



# Health Tool Guide

Software version: 4.70

Document release date: July 2016

Software release date: July 2016

## Contents

Overview .....	2
Configuration .....	2
Options .....	2
Configuration-properties file .....	3
Examples .....	6
Communicating with the Oracle or MS SQL database using SSL .....	7
Health Tool Reports .....	8
Online report .....	8
HTML report .....	9
Text report .....	10
Interpreting Health Tool reports .....	13
<b>Send documentation feedback .....</b>	<b>15</b>
<b>Legal notices .....</b>	<b>15</b>
<b>Warranty .....</b>	<b>15</b>
<b>Restricted rights legend .....</b>	<b>15</b>
<b>Copyright notice .....</b>	<b>15</b>
<b>Trademark notices .....</b>	<b>15</b>
<b>Documentation updates .....</b>	<b>15</b>
<b>Support .....</b>	<b>15</b>

# Overview

The Health Tool is a command-line interface that you can use to identify CSA issues, find out which component (such as the database, JBoss server, Management Console, Identity Management component, and Marketplace Portal) might be causing the issues, and decide if additional troubleshooting is needed.

The Tool provides CSA-component status (pass/fail) in online, HTML, and text-file reports. You must have database and REST API connections to display the corresponding information. Even when connections fail, the Health Tool might still be able to collect and display data about subscriptions, lifecycle transitions, and number of instances.

The Health Tool file (`health-tool.jar`) runs from and is located in `<CSA_installation_directory>\Tools\HealthTool`. If you run the tool from a different directory, you must specify the relative or absolute path.

## Configuration

This section describes Health Tool configuration.

### Options

This section describes Health Tool configuration options.

#### Supported options

Use the following command to list supported options:

Windows:

```
java.exe -jar health-tool.jar -h
```

Windows and Linux:

```
java -jar health-tool.jar -h
```

#### Option description

The following table describes Health Tool command options and suboptions.

Option	Option Description
<code>-h, --help</code>	Displays syntax and use.
<code>-g, --generate</code>	Generates a sample configuration properties file ( <code>config.properties</code> ) in the default location if the original file (which is automatically generated when CSA is installed) is missing (such as when the <code>health-tool.jar</code> file is moved or copied to a different location without the <code>config.properties</code> file). You might also want to update the configuration-properties file if the information used to communicate with the CSA database differs from what was automatically generated. If used with the <code>-o</code> option, existing files are overwritten.
<code>-c, --config-file &lt;config property file&gt;</code>	Optional. The location and name of the configuration properties file. If this option is specified, you must specify the name and location of the configuration properties property file. Linux example: <code>../../../../openjre/bin/java -jar health-tool.jar -c my.properties</code>  The location can be an absolute path or a path relative to the location where the Health Tool

Option	Option Description
	<p>is run. If the file is located in the same directory from which the Health Tool is run, the path does not need to be specified.</p> <p>If you specify the <code>-c</code> option but do not specify a file location and name, or if you do not specify the <code>-c</code> option, the Health Tool will look for a file called <code>config.properties</code> that is located in the same directory as the Health Tool (<code>&lt;csa_home&gt;\Tools\HealthTool\</code>).</p>
<code>-j,--jars &lt;Oracle JARs&gt;</code>	<p>Oracle only.</p> <p>Load the Oracle JDBC <code>.jar</code> files. Note that if more than one jar file is needed, the jar filenames must be separated by a comma (do not include any spaces between the comma and filename).</p> <p>The Oracle JDBC JAR files must be located in the same folder as the <code>health-tool.jar</code> file (<code>&lt;csa_home&gt;\Tools\HealthTool\</code>).</p>
<code>-o,--overwrite</code>	<p>Optional.</p> <p>Overwrites the <code>health_tool.log</code> (text) and <code>report.html</code> report files. If this option is not specified, the current report information is added at the top of the files.</p> <p>When used with the <code>-g</code> option, overwrites the <code>config.properties</code> file that is located in the same folder as the <code>health-tool.jar</code> file.</p>
<code>"&lt;csa_jre&gt;\bin\java" -jar health-tool.jar -h</code>	Display the Health Tool help in Oracle (SSL not enabled), MS SQL, and PostgreSQL
<code>"&lt;csa_jre&gt;\bin\java" -jar health-tool.jar -o -j ojdbc6.jar</code>	Run the health tool, overwriting existing logs and reports in Oracle (SSL not enabled)
<code>"&lt;csa_jre&gt;\bin\java" -jar health-tool.jar -o</code>	Run the health tool, overwriting existing logs and reports in MS SQL and PostgreSQL

## Configuration-properties file

The Health Tool accepts the configuration-properties file (`config.properties` - required) as input. This file is automatically generated during CSA installation, populated with database information that the CSA installer collects, and installed into the same directory as the Health Tool file is installed.

