSM cannot set the ciphers which are selected in the HPSM policy. This might be confusing as the device status can still be good:



☐ ✓ Passed 192.168.178.63 ✓ Good HP LaserJet Flow MFP M633 Licensed

An example of a policy which can cause this on a HP FutureSmart 5 device includes DES-CBC3-SHA and has Unsupported set to Ignore:



Web Encryption Settings or Active Ciphers

Security Manager Settings

Severity: Low — Medium — High

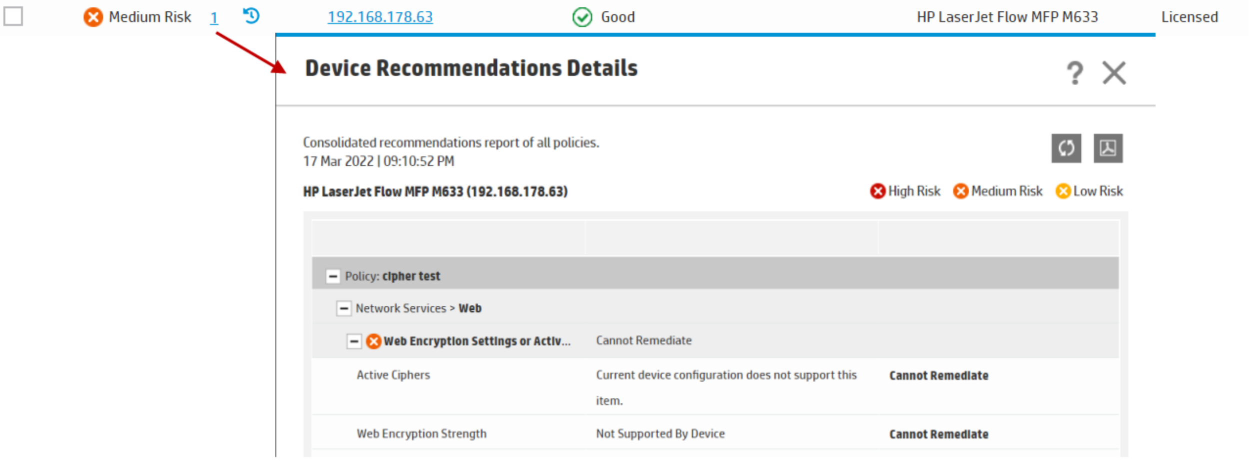
Remediation: Disable / Enable

Unsupported: Fail / Ignore

Device Settings

Web Encryption Strength	Medium
Active Ciphers	AES256-GCM-SHA384
	AES256-SHA256
	AES256-SHA
	AES128-GCM-SHA256
	AES128-SHA256
	DES-CBC3-SHA

After changing Unsupported to Fail, you will receive the following result for the same policy on the HP FutureSmart 5 device:



□	Medium Risk	1	192.168.178.63	Good	HP LaserJet Flow MFP M633	Licensed

Device Recommendations Details

Consolidated recommendations report of all policies.
17 Mar 2022 | 09:10:52 PM

HP LaserJet Flow MFP M633 (192.168.178.63)

High Risk Medium Risk Low Risk

Policy: **cipher test**		
Network Services > **Web**		
Web Encryption Settings or Activ...	Cannot Remediate	
Active Ciphers	Current device configuration does not support this item.	**Cannot Remediate**
Web Encryption Strength	Not Supported By Device	**Cannot Remediate**

The policy editor whitepaper lists in detail which ciphers are supported on HP FutureSmart 3, 4 and 5 and which ciphers are TLS 1.0 or higher.

To prevent the error message on a mixed fleet of devices, you might have to use separate policies.

‘Unable to read table/ when table is empty. Returning empty lists’ error

An error ‘Unable to read table/ when table is empty. Returning empty lists’ is listed in the HPSM_service.log file:

```
2022-02-08 10:35:34,015 DEBUG Service [5] - BizLogicMgrHelper.GetUserPreferencesById() - UserId is empty:
```

```
2022-02-08 10:35:34,015 ERROR Service [5] - UserPreferences - unable to read table/ when
table is empty. Returning empty lists.
2022-02-08 10:35:34,062 DEBUG Service [5] - BizLogicMgrHelper -
SetUpAssessmentAndPolicyUniqueIDFromQueryFilter
```

This means that the userPreferenceTable and UserTable are empty.

To fill the table with the user preference settings, do the following:

1. Log into HPSM.
2. Go to Settings and select **My preferences.**
3. Set Time Format to **24** hours and click **Save**.

NOTE: this error message does not seem to impact HPSM behavior.

The tables are populated with data. If preferred, you can revert the time to 12 hours, save the changes, and then the settings will be reflected in the database.