You use the information in the configuration-properties file to connect to the CSA database, log in to CSA, authenticate REST API calls, and connect to the Identity Management component.

To configure the configuration-properties file, enter CSA log-in information, REST API authentication information, and Identity Management component connection properties. See [Configuration properties file parameters](#) for more information about these properties.

**Note:** You might also want to update the configuration-properties file if the information used to communicate with the CSA database differs from what was automatically generated.

See [Configuration properties file parameters](#) for more information about the contents of the configuration properties file. See [Examples](#) for examples of this file.

## Generating sample properties files

This section describes the commands you must use to generate sample properties files. Before you issue the file-generating command(s), decide which scenario best fits your situation.

Scenarios	Command	Results and Action
<p><b>#1 - Sample property file does not exist</b></p> <p>The automatically generated sample properties file (<code>config.properties</code>) that the CSA installer created in the same folder as the <code>health-tool.jar</code> file (<code>&lt;csa_home&gt;\Tools\HealthTool\</code>) no longer exists in that file.</p>	<pre>"&lt;csa_jre&gt;\bin\java" -jar health-tool.jar -g</pre> <p>(Optional) Add the <code>--config-file</code> options to specify a different file or location</p>	<p><code>config.properties</code> file is created in the default location:  <code>&lt;csa_home&gt;\Tools\HealthTool\</code></p>
<p><b>#2 - Sample property file exists/overwrite the file</b></p> <p>There is already a sample-properties file in <code>&lt;csa_home&gt;\Tools\HealthTool\</code> and you want to <b>overwrite</b> its content (for example, you want to overwrite the file because it does not contain the most up-to-date information)</p>	<pre>"&lt;csa_jre&gt;\bin\java" -jar health-tool.jar -g -o</pre> <p>Add the <code>-o</code> option.</p>	<p>The Health Tool displays an error message saying that the file already exists. When prompted, enter the word <b>yes</b> to overwrite the file.</p> <p>The Health Tool overwrites the existing file contents, and then exits the file-generation process.</p>

**Note:** Additional command-line options are required if SSL is enabled between the Oracle database and CSA. See [Communicating with the Oracle or MS SQL database using SSL](#) for more information.

## Configuration properties file parameters

This table describes the configuration-properties file parameters.

Property Name	Description
<code>jdbc.driverClassName</code>	<p>The JDBC driver class.</p> <p><b>Examples</b></p> <p>Oracle</p> <pre>jdbc.driverClassName=oracle.jdbc.driver.OracleDriver</pre> <p>MS SQL</p> <pre>jdbc.driverClassName=net.sourceforge.jtds.jdbc.Driver</pre> <p>PostgreSQL</p> <pre>jdbc.driverClassName=org.postgresql.Driver</pre>
<code>jdbc.dialect</code>	<p>The name of the class that allows JDBC to generate optimized SQL for a particular database.</p> <p><b>Examples</b></p> <p>Oracle</p> <pre>jdbc.dialect=org.hibernate.dialect.OracleDialect</pre> <p>MS SQL</p> <pre>jdbc.dialect=org.hibernate.dialect.SQLServerDialect</pre> <p>PostgreSQL</p> <pre>jdbc.dialect=org.hibernate.dialect.PostgreSQLDialect</pre>
<code>jdbc.databaseUrl</code>	<p>The JDBC URL. When specifying an IPv6 address, it must be enclosed in square brackets.</p> <p><b>Examples</b></p> <p>Oracle (SSL not enabled)</p> <pre>jdbc.databaseUrl=jdbc:oracle:thin:@//127.0.0.1:1521/XE</pre>

Property Name	Description
	<p>Oracle (SSL not enabled, using an IPv6 address):</p> <pre>jdbc.databaseUrl=jdbc:oracle:thin:@//[f000:253c::9c10:b4b4]:1521/XE</pre> <p>Oracle (SSL enabled, CSA does not test the database DN)</p> <pre>jdbc.databaseUrl=jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS_LIST= (ADDRESS=(PROTOCOL = TCPS)(HOST = &lt;host&gt;)(PORT = 1521))) (CONNECT_DATA =(SERVICE_NAME = ORCL)))</pre> <p>where &lt;host&gt; is the name of the system on which the Oracle database server is installed.</p> <p>Oracle (SSL enabled, CSA tests the database DN)</p> <pre>jdbc.databaseUrl=jdbc:oracle:thin:@(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCPS)(HOST = &lt;host&gt;)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME = ORCL))(SECURITY=(SSL_SERVER_CERT_DN= "CN=abc,OU=dbserver,O=xyz,L=Sunnyvale,ST=CA,C=US")))</pre> <p>where &lt;host&gt; is the name of the system on which the Oracle database server is installed and the values for SSL_SERVER_CERT_DN are for the DN of the Oracle database server.</p> <p>MS SQL (SSL not enabled)</p> <pre>jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/ example;ssl=request</pre> <p>MS SQL (SSL not enabled, using an IPv6 address)</p> <pre>jdbc.databaseUrl=jdbc:jtds:sqlserver://[::1]:1433/ example;ssl=request</pre> <p>MS SQL (SSL enabled)</p> <pre>jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/ example;ssl=authenticate</pre> <p>MS SQL (FIPS 140-2 compliant)</p> <pre>jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/ example;ssl=authenticate</pre>
jdbc.username	The database user configured to access the CSA database.
jdbc.password	<p>This password:</p> <ul style="list-style-type: none"> <li>Is the password for the database user you used for the jdbc.username property.</li> <li>Is preceded by ENC, has no separating spaces, and is enclosed in parentheses.</li> <li>Should be encrypted (see the <i>CSA Configuration Guide</i> for instructions on encrypting passwords).</li> </ul> <p><b>Note:</b> If you will be configuring your CSA product to be FIPS 140-2 compliant, complete the configuration before you encrypt the password.</p> <p>Example:</p> <pre>jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0)</pre>
csa.username	A user who can access the CSA Management Console. This user is used to test the connection to CSA.
csa.password	<p>This password:</p> <ul style="list-style-type: none"> <li>Is the password for the CSA Management Console user you entered in the csa.username property.</li> <li>Is preceded by ENC, has no separating spaces, and is enclosed in parentheses.</li> <li>Should be encrypted (see the <i>CSA Configuration Guide</i> for instructions on encrypting passwords).</li> </ul> <p><b>Note:</b> If you will be configuring your CSA product to be FIPS 140-2 compliant, complete the configuration before you encrypt the password.</p> <p>Example:</p> <pre>csa.password=ENC(ac7fe2d25cf0578a9b45907ee721ab8099)</pre>

Property Name	Description
idm.tenantName	The provider-organization identifier of the CSA Management Console whose connection is being tested. Set this property to <code>Provider</code> .
idm.transportUser	A user configured to authenticate REST API calls. This user is used to test the REST API connection and to capture CSA license information.
idm.transportPassword	This password: <ul style="list-style-type: none"> <li>Is the password for the user you entered in the <code>idm.transportUser</code> property.</li> <li>Is preceded by ENC, has no separating spaces, and is enclosed in parentheses.</li> <li>Should be encrypted (see the <i>CSA Configuration Guide</i> for instructions on encrypting passwords).</li> </ul> <p><b>Note:</b> If you will be configuring your CSA product to be FIPS 140-2 compliant, complete the configuration before you encrypt the password.</p> <p><b>Example</b></p> <pre>idm.transportPassword=ENC(b5af870d6ce23951af09)</pre>
idm.username	A user who can connect to the Identity Management component.
idm.password	This password: <ul style="list-style-type: none"> <li>Is the password for the user you entered in the <code>idm.username</code> property.</li> <li>Is preceded by ENC, has no separating spaces, and is enclosed in parentheses.</li> <li>Should be encrypted (see the <i>CSA Configuration Guide</i> for instructions on encrypting passwords).</li> </ul> <p><b>Note:</b> If you will be configuring your CSA product to be FIPS 140-2 compliant, complete the configuration before you encrypt the password.</p> <p><b>Example</b></p> <pre>idm.password=ENC(79dfa03785cbe407001f7ab310e31)</pre>

## Examples

The following are examples of configured properties in the `config.properties` file.