Using Network Traces for Troubleshooting

Network traces are sometimes used to prove a certain behavior. Traces never lie. Common free applications such as Wireshark can be downloaded and installed to see exactly what is happening and why on the network. If possible, install it on the Security Manager server and capture all traffic to and from the server. Filters can be used when reading the traces to narrow down traffic between server and device.

Using Event Viewer for Troubleshooting

Event Viewer maintains logs about program, security, and system events on the server.

Many times, more information can be found regarding issues with services or applications. Logs can be exported and sent to support for analysis.

Appendix A Following a task in HPSM_service.log

When debug has been enabled for the HPSM_service.log file, the process details of a task can be seen in the log file.

The EAPTaskManager starts the task (using the taskname which is displayed in the UI. This task is running under on thread, in this case thread #4 which is the number in the square brackets.

```
2020-06-04 16:40:40,147 DEBUG Service  [4] - EAPTaskManager - ProcessTask:
TelnetAndRetainJobTask
```

Now the task is created (added and a taskID (id) and started under a new threadnumber (11):

```
2020-06-04 16:40:40,179 DEBUG Service  [4] -  - AddingTask - TelnetAndRetainJobTask id:
24c16d9f-227b-4150-be28-abd00112d6cc
2020-06-04 16:40:40,179 DEBUG Service  [4] -  # Tasks waiting in queue: - 0
2020-06-04 16:40:44,522 DEBUG Service  [11] -  Starting task: TelnetAndRetainJobTask - with ID
- 24c16d9f-227b-4150-be28-abd00112d6cc
2020-06-04 16:40:44,538 DEBUG Service  [4] - AssessmentTask - ExecuteTask Started:
TelnetAndRetainJobTask job: AssessAndRemediate processing step: notExpanded for task
dbID: 24c16d9f-227b-4150-be28-abd00112d6cc
```

If needed child tasks are created. Child tasks have the same ID as the parent but have a .xxx.# behind the task name, where xxx are characters and # is a number:

```
2020-06-04 16:40:45,835 DEBUG Service  [4] - BizLogicMgr Create Task name:
TelnetAndRetainJobTask.sbc.0 returning - 24c16d9f-227b-4150-be28-abd00112d6cc
2020-06-04 16:40:45,865 DEBUG Service  [4] -
Task.OptimizeNumberOfTasksAndSetupCheckPointRestart - Done
```

The number of child tasks depend upon the number of devices which are assessed and remediated and the configured number of devices for one thread – by default 25- for the following two settings in the HPSM_service.config:

```
<add key="numberOfDevicesInEAPRequest" value="25" />
<add key="numberDevicesInEAPTaskCheckpointInterval" value="25" />
```

Sometimes it is hard to know which device is causing a hang within a childtask (as a child task will serve 25 devices by default). You can change the numberOfDeviceInEAPRequest to 1 and restart the HPSM service. After that create a new task. Now each child-task will only serve one printer and it will be easier to detect which child task is hanging.

The DBO.ScheduledTaskTable can also help to understand the relationship between parent task and child task as it will show the ID and Names of parent task and child tasks.

The child task is running under its own thread number and registering its existence at the parent task.

```
2020-06-04 16:40:54,755 DEBUG Service   [16] - ScheduleTaskManager - Registereing task:
TelnetAndRetainJobTask.sbc.0 type:Worker 16 b8f39960-b872-40ea-b087-abd00112de33
2020-06-04 16:40:54,771 DEBUG Service   [16] - ScheduleTaskManager.UpdateTaskTracking
parentID: 24c16d9f-227b-4150-be28-abd00112d6cc A#: 0 R#: 0 D#: 0 total devices: 2
substractCounters: False
2020-06-04 16:40:54,771 DEBUG Service   [16] - ScheduleTaskManager.UpdateTaskTracking  -
parent found
2020-06-04 16:40:54,771 DEBUG Service   [16] -
ScheduleTaskManager.UpdateParentsToRunningTasksRelationshipAndCounters  with:
parentID: 24c16d9f-227b-4150-be28-abd00112d6cc A#: 0 R#: 0 D#: 0 total devices: 2
substractCounters: False final task status: None propagateStatusMsgToParent: False
2020-06-04 16:40:54,771 DEBUG Service   [16] -  Parent's Updated Counters:   ParentTask - dbID:
24c16d9f-227b-4150-be28-abd00112d6cc A#: 2 R#: 2 D#: 0 taskStatus: None
2020-06-04 16:40:54,771 DEBUG Service   [16] -
ScheduleTaskManager.UpdateDictOfRunningTasks   parentID: 24c16d9f-227b-4150-be28-
abd00112d6cc A#: 0 R#: 0 D#: 0 total devices: 2 substractCounters: False
2020-06-04 16:40:54,788 DEBUG Service   [16] - ScheduleTaskManager - Successfully
Registered task: TelnetAndRetainJobTask.sbc.0 type:Worker 16 b8f39960-b872-40ea-b087-
abd00112de33
2020-06-04 16:40:54,788 DEBUG Service   [16] - --Number of running tasks after Register: 1
```