Database configuration	Examples
Oracle (SSL not enabled)	<pre>jdbc.driverClassName=oracle.jdbc.driver.OracleDriver jdbc.databaseUrl=jdbc:oracle:thin:@//127.0.0.1:1521/XE jdbc.username=csadbuser jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0) jdbc.dialect=org.hibernate.dialect.OracleDialect</pre>
MS SQL (SSL not enabled)	<pre>jdbc.driverClassName=net.sourceforge.jtds.jdbc.Driver jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=request jdbc.username=csadbuser jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0) jdbc.dialect=org.hibernate.dialect.SQLServerDialect</pre>
MS SQL (SSL enabled)	<pre>jdbc.driverClassName=net.sourceforge.jtds.jdbc.Driver jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=authenticate jdbc.username=csadbuser jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0) jdbc.dialect=org.hibernate.dialect.SQLServerDialect</pre>
MS SQL (FIPS 140-2 compliant)	<pre>jdbc.driverClassName=net.sourceforge.jtds.jdbc.Driver jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=authenticate jdbc.username=csadbuser jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0) jdbc.dialect=org.hibernate.dialect.SQLServerDialect</pre>
PostgreSQL	<pre>jdbc.driverClassName=org.postgresql.Driver jdbc.databaseUrl=jdbc:postgresql://127.0.0.1:5432/csadb jdbc.username=csadbuser jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0) jdbc.dialect=org.hibernate.dialect.PostgreSQLDialect</pre>

Database configuration	Examples
CSA	# CSA credentials csa.username=admin csa.password=ENC(aJx51YfoPjzN3Dt8FWyugg==)
Identity Management Component	# IDM credentials idm.tenantName=CSA-Provider idm.transportUser=idmTransportUser idm.transportPassword=ENC(5BMf3m8nKYyJqnTgNj4FT/KqUyVIJ5ovEKtpmgUGDRA=) idm.username=admin idm.password=ENC(aJx51YfoPjzN3Dt8FWyugg==)

## Communicating with the Oracle or MS SQL database using SSL

If SSL is enabled between CSA and the Oracle or MS SQL database, additional command line options might be required and the URL property in the database-properties file must be configured correctly.

### Oracle Database

This table describes Oracle database configurations, command-line options, and `jdbc.databaseURL` Value information for different situations.

Configurations	Command-line options	jdbc.databaseURL Value
<b>CSA does not test the database DN and client authentication is enabled</b>		
SSL is enabled	-Djavax.net.ssl.keyStore="<certificate_key_file>" where:  <certificate_key_file> is the same keystore file defined by the certificate-keyfile attribute in the ssl element of the <csa_home>\jboss-as\standalone\configuration\standalone.xml file  <b>Example:</b> <csa_home>\jboss-as\standalone\configuration\.keystore	jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL = TCPS)(HOST = <host>)(PORT = 1521))) (CONNECT_DATA=(SERVICE_NAME = ORCL)))  where <host> is the name of the system on which the Oracle database server is installed.
CSA does not test the database DN	-Djavax.net.ssl.keyStorePassword=<certificate_key_file_password> where:  <certificate_key_file_password> is the password to the keystore file (for example, changeit)	
Client authentication is enabled	-Djavax.net.ssl.keyStoreType=<certificate_key_file_type> where:  <certificate_key_file_type> is the keystore type (for example, JKS or PKCS12)	
<b>CSA does not test the database DN and client authentication is not enabled</b>		
SSL is enabled	None	jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL = TCPS)(HOST = <host>)(PORT = 1521))) (CONNECT_DATA=(SERVICE_NAME = ORCL)))  where <host> is the name of the system on which the Oracle database server is installed
CSA does not test the database DN	None	
Client authentication is NOT enabled	None	
<b>CSA tests the database DN and client authentication is enabled</b>		
SSL is enabled	-Doracle.net.ssl_server_dn_match=true  <certificate_key_file> is the same keystore file defined by the certificate-keyfile attribute in the SSL element of the <csa_home>\jboss-as\standalone\configuration\standalone.xml file	jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL = TCPS)(HOST = <host>)(PORT = 1521)))

Configurations	Command-line options	jdbc.databaseURL Value
	(for example, <csa_home>\jboss-as\standalone\configuration\keystore)	(CONNECT_DATA = (SERVICE_NAME = ORCL))(SECURITY=(SSL_SERVER_CERT_DN="CN=abc,OU=dbserver,O=xyz,L=Sunnyvale,ST=CA,C=US"))
CSA tests the database DN	-Djavax.net.ssl.keyStore="<certificate_key_file>" -Djavax.net.ssl.keyStorePassword=<certificate_key_file_password> <certificate_key_file_password> is the password to the keystore file (for example, changeit)	where <host> is the name of the system on which the Oracle database server is installed and he values for
Client authentication is enabled	-Djavax.net.ssl.keyStoreType=<certificate_key_file_type> <certificate_key_file_type> is the keystore type (for example, JKS or PKCS12)	SSL_SERVER_CERT_DN are for the DN of the Oracle database server.
<b>CSA tests the database DN and client authentication is not enabled</b>		
SSL is enabled	None	jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS)(HOST=<host>)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=ORCL))(SECURITY=(SSL_SERVER_CERT_DN="CN=abc,OU=dbserver,O=xyz,L=Sunnyvale,ST=CA,C=US")))
CSA tests the database DN	None	where <host> is the name of the system on which the Oracle database server is installed and the values for
Client authentication is not enabled	None	SSL_SERVER_CERT_DN are for the DN of the Oracle database server.