When the client task has been completed it will inform the parent and unregister itself.

```
2020-06-04 16:41:20,303 DEBUG Service   [16] - ScheduledTaskMgr.Unregister - Task: b8f39960-
b872-40ea-b087-abd00112de33 name:TelnetAndRetainJobTask.sbc.0 type:Worker
2020-06-04 16:41:20,303 DEBUG Service   [16] - ScheduleTaskManager.UpdateTaskTracking
parentID: 24c16d9f-227b-4150-be28-abd00112d6cc A#: 2 R#: 2 D#: 0 total devices: 2
substractCounters: True
2020-06-04 16:41:20,303 DEBUG Service   [16] - ScheduleTaskManager.UpdateTaskTracking  -
parent found
2020-06-04 16:41:20,303 DEBUG Service   [16] - ScheduleTaskManager.UpdateTaskTracking  -
worker found
2020-06-04 16:41:20,303 DEBUG Service   [16] -
ScheduleTaskManager.UpdateParentsToRunningTasksRelationshipAndCounters  with:
parentID: 24c16d9f-227b-4150-be28-abd00112d6cc A#: 2 R#: 2 D#: 0 total devices: 2
substractCounters: True final task status: None propagateStatusMsgToParent: False
2020-06-04 16:41:20,303 DEBUG Service   [16] -  Parent's Updated Counters:   ParentTask - dbID:
24c16d9f-227b-4150-be28-abd00112d6cc A#: 0 R#: 0 D#: 0 taskStatus: None
2020-06-04 16:41:20,318 DEBUG Service   [16] - ScheduleTaskManager.DetermineStatusMsg:
2020-06-04 16:41:20,334 DEBUG Service   [16] - --Number of running remaining tasks after
UpdateTaskStatus:  ParentTask - dbID: 24c16d9f-227b-4150-be28-abd00112d6cc A#: 0 R#: 0 D#:
0 taskStatus: None
2020-06-04 16:41:20,350 DEBUG Service   [16] - AssessmentTask - ExecuteTask Ended:
TelnetAndRetainJobTask.sbc.0 with status : Completed job: AssessAndRemediate for task:
b8f39960-b872-40ea-b087-abd00112de33 time taken : { 25.6411117 }s
2020-06-04 16:41:20,350 DEBUG Service   [16] - Task - UnregisterAndSetTaskMsg -
TelnetAndRetainJobTask.sbc.0 -  with msg: Finished interacting with devices
2020-06-04 16:41:20,365 DEBUG Service   [16] - Task.UnRegisterTask:
TelnetAndRetainJobTask.sbc.0
```

For each client task, you will find a Registration task and UnregisterTask:

```
ScheduleTaskManager - Registereing task: TelnetAndRetainJobTask.sbc.0 type:Worker 16
b8f39960-b872-40ea-b087-abd00112de33
2020-06-04 16:41:20,365 DEBUG Service   [16] - Task.UnRegisterTask:
TelnetAndRetainJobTask.sbc.0
```

If you cannot find a UnregisterTask for a client task, then you have identified a hanging task.

After all child tasks have been completed, the parent task will be notified that the child tasks completed:

```
2020-06-04 16:41:20,365 DEBUG Service   [16] -
ScheduleTaskManager.UpdateDictOfRunningTasks   parentID: 24c16d9f-227b-4150-be28-
abd00112d6cc A#: 0 R#: 0 D#: 0 total devices: 2 substractCounters: True
2020-06-04 16:41:20,365 DEBUG Service   [16] -
ScheduleTaskManager.UpdateDictOfRunningTasks  removing from running tasks:  parentID:
24c16d9f-227b-4150-be28-abd00112d6cc A#: 0 R#: 0 D#: 0 total devices: 2
2020-06-04 16:41:20,365 DEBUG Service   [16] - TaskBase - ProcessShutdown: set shut down
msg to true: b8f39960-b872-40ea-b087-abd00112de33
2020-06-04 16:41:20,365 DEBUG Service   [16] -
ScheduleTaskManager.UpdateParentsToRunningTasksRelationshipAndCounters  with:
parentID: 24c16d9f-227b-4150-be28-abd00112d6cc A#: 0 R#: 0 D#: 0 total devices: 2
substractCounters: True final task status: Completed propagateStatusMsgToParent: True
2020-06-04 16:41:20,365 DEBUG Service   [16] -  Parent's Updated Counters:   ParentTask - dbID:
24c16d9f-227b-4150-be28-abd00112d6cc A#: 0 R#: 0 D#: 0 taskStatus: Completed
2020-06-04 16:41:20,381 DEBUG Service   [16] -
ScheduleTaskManager.CheckParentStateAndRemoveIfAppropriate:  24c16d9f-227b-4150-
be28-abd00112d6cc
2020-06-04 16:41:20,397 DEBUG Service   [16] -
ScheduleTaskMgr.GetListOfChildernTasksNotDone - # tasks: 0
2020-06-04 16:41:20,412 DEBUG Service   [16] - --  Updating parent task status to: Completed
2020-06-04 16:41:20,412 DEBUG Service   [16] -
ScheduleTaskManager.CheckParentStateAndRemoveIfAppropriate removing parent info
2020-06-04 16:41:20,459 DEBUG Service   [16] -
ScheduleTaskManager.CheckParentStateAndRemoveIfAppropriate  Updating parent task - all
childern are done processing
2020-06-04 16:41:20,459 DEBUG Service   [16] - TaskBase - SetNextRunTime name:
TelnetAndRetainJobTask type: Schedulable status: Completed next run:12/31/99 11:59
2020-06-04 16:41:20,459 DEBUG Service   [16] - ScheduleTaskManager -
UpdateTaskStatusAndRepeatCycleAfterShutdown: AssessAndRemediate name:
TelnetAndRetainJobTask to Completed
2020-06-04 16:41:20,505 DEBUG Service   [16] - Parent Task Finished: TelnetAndRetainJobTask
2020-06-04 16:41:20,505 DEBUG Service   [16] - --Number of running tasks after Unregister: 0
2020-06-04 16:41:20,505 DEBUG Service   [16] - ScheduledTaskMgr.Unregister Success - Task:
b8f39960-b872-40ea-b087-abd00112de33 name:TelnetAndRetainJobTask.sbc.0 type:Worker
```

After that, the parent task should stop and unregister as well on its own thread number:

```
Line 312: 2020-06-04 16:41:21,535 DEBUG Service   [4] -  Parent task stopping, created workers:
TelnetAndRetainJobTask
Line 313: 2020-06-04 16:41:21,DEBUG Service   [4] - AssessmentTask - ExecuteTask Ended:
TelnetAndRetainJobTask with status : None job: AssessAndRemediate for task: b8f39960-
b872-40ea-b087-abd00112de33 time taken : { 1.1715505 }s
Line 314: 2020-06-04 16:41:21,DEBUG Service   [4] - Task - UnregisterAndSetTaskMsg -
TelnetAndRetainJobTask -  with msg:
```

Appendix B Syntax for installDBrmt.bat (HPSM 3.4 and older)

Proper syntax for SQL server instance on same machine where you are running the installDBrmt.bat script:

installdbrmt .|instancename or *installdbrmt server|instancename*

The ".\"means same server so you can easily specify the server even though it is the same machine you are on.

Proper syntax for SQL server instance on remote machine where you are running the old scripts:

installdbrmt server|instancename

NOTE: If a default instance is used, you should be able to enter the server name, SQL knows if no instance is specified then use the default instance.

BAD SYNTAXES:

installdbrmt |server|instancename or installdbrmt instancename

Appendix C Other HP Security Manager Whitepapers and Manuals

There are a lot of whitepapers/manuals available for HP Security Manager.
The view them, go to the HP Security Manager Support page and select **Manuals**.
The following list of documents is available on the support page:

- Instant-On Security and Auto-Group Remediation (white paper)
- Automatic Email notification for remediation tasks and policy changes (white paper)
- Certificate Management (white paper)
- Credential Management (white paper)
- Device Discovery, Determining Device Details and Exporting Devices (whitepaper)
- Installation and Setup Guide
- Manage devices with HP FutureSmart 4.5 Firmware
- Policy Editor Settings including supported devices feature table (white paper)
- Release Notes with Ports (white paper)
- Reporting, Email Alert Subscriptions & Remediation Summary, Auditing & Syslog Functionality (white paper)
- Securing the HP Security Manager (white paper)
- Sizing and Performance (white paper)
- Supported Devices (white paper)
- Troubleshooting Issues (white paper)
- User Guide
- Using licenses (white paper)
- Using Microsoft® SQL Server (white paper)

The section **Product Information** on the HP Security Manager Support page contains the following information:

- Supported device features matrix (.xls) hp.com/go/support

Current HP driver, support,

and security alerts

delivered directly to your

desktop.

Created April 2024, rev34