## MS SQL Database

This table describes MS SQL Database configurations, command-line options, and jdbc.databaseURL Value information

Configurations	Command-line options	jdbc.databaseURL Value
SSL is enabled	None	jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=authenticate

## Health Tool Reports

The Health Tool generates reports in three different formats that provide different levels of information: [online](#), [HTML](#), and [text](#).

### Online report

The online report is displayed in the window from which the Health Tool is run, and provides general statuses (pass/fail) for:

- Database connection
- JBoss server connection
- CSA service
- Identity Management component connection
- Marketplace portal service
- CSA data tests

If the database and JBoss connections fail, these records will not be displayed in the report.



Here is an example of the online display output.

```
-----  
Start Health Tool at 4/13/15 11:55 AM  
Note: It is required to run this tool using the same Java as CSA is using.  
-----  
Test CSA database connection ... passed  
-----  
Test connection to JBoss ... passed  
-----  
Test CSA is running ... passed  
-----  
Test IDM is running ... passed  
-----  
Test MPP is running ... passed  
-----  
CSA Data Tests ... passed  
-----  
End Health Tool at 4/13/15 11:55 AM  
'report.html' report was created.  
Test files report.html and health_tool.log for detailed results.
```


## HTML report

The HTML report (`<csa_home>\Tools\HealthTool\report.html`) contains a table that displays status and response times for the tests listed below.

**Note:** If the database, Jboss, or REST API connections fail, the records that depend on each of these connections will not be displayed in the report. For example, if the REST-API connection fails, CSA licensing information and the global CSA data-test status will not be reported.

- Status (pass/fail) for each test
- Response times for each test (where applicable)
- Log messages for failed connections
- Database:
  - Number of records in the `csa_person` table
  - Type and version
  - Driver and version
- JBoss:
  - JMX connection
  - MBean server connection
  - Server system resource usage
  - Server memory usage
- CSA:
  - Management Console login
  - Number of active subscriptions
  - Number of transitions
  - Number of completed instances
  - Process state
  - Number of pending subscriptions
  - REST API connection and CSA licensing
  - All uncommented properties in the `csa.properties` file

Here is an example of the HTML report.

 <b>Health Tool Report</b>				
Check	Result	Message	Duration	Log
Ping database	PASSED	Database connection passed	50 milliseconds	
Table 'csa_person' rows count	PASSED	Database table 'csa_person' has 1 records.	0 milliseconds	
CSA database check	PASSED	Connection to CSA database passed.		
Get database info	PASSED	Connected to database: PostgreSQL 9.3.6	4 milliseconds	
Get database driver info	PASSED	Connected to database: PostgreSQL Native Driver PostgreSQL 9.0 JDBC4 (build 801)	0 milliseconds	
JMX connection check	PASSED	Connection to JBoss JMX passed.	346 milliseconds	
MBean Server connection check	PASSED	Connection to JBoss MBean Server	898 milliseconds	
MBean Server connection check	PASSED	JBoss MBean Server data load	0 milliseconds	Operating System ----- LoadAverage: 0.23 FreePhysicalMemory: 192 MB processCpuTime: 35112000000 committedVirtualMemorySize: 7996 MB freeSwapSpaceSize: 30498 MB totalPhysicalMemorySize: 15999 MB totalSwapSpaceSize: 30516 MB  Memory - Heap Memory Usage ----- committed : 1989 MB init : 2048 MB max : 1989 MB used : 549 MB percentage : 27 %  Memory - Non Heap Memory Usage ----- committed : 328 MB init : 2 MB max : 0 MB used : 310 MB
CSA running check	PASSED	CSA Service is running		
Login to CSA	PASSED	CSA login passed	407 milliseconds	
IDM running check	PASSED	Connection to IDM passed	230 milliseconds	
MPP running check	PASSED	MPP Service is running		
CSA LDAP check	PASSED	LDAP connection passed	72 milliseconds	
CSA data: Subscriptions	PASSED	ACTIVE: 25	10 milliseconds	
CSA data: Lifecycle Transitions	PASSED		2 milliseconds	
CSA data: Instances	PASSED	COMPLETED: 25	2 milliseconds	
CSA data: Process return code	PASSED	No NULL data found in 'CSA_PROCESS_INSTANCE.PROCESS_RETURN_CODE_ID'	2 milliseconds	
CSA data: Process state	PASSED	No NULL data found in 'CSA_PROCESS_INSTANCE.PROCESS_INSTANCE_STATE_ID'	2 milliseconds	
CSA data: Pending Subscriptions	PASSED	There are no Pending Subscriptions.	2 milliseconds	

## Text report

The text report (<csa\_home>\Tools\HealthTool\ health\_tool.log) contains the information below.

**Note:** If the database, Jboss, or REST API connections fail, the records that depend on each of these connections will not be displayed in the report. For example, if the REST-API connection fails, CSA licensing information and the global CSA data-test status will not be reported.

- General status (the same information that is displayed online)
- Log messages for failed connections
- Database:
  - Connection-response time
  - Number of records in the csa\_person table
  - Type and version
  - Driver and version

- JBoss:
  - JMX connection
  - MBean server connection
  - Server system resource usage
  - Server memory usage
- Identity Management component: connection response time
- CSA data:
  - Management Console login
  - Log-in response time
  - Subscriptions status
  - Lifecycle transitions status
  - Instances status
  - Process state status
  - Pending subscriptions status
  - REST API connection and CSA licensing
  - All uncommented properties in the `csa.properties` file

**Note:** If the database, Jboss, or REST API connections fail, the records that depend on each of these connections will not be displayed in the report. For example, if the REST-API connection fails, CSA licensing information and the global CSA data-test status will not be reported.

An example of the Health Tool log file is shown below.

```

-----
Start Health Tool at 4/13/15 11:55 AM
-----
Test CSA database connection ...
Database connection passed in 50 milliseconds
Database table 'csa_person' has 1 records.
Connected to database: PostgreSQL 9.3.6
Connected to database: PostgreSQL Native Driver PostgreSQL 9.0 JDBC4 (build 801)
passed
-----
Test connection to JBoss ...
Connection to JBoss JMX passed.
Connection to JBoss MBean Server
JBoss MBean Server data load
Operating System
-----
LoadAverage: 0.23
FreePhysicalMemory: 192 MB
processCpuTime: 351120000000
committedVirtualMemorySize: 7996 MB
freeSwapSpaceSize: 30498 MB
totalPhysicalMemorySize: 15999 MB
totalSwapSpaceSize: 30516 MB

Memory - Heap Memory Usage
-----
committed : 1989 MB
init       : 2048 MB
max        : 1989 MB
used       : 549 MB
percentage : 27 %

Memory - Non Heap Memory Usage
-----
committed : 328 MB
init       : 2 MB
max        : 0 MB
used       : 310 MB
percentage : -32572404800 %

passed
-----
Test CSA is running ...
passed
CSA login passed in 407 milliseconds.
-----
Test IDM is running ...
Connection to IDM passed in 230 milliseconds.
passed

```

```

-----
Test MPP is running ... passed
-----
CSA Data Tests ...
-----
CSA data: Subscriptions
Result: passed
-----
CSA data: Lifecycle Transitions
Result: passed
-----
CSA data: Instances
Result: passed
-----
CSA data: Process state
Result: passed
-----
CSA data: Pending Subscriptions
Result: passed
CSA REST call to 'license/'
{
  "activeOSInstanceCount" : 2,
  "totalOSInstanceLimit" : 0,
  "members" : [ {
    "licenseKey" : "ABCD 1234 HOPA CHF3 U4B5 H72F Y9J9 K7PL BP9H MZ9U D0AU 2C9M G1TG L762 KYW2 HWVA WPNH MCFY
TM3Q DBEV X6YR PW9D B9TS XFXC LK4U R46A V888 RCKY 5SCT JC4P 4QNJ 9GEJ\"InstantOn for 90 days with 1 capacity\"",
    "licenseType" : "INSTANT_ON",
    "daysRemaining" : 90,
    "expiresOn" : 1234567899000,
    "activeOSInstancesLimit" : 0,
    "productName" : "CSA"
  } ]
}

CSA Properties:
csa.provider.msvc.rest.protocol : http
com.hp.csa.service.process.ProcessExecutorDelegate.EXTERNAL_POOL_SIZE : 2
com.hp.ccue.consumption.disallowedExtensions : exe,bat,com,cmd
csa.productPerspective : enterprise
com.hp.csa.PEM.PARAM.PROCESS_INSTANCE_ID : CSA_PROCESS_ID
com.hp.csa.LifecycleExecutor.THREAD_POOL_SIZE : 2
com.hp.csa.TimeoutChecker.THREAD_WAKEUP_TIME : 300000
csa.consumer.legalNoticeUrl : http://www8.hp.com/us/en/privacy/privacy.html
csa.provider.msvc.port : 9000
csaAuditEnabled : true
com.hp.csa.ProcessExecutor.THREAD_WAKEUP_TIME : 5000
csaTruststorePassword : *****
com.hp.csa.service.process.ProcessExecutorDelegate.INTERNAL_POOL_SIZE : 2
securityCodarIntegrationUserPassword : *****
securityEncryptedSigningKey : *****
csa.group.numberOfApprovers : 10
com.hp.csa.OosMonitor.THREAD_WAKEUP_TIME : 60000
com.hp.csa.service.process.OosMonitorDelegate.MONITOR_POOL_SIZE : 2
com.hp.csa.oo.OOClient.SOCKET_TIMEOUT : 60000
com.hp.csa.service.ssl.insecure : true
securityCatalogAggregationTransportUserPassword : *****
csa.topology.cloudOsSpecEnabled : false
com.hp.csa.plugin.cloudos.util.TokenCache.TIMEOUT : 300000
TopologyDesignProvisioning.TIMEOUT : 7200
serviceRequestProcessorScheduler.period : 5000
com.hp.csa.ApprovalDecisionMaker.THREAD_WAKEUP_TIME : 1
csa.provider.rest.protocol : https
embedded.oo.root.dir : "C:/Program Files/Hewlett-Packard/CSA/emb_oo"
com.hp.csa.service.process.ProcessExecutorDelegate.MONITOR_POOL_SIZE : 2
csa.subscriber.portal.url : {protocol}://{host}:8089/org/{orgName}
integrationAccountUserList : admin,csaReportingUser,ooInboundUser,cdaInboundUser,
csaTransportUser,csaCatalogAggregationTransportUser
com.hp.csa.UserGroupExecutor.THREAD_WAKEUP_TIME : 20
csa.provider.es.name :
csa.maxFileUploadSize : 50
com.hp.csa.UserGroupExecutor.UserGroupDeletionBatchSize : 250
csa.additionalSupportedExtensionsForImport :
jboss.shutdown.log.location : C:/Program Files/Hewlett-Packard/CSA/jboss-as/bin/shutdown.log
securityIdmTransportUserPassword : *****
OrchestratedTopologyDesignProvisioning.ProviderSelection.Enabled : true
serviceRequestProcessorScheduler.maxInstancesToProcess : 100
csa.consumer.endDatePeriod : 12

```

```

DynamicPropertyFetch.READ_TIMEOUT : 30000
csa.security.enable : false
securityCsaReportingUserPassword : *****
csa.orgName.identifier : CSA-Provider
securityTransportPassword : *****
csa.provider.hostname : localhost
csa.consumer.featuredCategory : APPLICATION_SERVERS
securityOoInboundUserPassword : *****
OOS_PASSWORD : *****
csaTruststore : C:/Program Files/Hewlett-Packard/CSA/openjre/lib/security/cacerts
rest.restrict.fields : createdBy,updatedBy,createdOn,updatedOn,objectId,
isCriticalSystemObject,description,iconUrl,disabled,categoryType
com.hp.csa.PEM.PARAM_CONTEXT_ID : CSA_CONTEXT_ID
csa.provider.msvc.hostname : localhost
csa.consumer.termsOfUseUrl : http://www8.hp.com/us/en/privacy/terms-of-use.html
com.hp.csa.ProcessExecutor.THREAD_POOL_CORE_SIZE : 2
OOS_URL : https://localhost:8445
enableHPSSO : true
rest.excludedoc : false
loggerEnabled : false
csa.topology.expressDesignEnabled : false
OOS_USERNAME : admin
xAuthToken : X-Auth-Token
com.hp.csa.LifecycleExecutor.THREAD_WAKEUP_TIME : 5000
com.hp.csa.service.process.ProcessExecutorDelegate.CALLBACK_POOL_SIZE : 2
deploymentMode : single
com.hp.csa.UserGroupExecutor.CACHE_EXPIRATION_TIME : 30
csa.provider.port : 8444
rest.restrict : false
DynamicPropertyFetch.RESPONSE_SIZE : 50000
securityAdminPassword : *****
securityCdaInboundUserPassword : *****
csa.topology.calloutsEnabled : false
securityTransportUserName : csaTransportUser
com.hp.csa.import.BUILD_ARTIFACT_RELATIONSHIP : true
csa.provider.es.exists : no
com.hp.csa.aosMonitor.THREAD_WAKEUP_TIME : 20000
passed

```

---

End Health Tool at 4/13/15 11:55 AM

**Note:** The overall status of a test (passed/failed) is displayed at the end of each section.

## Interpreting Health Tool reports

The following table describes each test reported in the Health Tool reports and suggests troubleshooting actions.

Duration information (which depends on your environment) is provided to help locate where there may be performance or other issues. For example, longer duration for all connection tests might imply that there is a network issue, whereas longer duration for only one component-connection test implies that the component should be checked.

Test	Description
Ping database/CSA database test	Tests connectivity to the CSA database. If these tests fail, verify that the information in the <code>config.properties</code> file is correct.
Table <code>csa_person</code> row count	Tests that data can be accessed in the CSA database. If connectivity to the CSA database fails, this information is not reported.
Get database information	Displays the database type and version. See the <i>CSA Support Matrix</i> for more information on supported versions.
Get database driver information	Displays the JDBC drivers used by CSA to connect to the database. Use this information to verify that you are using drivers that are compatible with the database.
JMX connection test	Tests connectivity to the JBoss JMX server. If this test fails, start the JBoss JMX server.
MBean server connection test	Tests connectivity to the JBoss MBean server. If this test fails, start the JBoss MBean server.
MBean server connection test	Displays JBoss MBean server data load. If connectivity to the JBoss MBean server fails, this information is not reported. This call only occurs if the test passes for the MBean server connection call above.

Test	Description
CSA running test	Tests if the CSA service is running. If this test fails, start the CSA service.
Log in to CSA	Tests if the given user can log in to the Management Console. If this test fails, verify that the CSA credentials ( <code>csa.username</code> and <code>csa.password</code> ) in the <code>config.properties</code> file are valid and that the user has permissions to log in to the Management Console.
IdM running test	Tests connectivity to the Identity Management component. If this test fails, verify that the Identity Management component credentials ( <code>idm.username</code> and <code>idm.password</code> ) are valid and that the user has permissions to connect to the Identity Management component.
MPP running test	Tests if the Marketplace Portal service is running. If this test fails, start the Marketplace Portal service.
CSA data: Subscriptions	Displays the number of active subscriptions. If this value is high, this service could be causing performance issues.
CSA data: Lifecycle Transitions	Displays the number of lifecycle transitions. If this value is high, this service could be causing performance issues.
CSA data: Instances	Displays the number of operating system instances (OSIs) being used in current, active subscriptions. If this value is high, this service could be causing performance issues.
CSA data: Process state	Tests the value of <code>CSA_PROCESS_INSTANCE.PROCESS_INSTANCE_STATE_ID</code> . If this value is high, this service could be causing performance issues.
CSA data: Pending Subscriptions	Displays the number of pending subscriptions. If this value is high, this service could be causing performance issues.
CSA REST API Test	Tests the connection to CSA using the REST API. If this test fails, verify that the CSA credentials ( <code>idm.transportUser</code> and <code>idm.transportPassword</code> ) in the <code>config.properties</code> file are valid and that the user has permissions to connect to CSA using the REST API.
CSA REST API: License	Displays the CSA license information. If connectivity to CSA using the REST API fails, this information is not reported.
CSA REST API Test	Tests the connection to CSA using the REST API. If this test fails, verify that the CSA credentials ( <code>idm.transportUser</code> and <code>idm.transportPassword</code> ) in the <code>config.properties</code> file are valid and that the user has permissions to connect to CSA using the REST API.
CSA REST API: License	Displays the CSA license information. If connectivity to CSA using the REST API fails, this information is not reported.
CSA Properties	Displays all uncommented properties in the <code>&lt;csa_home&gt;\jboss-as\standalone\deployments\csa.war\WEB-INF\classes\csa.properties</code> file. If this test fails, verify that you are logged into the CSA system as a user who has access to the <code>csa.properties</code> file and that the file exists.

# Send documentation feedback

If you have comments about this document, you can send them to [clouddocs@hpe.com](mailto:clouddocs@hpe.com).

## Legal notices

### Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

### Restricted rights legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

### Copyright notice

© Copyright 2016 Hewlett Packard Enterprise Development Company, L.P.

### Trademark notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

The OpenStack word mark and the Square O Design, together or apart, are trademarks or registered trademarks of OpenStack Foundation in the United States and other countries, and are used with the OpenStack Foundation's permission.

### Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to the following URL and sign-in or register: <http://hpe.com/software/csa>.

Select Manuals from the Dashboard menu to view all available documentation. Use the search and filter functions to find documentation, whitepapers, and other information sources.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your Hewlett Packard Enterprise sales representative for details.

### Support

Visit the Hewlett Packard Enterprise Software Support Online web site at <https://www.hpe.com/us/en/support.html>.